

Incident Management: Human Factors and Minimising Mean Time to Restore Service

Submitted by
Katherine Mary O'Callaghan

A thesis submitted in total fulfilment of the requirements for the degree of
Doctor of Philosophy

School of Business (VIC)
Faculty of Arts & Sciences

Australian Catholic University
Research Services
Locked Bag 4115
115 Victoria Parade
Fitzroy, Victoria 3065
Australia

15 March 2010

Statement of Sources

This thesis contains no material published elsewhere or extracted in whole or in part from a thesis by which I have been qualified for or been awarded another degree or diploma.

No other person's work has been used without due acknowledgement in the main text of this thesis.

This thesis has not been submitted for the award of any degree or diploma in any other tertiary institution.

All research procedures reported in this thesis received the approval of the relevant Ethics/Safety Committees.

Katherine Mary O'Callaghan

15 March 2010

Acknowledgements

I would first like to thank my academic supervisors, without whom this work could not have been completed. Dr. Sugumar Mariappanadar provided extensive support for which I am grateful. As well, Dr. Theda Thomas' contribution made this undertaking viable, and her valuable support and her expressions of confidence in me are greatly appreciated.

I am also grateful to the survey respondents, whose input made this study possible. The corporations that allowed me to work with their staff and analyse their unplanned outage data are extended professional recognition for their participation in this work. I thank Sriram Ramachandran for his assistance, review, and verification of the data analysis and results obtained.

The author also acknowledges the Boston Red Sox, who always play great baseball and for every time they beat the New York Yankees. The Red Sox made the breaks I took in my studies both worthwhile and refreshing. The two World Series championships they clinched during my studies are made only sweeter by the next one they are certain to obtain.

Most importantly, I thank my husband, Scott Watters, who provided me encouragement and a sounding board throughout the duration of this work. My gratitude cannot be expressed deeply or profoundly enough to communicate it fully.

Abstract

Unplanned IT outages can cost businesses money, as well as lost customer satisfaction, and a variety of additional hidden costs. Incident managers are employed by organisations to restore service from unplanned IT outages as expeditiously as possible. This research focused on two components employed by incident managers in doing their job to determine if particular components, or combinations of these components, result in a shorter amount of time to restore service than do others. The components are the characteristics displayed by incident managers and the problem-solving approaches used by incident managers when working to restore service from unplanned IT outages. The characteristics studied were being authoritative, being communicative, being decisive, being demanding, being entrepreneurial, being facilitative and being pragmatic. The two problem-solving approaches used by incident managers and investigated were a solution-focused approach to solving problems and a problem-focused approach to solving problems. The research further determined whether the particular characteristics or problem-solving approaches or combinations of these in a reduction in the amount of time to restore service compared to others.

This research investigates the characteristics of incident managers, the problem-solving approaches they employ when working with others to restore service, and their attained Mean Time to Restore Service (MTRS). It answers the following three questions. What are the dominant characteristics displayed by incident managers when they work to restore service that has occurred due to an unplanned outage? What are the different problem-solving approaches used by incident managers when they work to restore service that has been lost due to an unplanned outage? What relationship exists, if any, between the dominant characteristics displayed by incident managers when an unplanned outage occurs, taking into account the problem-solving approaches they use, and the time to restore service they attain?

In addition to identifying the relationship between the characteristics displayed by incident managers and the approach to problem-solving that they use, this research identified the combination of those two attributes that optimise the performance of an incident manager working to restore service from an unplanned IT outage.

The research methodologies used in this research included both qualitative and quantitative research. The research itself was performed in two phases. The first phase engaged a focus group comprised of incident managers, technical support team personnel, and corporate managers to provide the researcher fundamental questions to pursue in the second phase of the research. It also provided the researcher a foundation from which to build the incident management questionnaire introduced in this research. The second phase was an empirical study that gathered data from two sources. First, data was obtained from incident managers through the use of an online questionnaire to identify the characteristics incident managers reported displaying and the approaches to solving problems they used when working to restore service from an unplanned outage. The second set of data was the

data captured by incident managers about high-impact unplanned outages that were experienced by a participating corporation.

This research reveals four key findings. The first shows the seven types of unplanned outages (acts of nature, hardware, human beings inside the affected company, human beings outside the affected company, software, system overload and vandalism) that can be assigned to an unplanned IT outage and, upon assignment, may contribute to activities to perform to restore service when an unplanned IT outage occurs. The second revealed is the two approaches to problem-solving used by incident managers (problem-focused problem solving and solution-focused problem solving), each of which, when complemented by specific characteristics displayed by incident managers when working to restore service from unplanned IT outages, moderate the duration of unplanned IT outages. The third is the characteristics incident managers display when working to restore service from an unplanned outage. These include being authoritative, being communicative, being decisive, being demanding, being entrepreneurial, being facilitative, and being pragmatic.

Additionally, this research identified the most effective combination of characteristic-displayed and problem-solving-approach-used by incident managers that results in the most expeditious restoration of service from an unplanned IT outage. That is, the research revealed that an incident manager who displayed the characteristic of being authoritative, with the use of a solution-focused approach to problem solving, attained the lowest MTRS values of all combinations that were investigated. This study represents a valuable step in establishing empirical evidence for directing the work habits of incident managers to optimise their ability to restore service from unplanned outages in an expeditious manner.

Table of Contents

Statement of Sources	ii
Acknowledgements	iii
Abstract	iv
Table of Contents	vi
List of Tables	x
List of Figures	xii
Chapter 1 : Introduction	1
1.1. Background to the Study	1
1.2. Financial Costs of Unplanned IT Outages.....	3
1.3. Managing Unplanned IT Outages	6
1.4. The Need for Research about Incident Managers.....	9
1.5. Research Questions.....	13
1.5.1. Question 1	13
1.5.2. Question 2	13
1.5.3. Question 3	13
1.6. Overview of the Methodology.....	14
1.6.1. Pilot Study	14
1.6.2. Main Study.....	15
1.7. Significance of this Research.....	16
1.8. Assumptions.....	17
1.9. Organisation of Dissertation	18
Chapter 2 : Literature Review	20
2.1. The Evolution of IT	21
2.1.1. Introduction.....	21
2.1.2. From Data to Information.....	21
2.1.3. Summary	24
2.2. IT Outages	25
2.2.1. Introduction.....	25
2.2.2. Planned and Unplanned Outages.....	26
2.2.2.1. Planned Outages	26
2.2.2.1.1. Planned Hardware Outages	28
2.2.2.1.2. Planned Firmware Outages.....	29
2.2.2.1.3. Planned Software Outages.....	29
2.2.2.1.4. Other Planned Outages.....	31
2.2.2.2. Unplanned Outages	31
2.2.2.2.1. Acts of Nature.....	32
2.2.2.2.2. Hardware.....	33
2.2.2.2.3. Human Beings.....	34
2.2.2.2.4. Software	36
2.2.2.2.5. System Overload.....	37
2.2.2.2.6. Vandalism.....	38
2.2.2.3. Classification of Unplanned Outages	39
2.2.3. Summary	40
2.3. Incident Managers.....	40
2.3.1. Introduction.....	40
2.3.2. The Role of Incident Managers.....	41
2.3.3. Information Technology Infrastructure Library (ITIL).....	45
2.3.4. Summary	47
2.4. Characteristics of Managers.....	47

2.4.1.	Introduction.....	47
2.4.2.	Characteristics Investigated.....	48
2.4.2.1.	Being Authoritative.....	49
2.4.2.2.	Being Compassionate.....	49
2.4.2.3.	Being Communicative.....	50
2.4.2.4.	Being Competitive.....	52
2.4.2.5.	Being Decisive.....	53
2.4.2.6.	Being Demanding.....	54
2.4.2.7.	Being Entrepreneurial.....	55
2.4.2.8.	Being Facilitative.....	57
2.4.2.9.	Being Pragmatic.....	58
2.4.2.10.	Having Leadership Ability.....	60
2.4.3.	Summary.....	63
2.5.	Approaches to Problem Solving and Restoring Service.....	64
2.5.1.	Introduction.....	64
2.5.1.1.	Problem-Focused Approach.....	65
2.5.1.2.	Solution-Focused Approach.....	72
2.5.2.	Summary.....	80
2.6.	What IT Departments Measure and What They Report.....	80
2.6.1.	Availability.....	81
2.6.2.	Mean Time to Restore Service (MTRS).....	86
Chapter 3 :	Pilot Study.....	90
3.1.	Focus Group.....	90
3.1.1.	Method.....	90
3.1.2.	Participants.....	91
3.1.3.	Procedure.....	93
3.1.4.	Results.....	96
3.1.4.1.	Thematic Analysis – Characteristics.....	96
3.1.4.2.	Thematic Analysis – Approaches to Solving Problems.....	98
3.1.4.3.	Summary from Thematic Analysis.....	99
3.1.4.4.	Content Analysis – Characteristics.....	99
3.1.4.5.	Content Analysis – Approach to Solving Problems.....	100
3.1.4.6.	Summary from Content Analysis.....	101
3.1.5.	Summary from Focus Group.....	101
3.2.	Questionnaires.....	102
3.2.1.	Method.....	102
3.2.1.1.	Content Validity.....	102
3.2.1.2.	Reliability.....	103
3.2.2.	Participants Replying to the Pilot Study Questionnaires.....	103
3.2.3.	Procedure.....	104
3.2.4.	Results.....	105
3.2.4.1.	Behavioural Characteristics Questionnaire Results.....	105
3.2.4.1.1.	Being Entrepreneurial.....	113
3.2.4.1.2.	Being Demanding.....	113
3.2.4.1.3.	Being Authoritative.....	114
3.2.4.1.4.	Being Communicative.....	115
3.2.4.1.5.	Being Facilitative.....	115
3.2.4.1.6.	Being Pragmatic.....	115
3.2.4.1.7.	Being Decisive.....	116
3.2.4.2.	Approach-to-Solving-Problems Questionnaire Results.....	116
3.2.4.2.1.	Problem-Focused Approach-to-Solving-Problems.....	120

3.2.4.2.2.	Solution-Focused Approach-to-Solving-Problems	120
3.3.	Discussion of the Pilot Study	121
Chapter 4 :	Main Study	122
4.1.	Hypotheses	122
4.1.1.	Characteristics and Approaches to Solving Problems	123
4.1.2.	Unplanned Outages and MTRS.....	124
4.2.	Main Study	127
4.3.	Component 1—Characteristics and Approaches to Solving Problems.....	128
4.3.1.	Method	129
4.3.2.	Participants and Tools	129
4.3.2.1.	Pyrux.....	130
4.3.2.2.	Pyrite.....	130
4.3.3.	Procedure	131
4.4.	Component 2—Characteristics, Approaches and MTRS	132
4.4.1.	Method	133
4.4.2.	Observations	133
4.4.3.	Participants—Matching Incident Managers to the Unplanned Outages They Restored	134
4.4.4.	Tools.....	136
4.4.5.	Method	137
4.4.6.	Procedure	137
4.5.	Summary.....	138
Chapter 5 :	Main Study Results	139
5.1	Demographic Information	139
5.1.1.	Gender	139
5.1.2.	Age	140
5.1.3	Education Level Obtained	140
5.1.4	Tenure Working as an Incident Manager.....	140
5.3	Hypothesis Testing.....	141
5.3.1	Results from Component 1 of the Main Study	141
5.3.2.1.	Characteristics Displayed.....	141
5.3.2.2.	Approaches Used by Incident Managers	143
5.3.2.3.	Characteristics and Solution-Focused Approach to Solving Problems 145	
5.3.2.4.	Characteristics and Problem-Focused Approach to Solving Problems 147	
5.3.2	Results from Component 2 of the Main Study	149
5.3.2.1.	Outage Types and MTRS	149
5.3.2.2.	Characteristics, Approaches, Hardware, MTRS.....	153
5.3.2.3.	Characteristics, Approaches, Humans, MTRS.....	156
5.3.2.4.	Characteristics, Approaches, Software, MTRS	158
5.3.2.5.	Moderating Effect of Approach.....	160
5.4	Summary.....	166
Chapter 6 :	Discussion and Conclusions	168
6.1.	Discussion.....	169
6.1.1.	Characteristics.....	170
6.1.2.	Approaches to Solving Problems.....	173
6.1.3.	MTRS	176
6.2.	Limitations.....	178
6.3.	Recommendations for Future Research	179
6.4.	Conclusion	181

Appendix A – Bass-Avolio Leadership Steps	183
Appendix B – Sample Participation Invitation.....	185
Appendix C – The KOZADAR Questionnaire	186
Appendix D – Author’s Conference Publications.....	194
Appendix E – Author’s Journal and other Publications.....	195
Appendix F – Ethics Approval.....	196
References.....	197

List of Tables

Table 2-1. <i>Types of Planned and Unplanned Outages</i>	26
Table 2-2. <i>Unplanned Network Outages – Descriptions and Targets</i>	39
Table 2-3. <i>Unplanned Software Outages – Descriptions and Targets</i>	40
Table 2-4. <i>The Ace of Diamonds Can be Identified Quickly</i>	44
Table 2-5. <i>The Five Leadership Fundamentals</i>	62
Table 2-6. <i>Steps in Problem Diagnosis</i>	66
Table 2-7. <i>Steps in Problem Resolution</i>	67
Table 2-8. <i>K-T Steps in Problem Solving</i>	68
Table 2-9. <i>Problem Analysis Worksheet</i>	69
Table 2-10. <i>The Steps of Total Quality Management</i>	71
Table 2-11. <i>Sigma Quality – Percentage of Defect-Free Products</i>	72
Table 2-12. <i>Steps when Making Change Using a Solution-Focused Approach</i>	75
Table 2-13. <i>Steps to Take, the Actions to Take, and the Questions to Ask</i>	78
Table 2-14. <i>Calculating Availability</i>	82
Table 2-15. <i>Availability, Downtime and Lost Revenue</i>	84
Table 2-16. <i>Calculating Availability and Calculating Reported Availability</i>	85
Table 2-17. <i>Calculating IT System Optimal Availability</i>	86
Table 2-18. <i>Calculating the Duration of an Unplanned Outage</i>	87
Table 3-1. <i>Composition of Focus Group</i>	92
Table 3-2. <i>Sample Questions Concerning Behavioural Characteristics</i>	95
Table 3-3. <i>Sample Questions Concerning Approaches-to-Solving-Problems</i>	96
Table 3-4. <i>Content Analysis from Focus Group – Behavioural Characteristics</i>	100
Table 3-5. <i>Content Analysis from Focus Group – Solving Problems</i>	101
Table 3-6. <i>Pilot Study Questionnaires and Responses: Characteristics</i>	104
Table 3-7. <i>Descriptive Statistics for Characteristics of Incident Managers</i>	106
Table 3-8. <i>Correlation Matrix for Characteristics of Incident Managers</i>	106
Table 3-9. <i>Communalities for Characteristics of Incident Managers</i>	107
Table 3-10. <i>Total Variance Explained from Pilot Study: Characteristics</i>	109
Table 3-11. <i>Descriptive Statistics from Factor Analysis of Pilot Study: Characteristics</i>	110
Table 3-12. <i>Items and Factor Analysis of Behavioural Characteristics of Incident Managers</i>	111
Table 3-13. <i>Descriptive Statistics of Approaches-to-Solving-Problems</i>	117
Table 3-14. <i>Correlation Matrix of Approaches-to-Solving-Problems</i>	117
Table 3-15. <i>Communalities of Approaches-to-Solving-Problems</i>	118
Table 3-16. <i>Total Variance Explained from Approaches-to-Solving-Problems</i>	118
Table 3-17. <i>Research Items/actor Analysis of Approaches-to-Solving-Problems</i> ..	119
Table 4-1. <i>Lists of Unplanned Outages</i>	125
Table 4-2. <i>Distribution and Collection of KOZADAR Questionnaires</i>	130
Table 4-3. <i>Fields Requested in Unplanned Outage Data</i>	134
Table 5-1. <i>Frequency: Gender</i>	139
Table 5-2. <i>Frequency: Age</i>	140
Table 5-3. <i>Frequency: Education</i>	140
Table 5-4. <i>Frequency: Tenure Working as an Incident Manager</i>	141
Table 5-5. <i>ANOVA Results of Incident Manager Characteristics</i>	142
Table 5-6. <i>Descriptive Statistics: Characteristics Displayed</i>	142
Table 5-7. <i>ANOVA Results of Approaches-to-Solving-Problems</i>	144
Table 5-8. <i>Descriptive Statistics: Approaches-to-Solving-Problems</i>	144
Table 5-9. <i>T-Test for Equality of Means</i>	144

Table 5-10. <i>Model Summary Output for Solution-Focused Approach</i>	146
Table 5-11. <i>Characteristics and the Use of a Solution-Focused Approach</i>	146
Table 5-12. <i>Characteristic (DEAD PFC) Coefficients Solution-Focused Approach</i>	147
Table 5-13. <i>Model Summary Output for Problem-Focused Approach</i>	148
Table 5-14. <i>Characteristics and the Use of a Problem-Focused Approach</i>	148
Table 5-15. <i>Characteristic (DEAD PFC) Coefficients Problem-Focused Approach</i>	149
Table 5-16. <i>Descriptive Analysis – Unplanned Outage Types</i>	150
Table 5-17. <i>Kruskal-Wallis Test: Unplanned Outages and MTRS</i>	151
Table 5-18. <i>Kolmogorov-Smirnov Test: Hardware-Software and MTRS</i>	151
Table 5-19. <i>Kolmogorov-Smirnov Test: Hardware-Humans and MTRS</i>	152
Table 5-20. <i>Kolmogorov-Smirnov Test: Software-Humans and MTRS</i>	152
Table 5-21. <i>Unplanned Hardware Outage Subsets and Respective MTRS</i>	154
Table 5-22. <i>MTRS for Server Down Unplanned Outages</i>	155
Table 5-23. <i>Hardware Outage Subsets and Occurrences of Each</i>	156
Table 5-24. <i>Outage Subsets with Humans and MTRS</i>	157
Table 5-25. <i>Unplanned Humans-In Outage Subsets and Occurrences of Each</i>	158
Table 5-26. <i>Unplanned Software Outage Subsets and Occurrences of Each</i>	158
Table 5-27. <i>Unplanned Software Outage Subsets and Respective MTRS</i>	159
Table 5-28. <i>Unplanned Software Outage Subsets and Quantity of Outages</i>	160
Table 5-29. <i>Descriptive Statistics</i>	162
Table 5-30. <i>Characteristics, Approaches, and MTRS → The Best Results</i>	164

List of Figures

<i>Figure 1-1. Construction of Communication</i>	1
<i>Figure 1-2. Costs of Unplanned Outages Increase as the Ability to Deliver the Services Lost Decrease when Traditional Restoration Actions are Used (Alonso, 2002, page 2)</i>	4
<i>Figure 1-3. Incident Management and the Restoration-of-Unplanned-Outages Universe</i>	8
<i>Figure 1-4. ITIL Influence on IT Service Support Processes (Sunrise, 2008)</i>	11
<i>Figure 1-5. KOZADAR Research Model</i>	12
<i>Figure 2-1. The Duration of the Ages of IT Development</i>	21
<i>Figure 2-2. The Identical Communications Model has been used as Technologies Developed and Allowed Increasingly Complex Communication (Kotler & Keller, 2006)</i>	22
<i>Figure 2-3. Coupling Facility (CF) to allow Continuous Availability (Jews et al., 2008, p. 507)</i>	30
<i>Figure 2-4. Service Design and Service Management Processes (Orr, 2008, p. 11)</i>	41
<i>Figure 2-5. Shannon and Weaver’s Communication Model (Deglar & Lewis, 2004)</i>	51
<i>Figure 2-6. Characteristics of an Entrepreneur (Hatch & Zweig, 2000, p. 69)</i>	56
<i>Figure 2-7. Pragmatic Managers Display of Specific Characteristics (McGovern, 1999, p. 59)</i>	59
<i>Figure 2-8. The Leadership-Technology Cube (Klenke, 1993, p. 221)</i>	63
<i>Figure 2-9. Example of an Ishikawa, aka Fishbone, Diagram (HCI, 2009)</i>	70
<i>Figure 2-10. The Four-Step Solution Focused Management Model, Superimposed on Deming’s Plan-Do-Check-Act Total Quality Management Model</i>	77
<i>Figure 2-11. Scaling Allows Users of a Solution-Focused Approach to Measure, albeit subjectively, the Progress Made While Taking Small Steps to Achieve a Desired State (Visser, 2009, p. 2)</i>	79
<i>Figure 2-12. How to Calculate MTRS</i>	86
<i>Figure 2-13. Keys to Decreasing the Mean Time to Restore Service (Smith & Hinchcliffe, 2006, p. 41)</i>	88
<i>Figure 2-14. Model Used to Test User Perception to MTRS (Song et al., 2004)</i>	89
<i>Figure 4-1. Factorial equation</i>	125
<i>Figure 4-2. The KOZADAR Research Model, Detailed</i>	128
<i>Figure 5-1. Ninety-five Percent Confidence Interval (Mean) for Characteristics Displayed by Incident Managers</i>	143
<i>Figure 5-2. Ninety-five Percent Confidence Interval (Mean) for Types of Problem-Solving Approaches Preferred to Restore Service</i>	145
<i>Figure 5-3. Box and Whisker Plots Display the Relationship Between Unplanned Outage Types and Their Associated Mean Times to Restore Service. (The Natural Logarithm of the MTRS is shown in the Y-Axis of the scale.)</i>	153
<i>Figure 5-4. Moderator Variables Model (Baron & Kenny, 1986)</i>	161
<i>Figure 6-1. Being Authoritative + Solution-Focused Minimises MTRS</i>	181
<i>Figure A-1. The Steps Required to Achieve Superior Leadership (Bass-Avolio, 2005)</i>	183

Chapter 1 : Introduction

1.1. Background to the Study

Modern living, in the developed world, is characterised by the technology revolution. Technology has changed the ways people work, live, play, and otherwise engage with one another (Döckel, 2003). Some people may argue that the history of Information Technology (IT) and computers began with rock paintings, the introduction of “zero” as a numeric value or the invention of the printing press (Butler, 1997). When or how it began, for the purpose of this research, is not important. The importance of technology is its ability to allow communication to occur. The ability to communicate that developed throughout history has contributed to the development of computer science, IT, and a sundry of scientific and mathematical learnings. Based upon a fundamental premise that technology was, and is today, used to solve the communications problems of its times, from its origins, information technology spanned five periods, commonly described as the premechanical, the mechanical, the electromechanical, the electronic (Butler, 1997) and the digital eras of technology. In each age the simple process followed allowed thoughts and data (input) from one being to be processed (processing) in a manner that produced meaning and information (output) for another being, resulting in communication (see Figure 1-1):

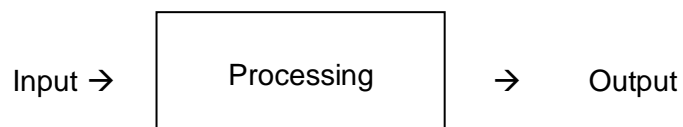


Figure 1-1. Construction of Communication

From rock art to computers that beat human world chess champions (Iqbal, 2008) computers are at the core of all communication that occurs today. Computers have become ubiquitous in government, small business, and Fortune 500 corporations alike. From the first computer, Hollerith’s tabulating machine to process the 1890 census data in the United States (Mann & Janzen, 2007) to the technology revolution that has occurred, and is still occurring, internationally (Im & Baskerville, 2005), computers are business tools that run the business. They are not, from a business perspective, anything other than tools. Advancements in computing have allowed companies to increase both financial accountability and profits by providing high quality, personalised service—easily and affordably. Information Technology (IT) not only lowers the cost to companies providing products and services, it creates avenues to enhance revenue through new services that companies can provide to their customers (Rust & Miu, 2006). One simple example is that, historically, banks required a customer to come into a bank branch to move funds from

Account A to Account B. A new and profitable service is to allow the transfer of funds to occur across the Internet, at the convenience of the customer, for a fee. Computers are used daily to allow, not just the processing of data, but the successful commercial operation of the businesses that own that data.

Having accepted the need for using computer systems in the operation of their businesses, industries accept the fact that the same computer systems on which they depend will fail and that unplanned outages will occur (Northrop, 2003; Ramakrishnan, Shenoy, & Van der Merwe, 2007). These include unplanned outages caused by software applications, operating systems, network components, hardware devices, microcode programs, incomplete documentation, human ineptitude, or some combination thereof. The United States Department of Energy (DOE) described unplanned outages in terms of their duration (Chang, 2004). The DOE definition states that an unplanned outage can be either one of only two types, short or long. In this research, however, unplanned outages are defined as the unexpected failure, or the less than acceptable level of operation of network components, hardware systems or software applications in a business that result in the need for the immediate (or as close to immediate as possible) return of the lost service(s) to the business experiencing the unplanned outage. The combination of hardware, software, network components, and human beings required to operate a corporate computer system or network production environment, increases both the complexity of that IT environment and the probability that unplanned outages will occur. An IT department's ability to provide to its business stakeholders high degrees of availability throughout the IT enterprise must be attained within the reality that the systems on which organisations depend do not operate flawlessly nor are faults always readily fixed (Fox & Patterson, 2003).

A business may pay millions of dollars for computer hardware, software and network systems—its IT enterprise—to aid the running of the business. Additionally, businesses may pay hundreds of thousands of dollars, annually, to each of the individuals—commonly called incident managers—employed to perform a single role for the organisation. Incident managers are employed to obtain the restoration of service when the aforementioned IT enterprise or its subsystems break or otherwise perform in an unexpected manner. This research was undertaken to investigate the business impact of unplanned IT outages and to determine if there are ways that the performance of individuals responsible for the restoration of the lost service that the unplanned outage caused can be optimised, in order to minimise the duration of the unplanned outage.

1.2. Financial Costs of Unplanned IT Outages

Unplanned outages are, in fact, IT issues; more importantly, however, they are business issues. Unplanned outages never produce revenue for the company experiencing them. With a scarcity of academic literature available on the costs associated with unplanned outages, it is assumed that few businesses seek to publish the impact (to themselves or to their customers) the cost of an unplanned IT outage. Interrogated research databases used during this study included Association for Computing Machinery (ACM), Emerald, Informit, Institute of Electrical and Electronics Engineers (IEEE), Proquest, and Science Direct. Unplanned downtime is estimated to have cost businesses, worldwide, approximately US \$1.6 trillion dollars in lost revenues—only in lost revenues—in the year 2000 (Alonso, 2002). A single citation of costs of unplanned outages in 2008 states that the average revenue cost of an unplanned application outage is estimated to be nearly US \$2.8 million dollars per hour (IBM, 2008). The 2008 citation notes only the lost revenue that results from only an application unplanned outage. Because companies increasingly work or operate in multiple locations across the world and rely on IT, an ever-larger number of business activities occur in “real time”. IT disruptions can affect the entire delivery chain of the products and/or services provided by a business (Alonso, 2002). Once ignored or incidental, planned outages are now as disruptive as unplanned outages. External and internal forces put pressure on IT departments to keep the computer systems and networks, and the applications running continuously on them, available to users. Disruptions—whether across a large company’s IT enterprise or to a hand-held device used by only one person—are accepted less and less frequently (Hitch & Sullivan, 2006). Concurrent maintenance is preferred only to no required maintenance. Twenty-four percent of organisations state that an unplanned outage of greater than two hours is unacceptable. Another 48 percent of organisations state that they cannot manage when unplanned outages exceed 24 hours (Alonso, 2002). Figure 1-2 suggests that a mathematical and absolute- and opposite-cardinal 1:1 relationship exists between the costs of an unplanned outage and an IT department’s ability to restore service from that outage; in some cases it may be measured and proven to have exactly that relationship. However, it is more accurate to state that Figure 1-2 shows the relative relationship of the costs of an unplanned outage and the ability to restore service. That relative relationship is money. Unplanned IT outages always cost money. A gap exists, and is widening, between the cost of unplanned downtime and an organisation’s ability to be effective with traditional response activities (Alonso, 2002). Traditional response activities—including server reboots, retrying activities to restore services that have failed in previous attempts, incident management’s inability to understand the technical environment or any other set of circumstances do, indeed, slow restoration and cost the business money.

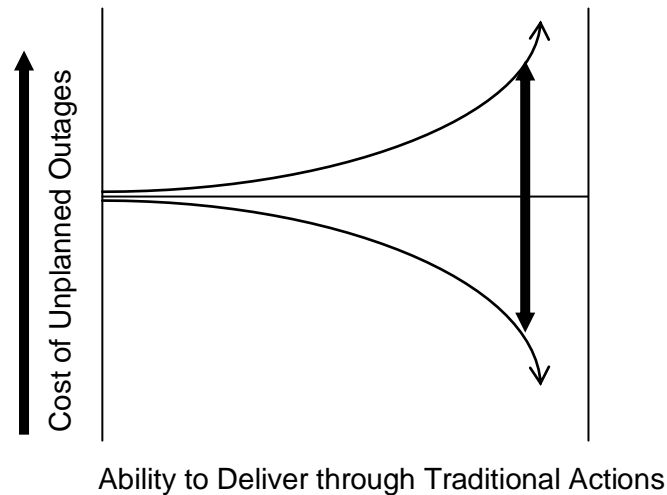


Figure 1-2. Costs of Unplanned Outages Increase as the Ability to Deliver the Services Lost Decrease when Traditional Restoration Actions are Used (Alonso, 2002, page 2)

When an unplanned outage occurs, associated costs are not, necessarily, insignificant nor are they, necessarily, directly related to the technical impacts the unplanned outage has caused. Corporate-brand damage can be a component of the costs of the unplanned IT outage, as it was when Qantas Airlines announced flight delays the first morning a new software computer system was used by ground staff in July 2008. That new software computer system failed in production and resulted in both delayed and cancelled flights (Bingermann, 2008). This IT failure and reports about it in the media exacerbated the bad press the company received only weeks prior when an oxygen tank exploded on an international flight forcing Qantas pilots to make an emergency landing. The costs of unplanned outages can include any number of individual or combination of components. Costs of unplanned outages can include delayed or lost receipt of revenues owed, as experienced by e-Bay, during a 22-hour unplanned outage in 1999. Its users, worldwide, trade \$US 1,900 worth of goods on its site every second (The World's OnLine Marketplace, 2008) and its 1999 unplanned outage cost e-Bay \$US 3.9 million in lost fees (Fordahl, 2001).

Costs of unplanned outages can include employee costs to resubmit data manually so that the data can be (re-)processed electronically, as were the costs incurred in 2007, when a computer technician doing maintenance on a (United States) State of Alaska Department of Revenue computer system deleted \$US 38 million from one of the state's bank accounts. Costs to recover the data were calculated once it was discovered that the only place from which the data could be restored was in 300 boxes of paper forms submitted by Alaskan taxpayers. Recovery costs alone exceeded \$US 200,000 (How to ctrl, alt, del, 2007).

Costs of unplanned outages can include a lowered stock price, as experienced by Amazon.com, a major US bookseller, with only an on-line presence, which was offline for two

hours on one Friday in 2008 because of an unspecified technology system failure. The company's stock fell 4.6 percent during trading on the same day. Those costs were coupled with the lost revenue Amazon.com experienced during the same unplanned outage. Reporting revenues of \$US 1.8 million dollars per hour (Tsuruoka, 2008), Amazon.com lost sales, alone, from its unspecified technology outage of \$US 3.6 million dollars. Costs of unplanned outages can include the embarrassment to a company's reputation, as experienced in early 2001, when Microsoft suffered an outage of nearly 24 hours due to the result of a human error, made while configuring one of its IT systems (Brown, 2004). Among notable embarrassments was that experienced by the US Department of Veteran Affairs (DVA) upon its disclosure that the data of 26.5 million US veterans, and their spouses, along with data of 2.2 million active military personnel, was lost when one worker's computer was stolen from his home. The only solace afforded the DVA was that similar reports of lost data were issued by Aetna Insurance, Ernst & Young, Union Pacific Railroads and the YMCA (Spangler, 2006).

Costs of unplanned outages can include any combination of the costs in the preceding discussion. Considerations of costs, in addition to those cited, include compensatory payments, corporate replies to media inquiries, corporate replies to media reports, costs incurred to restore lost services, delays in the shipment of customer-purchased products or services, lost customer loyalty, and lost customer satisfaction. This list does not include one cost that is always incurred because all companies accept that unplanned outages will occur. That cost is accepting that some number of hours of unplanned outages will occur and the unknown value of the costs that will be incurred when unplanned outages do happen (Robinson & Polozoff, 2003). In 1999, a computer failure at a US chocolate manufacturing company prevented it from shipping products for Halloween, costing the company a 19 percent drop in net income in the third quarter of its financial year (Hershey, 1999). An international stock exchange was available to traders for less than 66 percent of its trading day in 2001 due to a failed software deployment (Brancaccio, 2001).

Companies that experience unplanned outages always incur costs. Incurred costs increase until systems are restored to an acceptable operating level and, depending on any follow-on negative impact associated with the unplanned outage, may continue to be incurred even after systems are restored to an acceptable operating level (Houck, Kim, O'Reilly, Picklesimer, & Uzunalioglu, 2004). Unplanned outages are not only a technical issue, but are also a business issue (Hayes, 2005). Although, to some, unplanned outages may be technically interesting, unplanned outages are always an issue. They are a business issue.

1.3. *Managing Unplanned IT Outages*

Unlike some IT concepts, unplanned outages are very simple to understand. Imagine being a speaker in front of an audience and having a heart attack in the middle of your presentation. In the IT world, that is an unplanned outage. As the person having the heart attack, you are interested, likely, in having your heart restarted (having service restored). You are probably not too interested, at the moment the heart attack occurs, in why it happened—the fact that you are 20 kilograms overweight, that you smoke two packs of cigarettes a day, and that you drink at least a bottle of wine daily are not your primary interests at the moment you collapse. This is exactly what happens when an unplanned outage occurs in an IT environment. End-users who earn their living based on the sales they complete during a work shift, for example, want service restored immediately and are disinterested in why the system—previously available and allowing them to earn a living—became unavailable. The restoration of service is their primary concern. In business, unplanned IT outages are issues that influence the ability to draw revenue from customers, the ability to bill already-provided-for customers, as well as the ability to identify anomalies in reports required by legal authorities. Unplanned outages may be interesting from a technical perspective, but can be critical from a business perspective. Groups impacted from the unplanned outage, from within the company experiencing it, are the end users, the technical support group and corporate managers. All are negatively impacted when an unplanned outage occurs. When a computer hardware system, application software program or unidentified component of the IT enterprise stops being available, transactions are not processed. Only processed transactions, however, produce revenue for a company. When IT systems, or IT components, fail to operate and users are unable to process orders or receive funds from customers, neither the end-users nor the corporate managers care why the failure occurred. They only want service restored. Moreover, they want it restored quickly. Members of the technical support group, although possibly interested in the technical root cause of the issue that caused the unplanned outage, must focus on the restoration of service to return the business to its normal operating activities. The technical support group is responsible for the appropriate functioning of software and computer systems, as well as diagnosing and solving faults as they happen (O’Callaghan & Mariappanadar, 2006[a]). Being employed to restore service as quickly as possible, incident managers must assist technical support teams to focus on the actions required to restore the lost service, rather than on a detailed technical investigation to understand why the outage occurred.

Incident managers, hired solely to compel others to restore service, are the centerpieces of unplanned outages. Among those individuals impacted by unplanned outages, with other significant, impacted parties revolving around the instructions that incident managers give,

incident managers are wholly accountable for the restoration of service. When an unplanned outage occurs, it is expected that an “unplanned outage ticket”—an incident docket—is raised with the incident management team and identified as being of significant enough impact to require the assistance and support of incident management. Once notified of the unplanned outage, incident managers are obligated to restore service. Incident managers must engage all necessary technical, business, and vendor parties to take action to restore service. Incident managers must inform corporate managers of the impact of the outage and the lost functions to the business and end-users. Incident managers must also keep corporate managers informed of the prospect of lost revenue, brand damage, and all other, actual and prospective, costs of an unplanned outage that are possible as a result of the unplanned outage.

Figure 1-3 demonstrates the model used by organisations that hire incident managers to direct the restoration of service when unplanned IT outages occur. As is the sun in the solar system, incident management is at the centre of the restoration of unplanned outages. Circling that centre are multiple groups, including customers (not included in the figure). Importantly, incident management is surrounded by technical support groups and corporate managers; each has separate needs about the status of an unplanned outage and its restoration, yet both obtain information and direction from the incident manager responsible for the restoration of service. As the sun radiates heat and light, the incident management team directs actions and communications to both the technical support groups and the corporate managers. The actions of those two groups, in turn, affects the ability of end-users and customers to benefit from the service restored or, at least, to have information about its impending return to service.

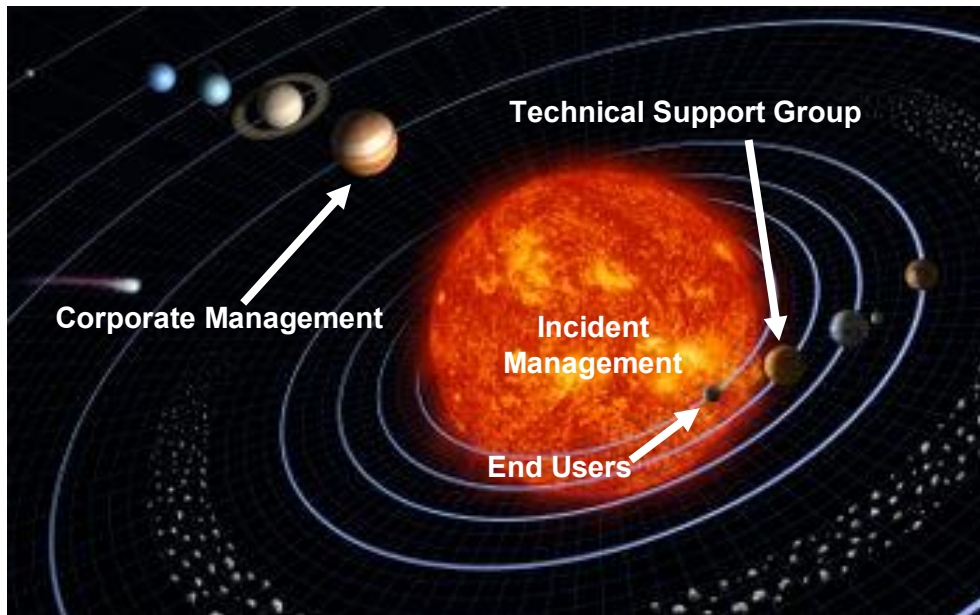


Figure 1-3. Incident Management and the Restoration-of-Unplanned-Outages Universe

Yet, immature trouble-shooters (incident managers, technical support group members or corporate managers providing *executive encouragement* to expedite the return of service) often restore service with a common use of hunches, instinct, and intuition (Marquis, 2006). The professional role of incident management has developed, in part, due to the establishment of the Information Technology Service Management Forum (itSMF). The focus on the delivery of IT Service Management functions, initiated in the 1980's, resulted in professional organisations being established internationally, under the banner of itSMF. Initially chartered in the United Kingdom in 1991, the organisation has nearly 50 chapters and 20,000 members, worldwide (Stanford, 2007). This professional body developed because of the response to the economic downturn in the late 1980's, when the Central Computer and Telecommunications Agency in the United Kingdom established the Information Technology Infrastructure Library (ITIL) framework to reduce costs and to manage more effectively the delivery of IT services (Sallé, 2004). Nearly twenty years later, in the release of its second edition, ITIL's service management volumes were comprised of two sub-components, service delivery and service support. Service delivery included service level-, financial-, capacity-, continuity-, and availability-management. Service support included service desk support, release-, configuration-, incident-, problem- and change-management. The release of third edition of the ITIL tomes occurred in 2007. Much of the work outlined for incident management remains unchanged. It is still the only, solely reactive function that exists within the ITIL framework.

Incident management is the set of activities performed by incident managers, including the characteristics they display and the problem-solving approach they employ to restore service, when an unplanned outage occurs in a corporation's information technology system. It is an ITIL goal that businesses experience fewer unplanned outages because of integrating the ITIL service management framework; however, the elimination of unplanned outages is in no way suggested as a likely outcome of investing in ITIL. The goals of ITIL, in part, are to reduce costs and to manage more effectively the delivery of IT services within an organisation (Cartlidge, Hanna, Rudd, Macfarlane, Windebank, & Rance, 2007). Though a goal of a well-executed ITIL framework is the reduction of the duration of unplanned outages, there is no suggestion that one of ITIL's goals is to eliminate unplanned outages or remove the need to employ incident managers.

Though IT technical support teams may be interested to know why an unplanned outage occurred, the end-users and corporate managers who depend on the availability of the systems are interested in the immediate (or as close to immediate as possible) restoration of service. In an effort to avoid unplanned outages, most businesses perform maintenance to hardware, software, and firmware during planned outages; however, business requirements increasingly demand that maintenance activities occur without any outage, allowing users to have system access as often as possible. The time and costs associated with determining the root cause of an unplanned outage, identifying a fix for it, developing and testing that fix, and verifying and deploying the fix into the production environment must be weighed against the time and cost of taking whatever actions are required to restore service, which may range from restarting the machine (technically referred to as "rebooting the server") and returning it to service to taking an enterprise-wide outage during the middle of a business day to restore lost data or take other restorative actions. When an unplanned outage occurs, the restoration of the service lost by the outage may be critical. Detailed in Section 1.2, it is evident that unplanned outages are not just a technical issue but also, more importantly, a business issue.

When presented with an unplanned outage, incident managers restore normal service operation as quickly as possible and minimise the adverse impact on business operations. Incident managers are paid by IT departments to identify, record, classify and progress unplanned outages to ensure the best achievable levels of availability and service are attained (Cartlidge et al., 2007). Incident managers earn their living by restoring service when unplanned outages occur. How it is they do that is one of the questions investigated in this research.

1.4. *The Need for Research about Incident Managers*

Information Technology is a wide and diverse industry with many professional roles, languages, environments, and tools. Incident Management is one of many of the

professional roles that exists within an IT organisation, yet those of the programmer, technical support specialist, technical architect, and change manager are, arguably, all more visible to those who work in the IT environment than is the incident manager. There is limited research on the responsibilities associated with performing the incident manager role and less so on one's ability to optimise performance in the role. The professional practice of incident management is, often, task-based, rather than people-centric or even goal-centric and much of the knowledge about its practice has been prepared by individuals interested in the whole of IT Service Management, a sub-component of a corporation's IT environment.

A list of actions to be performed during each unplanned outage includes the engagement of technical support teams, notification to corporate management, impact assessment to the business, and the documentation of technical progress as service is restored, among others. All must be performed so that an unplanned outage can be managed while simultaneously documenting the activities that are taken to return service. The costs of unplanned IT outages are not insignificant; yet, those charged with the restoration of service—incident managers—are under-studied. This research attempts to identify if incident managers can reduce the Mean Time to Restore Service (MTRS) values attained when working to restore service when unplanned outages occur.

Unplanned outages can be one of many types—including hardware errors, software malfunctions, network routing errors, and power failures, among others—and may require different sets of skills or knowledge to restore service; however, most IT organisations assign unplanned outages to generically skilled incident managers, without any, or with only limited expertise in any of the aforementioned unplanned outage types. How it is, and how it might be that those incident managers can reduce the attained MTRS when unplanned outages occur is why this research was undertaken.

This study investigates four major aspects of unplanned IT outages. First, it investigates the unplanned outages, themselves. These are more commonly referred to in IT departments as incidents and are the non-availability (or the less than acceptable performance) of hardware, software, or networking subsystems that are used by businesses. These subsystems contribute to the ability of the businesses to operate, not the IT environment, but the businesses, themselves, successfully. In addition to investigating the types of unplanned outages that can occur, this study also investigates the relationship between the IT unplanned outages and the time required to restore the service lost. As well, this study investigates the role of the characteristics displayed, and the problem-solving approaches used, by the individuals employed by IT departments whose sole job function is to restore service when an unplanned outage occurs. These individuals are more commonly referred to in IT departments as incident managers. It is their work that contributes to the time required to restore service when unplanned outages occur. It is, in fact, their

accountability (Cartlidge et al., 2007). The restoration of service lost due to an unplanned outage is performed under the direction of incident managers and the characteristics of those individuals are studied, as are the problem-solving approaches they use to restore service. Finally, this study investigates the relationship between the type of unplanned outage experienced, the characteristics displayed by the incident managers responsible for restoring service when the unplanned outage occurs, and the impact of the problem-solving approach used by the incident manager to restore service. That impact is measured in the resulting MTRS values attained when the lost service is restored and the unplanned outage no longer exists.

This research proposes to translate the role of an incident manager from a set of corporate job descriptions into a value-added professional whose contribution can provide a measurable addition to a company's bottom line. Incident management, a specific and detailed service support role identified in the ITIL tomes, is part of the increasing introduction of the ITIL framework at businesses across the world. The take-up of ITIL internationally continues to grow in both its use in IT departments and in their consumption of training and education in the ITIL framework. This information, and other data collected from surveys completed by IT leaders around the world (N = 350) indicate that the current overall take-up of ITIL is confirmed (Sunrise, 2008). Its current overall take-up is cited in Figure 1-4 (Sunrise, 2008):

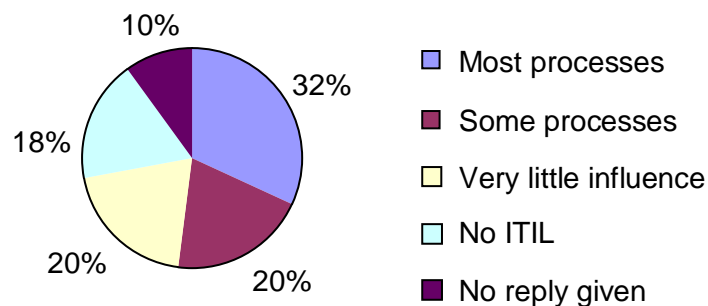


Figure 1-4. ITIL Influence on IT Service Support Processes (Sunrise, 2008)

Figure 1-4 clearly indicates that greater than half of the organisations surveyed have introduced at least some of the ITIL framework into their IT organisations. Neither the original nor the subsequent revisions of the ITIL library show evidence of removing incident management from the fundamental structure of the ITIL Service Support framework. There is no indication in any research or real-life IT experience that indicates unplanned outages will be eliminated. ITIL, and corporations that employ incident managers, agree that incident managers are important and that unplanned outages cost money to the company experiencing them; however, IT operations have been mostly ignored in research. There is limited research that is explicitly ITIL-related or itSMF-related (Galup, Quan, Dattero, &

Conger, 2007). Among the goals of this research is to consider incident management work from a scientific and research perspective, not from the “common use of hunches” in which it is noted to operate today (Marquis, 2006). Revealing the relationship between incident managers’ problem-solving approaches to the restoration of unplanned outages and the characteristics they display while restoring service, this research identifies how one can optimise the work of incident managers, saving corporations the costs associated with unplanned outages by employing specific actions to minimise their duration.

This research, therefore, seeks to undertake an investigation into the workings of how incident managers perform their roles and what the resulting impact is on the time taken to restore service from unplanned outages. The characteristics and problem-solving approaches of incident managers are considered to determine if some combination(s) positively or negatively affect the attained MTRS values by which the performance of incident managers can be measured. The KOZADAR research model (see Figure 1-5) was designed, developed and used to complete this research. The KOZADAR name was given in light of its being a combination of the moniker of the researcher (KOZ) and the name given to a month in the ancient Babylonian calendar, ADAR (Demsky, 1996). It describes the trio of variables investigated to determine the moderating effect a specific problem-solving approach may have on an attained MTRS, given the characteristics displayed by the incident manager.

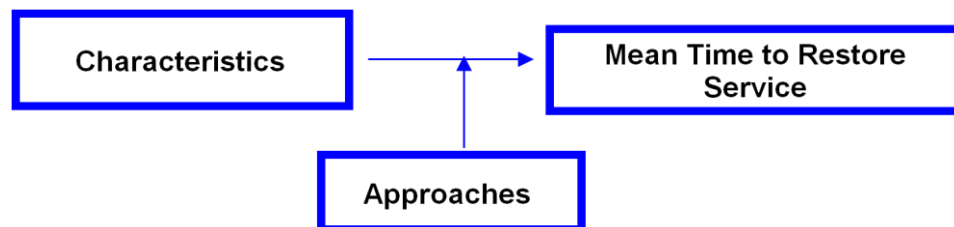


Figure 1-5. KOZADAR Research Model

Characteristics are those features displayed by incident managers when leading the restoration of service when an unplanned outage occurs. A general list of characteristics includes demonstrating leadership, being communicative, displaying charisma, loyalty, or discretion, among others. It is noted that the measure Mean Time to Restore (MTTR) service was defined by Cooper (2006); however; the release of ITIL version 3 in 2007 changed the nomenclature used by IT Service Management professionals and academics. This value is now referred to as the Mean Time to Restore Service (MTRS) and is defined, in part, as the average time taken to restore an IT service after a failure (Cartlidge et al., 2007). The MTRS is a mathematical value (the average of a series of time measurements that is divided by the number of observances), calculated upon the restoration of service from

multiple unplanned outages and a common key performance indicator of those responsible for restoring service (Cooper, 2006). The problem-solving approach is the tack taken by incident managers to get others to perform activities required to achieve the restoration of service. As seen in Figure 1-5, the model reveals the effect, if any, that the problem-solving approach may have on the MTRS attained, given the characteristics displayed by incident managers to obtain that restoration of service.

The KOZADAR Research Model accepts that the desired goal when an unplanned outage occurs is the restoration of the services lost. The duration of time taken to restore service, across multiple unplanned outages, is measured in the MTRS. The KOZADAR Research Model suggests that the MTRS is moderated by the problem-solving approach used by the incident manager responsible for restoring service.

1.5. Research Questions

The proposed research will be based on the KOZADAR Research Model, using both qualitative and quantitative research methodologies. The research questions unfolded during the literature review as specific areas of study were explored, and as a result of input provided by incident managers when this research was undertaken. These included general managerial characteristics displayed in corporations, problem-solving techniques, psychotherapeutic methodologies (modified and applied by corporate managers within traditional business settings), as well as the specific types of both planned and unplanned IT outages. From this foundation, the following research questions were formed and are those for which answers are sought in this research:

1.5.1. Question 1

What are the dominant characteristics displayed by incident managers when they work to restore service that has occurred due to an unplanned outage?

1.5.2. Question 2

What are the different problem-solving approaches used by incident managers when they work to restore service that has been lost due to an unplanned outage?

1.5.3. Question 3

What relationship exists, if any, between the dominant characteristics displayed by incident managers when an unplanned outage occurs, taking into account the problem-solving approaches they use, and the time to restore service they attain?

The aim of this research includes identifying the relationship between the characteristics of incident managers and the problem-solving approaches they use when they work to restore service when unplanned outages occur. Additionally, it is proposed to determine if there is a relationship between the problem-solving approaches used by incident managers and the MTRS they attain for different types of unplanned outages.

1.6. Overview of the Methodology

This research used both qualitative and quantitative analysis, in a multi-phased research method, to undertake the answering of the research questions cited in Section 1.5. A literature review by Bryman (2006) revealed that an examination of the value of both qualitative and quantitative methods in research were found to be viable, as long as they were pragmatic and allowed the research questions to be answered. Both qualitative and quantitative methodologies were used in Phase One of the research, allowing the exploration of multiple incident management concepts. These include the characteristics displayed by incident managers when unplanned outages occur, the impact of unplanned outages from a business perspective, as well as the problem-solving approaches applied by incident managers to engage individuals whose inputs are required to make decisions that would contribute to the restoration of service. As well, in Phase One the design and validation of an incident management questionnaire was undertaken—an incident management questionnaire. A quantitative methodology was used to complete the majority of the work performed in Phase Two of this research. This was the application of the validated questionnaire from Phase One and those results, an analysis of unplanned outages, and an assessment of the relationship between the responses from the questionnaire and the MTRS reported in the unplanned outages. The two phases of the research are described in the following sections.

1.6.1. Pilot Study

Phase One of this research included a literature review, a focus group and the development of a questionnaire to be validated and used in Phase Two of this research. All three were used to provide input that allowed Phase Two, the main study, to be performed. The literature review provided an understanding of prior research undertaken that addresses the concepts and applications of characteristics, problem-solving approaches, and measurements used by IT Service Management professionals. It also provided a context of the development of the IT Service Support profession. Additionally, Phase One included the hosting of a focus group and a factor analysis of the data obtained from a research questionnaire designed from the analysis of comments of members of the focus group. The focus group research methodology (Wituk, Bomhoff, Commer, Warren, & Meissen, 2003)

was used to collect data about incident managers, from those in the role and from those with whom they work. Participants were sought who work in the same IT organisation and included incident managers, corporate managers, and members of the technical support groups that perform the technical analysis of an incident and determine a technical path to restore service. The participation of corporate managers was sought because their perspective of an incident is not one of any technical impact, but of the business impact and the costs incurred because of the unplanned outage. The incident managers, accountable for the restoration of service and responsible for the most expeditious return of service from the unplanned outage that can be attained, were included as their work is the focus of this research. Together, these individuals were sought to discuss their perceptions of the characteristics of good incident managers, the characteristics such incident managers display during the course of time an unplanned outage is experienced by the company, and the problem-solving approaches incident managers use to assist the technical teams to restore service. The results of this output were analysed by reviewing the focus group transcript, identifying major themes in the answers to specific questions, as well as identifying any themes that were found to flow across the entire discussion. Upon completion, these results were summarised and incorporated into the major findings. Use of a focus group allowed authentic and detailed data to be captured by encouraging candour and lively discourse among the participants by the moderator. Additionally, it allows the participants to provide feedback to structured questions, giving them a voice to an area of their work (Jamieson & Williams, 2003) in which they spend significant portions, if not the entirety of their workdays.

Upon completion of the qualitative methodology in this research, quantitative methodologies were undertaken. A questionnaire was designed that further explores the major findings from the focus group. This questionnaire was designed to identify information about incident managers, from incident managers. The questionnaire was designed to obtain information, not about the type of incidents for which they were accountable to restore service, but about the characteristics they display during their work and the problem-solving approaches they use to motivate and obtain results from the teams performing the technical restoration of service from unplanned outages. Incident managers, technical support specialists, and corporate managers from the same large multi-national conglomerate were sought to participate in the focus group. A group of incident managers was sought to respond to the questionnaire that was drafted following analysis of the focus group output. The output of the pilot study questionnaires was used to develop and validate a final questionnaire, which was used in the main study.

1.6.2. Main Study

Upon completion of the analysis from the focus group transcript as well as the draft questionnaire performed in Phase One (pilot study) of this research, Phase Two (main study)

of this research was undertaken. The questionnaire designed and validated in Phase One, developed based on the findings from the pilot study, was distributed to a second group of incident managers. Some of the participants asked to participate in the main study were among those who participated in the focus group and work at the same multinational conglomerate as those individuals who responded to the questionnaire. Additional participants sought to participate in the main study were personnel from IT departments at different, large and international corporations. A corporation with greater than 20,000 personnel suggests a strong likelihood of having a large and/or technically complex IT enterprise, as well as a large number of personnel employed to support it. Among the additional IT organisations who were invited to participate, enough incident managers were sought who agreed to participate in Phase Two of this study. Unlike the data collected in Phase One (pilot study), in which paper-based questionnaire results were available and an analysis of the output from the focus group was reviewed, the final research questionnaires were delivered to and collected electronically from a secure website. The results from those questionnaires were analysed, identifying the problem-solving approaches used to restore service, and the characteristics displayed while restoring service. A modest amount of demographic information was also captured.

1.7. Significance of this Research

This study is among the limited number of academic or professional undertakings of its kind that provides a framework to explain the relationship between unplanned outages in a corporation, the characteristics displayed by and the approaches to solving problems used by incident managers employed by the IT organisation of that corporation and the time in which the unplanned outages are restored (measured through the MTRS). The overall structure for this research interrogates two avenues, incident managers and unplanned outages, also known as incidents. The results obtained identify the important crossroads of the two avenues. It also attempts to identify an optimal path to arrive at its final destination—as low as possible an MTRS. The significance of this study is highlighted for its contribution and benefits to academia, incident management, IT Service Management literature and IT professionalism.

Academically, this study investigates the approaches incident managers use to enthuse, demand, direct, and otherwise entice the actions of the technical support specialists who contribute to the restoration of service when an unplanned outage occurs. It is acknowledged, however, that, professionally, there is a need for information (and how it is provided) by corporate managers who need to know the status of the unplanned outage and the plan for, and time of, its (expected) restoration. The unplanned outages in this research are of the type considered to be greatly important or critical to the business that experiences them. This research identifies specific problem-solving approaches to the restoration of

service used by incident managers. It identifies the characteristics displayed by incident managers during the restoration of unplanned outages. The study seeks to determine the impact those problem-solving approaches have on the speed with which service from the unplanned outage is restored. Additionally, this study introduces a designed and validated questionnaire that identifies if an incident manager favours a particular problem-solving approach when restoring service. Previously, there had been no such tool available to identify the preferred problem-solving approaches used by incident management professionals. Additionally, it provides a foundation on which future research can be undertaken. This research introduces the KOZADAR Research Model, allowing future researchers to benefit from its creation, easing future investigations in IT Service Management.

The contribution to the literature is such that this study will expand the literature in the areas of IT Service Management, IT Service Support, and Incident Management, all of which are related, yet are able to stand independently from one another as each is deployed into a corporation's IT department. It will acknowledge the price paid by large corporations, specifically, to have effective incident managers available to save time and money when unplanned outages occur. This study contributes to the literature by its review of the types of problem-solving approaches that not only can be used, but also are used, by incident managers when unplanned outages occur. Additionally, this research introduces two validated research questionnaires that, respectively, capture information on the characteristics displayed and the problem-solving approaches used by incident managers in their professional roles.

1.8. Assumptions

This study is proposed to be completed acknowledging five major assumptions underlying its execution. The first assumption is that unplanned outages occur and unplanned outages can be expected to occur. This assumption is based on the information provided in Sections 1.1 and 1.2. The second assumption is that the restoration of service from an unplanned outage must occur expeditiously, as described in Section 1.3. The third assumption is that systems used by a large IT corporation are required to be available 24-hour-per-day, seven-days-per-week and 365 days-per-year (also known as 24-by-7-by-365), even though end-users may not operate the computer systems during all of those hours. Instead, those systems may be used to perform background processing of the day's work or perform other functions, making it needed by the business, but not, necessarily, by end-users. Although there are hours during a day when an IT system may not be required at all by the business, it will be required at a certain time of day and during certain times of day. The Internet has demanded a greater need for 24-by-7 availability than any IT enterprise since the inception of

IT. Software is not only doing more work but also has more users, often spread out across the globe, and requiring 24-by-7 availability (Robinson & Polozoff, 2003).

Excellent examples of systems that require 24-by-7 availability are those employed by Internet users to access google.com, wikipedia.com, amazon.com and any of the other innumerable websites that exist and end-users expect to be always available. Since unplanned outages must be restored in as timely a manner as possible, with the minimal MTRS being attained, the time of day (or night) that an unplanned outage occurs is of the same importance to the business, although the type of unplanned outage or its severity may vary. Those unplanned outages identified by the business as greatly important or critical require the restoration of service immediately (or as close to immediate as possible). The time of day or day of year when the unplanned outage occurs does not, normally, influence the need to restore service immediately (or as close to immediately as possible).

The fourth assumption is that the cost to businesses when unplanned outages occur is not only difficult to measure; it is also not readily disclosed by those organisations that incur it. The reticence of an organisation that experiences an unplanned outage to announce its costs does not modify the reality that unplanned outages cost money to the companies that experience them. Frequently, those costs cannot be recovered. Finally, it is assumed that an effective incident manager can contribute to the speed with which an unplanned outage is restored and that both the associated costs incurred and the MTRS attained will be lowered by that contribution.

1.9. Organisation of Dissertation

This dissertation is divided into six chapters with associated appendices and references. Following Chapter One, the dissertation is organised in the following way: Chapter Two includes a review of the literature on the issues for this research and is divided into six sections, briefly described as history, outages, incident managers, management characteristics, approaches to problem solving and IT performance reporting. The history section discusses the evolution of computers and their use in business. The outages section includes a review of literature on IT outages and reviews the types of planned and unplanned outages, the costs of unplanned outages, the impacts of unplanned outages on corporations affected by them and the impacts they have on the customers of those corporations. The section on incident managers includes a review of managerial characteristics and characteristics for personnel, in general, and in the field of information technology. It cites how those learnings about the characteristics of corporate managers and the characteristics of IT personnel, generally, can be applied to incident managers. It relates the broad topics of the characteristics of incident managers and the development of the professional role of an incident manager in IT and the key performance indicators of that role. Significantly, it reviews the literature on the problem-solving approaches that incident managers can use to

restore service to an acceptable operating level. Finally, Chapter Two reviews the key performance indicators of incident managers, how they are applied to the technical outages incident managers restore, how that restoration is measured and its importance to the IT department that delivers it and the corporation that pays for it. This provides the purposeful foundation for this research.

A pilot study was performed and is detailed in Chapter Three. This chapter reports the work undertaken in the pilot study, including its research methods, the hosting of a focus group, the development and validation of the research questionnaires and the analysis of the results obtained from investigating incident management characteristics and incident management problem-solving approaches to restoring service when unplanned outages occur. Chapter Four discusses the main study and includes the research methods used, the final questionnaires distributed to incident managers, the analysis of the responses to the questionnaires from incident managers, the analysis of actual unplanned outage data obtained from one participating company, as well as the relationship between incident management characteristics, problem-solving approaches and attained Mean Times to Restore Service (MTRS). Chapter Five discusses the results from all data analysis performed in the main study. Chapter Six includes an overall discussion of the research and its results, the conclusions that can be drawn from it, its significance, its limitations, and recommendations for future research. Chapter Six is followed by appropriate appendices and references.

Chapter 2 : Literature Review

The premise of this study is that the approach to problem solving that is used by incident managers who restore service when an unplanned IT outage occurs somehow moderates the duration of the unplanned outage experienced by the business. (See Figure 1-5.) Specifically, it argues that the characteristics displayed by an incident manager working to restore the services lost when an unplanned outage occurs will influence, and the impact of that influence will be moderated by, the problem-solving approach used by the incident manager on the resulting MTRS for each unplanned outage type. This literature review addresses the major components required to understand the design of and need for the research performed. These components include the history of computers and the reliance businesses today have on their availability and successful functioning; the outages that occur in an IT environment; the role performed by incident managers in relation to the IT Service Management (ITSM) professional framework and its internationally accepted *de facto* standards; and the values of the duration of unplanned outages, including the time taken to restore service when unplanned outages occur, the availability of computer systems and how each of these values is measured and reported. This literature review includes the areas of managerial characteristics, characteristics specifically identified as being displayed by IT professionals, the role of the incident manager when unplanned IT outages occur, the problem-solving approaches an incident manager can use to restore service when an unplanned IT outage occurs and the IT measurements, made and reported.

The literature review chapter comprises six sections. It is noted that the academic research performed on ITIL, IT Service Management, and Incident Management is limited. In order to establish current knowledge of multiple subjects and provide a critical examination, summary, and evaluation of published work, this qualitative method explored multiple research databases to complete the literature searches. These research databases included Association for Computing Machinery (ACM), EBSCO, Emerald, Informit, Institute of Electrical and Electronics Engineers (IEEE), Proquest, and Science Direct.

After establishing the historic background of the development of IT, its use by businesses and the requirements IT departments have to deliver services to the business that pays for their functions (Section 2.1), Section 2.2 reviews the types of IT outages that can be experienced by a company. Section 2.3 reviews the role of incident managers and the service management framework in which it is performed. Section 2.4 investigates a group of characteristics displayed by managers in business, in order to determine which of those, if any, can be applied to incident managers whose work involves the restoration of service when unplanned outages occur, rather than the supervision of personnel and their tasks. Section 2.5 addresses the problem-solving approaches an incident manager can use to

restore service when an unplanned outage occurs. Section 2.6 explores the ways in which the duration of an IT outage can be measured and how IT availability can be measured. It also explains why the values of each are optimised when reported to the corporation that pays for the functions and services performed by its IT department.

2.1. The Evolution of IT

2.1.1. Introduction

Information technology, throughout its evolution, has been used to solve communications problems. Its development has occurred across five time periods. These are commonly described as the premechanical, mechanical, electromechanical, electronic (Butler, 1997) and digital ages. The relative speed of recent IT development can be seen in the timeline shown in Figure 2-1, noting the millennia that spanned the years from the premechanical age to the electronic age and the few decades that have passed during the digital age:

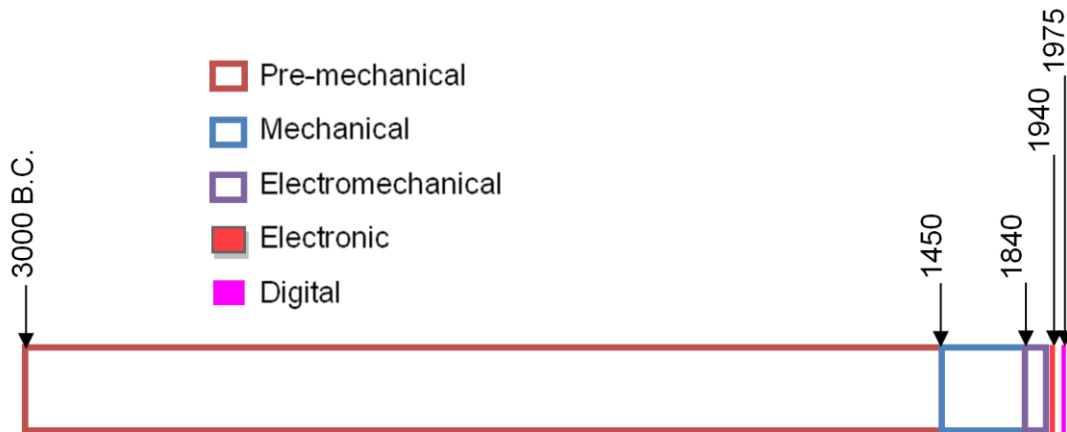


Figure 2-1. The Duration of the Ages of IT Development

In each age, there was a desire to translate some form of data into some form of information. The translation of data to information is explored in the following section.

2.1.2. From Data to Information

The successful translation of data into information ensures effective communication. As shown in Figure 2-2, communication occurs when data owned by one party is converted in order for a second party to understand the output produced. The input-process-output set of activities results in successful communication. This set of activities has been used repeatedly, though exercised differently, depending on available technology, throughout the five ages of the information technology evolution.

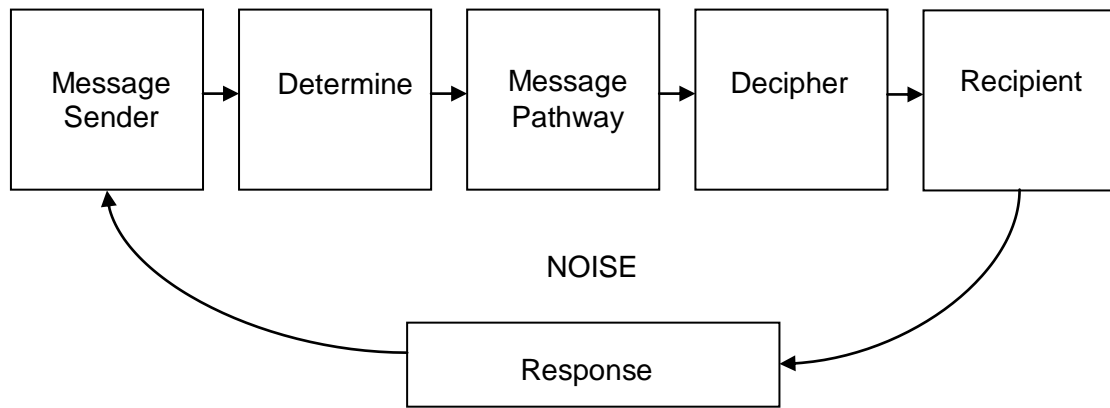


Figure 2-2. The Identical Communications Model has been used as Technologies Developed and Allowed Increasingly Complex Communication (Kotler & Keller, 2006)

The Premechanical Age of information technology is dated from 3000 B.C. through 1450 A.D. and is highlighted by petroglyphs and alphabets, both of which developed and aided communication. The Sumerians, in current-day southern Iraq, are credited with creating, in approximately 2800 B.C., the first written language. This was followed three thousand years later by the development of a written alphabet by the Phoenicians. The numbering of objects first occurred between 100 A.D. and 200 A.D. when Indian Hindus created a nine-digit number system. Nearly seven hundred years passed before zero became a written concept and was used as a numerical value (Butler, 1997). The importance of the introduction of the number “zero”, though primordial, proved critical to the development of IT and its uses. The ability to communicate “zero” and “one” is fundamental to computer processing (Larudogoitia, 2008). A true “information age” arrived when Gutenberg’s printing press was developed in 1450 and data, mostly words, were, relatively, easily duplicated and the distribution of those words occurred worldwide. The impact of movable type changed how communication could occur and how technology came to influence the masses. The word computer was first used in the third century, A.D., to describe the calculations used to determine the date of the Easter holiday (Aloisio, 2004). Further, it was used during the Mechanical Age (1450-1850) to describe the job function of individuals who worked with numbers.

Importantly, this era saw the contributions of Babbage, Pascal, and Leibniz—each of whom contributed a mathematical processor of some type—perpetuating the evolution of both information technology and computer technology. In 1801, the Frenchman Joseph Jacquard revealed the first use of programming a machine to perform a particular function when he introduced an automated loom, using punch cards to create patterns (Joyce, 2008). His application of binary logic created the real-time outputs of patterned fabrics. It was, however, the successful harnessing of electricity that introduced a new era of processing, the Electromechanical Age (1840-1940). Batteries, telegraphs, telephones, and the Morse code

all exploited the electronic pulses that allowed data to move from bursts of electronic data to packets of information, from sender to receiver. Originally used to send electronic pulses through wires, but refined to send data wirelessly across the Atlantic Ocean using Morse code (Wilkinson, 2007), Marconi's 1894 radio is a hallmark in the development of processing that contributed to the revolution that became computer technology, as it is known today. This epiphany was followed by the work of Herman Hollerith and James T. Watson, the founder of International Business Machines, more commonly referred to, simply, as IBM.

Computing, borne from rock art and transversing the scientific developments that introduced tabulating machines, was first used to wide acclaim by the United States federal government. Tabulating machines comprised, among other components, an apparatus for registering items constituting the record formed on a punch-record-card and totalling or integrating the items of any one or more columns of the punch-record-cards and also for sorting or classifying the punch-record-cards into different series (Hollerith, 1914). The first extensive application of an early computer is credited to a late-19th century event, following the taking, and manual calculation of the data taken, by the United States government in its 1880 census data. The counts and computations of the data obtained by 1880 census-takers were all done by hand and took seven years to complete. The taking of its next census, in 1890, could not be avoided, as it is a requirement embodied in the United States Constitution and required to be taken every ten years (Constitution of the United States, 1787). The United States established a competition to automate the processing of the data returned from the 1890 census. Herman Hollerith, who used a newly created tabulating machine to count the census data and provide results to the government in only five years, won the competition. Those five years were two fewer years than the previous census had taken and had a cost savings of \$5,000,000 (Biles, Bolton, & DiRe, 1998). After completing the census, Hollerith established one of the earliest pre-computer companies in 1896, the Tabulating Machine Company, which offered, among other products, the same punch cards that had been made famous during his 1890 census work.

The end of the Electromechanical Age came so swiftly, that, when replaced by the Electronic Age of computing (1940-1951), a revolution as significant as that which resulted from the introduction of Guttenberg's press, unfolded. The Electronic Age is best remembered for the UNIVersal Automatic Computer I, UNIVAC (the first commercially produced computer in the United States) and the Lyons Electronic Office (LEO) the first commercially used computer in the world. The Digital Age is best remembered for the Apple, handheld devices, and the Internet. The end of the digital age has yet to arrive, though it can only be expected to do so. Caminer (1997) wrote that it was in the 1950's that business computer applications were needed as part of running a business.

Computing, ultimately, is the conversion of data (text, graphic, numeric, voice, etc.) into numbers (zeroes and ones) and processing those numbers as prescribed by a software program executing against the data. The processing of that data comes at a cost. Information Technology, itself, is part of the cost businesses incur. E-commerce, via the Internet, is the most visible use of technology by businesses. Defined by DeMarie and Hitt (2000), e-commerce is the execution of business transactions across the Internet, and provides benefits to customers and businesses that historic “brick and mortar” or mail-order avenues cannot provide. There has never been a more important role for IT in the e-business environment of today. Integration of IT in internal processes and external markets is rapidly growing. Moreover, there is an adversarial relationship between business leaders and IT executives due to the credibility gap and the starkly different languages spoken by the business and by IT (Grover, Henry, & Thatcher, 2007). There is a need for executive management and IT executives to synchronise organisational IT with business needs (Craig, Kakamedala, & Tinaikar, 2007). Businesses benefit by having the customer perform data input and verification, saving on staffing costs. Available data, in electronic format, further aids the businesses that retain the data entered to assess information about their customers and products as they look to sustain and grow their current business success. Moreover, consumers can exist worldwide, rather than from, solely, the local neighbourhood or country. An Internet presence provides not only visibility of a product and/or service, but presents a market that would, otherwise, not be considered cost-effective to reach. E-commerce, however, is no panacea for business; it is but one vehicle through which companies may, or may not, succeed in selling products and services.

Toys-R-Us.com was a joint venture with its Toys-Я-U.s parent company and a venture capital organisation. Toys-R-Us.com suffered trying to blend an online presence with the Toys-Я-U.s physical presence. Toys-R-Us.com sought to carry a broader line of toys than could be found in the Toys-Я-U.s physical stores. Toys-R-Us.com sought to place kiosks in the Toys-Я-U.s physical stores so that customers could order items that were out-of-stock inside the physical store; Toys-R-Us.com sought to offer products at a sales price lower than the price at which the products were offered at the Toys-Я-U.s physical stores. Fundamentally different sales strategies between the e-commerce distribution avenue and the physical brick-and-mortar avenue resulted in the partnership between the two sales avenues disbanding (Useem, 1999). Though technology successfully offered the Toys-Я-U.s brand the chance to build its business and incorporate e-commerce, its business model could not successfully take advantage of that technology.

2.1.3. Summary

The beginnings of effective communication began millennia ago and effective communication continues to evolve. Improved tools and improved technology allow far

greater amounts of data to be understood in the 21st century than was available in previous centuries. From rock art to e-commerce, individuals and corporations have evolved in how it is that communication can occur and what data can be transformed into information in a manner that contributes to the success of the individual and the corporation. Evolution, indeed revolution, in IT development, design and demand will continue to occur. This overview provides an understanding of the evolution that made IT a reality and the unbounded and continuing invention of new and advanced technology will progress communication forward. The importance of IT to a corporation is the running of its core business, not in its running of IT. As demonstrated by the inability of the Toy-Я-U's brand to align its brick-and-mortar sales strategies with what it could offer through its e-commerce strategy, it is the use of technology, not the existence of technology that allows organisations to optimise their ability to sell products and services. The importance of IT to business is to help the business provide, not technology, but the products and services offered by the business to its customers. However, there is a fundamental corporate-wide and IT department-wide acceptance that, IT is important to the success of the business, unplanned IT outages will not only occur, they should be expected to occur. It is a false assumption that unplanned failures will not occur (Dashofy, van der Hoek & Taylor, 2002).

2.2. IT Outages

There are only two forms of IT outages. They are referred to as planned outages and unplanned outages. IT outages are expected to occur, even when the most robust of technologies are deployed into a business. Significant amounts of research have been done on how to avoid or minimise outages (Cocchiara, Davis, & Kinnaird, 2008; Loveland, Dow, LeFevre, Beyer & Chan, 2008; Lumpp, Schneider, Holtz, Mueller, Lenz, Biazetti, & Petersen, 2008; McLaughlin, Liu, DeGroff, & Fleck, 2008; Morrill, Beard, & Clitherow, 2008; Pelleg, Ben-Yehuda, Harper, Spainhower, & Adeshiyan, 2008; Zhong, Shen, & Seiferas, 2008). Alternately, as done in this research, investigations are made to optimise the expeditious restoration of service when unplanned outages occur. While avoiding outages provides technical researchers, technology architects and software programmers with opportunities to develop newer, faster, and more robust hardware and software, outages, of some type, are both expected and accepted.

2.2.1. Introduction

The Service Availability Forum, known more commonly within the IT industry internationally as either SAF or the SA Forum, is a consortium of industry-leading communications and computing companies working together to encourage IT solutions that enable the use of Commercial-Off-The-Shelf (COTS) building blocks in the creation of high availability network infrastructure products, systems and services. Supported, primarily, by

the telecommunications industry (Lumpp et al., 2008) SAF has championed the standardisation of availability. Similarly, research has been performed on actions that can be taken (and money that can be spent on tools) that purport to offer increases in the uptime of particular hardware, firmware, and software components of a network or IT environment (McLaughlin et al., 2008; Pelleg et al., 2008; Qi, Jin, Foster, & Gawor, 2008; Zhong et al., 2008). As a result of following independent paths for delivering IT and network environments at businesses, outages are not identical across organisations, even within the same industry. These outages are discussed here.

2.2.2. Planned and Unplanned Outages

Although this research focuses on unplanned outages and their restoration, it is valuable to identify the significant differences and impacts each type of outage can have on a business. In 2004, the majority of Fortune 500 companies experienced more than 90 minutes of outages (both planned and unplanned) per week (Roeber & Locsin, 2004).

Both planned and unplanned outages should be avoided, or minimised through appropriate technological duplication and redundancy (Wang, 2007), but even when it is accepted that this *should* be so, in fact, it is not. Outages occur. Table 2-1 shows the types of IT outages that can, and do occur. Each is described in detail in Sections 2.2.2.1 (planned outages) and 2.2.2.2 (unplanned outages).

Table 2-1.
Types of Planned and Unplanned Outages

Types of Planned IT Outages (Kimber, Zhang, Franklin & Bauer, 2006)	Types of Unplanned IT Outages (Enriquez, Brown & Patterson, 2002)
<ul style="list-style-type: none"> • Hardware • Software • Firmware • Other 	<ul style="list-style-type: none"> • Acts of Nature • Hardware • Humans Inside the Company • Humans Outside the Company • Software • System Overload • Vandalism

2.2.2.1. Planned Outages

Planned outages are the knowing removal of the use a software application, system, hardware, or network component, or some combination thereof, which is required by the business. A planned outage is required, if not desired, to improve the overall performance of the organisation’s computer systems. Historically scheduled during non-business hours, the events—planned outages—as the name suggests, are deliberate and premeditated.

As more and more businesses rely on their presence on the Internet for customers to purchase goods and services, businesses are closer and closer to having no business hours

that are non-business hours or are easily used for scheduling planned outages. Although the use of high availability databases, hardware redundancy and smooth transitions through cooperative versions of data help reduce planned outages (Wang, 2007), planned outages still occur. IT departments that provide services are increasingly concerned by required planned downtime and the need to minimise it (Bauer & Franklin, 2006). Examples of planned outages include the upgrade of operating system software, the expansion of a storage farm, or the replacement of a faulty network switch. These are all activities that, technically, must occur in order to keep the IT systems operating at what is considered an acceptable level of performance to support the activities of the business.

While a proactive maintenance strategy is one way in which planned outages, and their impacts to the business, can be managed, and the use of rolling upgrades and application load balancing can contribute to the minimisation of planned outages, they do not eliminate their occurrences or their impacts. Using a review of literature reporting on high availability and an evaluation about research performed by deploying server virtualization in a multi-server environment, researchers reported that new technologies, including live partition mobility and live application mobility features, may provide higher overall systems' availability, people and businesses seeking to minimise outages must weigh the costs and difficulties associated with their implementation (McLaughlin et al., 2008). Results delivered from applied research performed on newly designed hardware and firmware—on which innovative design verification techniques were implemented to ensure all complex components were designed, verified and delivered with the performance requirements sought by the manufacturer—included the acknowledgements that any planned outage costs time and money (Conklin, Hollenback, Mayer, & Winter, 2007). Results reported from case study information indicate that planned outage time can be predicted and is often of shorter duration than that experienced during unplanned outages because planned outages engage trained staff, often with documentation and necessary tools and parts, to perform the work needed to be performed during the outage. With experience, that allows an accurate estimate of the amount of time required to complete the work to be performed during the planned outage (Zhang, Sharma, & Franklin, 2005).

Though a retained commitment to cooperative versions of data can reduce planned outages (Wang, 2007), they are not eliminated and can greatly influence the businesses experiencing them. An IT organisation supporting its business must be perceived as being available whenever it is needed and planned outages are masked from end-users, even though they actually occur (McLaughlin et al., 2008). A method for modeling planned downtime should account for meeting requirements of users, analysing the benefits of downtime alternatives, and determining how to spend effort to reduce planned downtime was delivered in a publication of a planned outage taxonomy (Kimber et al., 2006). This

taxonomy classifies planned outages in one of four categories. These are planned hardware outage events, planned firmware outage events, planned software outage events and other planned outage events. Each is discussed in the following sections, though the examples cited in each section are not to be considered exhaustive.

2.2.2.1.1. *Planned Hardware Outages*

Planned outages exclusively related to hardware—which may include storage devices, computers, network switches or tape libraries—are one of four types. They are hardware updates, hardware upgrades, hardware repairs and routine maintenance. Hardware updates, which include changes that are deployed to fix minor design issues, are deployed to ensure that hardware used is current and still within the level of operation that the hardware manufacturers will support; hardware upgrades allow new features and functions to be introduced, providing more horsepower to the hardware being used; hardware repairs fix identified problems that caused unplanned outages; and routine maintenance, that includes cleaning trays, filters on a cooling system or other standard work performed ensuring optimum operability of the hardware (Kimber et al., 2006). A review (Clarke, Alves, Dell, Elfering, Kubala et al., 2009) of Reliability, Availability, and Serviceability (RAS) literature, coupled with a case study that analysed specific hardware developments that includes memory subsystem changes and the addition of a cryptographic engine, concludes with a predictive model for the integration of hardware to improve overall system reliability. Hardware planned outages have been designed to be minimised with the introduction of parity-protection, compartment deletions, and spare array capacity; however, the use of hardware in a business IT environment requires some planned hardware outages to occur. Yet, some businesses are unable to make non-disruptive changes and, in fact, hesitate to make any changes, even when the IT support organisations that provide IT services to the business recommend the changes and inform the business that some changes are needed urgently (McLaughlin et al., 2008).

An example of an event that requires a planned hardware outage, even when the goal of the business is to have few, if any, planned outages, occurs when a payroll production company is unable to print payroll cheques due to an error with the printer. When there is a known error in the printer and the printer is required, a planned hardware outage may impact the timing of its use; however, in the absence of the planned outage, the printer may not perform adequately to perform its required function. A review of the literature includes the citation that there is remarkable pleasure experienced by those who receive a paycheck; yet, there is a sometimes corresponding feeling of pain and frustration experienced by those who have to produce the physical paycheck—not simply to ensure that there are funds available in order for the recipient to deposit the cheque or convert the cheque to cash—but to process the hours worked, the salary earned, the taxes due and print a payroll cheque that can be

taken to a bank (Anonymous, 2009[b]). While many companies now handle payroll processing electronically, the same cannot be said of the bill processing that is done, also requiring printers to be available, required to ensure the company that is owed funds is able to send bills to owing customers so that the company can, in turn, receive payments from those owing customers. When printers have a planned outage, the impact to the recipients who receive delayed pay cheques or the receipt of bills from companies to which money is owed can have a ripple effect on the timing of the use of those funds received.

2.2.2.1.2. *Planned Firmware Outages*

Firmware is a specific combination of both hardware and software in which the software is embedded in a hardware device. Central processing units and storage devices, for example, both require firmware to operate. These read-only components of hardware include read-only memory (ROM), programmable read-only memory (PROM), and erasable programmable read-only memory (EPROM). It is noted that only PROM and EPROM firmware can be upgraded with software releases that are deployed into the hardware; ROM firmware must be physically replaced to be changed (Apple, 2008). One method to minimise planned firmware outages was suggested by Loveland, Dow, LeFevre, Beyer, and Chan (2008). Their case study of one manufacturer's high availability solution recommended the use of a logical supervisor of all activities on a set of hardware devices so that planned outages can occur in a serial manner. The researchers conclude that high availability can be achieved using active/active and active/passive implementations within virtualized environments to optimise high availability. Though the planned outage occurs, its impact to the business experiencing it has lesser impact because not all firmware is changed at one time, but is changed in each hardware component in which the firmware resides. Using the firmware "hypervisor", planned firmware outages can be managed; however, like all outages, they come at a cost. Though planned hardware outages are required to introduce hardware updates, hardware upgrades, hardware repairs or routine maintenance, planned firmware outages are only required to fix design issues that result in firmware updates or the delivery of new features or functions, resulting in firmware updates (Kimber et al., 2006).

2.2.2.1.3. *Planned Software Outages*

Similarly to planned hardware outages, planned software outages occur when there is a need to perform a software update, a software upgrade, a software repair, or to perform software maintenance. Planned software outages can deliver increased application functionality or can introduce software to an IT system enterprise that will eliminate the prospect of a future unplanned outage (Kimber et al., 2006). Design of an IT environment can include making planned software outages invisible to users, ensuring that enough components have access to the applications needed by users so that planned software

outages can occur without causing negative impact. The need for high availability is challenged by the need of businesses for continuous availability (Jews, Ahmad & Surman, 2008). This requirement specifically means that any outage is unacceptable and that some outages that are required must occur without affecting the business. Figure 2-3 depicts a coupling facility (CF) that allows continuous availability, by allowing access to data by more than one piece of computer hardware.

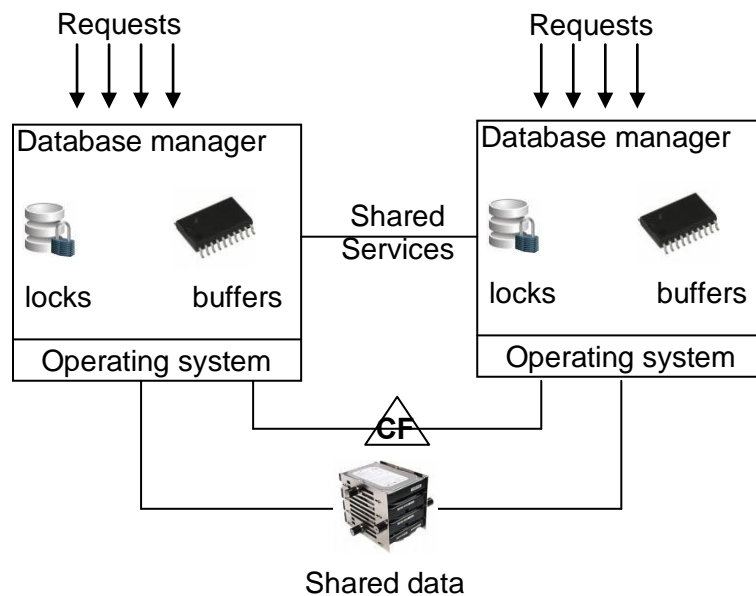


Figure 2-3. Coupling Facility (CF) to allow Continuous Availability (Jews et al., 2008, p. 507)

Planned software maintenance is necessary and can require a server to be restarted, taking an increased amount of time to complete a planned software outage than would be necessary if the software was able to be used immediately after it is installed. Of particular advantage in having planned software outages is that they are, in fact, planned. The technical, human, and managerial skills required to execute activity during the outages can be well organised. Expected durations of time are likely for the successful execution of the planned outage and, when errors occur during its execution, extending the expected duration, the technical skills to resolve the error are often already engaged and further time is not incurred by awaiting their engagement. Using canonical models to identify outage durations and their automatic and manual recovery distribution curves, Bauer and Franklin (2006) link planned outage durations and their failure rates with availability, citing that effective management of those outages contributes to increased system availability. Though tolerance for all planned outages is limited, the advantage of experiencing unplanned outages as a result of a planned outage is the potential time saved in already having technical staff available to complete the outage activities or reverse them.

2.2.2.1.4. Other Planned Outages

Other planned outages that occur in an IT environment may include specific network activity and scheduled power activity that cannot be classified as hardware, firmware, or software planned outages. A report published in 2004 cites the experiences investigated through two case studies and notes that under-planning other planned outages can cost a company millions of dollars. Taking into account the recommended ten-year power plan an IT organisation should have, when a planned power outage is required, planned outages for hardware, software, and firmware must also be planned (Eckhaus, 2004). In a large organisation with a significant IT environment, a data centre needs two uninterruptible power supplies (UPS's), two generators and a utility feed (Fitchett, 2004). When these requirements are not met, or are met but fail to meet performance requirements, a planned outage must be taken to establish either the required environment or introduce a solution that, when deployed, will be known not to meet the requirements. Introducing a solution during a planned outage that is known not to be able to meet the needs of the business can result in future unplanned outages. Outages taken when the needs of a data centre are addressed must be planned. Another example of a planned outage that is not hardware, firmware or software, though may cause planned hardware, planned firmware, and planned software outages, is associated with data centres themselves and not just the power feeds to those data centres. When a data centre is relocated or a new data centre is established, there is a rebalancing of the IT processing occurring at currently established data centres, including the use of production, stand-by and staging servers (Cocchiara et al., 2008) and their relocation to the new data centres. The planning for these types of outages can be significant, given that the activities being performed are not standard operating procedures for the companies performing them, unless, in fact, those companies are in business solely to sell their expertise in the field of data centre establishment to the company that requires different or expanded IT data floor space.

2.2.2.2. Unplanned Outages

All industries accept that computer components and systems used to run their businesses will have failures and that unplanned outages will occur (Bellowin, 2008; Fox, 2002; Kiciman & Fox, 2005; Northrop, 2003; Ramakrishnan et al., 2007). The use of the ITIL framework (see Section 2.2.3) suggests that unplanned outages would be reduced if even part of the ITIL framework was deployed by an IT organisation. It is estimated that 70 percent of all unplanned outages, commonly referred to as incidents, occur because of failed change management activities (Kim, 2006). Although research performed by means of a literature review and a case study reports that unplanned outages occur for only six reasons (Morrill et al., 2008). This list includes physical breakage, design errors, environmental events, operator inexperience or malice, natural disasters and accidents, and human caused

unplanned outages. More accurate and complete is the list of unplanned outages identified by Enriquez, Brown, and Patterson (2002). This list includes acts of nature, hardware, human beings inside an affected company, human beings outside of an affected company, software, system overload, and vandalism. Sometimes, long investigations must occur before it is known into what category the unplanned outage will fall. Not yet assigned to the unplanned outage type of either a human being's error or vandalism are the two 2008 internet cable cuts that left voice, data, video and internet traffic disrupted in the United Arab Emirates that affected 60 million users in India, 12 million users in Pakistan, six million users in Egypt and nearly five million users in Saudi Arabia. Rerouting of all traffic was undertaken to restore service (Zain, 2008). Much of the reported evidence about treachery in the IT and networks of organisations around the world is burdened by the variety of descriptions assigned to events and their impacts. Organisations as diverse as Deloitte's, Ernst & Young and the U.S. Federal Bureau of Investigation have researched the technical invasion of their data by unauthorised parties, but cannot yet determine if the number of electronic crimes or network- system- or data-intrusions can be correlated with any form of security breach (Pfleeger & Rue, 2008). Unplanned outages are not so much unexpected events as they are known events that occur at an unknown time (O'Callaghan, 2008; O'Callaghan & Mariappanadar, 2006[a]; O'Callaghan & Mariappanadar, 2006[b]; O'Callaghan & Mariappanadar, 2008). A review of each of the seven types of unplanned outages follows.

2.2.2.1. Acts of Nature

Sometimes resulting in a disaster, acts of nature that can cause unplanned IT and communications outages include fires, floods, earthquakes, tsunamis or some other catastrophe for which there may (or may not) be time to organise an alternate technology environment. In 2005, Hurricane Katrina changed the face of the city of New Orleans in the southern United States. The reality of the impact to the New Orleans School District, alone, reflects the impact of the disaster to one IT organisation. While some buildings were reclaimed after the hurricane and its downpour of rain subsided, the school district's computer, networking, and technology systems were a total loss. Much of the infrastructure was underwater and, what was not underwater was inoperable because of the winds and the impact of the hurricane that was not water-related (Gonzalez, 2008).

Following a 9.0 magnitude earthquake off the coast of Sumatra, a massive tsunami struck Sri Lanka on 26 December 2004, killing greater than 30,000 people. Restoration of IT services was not an initial concern, given the devastation to the Indonesian-island and its inhabitants; however, telecommunications systems were desperately needed for relatives to find one another, both within and from without Sumatra, and for emergency aid services to locate priority sites that required attention. Those telecommunications systems began to return within a day (Tanner, 2005), through Short-Message-Service (SMS). Internet access

was available through many parts of the impacted island and amateur videos were posted on the Internet that showed the world the tsunami as it hit land (Manafy, 2005). In this research, Acts of Nature include earthquakes, fires, flood, hurricanes, tornadoes, and tsunamis.

2.2.2.2. Hardware

There is a technology rule of thumb that is commonly referred to as Moore's Law that states that the number of transistors on an integrated circuit—effectively, the processing power of a computer—will double every 18 months (Moore, 1965). Disk storage capacity has increased by 60 percent to 100 percent every year since 1984 (Canali, Colajanni, & Lancellotti, 2009). Moreover, the cost of disk storage, as well as computational power, continues to decrease. In an IT environment, hardware is the single category under which computers, printers, monitors, switches, hubs, routers, cables, disks, hard drives, central processing units and other computer peripherals are included. Continually faster and cheaper, when they fail and an unplanned outage is experienced, the results can include, among other impacts, a computer "crash", resulting in the complete unavailability of the computer and the applications running on it. Central processing units (cpu's), tightly coupled with low-level software, can experience a "kernel panic", the result of actions taken by the UNIX (or UNIX-like) operating system when it is unable to recover safely from an internal and fatal error. When the Microsoft operating system detects a critical system failure, it is referred to as the blue screen of death, because when the error occurs, the monitor screen turns blue, and the computer usually freezes and needs to be restarted (Spector, 2008). Computers, alone, do not comprise an entire computer environment, even from a hardware perspective.

A storage device that fails because it is too full can cause the complete unavailability of the data that resides on the storage device. Technology is used to provide improved availability of data to computer system users, not the improved availability of computer systems themselves.

The improved availability of system hardware can be provided through the use of software, referred to as a hypervisor. This software allows multiple operating systems to run concurrently on a piece of computer hardware and establishes a virtual environment within a single computer. This, in turn, effectively packages an entire operating system, and application within, in the firmware so that it can be monitored and managed (Pelleg et al., 2008). Hypervisors can, when deployed and managed successfully, increase the availability of computer systems by allowing hardware replacements without taking the host computer system offline. It does not ensure 100 percent availability will be attained. Hardware does fail and unplanned outages do occur. Moreover, both reliability and availability are required by the business that pays for an IT enterprise.

It is both the reliability and availability that are represented as being able to provide value to the buyers of hardware. Reliability is most often measured and reported by the manufacturers of the hardware about which hardware reliability is reported. Hardware testing by manufacturers generates reports of *millions* of hours between failures, suggesting that Brand X hardware is superior to Brand Y hardware. Yet, despite efforts from industry and academia, high reliability is an ongoing challenge for managers running IT systems (Schroeder & Gibson, 2007).

An experimental study on the reliability of storage systems found that the size of storage devices has become so great that component failure is the norm rather than the exception (Ghemawat, Gobiuff, & Leung, 2003). Yet, the failure of the storage device can mean that required data is temporarily unavailable to users. Hardware outages were determined to be expected. Through an observational study, hardware component failures in large IT organisations were identified as ever-increasing problems as a single storage environment approaches the inclusion of nearly one million components (Schroeder & Gibson, 2007). When hardware is unavailable, the data attached to it is also unavailable. When data is lost, productivity, revenue and customer satisfaction are also lost (Mayer, 2005). When the business pays for hardware components that ensure an increased amount of data is available to it, on an immediate basis, the business expects that data to be available.

As the cost of hardware continues to decrease, more hardware will be added to an IT organisation's environment in order to provide support and service to its customers. To that end, the negative experiences that result due to data loss is exacerbated by similar experiences that occur when unplanned outages occur in central processing units, hand-held devices, printers and the array of devices commonly referred to as hardware. In this research, unplanned hardware outages include firewall failures, hardware itself, network routers, network switches, power loss or degradation, printer errors and failures, server errors and failures, and storage device failures, including those that occur on disk drives, tape drives, tape libraries and optical devices.

2.2.2.2.3. Human Beings

Research published in 1997 cited only five types of IT-related outages, in a client-server environment, after completing three case studies (Arthur, 1997). Human error was not on the list. In 2002, human error was credited with 15 percent of unplanned outages (Margeson, 2003). In 2007, human beings were credited with 40 percent of unplanned outages (Morrill et al., 2008). While the use of the ITIL framework (See Section 2.3.3) suggests that unplanned outages would be minimised with the development and deployment of appropriate and effective change- and problem-management processes, ITIL recognises that unplanned outages will not be eliminated. The combination of hardware, software, network components, and human error, when joined to create and operate a corporate

computer production environment, increases the probability that unplanned outages will occur. The U.S. Congress passed legislation making it illegal for individuals to obtain defence information, financial information, or consumer information from the government. The goal of Congress was to protect potential victims from identity theft, among other illegal actions. It was not until five further revisions of the law, in 2002, that private corporations were afforded the same protections from individuals misusing their IT data (Nahrstadt, 2009). Moreover, people can be identified as members of one of two, but not both, groups. They are either individuals inside of the affected company or individuals outside of the affected company that cause unplanned outages.

It is possible for individuals inside an affected company to cause unplanned outages. In fact, human error is one of the most insidious sources of failure and data loss in today's IT environments. Brown (2004) cites two significant unplanned IT outages that occurred nearly ten years ago. The first, in early 2001, Microsoft suffered a nearly 24-hour unplanned outage in its website as a result of a human error made while configuring a name resolution system. The second occurred later in the same year when an hour of trading on the NASDAQ stock exchange was disrupted because of a technician's mistake while testing a development system. Alternately, there are human errors caused when an employee makes mistakes while attempting to complete a task. Unplanned outages of any kind, when data is lost, can be exacerbated by the manual return of that data, as entering large volumes of data manually increases the likelihood of human errors, confirmed in case studies (N = 4) reviewed in which instances of such activity are cited (McKinney, 2007).

In this research, unplanned outages caused by human beings inside the affected company include outages caused by faulty documentation, security flaws identified as the result of action, or inaction, taken by an individual inside the company, an employee or contractor whose use of the application resulted in an unplanned outage and any unplanned outage identified with the reason for its occurrence as "no error found". "No error found" is the output of an investigation of an unplanned outage whose source could not be identified due to poorly written software, actions taken but not admitted to by the person(s) who performed the action, or any other unplanned event whose source cannot be located as a result of a human being not providing enough information for it to be otherwise identified as the result of a person inside the impacted business.

When an organisation experiences an unplanned IT or network outage, it often invests time and money in identifying the root cause of the outage for the purpose of permanently removing it so that the particular unplanned outage will not recur. However, when unplanned outages are caused by individuals not employed by the affected company or are employed by an organisation supporting the affected company (as a vendor, outsource provider, or contractor), stopping those unplanned outages rely on a change in behaviour of individuals

upon whom the company has little, if any, control. The importance of avoiding unplanned outages has resulted, in the United States, of the “Call Before You Dig” national support phone line to help individuals and businesses digging ditches or installing fences to ensure they do not inadvertently hit a cable or power line or some underground utility feature. A severed fibre-optic cable can easily cause millions of dollars in damages, in addition to those incurred when a gas line or water main is inadvertently hit (An 811 “Call Before You Dig” Ring, 2007). Errors, though, are only one contributor to unplanned outages caused by individuals outside of a company that is affected by the outage.

Alternately, there are nefarious activities that result in unplanned outages. The attack on the World Trade Centre buildings in New York City on September 11, 2001 are an example of individuals outside the company taking action that stopped computer systems in the businesses that were operating within the Twin Towers at the time of their destruction. No computer system is invulnerable to actions that result in catastrophic failure disasters such as that which has been come to be known as “9/11”. In a summary report on the communications impact of this single case study, the authors (Taylor & Skjei, 2002) acknowledge that the events of that day have led to a renewed interest in analysing existing emergency and local government response mechanisms and evaluating the measures to take to provide additional safeguards and backup communications in the event of future disasters. Communication networks can, themselves, suffer damage, resulting in reduced or unavailable service, and networks can be overloaded as government and disaster personnel, as well as average citizens, seek to stay informed and communicate with family members and others, actually or potentially impacted by a catastrophe.

In this research, unplanned outages caused by human beings outside the affected company include outages caused by individuals determined to cause physical disruption to the environment, as well as by those causing physical disruption without intention.

2.2.2.2.4. Software

Application software is responsible for 40 percent of unplanned outages (Morrill et al., 2008). Some of those unplanned software outages result in a requirement for a planned outage to occur so that the software component that caused the unplanned outage can be fixed. Software failures are often reported by the public press and referred to as “glitches”, as was reported when Gatwick Airport in England failed to have its clocks automatically convert to Daylight Savings Time in 2007, resulting in incorrect flight schedules being posted and an increase in missed on-time arrivals by incoming aircraft (Junelle & Neumann, 2007). The recognition that the impact of software outages can be notorious was sounded by a New York Times reporter who confirmed that the electronic timer set to measure the performance of each participant in the annual New York City marathon failed (Lorge, 2007). This failure occurred in a foot race, with more participants than any other of its type in the world, and had

a cash prize package for its winners. In 2010, that cash prize will exceed \$750,000 (New York Road Runners, 2009). The degree to which a software outage affects individuals or organisations is, clearly, dependent upon whose data is inaccurate or missing and for how long it is inaccurate or missing. In all cases, an unplanned software outage can have an impact that may range from annoying to devastating upon those who experience it. Hinson and Neumann (2008) report the results of a military anti-aircraft gun automatically turning and firing and killing nine soldiers. While the gun was locked into “manual” mode, it should not have operated at all. These so-called glitches are, in fact, software bugs. The term “bug” was used when Thomas Edison was alive in the late 1800’s and meant an industrial defect. Grace Hopper documented the finding of the first software bug (Hopper, 1981). Software bugs result in unexpected computer systems’ performance and/or unplanned software outages. They can include application software failures, database failures, operating systems failures, and, simply, software, in which the description of the error could did not include reference to what type of software it was in which the bug resided. This sub-type, software, includes failures that could not be associated to any of the other three sub-types (operating systems, databases, or application software), but include software failures referred to as Mandelbugs, Bohrbugs, Heisenbugs and Aging-Related failures. Mandelbugs are faults whose activation and/or error propagation are complex, where “complexity” can either be caused by interactions of the software application with its system-internal environment (hardware, operating system, other applications), or by a time lag between the fault activation and the occurrence of a failure. Bohrbugs, alternately, are faults that activate themselves, repeatedly, under a well-defined and, therefore, not considered complex, set of conditions. They are often considered the opposite of Mandelbugs. Heisenbugs are faults that, when inspected or investigated, actually change themselves or make themselves invisible, so that detecting and finding them is difficult. Aging related faults lead to an accumulation of internal errors, the source of which, in all cases, cannot be assigned to any other unplanned outage type (and sub-type) other than software (Grottke & Trivedi, 2005[a]; Grottke & Trivedi, 2005[b]).

2.2.2.2.5. System Overload

System overload, simply, is what occurs when not enough resources are available to perform tasks that need to be performed. In IT, system overload is the result of a computer system having inputs arrive at a rate so fast that they cannot be processed quickly enough and cause the computer system, itself, to fail. Fundamentally, the victim-computer is bombarded with inputs to the point that it is incapable of performing normal processing. System overload can be caused by a poorly structured data processing design, a poorly written software program by a software developer in the company or a well-written software program written by a hacker. Its result is the unavailability of a computer system due to its

inability to process all data inputs, due to the speed of their arrival, as opposed to the rate at which they are processed. How the processing of information occurs when its arrival rate exceeds the ability of the host to accept it was researched using case study data (N = 4) and determining the factors of the data packets to identify those to be discarded (Kim, Lau, Chuah, & Chao, 2006). When a threshold of processing is exceeded, the system, literally, overloads and fails. In addition to monitoring system performance and introducing load balancing (the distribution of processing activity evenly across multiple computers or networks so that no one device is overloaded), IT departments schedule processing during less-than-high-performance windows in order to avoid system overload (Schwartz, 2008).

2.2.2.2.6. Vandalism

Unlike the fifth-century German tribe whose name became synonymous with the ransacking and pillaging of towns and villages, vandals today are more sophisticated, with motivation ranging from the pure pleasure of being an IT vandal to the theft of identity and data, the bombardment of electronic spam, the promotion of denials-of-service, as well as the exploitation of a known software or system vulnerability. Malicious computer software (malware) has evolved from what was once a demonstration of technical skills to what is now a global criminal industry motivated by financial profits, as well as military and political persuasion. Malware is increasingly deployed with motivations of financial gain, access to classified data and the disruption of services. The costs of the impacts, as described by Volynkin (2007) in his doctoral dissertation, can be estimated using the valuation method, real options loss analysis, or present value loss analysis, each of which indicates some dollar loss due to the attack of malware. IT vandals perform cyber attacks that include five methods of attack. These include hacking to gain unauthorised access to a system, often for the purpose of stealing customer data, intellectual property or damaging data files; phishing, designing and using fraudulent websites and performing identity theft; defacing a company website; extortion and the denials of service to users attempting to access a company's website; and the release of malware into a network. Recent research introduced a new method to calculate the actual value of the data lost when vandals strike, real options analysis, applying alternative methods of loss estimation. This new application of real options analysis, used previously to produce capital budget alternatives, provides what is proposed to be the most comprehensive valuation of intangible loss estimations of cyber attacks (Smith & Amoruso, 2006). IT vandals do more than steal; they infect systems with viruses and otherwise plague corporate data systems, mobile phones, and all other technology for the purpose of doing harm. This was researched by means of the development of an event-driven simulator, used to investigate the propagation of malware. The results conclude that the potential effects of malware include excessive charges to customers, public relations disasters, loss of revenue for affected companies, degraded

service (Fleizach, Liljenstam, Johansson, Voelker, & Méhes, 2007) and fulltime employment for virus-hunters. Although an early virus, though not the first, Melissa infected computers in 1999 that had a WORD application opened by a user and caused \$US 80 million dollars in damage; it was the first virus to travel via email. Its author was jailed for 20 months in the United States and fined \$US five thousand dollars (Mills, 2009).

2.2.2.3. Classification of Unplanned Outages

As are injuries to a human being, unplanned outages are classified in terms of the degree of pain they cause the company impacted by them. While a physician may classify a heart attack as a serious event, the person having the heart attack may classify it as critical. Alternatively, both may consider it critical. By both impacted and affected parties it is, indeed, classified. So much so, that time spent in a hospital waiting room is certain to be longer for an individual with the injury classified as least important to those hospital personnel paid to manage the triage of emergency room patients. Unplanned outages are also classified as to their impact on the company experiencing them. Moreover, following the ITIL framework, unplanned outages are classified into a particular level of importance to the organisation experiencing them and, using ITIL’s Service Level Management function, time targets for service restoration should be established so that the performance of teams who restore service when unplanned outages occur can be measured. This time target (or Service Level Agreement) value is established based on the impact the unplanned outage has on the business. An example of the description of unplanned network outages for which incidents have been raised and severities have been assigned is listed in Table 2-2 and is from a set of case studies investigated by researchers at Bell Labs, in the United States, and support network and network-maintenance operations (Hartley, 2005).

Table 2-2.
Unplanned Network Outages – Descriptions and Targets

Severity	Description	Time to Restore to be Achieved to Meet Service Level Agreement
1	Emergency	4 Hours
2	Critical	4 Hours
3	Major	48 Hours
4	Minor	90 Days

Table 2-3 displays the severity of incidents described in a software application support environment, as well as a description of their impact and their expected time of restoration. These are extracted directly from a contract between a corporation and the provider delivering software support services to that corporation (Orbitz, 2003).

Table 2-3.

Unplanned Software Outages – Descriptions and Targets

Severity	Description	Time to Restore to be Achieved to Meet Service Level Agreement
1	Mission-Critical Impact	Within 45 minutes
2	High Systems Impact	Within 2 Hours
3	Business Productivity Impact	Within 72 hours
4	Minor Service Impact	120 days or fewer

2.2.3. Summary

Planned and unplanned outages will occur, all the while technologists work to eliminate them through the use of redundancy, hypervisors, dual channels and other technical avenues to support the continuous availability of IT systems. When planned outages occur they can be only one of four types (or a combination thereof); when unplanned outages occur, they can be only one of seven types (or a combination thereof). When unplanned outages occur, they are categorised in reference to the impact they have on the company experiencing them and are often referred to as Emergency (or Severity 1), Critical (or Severity 2), Major (or Severity 3) or Minor (or Severity 4). For each, a service level agreement is established between the business and the IT department so that the duration of time in which each unplanned outage is restored is measured and determined to having met the service level agreement or not.

Outages occur in IT environments and a business that uses those environments must be prepared to operate without fully available technology to support it. Regardless of whether an IT system processes and transmits corporate e-mail, makes available a banking application or keeps data about customers in a corporate database, downtime has become unacceptable. Mandates for high-availability computing are being driven from the top of the organisations (Graham & Sherman, 2003).

2.3. Incident Managers

2.3.1. Introduction

The role of an incident manager in an IT organisation exists within the context of incident managers contributing to the ability of an IT department to provide service support activities to its sponsoring business. The specific role delivers the restoration of service caused by unplanned outages. Additionally, it should be understood that the role is complemented by work performed by others, including change managers and problem managers. The incident manager contributes only one component of the services provided by IT departments to the business-at-large. Incident managers restore service; change managers prevent system changes that could cause unplanned outages; problem managers find the root cause of the

unplanned outages that occur. Incident managers can only provide their services successfully within the framework of many teams working to ensure IT services are available to the business when they are required.

2.3.2. The Role of Incident Managers

Although difficult jobs to perform, the job descriptions of the professional footballer, the nun, the solicitor and the teacher can all be defined through one-on-one experience with those professionals, through what one observes on the television, in the courtroom or in the classroom. These roles are visible to many. The job descriptions for each of these professionals, given by observers, may be incomplete, but are not, necessarily, incorrect. Incident managers, however, are not seen by masses and their job description is difficult to explain. To individuals outside of an IT department the role of incident managers are unlikely to be understood as a profession, in terms of the tasks that need to be performed, or as an IT profession. Simply, the incident manager's role is to restore normal service operation as quickly as possible and minimise the adverse impact of the unplanned outage on business operations (Cartlidge et al., 2007). The role of incident manager is one of only a few roles in the IT subspecialty referred to as Service Support. In large organisations, Service Support is one of five process segments (see Figure 2-4), each of which has accountability to perform some function(s) that allow optimal performance in the IT production environment.

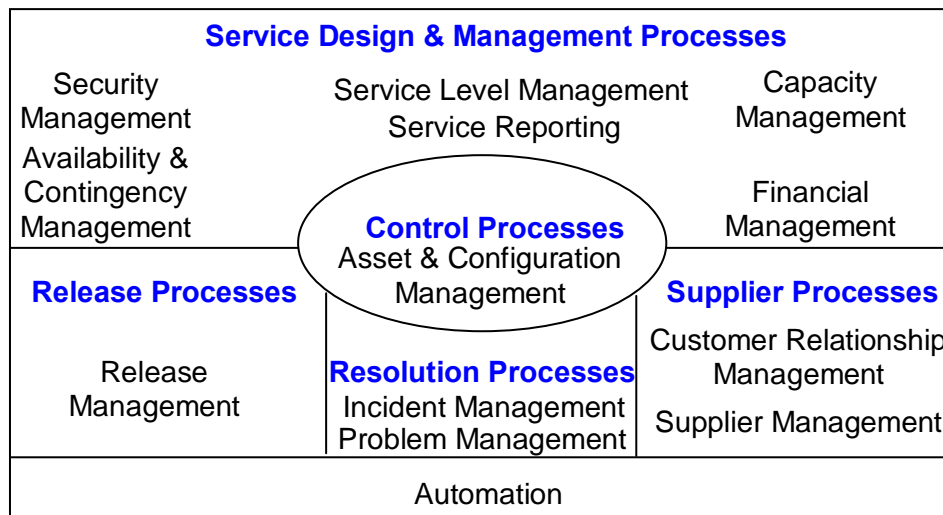


Figure 2-4. Service Design and Service Management Processes (Orr, 2008, p. 11)

The Service Design and Management Processes, the Release Processes, the Control Processes and the Supplier Processes are components of Service Support, but are not within the scope of this research. Service Design and Management Processes are those activities performed that result in the collection and documentation of business requirements, the design and development of solutions to meet the aforementioned requirements, the

working with all other required parties to ensure what is required and what is designed align to meet not only IT requirements but business requirements, the production and maintenance of all required documentation, and the associated activities to ensure requirements identified can be met and achieved. Release Processes are those activities performed to ensure that new and changed services deliver significant business value by delivering changes at optimised speed, minimised risk, and effective cost, while offering consistent and appropriate implementation of those changes. Control Processes are actions taken to identify, control and account for assets of the IT environment, ensuring integrity of that environment. Supplier Management is performed to ensure that a business is receiving value for the money it spends for all work performed from IT suppliers and that the contracts established to perform the work are aligned with the needs of the business (Cartlidge et al., 2007).

The set of work performed by incident managers within the Resolution Processes is key to the successful and continuous running of an IT environment (Ritchie, 2008). The primary goal of incident managers is to improve the quality of service provided to the IT customers by returning lost service to the users in as short a time as possible, with as minimal a business impact as possible. It is the restoration of service when unplanned outages occur that is the Resolution Process for which incident managers are accountable.

Though both incident management and problem management are components of the Resolution Processes, an important distinction is made between what each of those functions is designed to do and the tasks executed by individuals performing them. The objective of incident management is to restore service as quickly as possible when an unplanned outage occurs. Alternately, the objective of problem management is to diagnose the root causes of incidents and to provide workarounds or permanent fixes. While an incident is active until the service is restored, a problem is active until appropriate changes are implemented (Anonymous, 2005). If, for example, a computer server fails daily at 00:01, its service can be restored by restarting the server and using it until 00:01 the next morning, when it is known that it will fail. Incident managers are tasked with ensuring the server is available when it is needed; the action required to ensure its availability may include knowing that it will need to be restarted after it fails, again, at 00:01. Making the lost service available is the job of the incident manager. This is known as restoring service. Problem managers, however, are responsible to determine why the server fails at 00:01 each morning and to take actions to ensure it stops failing and continues to work without interruption. When the problem manager has identified and deployed a permanent fix that stops the daily failure of the service, the service has been restored permanently. This is known as resolving the problem.

Incident managers provide the greatest value to the organisations they support by having a business focus to ensure the optimization of resources; it should be viewed as a discipline to bring value to the organisation that uses it, rather than as a firefighting exercise (Holden & Thomson, 2006). To achieve this, an incident manager must help technical support teams and corporate managers work together to restore service. Alternatives must be found and selected for use, sequentially if not in parallel, in the expectation that one alternative will restore service. To determine what alternatives are viable, the asking of questions is important.

A study was performed by means of engaging business executives (N = 18) on a one-hour telephone call, asking open-ended questions, and speaking individually and confidentially to each of the respondents (Armenakis, Harris, Cole, Fillmer & Self, 2007). Through the use of this telephone survey, the researchers found that the data collected were responses to broad questions and that the responses were nondirective. However, other studies indicate that the asking of questions can provide insightful information into a problem trying to be solved, when the questions asked were not broad, but were binary. In a case study on the responses from a single patient in a medically diagnosed vegetative state due to a car accident, research was done on brain wave performance. The subject studied was asked only binary questions in order to monitor the brain waves when responses were given from the non-verbal medical patient. The patient thinking about tennis conveyed the value of yes; the patient thinking about a house conveyed the value of no. Each of these thoughts (tennis and house) result in stimulating different areas of the brain, allowing researchers to ensure they clearly understood if the answers they were receiving were yes or no, since the brain imaging used reported activity in one part of the brain when tennis was imagined (yes) and another part of the brain a house was imagined (no). The results indicate that clear communication can occur even when verbal skills are diminished (Singer, 2007). Applying the findings from this research to incident managers, one concludes that incident managers benefit from obtaining information available from responses to binary questions, allowing all parties engaged in the restoration of service to determine in what areas each party needs further detail without detaining those engaged, en masse. The use of binary questions by incident managers offers a simple tool to determine the general technology area that is experiencing the problem that caused the unplanned outage and work to restore service. There are two important factors to remember. The first is that the participants in the restoration of service from unplanned outages are rarely non-verbal and the second is that the incident manager must control the conversations in order to expedite the restoration of service.

A simple example of trying to find information is having an individual remove a card from a deck of playing cards. For ease of understanding, assume the deck has 52 cards and

there are no jokers. The person who does not know which card has been chosen can ask, card-by-card, if a specific card has been drawn from the deck. This use of binary questions will, in fact, result in the eventual identification of the selected card. Table 2-4 shows the number of questions that need to be asked to determine which card is drawn. It is obvious that luck will result in a short exercise if, using a card-by-card approach, the person determining the identity of the drawn card intercepts the selected card prior to asking 51 times “Is it the . . . ?” Alternately, by eliminating groups of cards, one question at a time, the person determining the identity of the drawn card eliminates blocks of cards as questions are asked and answered. Using binary questions that reveal more valuable information than a “yes” or “no” allows the identity of the selected card to be obtained by asking seven questions instead of 52 questions. Indeed, if time is a measurement of performance and it is considered of greater benefit when the duration of time is short, either set of binary questions will identify the selected card; however, the wise selection of binary questions can expedite its identification.

Table 2-4.
The Ace of Diamonds Can be Identified Quickly

Question	When binary is yes or no	When binary is x or y
1	Is it the king of hearts?	Is it a red card or a black card? (red)
2	Is it the queen of hearts?	Is it a heart or a diamond? (diamond)
3	Is it the jack of hearts?	Is it a face card or a number card? (number)
4	Is it the ten of hearts?	Is the value of card an odd number or an even number? (odd)
5	Is it the nine of hearts?	Is the value of the card greater than four? (no)
6	Is it the eight of hearts?	Is it the three of diamonds? (no)
7	Is it the seven of hearts. . . ?	It is the ace of diamonds.
14	Is it the king of spades . . . ?	
26	Is it the king of clubs . . . ?	
39	Is it the king of diamonds . . . ?	
52	It the ace of diamonds.	

When an incident manager uses binary questions from groups of options for why it is that an unplanned outage has occurred, the likelihood of restoring the lost service increases because the worst-case scenario of selecting one avenue of exploration after another avenue is removed and groups of unlikely options are eliminated en masse from investigation.

It is reported that incident management is all about urgency (Cartlidge et al., 2007). Technical support teams must restore service urgently. Good incident managers live on adrenalin, quick wits, among other skills, combined with resourcefulness (Waschke, 2006). Key skills of incident managers were identified as the ability to build relationships, maintain

focus, be organised, coordinate different teams, delegate, demonstrate leadership, listen, use intuition and have a customer focus (O'Callaghan & Mariappanadar, 2006[a]). In all cases, the speedy return to service that failed and caused an unplanned outage is the goal of all incident managers.

2.3.3. Information Technology Infrastructure Library (ITIL)

A competitive edge in every industry that depends on IT to operate successfully includes a framework that anchors the goals of IT with the goals of the business that IT supports. The Information Technology Infrastructure Library (ITIL) provides such a framework (Steinberg & Goodwin, 2006). Additionally, the interest in IT Service Management has increased and the ITSMF has established an International Organisation for Standardisation (commonly referred to as ISO) cachet, ISO/IEC 20000. This is the quality standard for IT Service Management; industry participants seeking certification in their delivery of quality IT Service Management services can engage an assessor to validate and verify compliance to the standard and be awarded use of the identifying logo of the certifying body. It is commonly referred to as the ITIL best practice for IT service delivery (Ramanathan, Ramnath & Glasgow, 2009). Using IT to support a business requires IT to support IT, itself. IT Service Management—the professional delivery of the management of IT in an organisation focusing on the customer, not the technology—was formalised with the introduction of ITIL. Non-proprietary (though the British monarchy owns the copyright) (Grenier, 2007), ITIL is an IT service management framework deployed in many of the best run IT shops internationally. Using a case study, McLaughlin and Damiano (2007) conclude that there is value in ITIL and it is demonstrated by the IT shops that have deployed it. ITIL Version 1 was a library of more than 30 volumes that provided guidance on IT operations management, as opposed to IT implementations. Beginning in the mid-1990's, the ITIL books were refined and condensed into nine core volumes and published as ITIL Version 2. ITIL Version 2 offered guidance on how to provide IT services to businesses through focusing on the processes used by IT Service Management. The changes made from ITIL Version 1 to ITIL Version 2 provided a strong link between business strategy and the investment in information and communication technology (Davies, 2003). Driven by industry change, ITIL Version 3, in only five volumes, was released in 2007. This library is comprised of Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement tomes. ITIL Version 3 focuses on the needs of the business and the manner in which IT Service Management can meet those business needs.

ITIL provides a systematic, professional approach to the delivery of IT Service Management and is the accepted, *de facto* world standard for IT Service Management (Holden & Thompson, 2006; Strechay & White, 2007). ITIL's goal is to move the delivery of IT in an organisation from a complex set of independent silos to an organisation working in

concert. ITIL's goal is to establish a structured and planned deployment of IT services to an organisation. Praeg and Schnabel (2006) propose an IT service framework comprised of four levels: strategic, business process, IT service, and tools. They argue that it is important for IT service managers to understand the business they support and the goals of the organisation.

IT is not just a technological area in the business, but a manner through which the business can provide goods and services to its customers. ITIL provides benefits to organisations that include, and are not limited to, a predictable infrastructure, improved testing, improved system changes, improved consultation with IT groups, smoother negotiation of Service Level Agreements, reduced server faults, more seamless end-to-end service, documented and consistent IT service management processes across the organisation (Cater-Steel, Toleman, & Tan, 2006).

ITIL, the most widely accepted approach to IT service management in the world, provides a set of service management best practices (Behr, Kim, & Spafford, 2005). It provides a framework for groups that provide IT service management within corporate, government, non-profit or other computer-using organisations. Its increase in use is significant. Results from a 2007 survey of 100 IT managers and directors in the United Kingdom showed that 62 percent of those managers indicate they are planning to migrate to ITIL in their IT organisations and 17 percent have timelines in place for doing so. Additionally, nine percent of manufacturing respondents claimed to be ready for a change to ITIL in their organisations, and 13 percent plan to introduce the ITIL framework to deliver IT service management within their organisations within twelve months of the survey being taken (ILX Group PLC, 2007).

There is a significant growth of IT Service Management practices in industry. IT executives expect to use out-of-the-box software to provide IT service management in their organisations, an increase from 67 to 83 percent in 2007 (Materna). Yet, minimal scholarly work exists on the topic of IT Service Management and there is little research that is explicitly ITIL-related (Galup et al., 2007). The key area of interest in this research, vis-à-vis the ITIL framework, is incident management. In the Service Operation book in the ITIL Version 3 library, focus is on the activities required to operate services and maintain their functionality, defined in the Service Level Agreements established with customers. A 2007 on-line survey of IT decision makers (N = 100), working in either Austria, Denmark, Finland, Germany or Sweden, revealed that incident management is the most frequently implemented ITIL discipline (67 percent), followed by the deployment of service desk (66 percent), problem management (49 percent) and change management (41 percent) processes (Materna, 2007). The annual on-line survey that followed in 2008 revealed that incident management is the most frequently deployed ITIL discipline. Moreover, 84 percent of survey respondents

identified themselves as having fully integrated IT with the needs of the business for which the IT organisation performs its work (Materna, 2008).

2.3.4. Summary

Incident managers perform a role best-understood by IT service support personnel; its effectiveness is optimised, as identified by Cummings and Kiesler (2008) who analysed the collaborative efforts of pairs of workers (N = 3,911). When every worker optimizes his/her contribution it allows that that the sum of the parts is greater than its whole. With this large study, it is reasonable to apply such collaboration success to incident managers when they work with each other, with technical team members, problem managers or change managers to restore service. For the purpose of most HR organisations, incident managers are considered part of the technical team and are remunerated within the confines of technical specialists rather than as business specialists; however, their contribution directly complements the goals of the business. Working in concert with change and problem managers, incident managers can keep an IT environment stable and available for its users. Incident management was formalised as a specific deliverable by IT departments with the introduction of the ITIL framework—providing guidelines, not rules or recommendations—on how a company can introduce the incident management role into an IT environment and achieve its purposes. Most research undertaken to investigate increasing systems reliability and availability has been done within the context of avoiding unplanned outages, yet that research does not actually suggest that unplanned outages will not occur, thereby requiring the skills of incident managers. This research accepts that unplanned outages will occur and investigates the human factors involved in the restoration of service from them.

2.4. Characteristics of Managers

2.4.1. Introduction

One of the key questions that initiated this research was “What is it that makes some incident managers so much better at what they do than others in the same role?” The characteristics displayed by incident managers were considered a viable avenue through which to begin the literature review. As ITIL proselytises the importance of the alignment of the IT department to the business (Carr, 2006; Steinberg & Goodwin, 2006), exploring the characteristics of business managers provided a foundation on which to investigate characteristics that might be displayed by incident managers. A study using stratified sampling techniques, with a response rate to distributed questionnaires in excess of 66 percent, attempted to investigate the age, gender, years in the workplace, and education of the respondents, citing these factors as characteristics (Okpara, 2006). These items are, to this researcher, demographic values, not characteristics; however, the study did investigate the relationship between these values to a specific characteristic in the workplace: job

satisfaction. Additionally, leadership was identified in multiple research works as a key characteristic for managers to display within a business. Duehr and Bono (2006) surveyed managers and students (N = 1,308), using seven different surveys and organising the participants into four different groups, to identify gender role perception and leadership in the workplace. Kozak and Uca (2008) used a questionnaire (N = 227) to identify leadership qualities in managers. Both research teams confirm that leadership is a strong and positive managerial characteristic. Another study, completed using both correlational and regression analysis from responses to the Schein Descriptive Index, citing 92 descriptive words or phrases expressing characteristics that could be considered important or impacting (either negatively or positively) for managers in business (Dorio, 2005). Multiple studies (de Pillis, Kernochan, Meilich, Prosser, & Whiting, 2008; Dorio, 2005; Duehr & Bono, 2006) used the Schein Descriptive Index and its 92 items describing common characteristics, allowing the researchers to take a comprehensive look at gender and other demographic data, in addition to characteristics (Schein, 1973, 1975). A reduced list of the Schein Descriptive Index was produced allowing only 13 characteristics to be assigned to managers described by survey respondents (de Pillis & Meilich, 2006). Limiting the numbers of characteristics which could be assigned by survey participants, the shorter version has the advantage of taking less time to complete than did the research done with the 92 item list, resulting in the likelihood of receiving a higher percentage of completed responses to items surveyed.

2.4.2. Characteristics Investigated

From the list of characteristics produced by Schein (1973, 1975), four items were explored in the literature. These include the characteristics of being authoritative, being competitive, being decisive, and having leadership. From the short list of characteristics developed by de Pillis and Meilich (2006) the item explored for this research was that of being compassionate. In addition to the five selected from the work performed by Schein, de Pillis and Meilich, another five were selected due to the researcher's professional experience and expectation that they were also like to be displayed by incident managers. These include being communicative, being demanding, being entrepreneurial, being facilitative, and being pragmatic. These were identified by the researcher who has spent more than twenty years in the service support and service management areas of IT departments internationally. These ten characteristics were explored in the literature, with an eye to unfold the contribution made to the business, if any, by the characteristic displayed. As well, it was sought to determine the extent to which IT personnel displayed any of these characteristics. For ease of reference, the complete list of the characteristics investigated is provided here, alphabetically: being authoritative, being compassionate, being communicative, being competitive, being decisive, being demanding, being entrepreneurial,

being facilitative, being pragmatic, and having leadership ability. They are reviewed in the following sections.

2.4.2.1. *Being Authoritative*

Distinct from authoritarian—the demonstration of tyranny and rigidity—being authoritative earns respect for those who use it from those who operate under it. Using multi-level modeling on subjects (N = 8,670) to test the effect of socialisation, researchers determined that being authoritative is characterised by having high standards for behaviour and maturity, and firm enforcement of rules and high levels of warmth and open communication, as well as being respectful for the developmental needs of the parties with whom one interacts (Perillin, 2005). Perillin's (2005) findings in relation to being authoritative may also apply to incident managers. Qualitative discourse analysis (N = 22) found certain features common in the communication of authoritative control and leadership, including the use of questions and rephrasing statements heard (Yeung, 2004). One may extrapolate the research done about authoritative parents and their children and apply the learnings to managers and their staff and incident managers and the individuals with whom those incident managers work when they restore service. While children with authoritative parents have been shown to have higher social and cognitive competence, higher aspirations, better academic performance, better psychological well-being and better behaviour compared to others (Lamborn, Mounts, Steinberg & Dornbusch, 1991; Shucksmith, Hendry, & Glendinning, 1995) authoritarian parents are tyrannical and rigid and, generally, have children who do not achieve the levels of success attained by children of authoritative parents.

Applying the findings from this research to incident managers, displaying an authoritative characteristic affords incident managers the ability to achieve the required goal (restoring service) while positively engaging the technical support groups and corporate managers with whom they work. They insist on structure, yet are flexible in their decision-making processes and their management of personnel. The authoritative characteristic of an incident manager combines the three necessary pillars of structure, control, and sensitivity cited by Bielous (1994) in his assessment of authoritative managers.

2.4.2.2. *Being Compassionate*

Showing compassion is considered one of the four major elements that organisations are encouraged to understand and display when facing what researchers identified as a critical incident (Gillingham & Noizet, 2007). An analysis of five case studies of international corporations that were confronted with potentially damaging media reports about products or processes included the acknowledgement that the impact of the potentially damaging media reports must be managed well in order to be minimised. Managing potentially damaging media reports of a critical event included the management of the media, the management of

employees, and understanding the impact of the potential damage to the organisation's brand, viewed in the short-term and in the long-term. The researchers premise that the management of a critical incident is important and that the management must include being seen as warm and human, rather than cold and calculating; however, the researchers never suggest that actually demonstrating compassion or being compassionate is important. They focus on the perception of how the incident is perceived to be managed, rather than how it is actually managed. While encouraged to act ethically and be seen to care about people, safety and victims (Bierck, 2000), actually being seen as compassionate and being seen to have concern were identified as being important to how an incident should be managed. This researcher does not challenge the value of managing perception when significant events occur that negatively impact businesses and corporations; however compassion is being aware of the needs of people around us and responding to those needs authentically (McKee & Massimilian, 2006), not responding in a manner packaged for consumption by an audience. Though viewed as a humanitarian value, being compassionate is more than relevant to businesses; it is integral.

Being compassionate gained a cachet when communicated by Bill Gates, co-founder of the Microsoft Corporation and its current Chairman of the Board. Gates presented an address to the 2007 graduates of Harvard University. At the time of his address, Gates was, literally, the richest man in the world; he challenged the well-heeled, well-educated, and highly intellectual graduates of the university from which he dropped out thirty years prior, Gates (2007) proselytised the importance of extending interest in others with whom his audience has nothing in common except their humanity. Indeed, being compassionate is rarely discussed within the confines of business; yet, inherently, it requires being attuned to people near us (McKee & Massimilian, 2006). As more hours are spent at the workplace, the people with whom we are physically most near, with increasing frequency, are our business associates.

Indeed, displays of compassion towards the opinions, needs and concerns of others in the company are a hallmark of a good leader (Anonymous, 2009[a]). Using a literature review to summarise the success of Motivational Language Theory, being compassionate is cited as one important tool in the arsenal of its users. Offered as a foundation for speaking practices by leaders, Motivational Language cites being compassionate as valuable in its use in strategic verbal communication and is associated, in part, with an employee performance improvement rating of 17 percent, a 70 percent increase in job satisfaction, and a 20 percent increase in innovation (Mayfield, 2009).

2.4.2.3. *Being Communicative*

Research on communication theory thrived following the development of a communication model built by engineers working at the Bell Laboratory in New Jersey in the

United States. Their research goal was to ensure the maximum efficiency of telephone cables and radio waves. They developed a communication model that established a mathematical theory of communication. What they created, however, was an original five-step model of communication. These steps were the sender having an idea, the sender encoding a message, a channel carrying the message, a receiver decoding the message, and the receiver sending feedback about the message (Deglar & Lewis, 2004). See Figure 2-5.

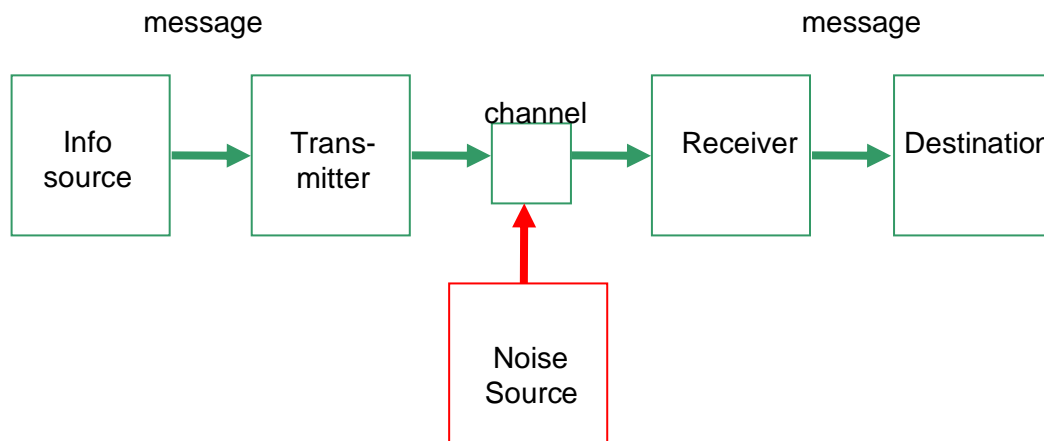


Figure 2-5. Shannon and Weaver's Communication Model (Deglar & Lewis, 2004)

Communication in business, however, is not an isolated activity conducted at an interpersonal level between the message sender and the message receiver; its significance lies in its use as a flexible, strategic tool for the organisation to orient and motivate employees towards a long-term productive end (Shockley-Zalabak, 2001). In the case of incident managers, that productive end is always the restoration of service after an unplanned outage occurs.

Shannon and Weaver's Communication Model launched a variety of theories to define the relationship of the message sender and the message receiver, resulting in the conclusion that communication is, fundamentally, a social behaviour (Kirby, 1997). Communication theory has identified the importance of communication "style" in assembling meaning and securing commitment to a productive purpose. Using two independent samples (N = 80 and N = 1,086, respectively), Norton (1978) analysed communications in terms of variable clustering, dimensionality within the structure of intercorrelations and best predictor variables. He introduced nine different communication styles that could be identified when people spoke. These are animated, attentive, contentious, dominant, dramatic, friendly, impression leaving, open, and relaxed. Alternatively, Phillip Clampitt (1991) identified three styles of management communication, which he cites as Arrow, Circuit and Dance. As noted in the application of psychological attributes in management performance, the psychotherapeutic techniques of Transactional Analysis focus on the communication framework found in all

levels of communications where the only roles are that of Parent, Adult and Child (Berne, 1964). In the research presented here, communication is defined as the formal and informal sharing of relevant, reliable, and timely information in a process through which individuals share and create information in order to reach their common goal (Anderson & Narus, 1990; Johnson & Lederer, 2005; Walczuch, Seelen, & Lundgren, 2001).

2.4.2.4. *Being Competitive*

Individuals who do not perceive themselves as being competitive may consider the characteristic as either genetic or, simply, annoying, but it is physically driven by an adrenaline-fuelled emotional state known as competitive arousal. A review of case studies in which overbidding at auctions was analysed, participants acknowledged that the decision to overbid, or to stop bidding, was made not from data but from the emotional state from which their bids made (Malhotra, Ku & Murnighan, 2008). Though self-perception may not exist during the competitive event itself, the fundamental desire to live is the most common expression of competitiveness found among all (Darwin, 1859; Maslow, 1943). Every professional athlete, for example, displays competitive arousal, whether the athlete's competitor is a clock, a human being, a team or a machine. A competitive balance, itself, advocates the central element for maintaining competitive balance. After providing a brief overview of the development of sport as an industry, the researcher explored its differences from other industry sectors or commercial products. The application of generic management research within the sports industry is rejected for a variety of reasons, not the least of which is that sporting, as an industry, is comprised of atypical participants at its core and the application of generic management research models used on atypical participants do not apply (Chadwick, 2009). A standard and typical research model was used to determine the value of competitiveness and performance at work. It was completed using qualitative surveys at ten French companies and 14 interviews with senior executives who were decision-makers in their company's sport-related activities. The researchers identified various sport-related activities, including structures *in situ*, events, company sporting associations, sponsorship, and others. Its functions are often interrelated and integrated into human resources management (as training and motivational tools) and both internal and external communication policies. Furthermore, they contribute to the social policy of the company. The conclusion drawn is that an athlete's use of performance, courage, surpassing oneself, ambition, self-respect, and respect for others puts a spotlight on the achievement when athletic practices result in athletic prowess and victory in competition (Pichot, Pierre & Burlot, 2009). To attain achievement and victory, however, successful athletes experience solidarity and otherness, both publicly unacknowledged, as athletes practice prior to public and professional competitions. Those practices contribute to success.

Being competitive forces those who genuinely display the characteristic to take risks and argue for their position to be supported. Competitors do not always win; however, they do always strive to win.

2.4.2.5. *Being Decisive*

Managers in business must balance the physically initiated emotional state that results in competitive arousal with the reality that time pressure seriously impairs decision-making. The increasing arousal caused in a competitive environment, coupled with a decreasing ability to apply and find relative information to make rational decisions, leads to an over-reliance on heuristics (Malhotra et al., 2008). Application of a speculative framework to guide decisions results in decisions being made, but not, necessarily, in good decisions being made.

Decisiveness must be defined clearly, insofar as one is able to be decisive without, necessarily, making a correct decision. The time to worry about a decision is before it is made (Syverud, 2006). The three definitions of decisive war battles, first documented by Sir Edward Creasy (1851), are provided in order to provide the core elements of both the ability to decide and the ability to decide well. The first definition of a decisive battle declares that it achieves operational objectives; the second definition states a battle is decisive when it ends a conflict by achieving strategic objectives of one side; the third definition is that a decisive battle not only ends conflict but results in lasting peace between conflicting parties (Goss, 2004). In this research, the first definition can be easily applied in business (operational objectives are achieved); the second requires a winner and a loser to be determined. The third requires a result unnecessary in business (lasting peace between conflicting parties).

Research that focuses on decisiveness shows it to be a key leadership quality. Using the two-step model of attributional processes, Nordstrom and Thomas (2007) studied the impression of college students (N = 125) on political situations. Students read political scenarios given to them by the researchers and, after reading the scenarios, participants first filled out a brief manipulation check measure. They then completed a two-item measure. Participants indicated their likelihood of voting for the candidate, and filled out the Trait and Demographic measures. Finally, they completed the individual difference measures, and were debriefed. The data gathered was assessed using multiple analysis tools, including ANCOVA, a series of one-way ANOVA's with a Bonferroni correction, and an exploratory analysis. The results, though not proving the researchers' hypotheses in all cases, did confirm the importance of decisiveness as a key leadership quality, confirming reports by Yukl (1998) in which a leader, acting decisively, is viewed as very effective.

In 2009, Free and Radcliffe investigated government reforms in Canada and, though focusing on the accountability of the government in crisis situations, they were unable to avoid citing decisiveness and decision-making practices as contributing to the crisis in which

the Canadian government found itself. The focus of their work was undertaken using a combination of literature review, document analysis, workshop attendance, and semi-formal interviews with key government officials. Within the constraints of their decision-making conclusions was that unnamed tools were necessary for effective decision making. Moreover, as did the researchers in previously cited literature, they note the importance of being decisive and the manner in which decisions were made, including the costs and inefficiencies in which certain decisions can result.

Semi-structured interviews held with 45 executives by Caulkins, Morrison and Weidemann (2007), discussing not only their being decisive, but their being decisive in light of the fact that they considered some of the data on which the decisions were based to be fundamentally in error, provided two significant findings. The researchers' data analysis confirmed that decision-makers knowingly make significant decisions using data that is known to be flawed. Secondly, the decision maker would not announce that a bad decision was made, even with the knowledge that bad data had been used to make it. This suggests that the making of a decision can occur without any review as to its viability or accuracy by the person who made it. Though acknowledging errors exist in the data used to make decisions, the researchers report that decision makers identified quality control as important prior to the presentation of data for use in a decision, not the need for the decision maker to acknowledge that data may be flawed when the data is presented or a decision is made (Caulkins, Morrison, & Weidemann, 2007).

Similarly, incident managers make decisions with all available data, without necessarily knowing that it is accurate or that it is sourced from the correct groundwork having been completed. Working with technical support specialists, incident managers must direct the actions of others based on all available data being assessed, knowing that, unless the root cause of the unplanned outage is unquestionably identified, being decisive will result in a decision, though not necessarily the correct one.

2.4.2.6. *Being Demanding*

There are two important components of being demanding. The first is to call for intensive effort or attention. The second is to determine how that call is to be made—in a severe and aggressive manner or in a direct, but unemotional manner. The components of how it is that desired actions are demanded are the need for intensive effort to be given in order to solve the issue at hand and the expression of the request for that effort. For incident managers, that intensive effort is engaged solely for the purpose of restoring service from unplanned outages.

Research in the behavior of making demands is varied, but a study performed by Malis and Roloff (2006) explored the serial arguments of individuals with demanding-withdrawing patterns of communications. Demand-withdraw refers to a communication pattern in which

one person demands, complains, nags or criticises, while the other person withdraws or otherwise attempts to remove himself from the discussion (Caughlin, 2002; Eldridge & Christensen, 2002). Malis and Roloff (2006) used bivariate associations for which controls were established, hierarchical regression was performed on the results of surveys completed by participants (N = 219) who identified their own patterns of demand-withdraw behaviour in conflicts. Findings revealed that most demand-withdraw communication is initiated by the one who demands, at a point of anger that cannot be expressed in another manner, as well as falling into response patterns that repeatedly place one party in the role of demander.

A 2003 survey (N = 680) showed that 47 percent of the private sector respondents reported unreasonable demands placed upon them was the top reason for stress among employees and that unreasonable demands placed upon staff were the biggest causes of workplace stress (Reade, 2003). A 2007 questionnaire of teenage girls (N = 224) showed that demanding was a term used to describe an individual with an excitability personality trait, along with being termed impatient and seeking attention (Silva, 2007). A 2009 survey cited 20 percent of participants (N = 4,824) as having described their immediate professional superior as bossy, demanding, and domineering and selected the associated personality trait of dominating to describe the person (Harris Interactive, 2009). Medical patients report wanting a physician who is, among other things, demanding of himself and of others, when looking for qualities in a doctor (Pinto & Piso, 2009). A four-year study using sentence completion to understand how old people were perceived by university students (N = 210) resulted in old people being described as demanding within the context of being old and curmudgeon-like (Thompson, 2006).

Overall, the assessment of the characteristic of being demanding either demonstrates strong confidence or, more frequently, a characteristic that is annoying, unpleasant to see expressed, and not normally recognised as a valuable asset by those who are subject to its power.

2.4.2.7. *Being Entrepreneurial*

Sourced from the French and Latin words, respectively, 'entre' (to enter) and 'prendre' (to take), the term "entrepreneur" has evolved to identify someone who undertakes activities that combine passion (Bird, 1989; Smilor, 1997), the deployment of resources in pursuit of an opportunity (Johannisson, 1998), and strategic change (Brunninge & Nordqvist, 2004) to achieve a goal. Hatch and Zweig (2000) conducted in-depth interviews with the founders of rapidly growing firms (N = 50) in Chicago, the third-largest city in the United States, and identified specific and common characteristics that contribute to entrepreneurs being in business, whether they were successful in that business or not. Their research concludes that what "makes" an entrepreneur is the combination of the risk tolerance, a desire to

control, a desire to succeed, perseverance, and decisiveness. The additional components of the “making” of an entrepreneur are shown in Figure 2-6.

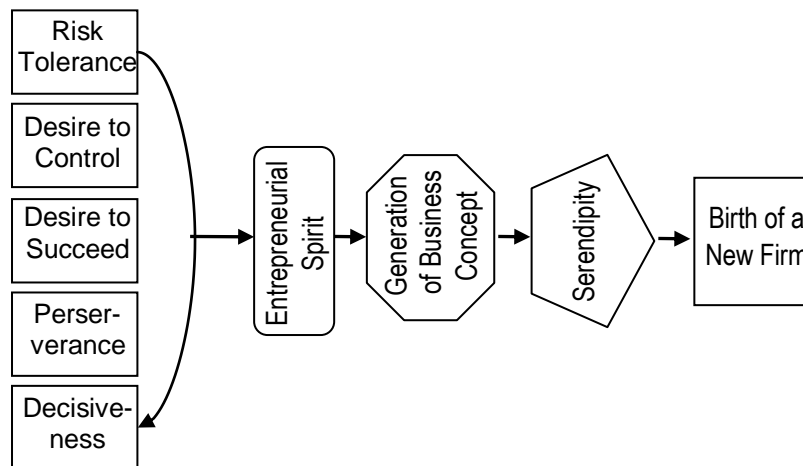


Figure 2-6. Characteristics of an Entrepreneur (Hatch & Zweig, 2000, p. 69)

This framework is complemented by the simpler, albeit essential characteristics that distinguish an entrepreneurial organisation from non-entrepreneurial businesses. These are innovation, potential for growth, and strategic objectives (Wickham, 2004).

Entrepreneurial organisations and entrepreneurial aspects within existing business entities and institutions are widely discussed in the literature. Many authors provide definitions related to entrepreneurship and its many different characteristics (Baden-Fuller & Stopford, 1994; Hisrich, 1986; Hurst, Rush, & White, 1989; Miller, 1983; Schumpeter, 1982; Sharma & Chrisman, 1999; Stevenson & Jarillo, 1990). Though each of these authors and researchers provide unique examples of successful entrepreneurs, one common denominator for many entrepreneurial ventures is a clearly observable distinction separating the entrepreneurial organisation from traditional organisations (Wickham, 2004). Turner (2002) provides a definition of the entrepreneurial organisation that promotes entrepreneurial activity adapting structure, management, and processes to gain the required agility, speed, creativity and drive to act profitably upon specific opportunities. Use of a questionnaire (N = 644) and the responses obtained allowed other researchers on entrepreneurship to conclude that passion and tenacity were valuable characteristics of an entrepreneurial individual, although not necessarily predictors of being entrepreneurial (Baum & Locke, 2004). Passion was found to be relevant in an entrepreneurial setting because it encourages entrepreneurs to face extreme uncertainty and resource shortages (Timmons, 2000).

Entrepreneurship poses a unique dilemma in companies. In theory, control systems—administrative, budgetary, and managerial controls, specifically—are designed in a manner that facilitates effective outcomes, including risk reduction, elimination of uncertainty, highly efficient operations, goal conformance, and specific role definitions. However, entrepreneurship appears to be consistent with an environment that encourages

management of uncertainty, promotes risk tolerance, encourages focused experimentation, and empowers employees, as concluded from the results of self-administered questionnaires (N = 475) (Morris, Allen, Schindehutte, & Avila, 2006).

Research was undertaken that investigated the “new”-ness of employees at entrepreneurial organisations. Two studies were performed that explored facets of entrepreneurship. The first study, referred to here as the “newness” study, was a socio-metric, Likert-scale survey that was given to all prospective respondents (Rollag, 2007). After creating a correlation matrix of all variables in the obtained dataset, an analysis was performed through hierarchical regression analysis, evaluating the relationships between the variables. Using a sociometric study at high-tech organisations (N = 4), where staff size ranged from 34 to 89 employees in California, U.S., data analysis was performed using a combination of techniques, including meta-analysis, regression analysis, and factor analysis. Rollag (2007) concluded that new-ness (within an organisation) is related to the duration of time an individual works within a particular group within the organisation and not for the organisation as a whole.

The second study (Morris et al., 2006), referred to here as the “control” study, investigated the relationship between administrative-, budgetary- and managerial-control in small-to-mid-size companies in the United States. This was an empirically based review of data obtained using two surveys. The first survey was distributed at 75 different firms. The second survey was distributed at 87 different firms. Responses (N = 475) were collected from individuals at all participating firms. The surveys were directed at a cross-section of corporate managers. The surveys stated that controls (administrative, budgetary, and managerial) are intended to guard against the possibility that people will do something the organisation does not want them to do or fail to do something they should do. A principal components factor analysis with oblique rotation was performed on the controls and the entrepreneurial measures, revealing relationships for formal controls, discretionary controls, and entrepreneurial orientation. Morris, Allen, Schindehutte, and Avila (2006) provide results that present clear evidence that control systems impact the level of entrepreneurship in companies.

Incident managers, responsible for the restoration of service from unplanned outages, whose financial impacts have been reviewed (see Section 1.2), must be aware of the tolerance of their organisation to controls required to be met by their organisation prior to taking action that would appear to be contrary to those controls or, otherwise, display entrepreneurial actions.

2.4.2.8. *Being Facilitative*

Incorrectly, being facilitative can be considered as being nice to all parties from whom something is desired, even when each party is disinterested in giving what is required to

provide an acceptable, if not optimal solution to a given problem. Rather, being facilitative occurs because individuals exploit available means to achieve intrinsic propensities toward higher levels of complexity (Grzwacz & Butler, 2005). Use of a short-form Social Desirability Scale and a Sport Anxiety Scale provided data used to determine if anxiety prior to a competitive sporting event was facilitative to an athlete's actual performance during competition. The researchers found that there was no support to interpret anxiety symptoms as more facilitative among the individuals studied. Scales were used both prior to and after a competitive event and all competitors completed the scales (N = 69). The data was analysed with both MANOVA and ANOVA to examine the responses of participants and a power analysis was conducted to refine scored details for individuals (Jones, Smith & Holmes, 2004). In a health-care study that illustrated how the profile of nurses was increased through the learning of a facilitative process, it was the opposite of how being facilitative was described that cited suspicion-based and fear-inducing alternatives of checklist monitoring. This research was performed using case studies (N = 4) (Larsen, Maundrill, Morgan, & Moulard, 2005). The extent to which an individual participates in work is made easier by the skills acquired in families. Identified in a telephone survey conducted across the United States, researchers determined that individuals in jobs with more autonomy and variety, and which required greater complexity and social skill, experienced a higher level of work-to-family facilitation than those who held work positions that did not afford the incumbent those flexibilities. Results were from interviews with participants (N = 2,045) identified through random sampling, who agreed to participate in a forty-minute conversation with the researchers (Grzwacz & Butler, 2005). The results were examined using hierarchical linear regression analysis to draw the conclusion that the ability to engage in work autonomy, variety, complexity and social skill afforded workers stronger facilitative behaviours between work and family.

Interprofessional working was identified as enabling teams to plan their work based on in-depth and confident knowledge of each member of the team. The case study analysed revealed that such teams had open communication, shared protocols, and were supported by leaders practicing facilitative management across professional boundaries (Kesby, 2002). Though Kesby's work was performed in a health care setting, her conclusion applies to incident managers, insofar as facilitative managers supports their teams, across professional boundaries.

2.4.2.9. *Being Pragmatic*

Investigations on the research of pragmatism leads one, inevitably, to the work of Charles Peirce, an early 19th century philosopher from the United States, whose work on pragmatism defined it as an allegiance to a distinct set of philosophical principles rather than a commitment to answering certain kinds of questions (Bryman, 2006). Peirce did not suggest

that pragmatism was a philosophy that asserts the importance of actual experience for informed learning and adaptation; it is not the simple view of pursuing the easy course of action (Emison, 2004).

Being pragmatic, as a characteristic, is the ability to execute plans to attain a necessary goal and negotiate with other interested parties solely to attain the goal. Pragmatic managers are those who do what is practical and expedient, all the while following Peirce’s philosophy that the pragmatist has allegiance to a distinct set of philosophical principles. Individuals who do not concern themselves with theories or big ideas are, by definition, pragmatic. They want to get a job done and are happy with a satisfactory outcome rather than striving for an optimal outcome. Painless courses of actions are not sought; wise courses of action are sought.

The *Unwritten Rules of the Game* (Scott-Morgan, 1994) explores the analysis and resolution of problems encountered in managing organisational change—change being an outcome that can be achieved with a pragmatic approach. Basing his work on available research, McGovern (1997), confirmed three themes of management and applied constituent characteristics to them from Scott-Morgan’s framework, advising that they appeal to the pragmatic nature of managers, even when the intellectual argument as to their value is not a strong one. The themes referenced and the constituent characteristics of the *Unwritten Rules* are identified in Figure 2-7:

<u>Main Theme</u>	<u>Constituent Characteristics</u>
Understanding the work world	{ <ul style="list-style-type: none"> Communication Individual focus Malleable human nature
Status enhancement	{ <ul style="list-style-type: none"> Unitary perspective
Practical application	{ <ul style="list-style-type: none"> Control Steps Authorisation

Figure 2-7. Pragmatic Managers Display of Specific Characteristics
(McGovern, 1999, p. 59)

Management gurus, including Peter Drucker, John Kotter, and Peter Senge, are some of the most influential management consultants in the world (Greatbatch & Clark, 2002) and McGovern (1997) argues, through an analysis of one publication on management, that successful ‘pop’ management ideas offer practical solutions to business problems and it is that set of practical solutions that are of the most appealing aspects for the pragmatic manager. McGovern cites three characteristics, originally identified by Huczynski (1993),

that apply to this pragmatic manager. They are control, steps, and authorisation. Control is offered as one of the achievements of successful managers, and certainly of successful incident managers. In particular, they offer the possibility of greater control over the most unpredictable of all organisational elements: people. Control also offers the ability to deal with “soft issues” associated with people and address them in a hard and direct manner. Steps are the set of actions one takes to learn what has been taught and apply it in real life. For incident managers, this is the application of getting individuals to perform work that may be outside of their comfort zone, but must be performed to restore service. Authorisation is the permission or power granted by an organisation that allows one to direct the work of others; a key requirement of incident managers.

2.4.2.10. *Having Leadership Ability*

Leadership research has been investigated in education, nursing, and other specific industry or work groups (Leithwood & Slegers, 2006). Kotter’s (2001) review of management and leadership summarised much of the writings on the topic of leadership, including the need for leadership and the ability to identify a good leader. Kotter concludes that leadership is about coping with change. This is opposed to management, which is about coping with complexity. Why the change occurs is less important than the fact that there is someone directing the actions of others to cope with the change to achieve a successful end. These conclusions narrow the requirements of leadership and identify it as necessary when change does occur or will occur, and unnecessary when change is not likely to occur. Kotter states that the function of leadership is to produce change. Beasley (2005) reports conclusions drawn from a literature review and suggests that leaders are visible in their corporate organisation and adapt their actions to the needs of a particular situation. One review of leadership was completed by intentionally omitting individuals whose performance provided negative results in a longitudinal study over six years (N = 335), ensuring that the results of individuals studied statistically, previously proven to be capable of leading, were the only participants from whom data was collected. Using structural equation modeling, a complex web of relationships was identified, as was the demonstration of multiple behaviours and characteristics, including passion, tenacity, communication and self-efficacy (Baum & Locke, 2004).

Having leadership ability was identified in research as a key characteristic for managers to display within a business. Duehr and Bono (2006) surveyed managers and students (N = 1,308) using seven different surveys and organising the participants into four different groups to identify gender role perception and leadership in the workplace. Although both managers and students were surveyed, each was surveyed only on the gender role perception and leadership in the workplace, not in the student environment. Kozak and Uca (2008) used a questionnaire (N = 227) in their empirical study to identify leadership qualities in managers.

Both research teams confirm the importance of leadership as a strong and positive managerial characteristic when effectively displayed. An investigation into nursing leadership defined leadership as the process through which an individual “attempts to intentionally [sic] influence another . . . to accomplish a goal” (Shortell & Kaluzny, 2000).

Through the analysis of previously performed quantitative studies and the review of leadership articles (N = 1,214), researchers concluded the effect of strongly demonstrated leadership contributes to a positive outcome (Wong & Cummings, 2007). This is of particular interest when it is recognised that this strongly demonstrated leadership was provided by nurses to patients and the positive outcome was associated to the patients’ health and well-being. In many studies, leadership was measured as practices, styles, behaviours, and competencies. One tool, the Multifactor Leadership Questionnaire (MLQ), used in both academic and corporate environments, purports to identify individuals not only as leaders, but also as particular types of leaders. The MLQ is a 360-degree feedback tool, developed by Bass (1985) and Bass and Avolio (1993) and is considered one of the most comprehensive assessments of leadership. Though Bass and Avolio (2005) reported transformational, transactional, non-transactional (also known as laissez-faire) leadership styles, those leadership styles have become targets to attain, providing individuals a professional leadership development path with attainable milestones to reach. See Appendix A for further detail on the Bass-Avolio Leadership steps.

Some researchers used the MLQ model of transformational leadership proffered by Bass and Avolio (1995); others used the Kouzes and Posner (2003) leadership model. Kouzes and Posner (2003) refer to the “Five Fundamentals” and suggest that whenever any events occur that require leadership styles to be demonstrated, there are five items that never change. That list is shown in Table 2-5.

Table 2-5.

The Five Leadership Fundamentals (Kouzes & Posner, 2003)

<i>Character counts</i>	Be careful your thoughts, for your thoughts become your words. Be careful your words, for your words become your deeds. Be careful your deeds, because your deeds become your habits. Be careful your habits, because your habits become your character. Be careful your characters, because your character becomes your destiny.
<i>Individuals act, organisations create culture</i>	Organisations do not act, individuals do. Organisations do not create breakthrough products, individuals do. Organisations do not defraud, individuals do. Leadership is personal. We must take personal responsibility for what we do.
<i>Our system is based on trust</i>	Our entire capitalist system is based on trust. It is not based on an investment model, the price earnings ratio, an income statement, a balance sheet, or on any set of numbers. It is based on whether people <i>believe</i> in the numbers and in the people who supply them.
<i>The legacy you leave is the life you lead.</i>	Exemplary leaders know that constituents are moved by deeds. They expect leaders to show up, pay attention, and participate in getting extraordinary things done. Leaders are judged by how they spend their time, how they react to critical incidents, the stories they tell, the questions they ask, the language and examples they choose and the measures they use.
<i>You can make a difference</i>	People want leaders who hold an ethic of service and who put principles ahead of politics or profits and other people before self-interests. Leadership matters. Success in initiating or responding to change is inextricably linked to the credibility of those leading the efforts.

A somewhat dated, but nonetheless valuable investigation of leadership within a rapidly changing IT industry was undertaken by Klenke (1993). The research identified four roles of IT personnel that should be considered as rapid changes in IT development and use occurred. These included IT professionals as decision makers, as motivators, as change agents, and as strategic leaders. A key function of that leadership is purported to be its focus on hope for the future rather than problems of the past. This research introduced the Leadership-Technology Cube, a conceptual model that links leadership skills and leadership roles to IT personnel and affects the outcomes of work performed (see Figure 2-8).

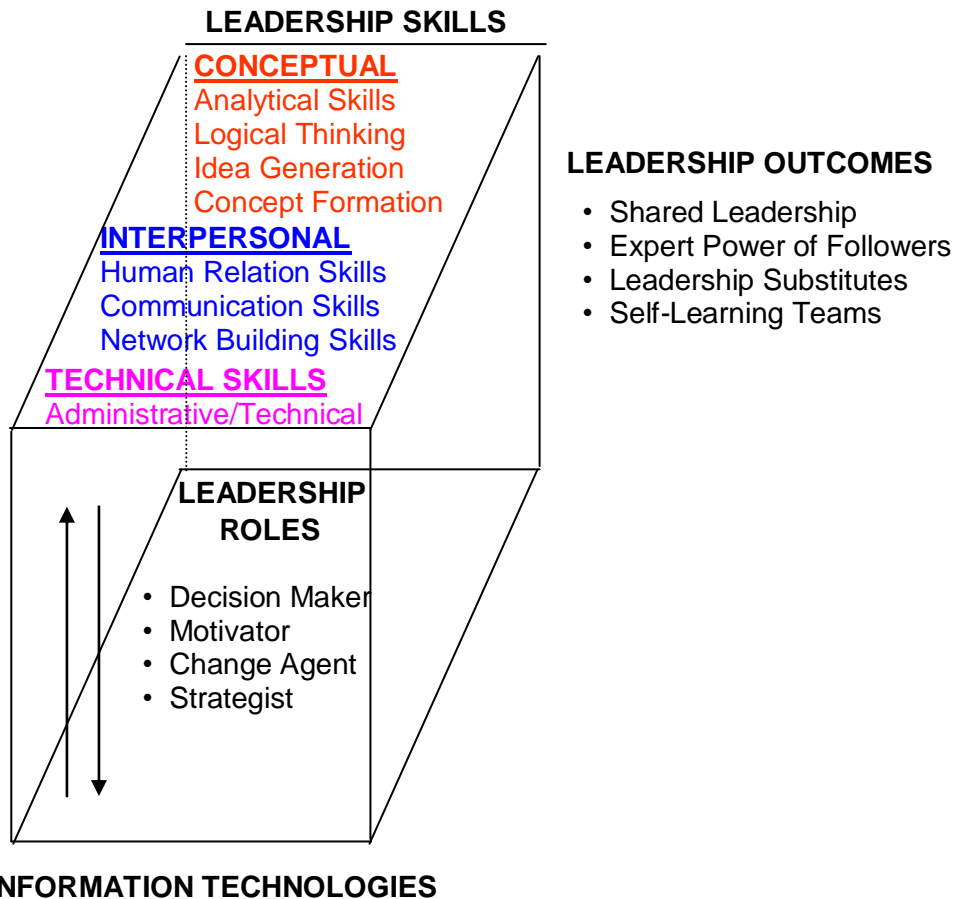


Figure 2-8. The Leadership-Technology Cube (Klenke, 1993, p. 221)

2.4.3. Summary

Research provides innumerable texts that can be reviewed for each of the characteristics cited in the Schein Descriptive Index, of which four were selected for this literature review. These include being authoritative, being competitive, being decisive and having leadership ability. A fifth, selected from the abbreviated Schein Descriptive Index, presented by de Pillis and Meilich (2006), was being compassionate. In addition to the five selected from the work performed by Schein, de Pillis and Meilich, another five were selected due to the researcher's professional experience and expectation that they were also like to be displayed by incident managers. These include being communicative, being demanding, being entrepreneurial, being facilitative, and being pragmatic. These were identified by the researcher who has spent more than twenty years in the service support and service management areas of IT departments internationally. There are limited literary references that relate specifically to the characteristics of incident managers. Reviewing the broad spectrum of research completed on the characteristics of managers and IT professionals, application of those characteristics determined important to managers and/or IT

professionals were analysed to determine which set of characteristics would be important to include in this research.

2.5. Approaches to Problem Solving and Restoring Service

In an effort to avoid unplanned outages, most organisations perform maintenance to software and hardware during planned outages; however, business requirements increasingly demand that those maintenance activities occur without any outage, allowing users to have system access as often as possible. Concurrent maintenance is preferred only to no required maintenance. Though technical support teams may be interested to know the technical reason(s) an unplanned outage occurred, business groups that depend on the availability of computer systems are interested in the immediate (or as close to immediate as possible) return of service. In addition, both the technical support groups and the business managers must accept the reality that IT systems do not operate flawlessly and that faults are not always readily fixed (Fox & Patterson, 2003). The time and costs associated with determining the root cause of an unplanned outage, identifying a fix for it, developing and testing that fix, and deploying the fix into the production environment must be weighed against the time and cost of taking simple, if dramatic, actions (such as rebooting a server issuing error messages) and returning it to service. When an unplanned outage occurs, the restoration of the service lost due to the unplanned outage may be critical.

2.5.1. Introduction

When presented with an unplanned outage, one of the steps taken in its restoration is the assessment of the criticality of the lost service(s) to the business impacted by it. This allows everyone aware of the unplanned outage to identify its impact on the business affected. When unplanned outages are reported, by end users or by technical support groups, help desk personnel use predetermined definitions of the criticality of unplanned outages and assign a value to it. Common values assigned are those ranging from critical, high, medium to low or values of Severity 1, Severity 2, Severity 3 or Severity 4. Unplanned outages are expected to be identified in a ticketing system so that there is a place to track all information discovered about the outage. Each impact of the unplanned outage is expected to have a value assigned to it and can be expected to have Service Levels Agreements established between the business and the IT organisation providing support services to indicate the expected duration in which the lost service will be restored. A Severity 1 incident, therefore, indicates the incident has significant impact on the services offered to the business and customers; a Severity 4 incident is assigned to minor incidents that do not require immediate restoration (Virzi, 2006).

When presented with an unplanned outage, impacted parties can focus either on the problem or on its solution. Following standard problem-solving processes, restoring service

from an unplanned outage can occur with a problem-focused approach or a solution-focused approach by the incident manager charged with engaging all parties to stop the business impact caused by the unplanned outage. Both problem-solving approaches use delineated, specific questions to achieve the restoration of service from an unplanned outage. Problem-focused problem-solving experts approach problems from the top down and generalise a problem (Schenk, Vitalari, & Davis, 1998) in order to solve it. Solution-focused problem-solving experts concentrate on a preferred state and acknowledge, but do not focus on the problem or its impact (Jackson & McKergow, 2007).

2.5.1.1. Problem-Focused Approach

A problem-focused approach to problem solving is self-defined and focuses on the problem. The person trying to solve the problem focuses on the problem by determining the root cause of the problem. Attempts are made to remove the problem by removing its root cause. It is not unusual for corporate managers to struggle with issues in a complex IT environment when the solution to the problem is decided to lie within the organisation's ability to break the problem down into compartments, solving each sub-problem before solving the entire problem (Coppola, 1997). The use of problem-focused problem solving focuses on the problem while working to remove the problem. In a qualitative study (N = 18) in which researchers asked broad questions during telephone interviews, one conclusion drawn was that a requirement of effective problem solving is to realise that each situation is unique and that corrective actions should be aligned to the given situation (Armenakis et al., 2007).

A problem-focused approach to problem solving dominates the problem solving literature. Volkema (2006) suggests that problem-focused problem solving provides adequate solutions whether people are intimately affected by the problem, have little stake in the outcome, or are simply interested in it. Finding a way to fix the problem begins with the diagnosis of the problem, defined as the identification of all components as either failing or not failing to explain the symptoms observed (de Kleer, Mackworth & Reiter, 1990).

Problem solving, as commonly taught, is analytical or procedural, employing almost exclusively the left hemisphere of the brain. A problem-focused approach requires specific, quantitative data about the entire problem and the environment in which it occurred. In a longitudinal study performed in the 1990's, Lumsdaine and Lumsdaine (1994) investigated the results from responses of engineering students to the Herrmann Brain Dominance Instrument (HBDI). This 120-question survey indicates the preference of problem-solvers to use analytical or creative thinking in their use of problem-focused problem solving skills. Shown in Table 2-6, there are five steps in the diagnosis of a problem, using a problem-focused problem solving approach.

Table 2-6.
Steps in Problem Diagnosis (Coppola, 1997)

Step	Problem Diagnosis
1.	Define the problem.
2.	Gather the information.
3.	List the possible solutions.
4.	Test solutions.
5.	Select the best course of action.

The first step is to define the problem. Defining the problem includes identifying the state of being of a problem and the perception of the presence or absence of an error (Miettinen & Flegel, 2003). One must determine what it is that has occurred that suggests a problem exists. In the case of incident managers, the occurrence of an unplanned outage is the problem that is perceived to exist. Normally, identifying what has stopped working, or what has begun to work differently than expected, characterises the state of being and defines the problem. The next step in diagnosing a problem is to gather information that is available, including the domain of the problem. The domain of a problem is the location where the problem occurred. In IT, the domain may be a network failure, a hardware failure, a software failure, or some other location where the problem or its symptoms are visible. Once the information about the problem has been gathered, solutions must be tested to determine which will resolve the problem; this is determined by identifying the root cause of the problem. Once done, the best course of action can be selected, implemented and the problem can be fixed. If, for example, the symptom of an unplanned IT outage indicates that the problem is the lack of response from a software application, the root cause of the problem may be that there is data contention on the network. The symptom of no network transactions being seen guides the problem solver to the problem, rather than to its symptom. The problem may be resolved by increasing the network bandwidth in order to remove the contention for network resources. The final step in a problem-focused approach to problem solving must occur. The problem must be removed through the selection of the best course of action to do so. Unplanned outages with significant negative impact to the end users or to the business often result in technical teams receiving *executive encouragement*—pressure from the corporate management team to fix the problem. Like its use in other industries, including law and criminal justice, executive encouragement is not necessary to accept when decisions are required; however, in some corporate cultures that exist in organisations, there is wisdom in accepting such encouragement (Meletta, 2008). When executive encouragement is given to incident managers, it occurs during times when unplanned outages being managed are not restored in as timely a manner as the business requires and the executive managers are, often, hearing directly from customers and end-

users who cannot use the IT systems at the company. Executive encouragement is designed to deliver service restoration through the active oversight of technical support groups already working to restore service. As well, it is used to communicate the importance of problem resolution. The process of problem resolution occurs after the problem has been diagnosed. (See Table 2-7.)

Table 2-7.
Steps in Problem Resolution (Kepner & Tregoe, 1996)

Step	Problem Resolution
1.	Understand the problem situation.
2.	Understand the purpose to be served.
3.	Involve the people who can help solve the problem.
4.	Get a complete and accurate picture of the problem.
5.	Find the cause and prove it.
6.	Set the criteria for effective action.
7.	Find the best actions to resolve the problem.
8.	Create a workable first draft of a plan.
9.	Fine-tune the plan into a program of action.
10.	Communicate to gain understanding and acceptance.

This traditional problem-solving method is linear and the steps are taken sequentially; it is not always an optimal problem-solving approach for multi-dimensional problems (Coppola, 1997). These steps, however, can be taken and applied to all problems, though these steps may prove time consuming.

Most available research investigates the use of a problem-solving approach to solving problems and finds that approach to be methodical, simple, and effective. It does not, however, indicate that it can be performed expeditiously. The application of the Kepner-Tregoe problem-solving analysis to determine why Apollo XIII failed took weeks to complete; yet, the work to return the astronauts to earth could not wait weeks. All the while promoting a problem-focused approach to solving its problems, the U.S. National Aeronautics and Space Administration (NASA) used a solution-focused approach to get the astronauts back to earth in days. Though referred to as an “abbreviated use of the problem analysis” (Kepner & Tregoe, 1997), what the team of engineers on the ground did to return the astronauts to earth was to focus on the solutions available to achieve their goal. Their goal was the safe return of the astronauts to earth; that an oxygen tank exploded mid-flight was identified as the root cause of the disaster, through problem-focused techniques, was used after the solution-focused approach achieved its goal. This aligns precisely with the work of de Kleer,

Mackworth and Reiter (1990) who state that to fix a problem begins with the diagnosis of the problem, defined as the identification of all components as either failing or not failing to explain the symptoms observed. NASA had no such time to apply these techniques.

ITIL identifies the steps of root cause analysis performed when desiring the permanent removal of a problem by means of the Kepner-Tregoe method (Taylor, 2007). Actually named the Kepner-Tregoe Problem Solving and Decision Making (PSDM) process, “Kepner-Tregoe” and “K-T” have become common nomenclature for solving problems. Its four steps are cited in Table 2-8:

Table 2-8.
K-T Steps in Problem Solving (Continuous Improvement Facilitators, 2006)

Step	Problem Resolution
1.	Describe the problem.
2.	Identify possible causes.
3.	Explore possible causes.
4.	Verify the true cause.

Use of the Kepner-Tregoe problem-solving method affords incident managers an alternative to a common use of hunches, instinct, and intuition to restore service (Marquis, 2006). A problem-focused approach to restoring service makes use of the combined knowledge, experience, insight, and judgment of a team, resulting in faster and better decisions. Though the K-T method describes ITIL’s problem management function, it is often applied as an incident management tool when the restoration of service is less important than determining the root cause of the problem that caused the unplanned outage. A primer to its application is offered in Table 2-9, in which the correct K-T questions are asked, for which answers are sought.

Table 2-9.
Problem Analysis Worksheet (Taylor, 2007)

	Is	Could Be But Is Not	Differences	Changes
What	System failure	Similar systems/situations not failed	Staff; time of day it occurred; applied fix during time of time of day it occurred	New fix deployed. NOTE: change was authorised to proceed
Where	Failure location	Other locations that did not fail	Done by paid staff—normally done by vendor	Vendor did not perform work; this is odd, as the vendor in fact, performs most of these changes
When	Failure time	Other times where failure did not occur	As stated, above	As stated, above
Extent	Other failed systems	Other systems without failure	Everything else is okay	Everything else is okay

Table 2-9 describes the four aspects of every problem—what it is, where it happens, when it happened, and how severe its pain was to the impacted party. The IS column provides space to describe specifics about the problem. The COULD BE but IS NOT column provides space to list items related to the problem, excluding detail. These two columns can assist in removing both intuitive and incorrect assumptions about the problem. With columns one and two completed, the third column provides space to detail the differences between what IS and COULD BE but IS NOT. The last column provides space to list any changes made that could account for the differences (Taylor, 2007).

Kepner-Tregoe problem-solving is one of a variety of problem-focused approaches used by problem solvers working to determine why an event has become a problem. Unlike solution-focused managers, problem-focused managers not only ask, “What happened?” but work to discover the answer to the question. Other problem-focused problem solving tools and techniques are quality improvement programs including Ishikawa diagrams, Total Quality Management (TQM), and Six Sigma. All are designed to solve problems.

The Ishikawa diagram, also known as a cause-and-effect or fishbone diagram, is one of seven basic tools used in quality management to solve problems. The other six are histograms, Pareto charts, check sheets, control charts, flowcharts, and scatter diagrams (Calabrese, Foo & Ramsay, 2007; Maze-Emery, 2008). The other six are not discussed here

in detail, yet their applicability to problem solving is, in fact, variations on the themes identified through the use of the Ishikawa diagram. Developed in the 20th century, the Ishikawa diagram is credited to a Japanese quality manager, Karou Ishikawa, who first introduced this problem-solving tool in 1943 (Rooney, Kubiak, Westcott, Reid, Wagoner, Pylipowe, et al., 2009). Ishikawa diagrams are used to aid problem solvers in determining the root cause of an issue and to understand why the issue is experienced. It forces the participants in its creation to determine why the process to be delivered is not being delivered as expected (or at all), and to identify from where data should be obtained to fix the issue. Ishikawa diagrams illustrate the main causes and sub-causes that lead to an effect. It provides problem-solvers information, not data, in a graphic format. Ishikawa diagrams, as well as the other six basic quality management tools, provide graphical information for consideration when working to determine the cause of a problem. An example of an Ishikawa diagram can be seen in Figure 2-9.

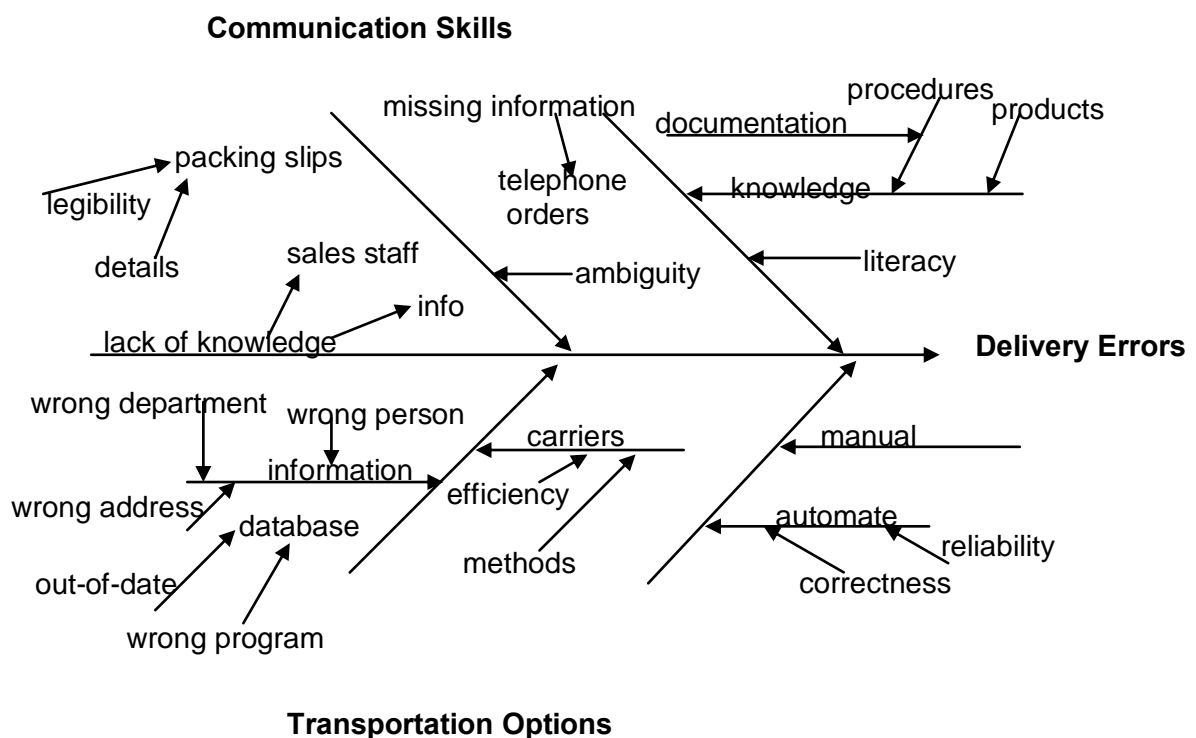


Figure 2-9. Example of an Ishikawa, aka Fishbone, Diagram (HCI, 2009)

Total Quality Management (TQM), a problem solving tool that contributed to the fundamental problem-solving activities performed in manufacturing organisations in Japan, has multiple theories as to its origin; however, in the 1980's its use was applied internationally and its origin is credited, primarily, to four quality management experts, including W. Edwards Deming, Joseph Juran, Philip Crosby, and Kaoru Ishikawa (cited previously for the problem solving tool commonly referred to as the Ishikawa "fishbone" diagram). The aim of TQM is to reduce variation from every process used to create a product in order to increase consistency in the delivered product (Royse, Thyer, Padgett, &

Logan, 2006). Unquestionably, it requires measuring performance, making improvements, re-measuring performance, and ensuring that all parties using the process apply all improvements made in a consistent manner. Additionally, one key component of TQM is its consideration by all parties performing the processes. Workers are not asked just to perform, but to be responsible and accountable for their performance to ensure improvements are incorporated consistently.

TQM comprises four steps, each with a Japanese name, given that the Japanese first successfully deployed TQM on a broad scale. The steps are cited in Table 2-10.

Table 2-10.
The Steps of Total Quality Management (de Villiers, 2006)

<u>STEPS</u>	<u>ACTIVITIES</u>
Kaizen	Focuses on continuous process improvements, using a team to obtain input from all impacted parties and makes processes visible, consistent, and measurable
Atarimae Hinshitsu	Focuses on the intangible effects of processes and focuses on quality that is expected by the user
Kansei	Examines the manner in which the user of the product actually uses the product in order to improve the product
Miryokuteki Hinshitsu	Requires that the product has an aesthetic quality and it is pleasing to use so that a user will use it

Unlike other problem solving tools, Six Sigma is a management process designed not to improve products or services, but to remove defects, defined as anything that causes customer dissatisfaction. Introduced by the Motorola Corporation in the United States in 1982, Six Sigma is considered more a business strategy than a quality program, although its successful deployment undoubtedly improves product quality (Maguad, 2006). Although a subtle alternative to solving problems, Six Sigma processes focus on the identification of defects and their removal, measuring defects in order to obtain a degree of performance and acceptable quality at the mathematical value of Six Sigma. The Six Sigma process measures the number of defects per opportunity to have a defect, with the goal of achieving Six Sigma performance. Sigma, expressed mathematically using the Greek letter σ , represents the standard deviation of quality from perfection. Table 2-11 identifies the level of quality and accurate products made when achieving each of the first six levels of sigma performance. Achieving Six Sigma states that only 3.4 defects occur from the 1,000,000 opportunities in which a defect could occur.

Table 2-11.
Sigma Quality – The Percentage of Defect-Free Products

Sigma	Percent of Quality and Defect-Free Products Produced
1	31.00000%
2	69.20000%
3	93.32000%
4	99.37900%
5	99.97700%
6	99.99966%

A problem-focused approach to problem solving, when done effectively, finds the cause of the problem and eliminates it. A problem-focused approach to solving problems is not used to determine if information exists to solve the problem, but to stimulate new learning to solve the problem (Hallinger & Kantamara, 2001). It is a time-weathered approach to bringing forward solutions and allows for creative thinking in identifying alternative solutions that may resolve a given problem. Solutions must meet the needs of the parties experiencing the problem; problem-solving techniques are used to identify the cause of the problem in order to determine a solution. Known as effective vehicles to improve quality, problem-focused problem solving is presented within the frameworks of Ishikawa diagrams, Six Sigma, TQM, K-T problem solving and other alternatives that have strict measuring guidelines to determine performance. It is among the K-T framework that ITIL promotes work within the problem management slice of service management to perform problem-focused problem solving. ITIL recommends no approach for managing incidents.

2.5.1.2. Solution-Focused Approach

A solution-focused approach to problem solving acknowledges a problem exists and some “fix” is required, but a solution-focused approach directs its users not to focus on the problem and not to focus on the cause of the problem. A solution-focused approach to problem solving requires all discussion about the problem (and, for incident managers, about the unplanned outage) be on the desired state, not on the current state and not on the problem. This problem-solving approach was founded on the psychological work done that is known as Solution-Focused Brief Therapy.

Solution focused therapy developed roots in California, in the United States, in the 1960’s at the Mental Research Institute (MRI), established to study communication between mentally ill patients and members of their families. A three-step approach was identified to solve problems patients presented to psychotherapists working at MRI. Clinicians worked with patients to perform the following steps, in the following sequence. First, patients were directed to stop fixing what was not broken. Secondly, they were directed to stop doing what

did not work and do something else, instead. Finally, they were directed to do more of what did work. The focus of all of the work, until the late 1970's, was on the problems presented by the patients. In 1979, however, two individuals who set up their own Brief Therapy centre in Wisconsin, in the United States, brought a radical change to the approach introduced at MRI. Steve de Shazer and Insoo Kim Berg are credited for the establishment of the psychotherapeutic school of Solution Focused Brief Therapy (Trepper, Dolan, McCollum & Nelson, 2006). They realised that while problems happened, they did not occur consistently nor did they always occur. Periods of time passed when no problem existed. This insight resulted in them applying the three steps offered by MRI in a different sequence. These solution-focused leaders agreed the first step to finding a solution to a problem was not to fix something not broken. However, de Shazer and Berg had patients take as the second step the doing more of what works. They moved MRI's second step to the third in their trilogy and told patients to stop doing what did not work and do something different. At first blush, exchanging the order in which steps two and three were performed appears to be a minor revision of the work done in California; however, it unfolded into a radical shift in the approach to solving problems, establishing a solution-focused approach to problem solving. This changed the framework of how it was the individual patients visualised the problems they reported from being their focus to the simple acceptance that the problem existed and identifying ways to lessen it, with a goal to remove it, if, in fact, removing the problem was the solution to the problem.

de Shazer and Berg expanded on work performed by Watzlawick, Weakland, and Fisch (1974) who found that problems were often perpetuated when time was taken to understand their origins; problems were lessened when actions were taken to find solutions to the problems. de Shazer and Berg identified one behaviour in therapists that resulted in clients being four times more likely to discuss solutions instead of the problem. That behaviour was the asking of questions (Bannink, 2007). This included questioning solutions, questioning change, and questioning resources. The behaviour was the asking of questions that identified solutions that could be attained by removing, not necessarily understanding the cause of the problem. They included the questioning the details of what specific actions could be taken to achieve the solution; and they included the giving of verbal rewards—compliments—to reinforce trains of thought and activities that would result in a desired state. Cepeda and Davenport (2006) align person-centred therapy with its focus on now, and Solution Focused Brief Therapy with its focus on future, as both therapeutic techniques raise awareness of the ability, skills, and resources available to the individual experiencing a problem. Use of a solution-focused approach builds on client resources, helping the clients move closer to their desired state. It is uniquely suited to facilitating positive outcomes (Froerer, Smock, & Seedall, 2009).

An example of a solution-focused approach to solving a problem is one undertaken by millions of people, worldwide, each day. According to the World Health Organisation, more than one billion adults are overweight (Mulier, 2008). In 2006, the U.S. Centres for Disease Control and Prevention ranked one of that country's fifty states among fattest in the nation and identified greater than 65 percent of the population of that state as overweight, if not obese (Stump, 2007). Referred to as a worldwide concern (Brown, Hockey & Dobson, 2007), overweight people who look to solve their problem of being overweight have innumerable options for taking action, all of which require change. While the global economic crisis of 2008 impacted revenue for Weight Watchers, Jenny Craig, and Nutrisystem during that financial year, all three companies continue to generate revenue and are considered viable businesses, negatively impacted by the economic downturn, not crippled by it (Mulier, 2008). Fat people who actively pursue a weight reduction program do not look, necessarily at the end goal, but at each meal they eat and each kilogram of weight they lose as a success to achieving their weight loss goal. By using the simple steps prescribed through a solution-focus approach to problem solving, an overweight individual acknowledges there is a problem to solve, but does not dwell on the problem. Every kilogram lost is a success in itself and support is obtained from others. Solution focused therapy spotlights and acknowledges patient successes through compliments and verbal recognition of the success, even when they are nominal successes.

This strengths-based approach in therapy encourages the use of personal resources and their application to making change. A review of experimental and quasi-experimental research conducted from 1985 to 2006 was published and cites the implications for use of solution-focused therapy in social work (Corcoran & Pillai, 2009), though less available is research performed in the use of solution-focused approaches to solving problems used in business and management. There is a school of management, referred to as the "Tiger Woods School of Management" (after the professional athlete, Tiger Woods), that cites his strengths in his long game (use of his woods and irons). It also cites his strength as a golf putter. Yet, it acknowledges his position of 61 in the ability to extricate himself from sand traps (in golf, a bad place to be) (Buckingham & Clifton, 2001). Woods' ability to focus on his professional strengths, as opposed to his weaknesses, allows him to excel in areas that help him avoid ever experiencing his weakness. He focuses not on the problem of winning a golf tournament, but on the activities he must perform, actually, to win a golf tournament. Others, less famous than Tiger Woods, have committed themselves to the benefits of focusing, not on a problem or its origin, but on a goal—a solution—and its attainment.

Solution Focused Brief Therapy bore the foundations of Solution Focused "anything" and its application in business. From the establishment of the Brief Therapy Centre, work unfolded to provide great value to individuals in psychotherapy disinterested in the "why" of

their distress, but in its resolution. A solution-focused approach to solving problems was developed by de Shazer and Berg and is well established across many areas (Smock, Trepper, Wetchler, McCollum, Ray, & Pierce, 2008). Looking to do things differently, de Shazer and Berg identified areas of concern and focused, not on the causes, but on the resolution of those concerns. A 2005 special, double issue of the Journal of Family Psychotherapy published writings on a variety of solution-focused experiments, reports, and research completed that highlight the values of this approach in psychotherapy; yet, its use in the business world can be seen. Its application spread during the end of the twentieth century and is used in education, prisons, parenting, and occupational therapy, in addition to its continued use in psychotherapy (Jackson & McKergow, 2007). Solution Focused Management (SFM) has been as successful in business as the tenets of other psychotherapy techniques, including psychoanalysis (Hunt & McCollom, 1994) and rational-emotive therapy (Fourali, 1999).

Applied generally, a solution-focused approach to solving problems identifies five steps that must be taken to cause change, highlighted in Table 2-12 (Visser & Bodien, 2005).

Table 2-12.
Steps Taken when Making Change Using a Solution-Focused Approach

Step	Action	Step 5 Complimenting: Acknowledge the work performed by the people making the change
1	<u>Acknowledging a problem exists:</u> Acknowledge the problem without paying attention to its cause(s).	
2	<u>Describing Success:</u> Determine the definition of success.	
3	<u>Identifying and analysing positive exceptions:</u> Identify instances when the problem didn't exist.	
4	<u>Taking small steps forward:</u> Assist the people with the problem focus on the solution	

With the exception of one step, the steps are taken sequentially. The fifth step, complimenting, occurs throughout the taking of all other steps to reinforce the actions and the results obtained. Steps one through four include acknowledging a problem exists, disregarding its cause(s); determining the problem's impact and defining success; identifying times when the problem did not exist; and identifying and taking small steps to change the current situation (O'Callaghan & Mariappanadar, 2008).

The steps taken when using a problem-focused approach and solution-focused approach can be highlighted by two significant differences taken by individuals attempting to solve a given problem. Each one focuses at alternate ends of the spectrum in terms of what is needed. The first needs to solve a problem by focusing on it; the second needs to find a solution to a problem, by focusing on it. More importantly, however, is the active and expressed appreciation by someone to the parties working through the required actions to achieve the desired outcome that greatly distinguishes the solution-focused approach from the problem-focused approach to solving problems. To this end, the world of the overweight looms large in its use of complimenting. With nearly 50,000 weekly meetings held across the world (Potketwitz, 2008) for individuals enrolled in the Weight Watchers program, one focus of those meetings is “lots of support, inspiration, and motivation” (Weight Watchers, 2009). Support, inspiration, and motivation are all forms of complimenting offered to those working to achieve change.

Use of a solution-focused approach to solving business problems has developed into the management field commonly referred to as Solutions Focused Management (SFM). Examples of its use are found in its successful application in marketing, sales, human resource management, and project management (Verlag, 2006). A review of the literature finds its framework in teaching, nursing and other medical fields. The U.S.-based Northwest Brief Therapy Training Centre defines SFM as a way to achieve positive change with people, teams, and organisations (Langer, 2006). As is true with all solution-focused approaches used to solve problems, solution focused management emphasizes strengths, resources, and abilities to establish a preferred state rather than a current problem-centric state. In all cases, the same, fundamental five-step method is followed, maintaining the foundation introduced in Solution Focused Brief Therapy. These steps include the repeated asking of specific questions and the recognition that small successes are successes. The Deming Cycle (Aggarwal & Adlakha, 2006) is a method to aid stabilising processes and pursuing continuous process improvement. This cycle is comprised of the repeated stages of Plan-Do-Check-Act. The contributions of Visser (2009) through applying Solution Focused Brief Therapy practices inside of business organisations, provides, literally, step-by-step actions to be taken by the organisation that wants to ensure change, and quality improvements are attained. Superimposed on the famous Plan-Do-Check-Act model, the five-step method of solution-focused management provides the simplest of frameworks to achieve solution-focused results (Visser & Bodien, 2005). First, acknowledge the problem by asking questions about its impact, how it hinders those experiencing it and why it is a problem to one group and not another. Secondly, describe success by asking questions about what would be better if the problem did not exist and what behaviour would need to change for the problem to be solved. Thirdly, identify and analyse positive exceptions by asking when the

problem did not exist and what has already occurred that lessened the negative impact of the problem, finding out how the individual affected by the success contributed to it. The fourth step is to take one small step forward, followed by another. Throughout these activities, the giving of compliments occurs. Having already identified something in step three that contributed to an improvement, taking an action will contribute to another improvement. This is done in step four. The models are presented together because, as shown in Figure 2-10, both identify practices to improve quality.

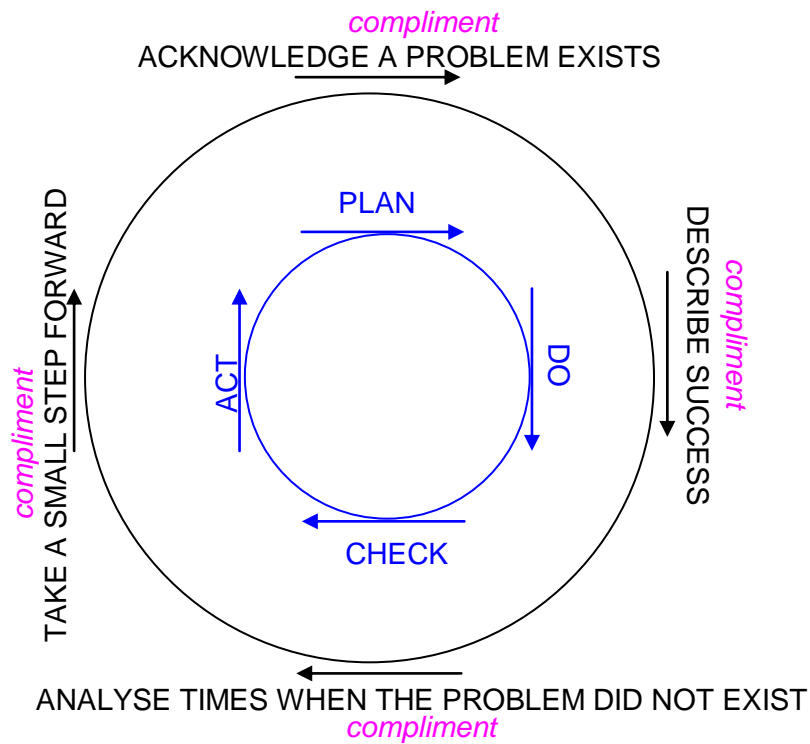


Figure 2-10. The Four-Step Solution Focused Management Model, Superimposed on Deming's Plan-Do-Check-Act Total Quality Management Model

The importance in each of these managerial frameworks, however, is not in the steps taken, but in the questions asked and answered as the steps are taken. Both frameworks ask questions, as identified and compared in Table 2-13.

Table 2-13.

The Parallels in Quality Management and Solution Focused Management are the Steps to Take, the Actions to Take, and the Questions to Ask

Step	Total Quality Management	Solution Focused Management
	Plan	Acknowledge the problem
1 and ask	What should be accomplished? What needs to be achieved? What needs to be identified?	Has the problem resulted in hurt, sad or angry feelings? Has the problem stopped performance? Has looking at the problem ever made it disappear? (<i>Compliment</i>)
	Do	Describe success
2 and ask	What should be different? How can it be done differently? Can it be done less expensively? Can it be done more quickly? Can the change or its results be measured?	If the problem was never there, what would look different? Would there a better feeling within the group? Is performance improved? Can success happen? (<i>Compliment</i>)
	Check	Analyse when the problem did not exist
3 and ask	Are the measures in place? Are the results as expected? Did the change cause an improvement?	How did the problem become visible? Is there a way to make it go away? What are the differences in the noise you experience because of the problem? Are people yelling now who were quiet before? Is the yelling annoying? (<i>Compliment</i>)
	Act	Take a step forward
4 and ask	What has been learned? Are more changes needed? Do the metrics tell me how to continue to make improvements?	Is there a single action that can be taken and the results measured to determine if it contributed to making the problem less impacting? Can that single action be done? Are there other steps that can be taken? (<i>Compliment</i>)

The experience of taking step four in Solution Focused Management moves its applicant to ask further questions, within the context of using a solution-focused approach. They are referred to as scaling questions. Simply, on a scale of one-to-ten, measure whatever needs measuring about the success of the result of the step taken. Coert Visser (2009), a European-based solution-focused management consultant, wrote that visualising the scale on which the answers to scaling questions can be assigned provides a level of measurement of the success the solution-focused approach has provided. He highlights the meanings of the scale integers to make simple the use of and value of scaling in an SFM context (see Figure 2-11).

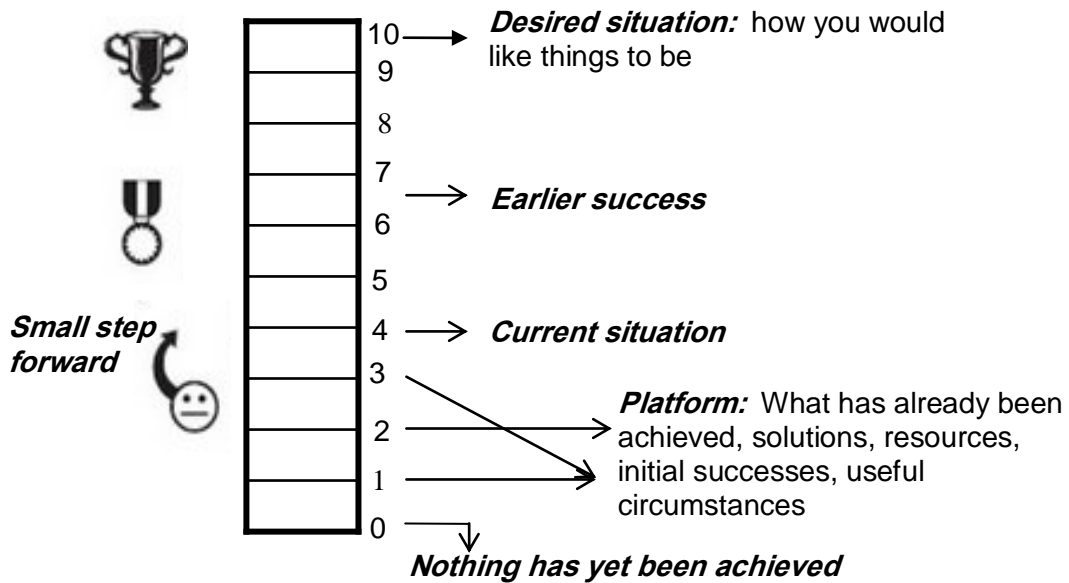


Figure 2-11. Scaling Allows Users of a Solution-Focused Approach to Measure, albeit subjectively, the Progress Made While Taking Small Steps to Achieve a Desired State (Visser, 2009, p. 2)

The foundations of Solution Focused Brief Therapy have provided a valuable tool to use in a corporate environment and improve the delivery of business functions by groups employed to do so.

It is important to note that, given an unplanned IT outage, one’s desired situation is not—necessarily—identical to the situation in which the IT environment ran prior to the unplanned outage. For an incident manager, the desired situation, indeed, is the return of service; however, that desired situation may be obtained by either returning to a previous state or changing the current state in whatever manner is required to restore service. An incident manager’s goal is always a viable and working production environment.

A relative newcomer to business, solution-focused problem solving disregards the source or cause of an issue but is used to change a current state to a preferred state by focusing on achieving the preferred state. Much of the application of solution-focused problem solving has been within the confines of the mental health industry and the fat-fighting industry. Its use in the practical day-to-day solving of problems in business is only recently being seen in areas of personal coaching and development, leadership training, and in business operations. Like problem-focused problem solving, there are a set of steps to be taken to achieve the goal of finding a solution; however, the starting point of those steps is significantly different.

2.5.2. Summary

Problems are pervasive in business and few organisations experience progress without encountering difficulties. With multiple avenues down which one may travel to obtain a solution to a problem, problem solving has become a corporate enterprise in its own right. Applying the review of applications of both problem-focused approach and solution-focused approach to problem solving, one must draw a conclusion that the former technique is often used and well developed, while the latter is only beginning to gain a foothold across corporations. It provides tools that are new, and effective, to problem solvers. The concept of complimenting problem solvers throughout the problem-focused problem solving process is foreign to problem-focused problem solvers because their focus is on the problem, rather than on the solution or the people impacted by the problem.

2.6. What IT Departments Measure and What They Report

One goal of IT departments is to provide the business information, not data, which allows senior managers to make knowledgeable decisions. Measuring makes use of available data to give information about how performance is occurring. The manner in which the information is presented is absorbed by decision makers—how that information is presented influences both the speed of the absorption of the information and the accuracy of the decision made having absorbed it. A 2004 study (De Vries, Mulig, & Lowery) provided data concerning ten U.S. cities to research participants (N = 120) and required decisions to be made about the information provided to them. The information was provided in three formats. Data was used to create tables, bar charts and schematic faces. The schematic faces were tantamount to emoticons or happy faces. The researchers found that the subjects were most quickly able to absorb information provided via the schematic faces presented; moreover, the best decisions were made based on the use of the schematic faces. This indicates that both the data content and its representative delivery are important to its being understood and used as information.

How information is reported complements the realisation that if data cannot be measured it cannot be monitored nor can it be improved (Duncan, 2008). From data, information is revealed. Examples of the importance of measuring and reporting are found across industries. Public libraries are outcome driven and need to be able to measure the impact of the services offered in order to justify the continuation of the service (Harding, 2008). Research done in the public library sector includes a study completed using stratified sampling (N = 57) to obtain responses to a questionnaire that indicated the readiness of one South African province to increase its work on literacy. Though not all hardships experienced during the apartheid era in South Africa have yet been overcome, library personnel indicated a strong readiness to increase work on literacy (Hart, 2006). The results from a case study performed identified that because a relationship between community

policing and a reduction in crime could not be easily measured, the police force studied was unenthusiastic for making organizational changes to support organizational change (Casey & Pike, 2007). Research in human resource management supports the systematic process of measurement that allows managers to obtain and evaluate evidence about the performance of staff initiatives. This work was completed through both a comprehensive literature review and the hosting of multiple focus groups in which participants (N = 27) acknowledged not only the need for measurement, but also the important gaps in what is measured (Bardoel, De Cieri, & Mayson, 2008). While there is a general acceptance of the importance of taking measurements to identify how a group, a program, or an initiative performs, not all parties being measured are, necessarily, glad that it occurs. A study, using unstructured interviews, with employees (N = 12) whose job was related to what would be measured by an IT management group, found dissension among software programmers who, in part, were concerned that the measurements would be used against them (Umjari & Seaman, 2008). Measuring provides data that gives information about how performance is occurring. Conclusions drawn from a narrow literature review indicate that some individuals perceive reporting as a potential threat by those being measured; others see that same reporting as a contribution to their annual performance review and pay increase (Burstin, 2008).

Within the context of service management, service support and incident management, the number of incidents that are reported, the types of incidents that are reported, and the duration of those incidents are considered fundamental data on which to report performance. The cost of delivering IT services represents between three percent and 15 percent of an organization's revenue. Some organisations assign their IT costs to four percent of their total revenue and 50 percent of their capital expenses. In all cases, IT capability must be managed, measured, and governed to be effective (Holden & Thompson, 2006). Two of the key measurements reviewed by both IT management teams and the senior business managers to whom IT services are delivered are availability and MTRS when unplanned outages occur. How these measurements are reported provide information to the business that pays for the IT services they receive.

2.6.1. Availability

The amount of time an IT service is usable is referred to as its availability; availability represents the percentage of time that the hardware and software in use offers the service that it was deployed to provide (Bauer & Franklin, 2006). IT departments ensure the timely and reliable access to and use of information when the data and the information system on which it resides are available (Government Accounting Office (GAO), 2009). Availability is measured so that the business that uses the computer hardware systems, software applications, and network components on which it depends can make decisions about the performance of those systems. Measuring availability allows the business to determine the

ability of the IT department to provide the tools needed to operate the business. Availability is the time that computer systems can be used by a business to enable it to satisfy its objectives and is expressed as the percentage of the agreed service hours for which the component or service is available (Cartlidge et al., 2007). Because there are a finite and measurable number of minutes in a year, the annual availability of a computer environment can be easily calculated. Simply expressed, availability is the total number of minutes in a year minus the minutes that the computer environment was not available, presented as a percentage. This equation is shown in Table 2-14. The only times when a computer system can be not available is when there is a planned or unplanned outage.

Table 2-14.
Calculating Availability

Availability	Variable Values
$A = \frac{(M-P-U)}{M}$	<p>A = Availability</p> <p>M = Minutes per Year</p> <p>U = Unplanned Outage Minutes per Year</p> <p>P = Planned Outage Minutes per Year</p>

Availability has become increasingly important and can now be reviewed as a three-phase evolution during which the attention of both the IT departments and the business changed from IT component availability to business process availability. In phase one, technical teams designed for individual hardware components to ensure they were able to stay available. In phase two, availability focused on the needs of the IT end-users and their perspective of availability, including software applications and data. The third phase, however, focuses on the needs of the business that pays for the IT environment and the processes it uses to run its business (Bailey, Frank-Schultz, Lindeque, & Temple, 2008). The Service Availability Forum (SAF) has championed the standardisation of availability and has been driven, primarily, by the telecommunications industry (Lumpp et al., 2008). A consortium of telecommunications and computer companies across the world, the SAF was established to encourage the use of commercial-off-the-shelf (COTS) technology solutions to create high availability IT environments. Though SAF has focused on two major technology areas to achieve high availability (hardware and the integration of software), it is comprised of a variety of computer application, hardware, and component organisations, including Nokia Siemens, Sun Microsystems, Oracle, Hewlett-Packard and Alcatel-Lucent, among others. SAF defines high availability at 99.999 percent (Industry Leaders, 2009). Knowing that use of the Internet by business is growing and there is a desire to move the costs associated with servicing customers from personal contact to having customers use on-line

self-service options, the high availability of a computer enterprise is critical. The typical requirement for a telecommunication network, for instance is 99.999 percent availability (Guida, Longo, & Postiglione, 2008). Referred to as the gold standard for availability, “five-nines” provides 99.999 percent availability. That gold standard allows a total of 5.26 minutes of outage time per year (Bauer & Franklin, 2006; Kimber et al., 2006). Those 5.26 minutes include both planned and unplanned outages.

This desired level of computer system and component availability (Ganesh, Illsley, Rodger & Thompson, 2008) is costly and difficult to achieve, yet many organisations appear as if they are making inroads to attain it. An availability attainment of 99.999 percent is a requirement for some businesses (Boam, Gilbert, Mathew, Rasovsky, & Sistla, 2003; Hochmuth, 2004; Prabhakar, Rastogi, & Thottan, 2005) and there has been an integration of computer-centric features for resiliency, redundancy, serviceability and manageability (Boam et al., 2003) to minimise the number of and duration of planned outages. More importantly, these contribute to meeting the actual needs of the business (Ganesh et al., 2008). There is no challenge that high availability is valuable to many businesses. There is also no challenge that achieving high availability is costly. It is also noted that some businesses need IT systems available only when the IT systems are actually used. Some applications do not need 99.999 percent availability (Mankowski, 2007; Radhakrishnan, Mark & Powell, 2008). Most organisations use a combination of models, management tools, and analysis to determine the level of availability needed by a particular application or computer system. Once it is classified as either mission- or business-critical, its availability is, generally, set at 99.9 percent or higher, allowing, at most, just fewer than 526 minutes (approximately nine hours) of planned and unplanned downtime per year (Radhakrishnan et al., 2008). High availability is not a new concept in the IT industry nor is the understanding that it cannot be attained due to system failures, human error or both. Understanding it from the perspective of the end user is not well researched; however, decisions are made by the businesses that pay for IT departments without all necessary information to make informed decisions (Zeng, 2007). Table 2-15 lists only the costs of annual lost revenue to some industry sectors, even when commitments and investments have been made in order to achieve some degree of high availability. The lost values are increased if the availability value listed is not obtained and greater amounts of annual downtime are experienced.

Table 2-15.
Availability, Annual Allowed Downtime and Annual Lost Revenue, by Industry, when Allowed Downtime is Achieved, in US dollars (Zeng, 2007, p. 24)

Lost Annual Revenue Shown in \$US Dollars by Industry						
Availability	Annual Downtime (hours-minutes)	Energy	Manufacturing	Banking	Insurance	Retail
99.000 %	87-36	\$247.0 M	\$141.0 M	\$131.0 M	\$105.0 M	\$97.0 M
99.500 %	43-48	\$123.0 M	\$70.0 M	\$65.0 M	\$53.0 M	\$48.0 M
99.900 %	08-46	\$ 20.0 M	\$14.0 M	\$13.0 M	\$11.0 M	\$9.8 M
99.950 %	04-23	\$ 13.0 M	\$7.0 M	\$6.9 M	\$5.5 M	\$5.1 M
99.990 %	00-53	\$ 2.5 M	\$1.1 M	\$1.3 M	\$1.1 M	\$1.0 M
99.999 % ^a	00-05	\$ 235.0 K	\$134.0 K	\$125.0 K	\$100.0 K	\$92.0 K

^a Also referred to as “five nine’s” or the “gold standard”

Though availability is measured, there are additional pieces of data that are reported that can provide a business, and its IT department, valuable information on the unplanned outages being experienced. These include the number of unplanned outages reported, by type, by time period, by group of users and by impact to the business; the percentage of incidents by root cause; the overall time to recover from incidents, etcetera. Few IT departments want to report systems’ availability that does not, at least, sound good to the business that pays for its services. In some cases, there will be too detailed information available to corporate managers about the performance by the IT department and, in other cases, too technical information (GAO, 2009).

One attraction of measuring availability is that a percentage is easy for senior managers to understand. One of the principles applied to optimise the likelihood that computer hardware systems and application software are highly available is to minimise change—in hardware, software, firmware, support personnel, etcetera—in any area that might influence the systems’ stability, and therefore, availability. However, change is a required activity in an IT environment. At some point in time, bug fixes must be deployed; firmware must be upgraded; new hardware subcomponents must be added or replaced. While the actual value of availability may be correctly calculated, it is often reported by IT departments as a value designed to indicate a higher availability delivered than actually attained. Table 2-16 provides an example of how availability can be calculated and how that availability can be reported to the business.

Table 2-16.

Calculating Availability and Calculating Reported Availability

A = Availability	
M = Minutes per Year	(525,600)
U = Unplanned Outage Minutes per Year	(5,244)
P = Planned Outage Minutes per Year	(47,200)
<hr/>	
Availability	Reported Availability
<hr/>	
$A = \frac{(M-P-U)}{M}$	$A = \frac{(M-U)}{M}$
(525,600)-(47,200)-(5,244) = 90.02%	(525,600)-(5,244) = 99.00%
525,600	525,600
A = 90.02%	A = 99.00%
<hr/>	

By ignoring the duration of planned outages as needing to be included in the availability percentage achieved by the IT department, the reported availability is nearly nine percent higher than the actual availability attained. It allows the IT department to report it has delivered systems that provided the company high availability. When reporting to an executive committee holding the purse strings for the coming year's IT budget, IT personnel are likely to report optimal data and await questions as how it was calculated.

In addition to the actual data values used when reporting availability, the report creators and the users of the reports benefit from knowing that availability is the product of the availability of the system components factors that comprise an IT environment (Zeng, 2007). When, for example, a database is not available, it may be not available because of the hardware on which it resides (the storage), the database software itself, or the server on which the database software executes. If each of the three components has different availability values, the best availability that can be provided is the product of the three values, never allowing for gold standard availability in total, even if each subcomponent has gold standard availability. As shown in Table 2-17, the best possible availability of the subsystem is always less than the best possible availability of any single component, being the product of the best availability of all subcomponents of the subsystem.

Table 2-17.

Overall IT Availability Cannot Meet the Optimal Availability of the Least Available Subcomponent in an IT Environment

Overall Desired Availability	=	99.99%
Server Availability	=	99.90%
Storage Likelihood Availability	=	99.99%
Database Likelihood Availability	=	99.00%
Best Achievable Availability	=	Availability (Server × Storage × Database)
Best Achievable Availability	=	(99.90 × 99.99 × 99.00) = 98.89%

2.6.2. Mean Time to Restore Service (MTRS)

The calculation and reporting of availability can be, and are, different in different organisations. So, too, can the measure of the duration of the MTRS from an unplanned outage. It is noted here that the use of MTRS, rather than MTTR, a recent addition to the nomenclature of IT Service Management (Cartlidge, et al., 2007), instances where it was reported as the Mean Time to Restore (MTTR) are presented here as MTRS to avoid confusion by the reader. The MTRS is the time taken to restore service to an acceptable operating level (Gupta & Shoshan, 2003). It is calculated as shown in Figure 2-12.

$$\text{MTRS} = \frac{\sum_{i=1}^n T_i}{n}$$

Figure 2-12. How to Calculate MTRS

Table 2-18 reveals how different values can be used to perform the calculation of the duration of an unplanned IT outage; an optimal duration of the unplanned downtime can be calculated, contributing to an optimal MTRS.

Table 2-18.

Alternate Ways to Calculate the Duration of an Unplanned Outage

A	=	Incident Docket Raised	00:00
B	=	Technical Support Notified an Incident has been Raised	00:20
C	=	Service Restored: Technical Support Completes Work	03:15
D	=	Service Restored: Business Verifies Service is Restored	09:30
E	=	Duration of an Unplanned IT Outage	

Option One and Example One

Option Two and Example Two

$$E = C - B$$

$$E = D - A$$

$$E = 03:15 - 00:20 = 2.9 \text{ Hours}$$

$$E = 09:30 - 00:00 = 9.5 \text{ Hours}$$

Therefore, the (Unplanned Outage Start Time) may equal Value A or Value B and that the (Unplanned Outage End Time) may equal Value C or Value D. Use of Values C and B would assure the reported duration of the unplanned IT outages used to calculate the MTRS is less than that calculated if the Values A and D were used to calculate the duration of the unplanned IT outages and the resulting MTRS values. Imagine a hardware server suddenly became unavailable. If the (Unplanned Outage Start Time) is equal to the time the hardware vendor arrived on-site or advised the impacted party that an error had been reported, the (Unplanned Outage Start Time) may equal fifteen minutes; however, if the (Unplanned Outage Start Time) is the time an error ticket was logged by an impacted user, that time could be as little as three minutes, given an impacted user may immediately ring a Help Desk to advise there is some type of error with the system that user needs to perform work.

Accepting that the MTRS can be manipulated when reported in order to present optimal service performance by the IT department—as a result of the duration of the unplanned IT outage being able to be manipulated—to the organisation’s management team that pays for IT services, the importance of tracking the MTRS of unplanned outages provides valuable information to the IT department that captures and manages the data. Figure 2-13, based on work performed by Smith and Hinchcliffe (2006) in an analysis on improving availability, identifies actions an organisation can perform to reduce MTRS. These are cited as key contributors to increased availability.

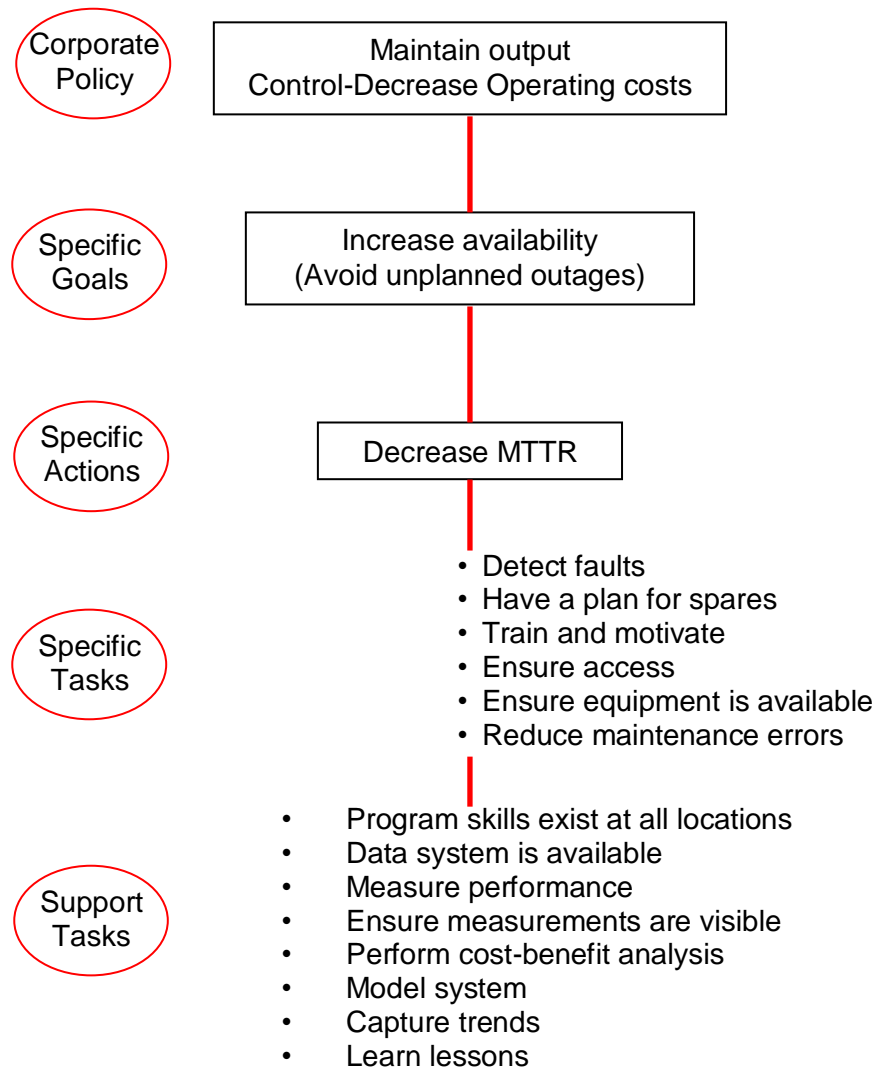


Figure 2-13. Keys to Decreasing the Mean Time to Restore Service (Smith & Hinchcliffe, 2006, p. 41)

Profit centres are considered of great value to businesses and cost centres are those that require great attention when costs need to be contained or decreased. When considering, and operating, data centres and IT departments as profit centres, they can deliver results to the company that confirm they are profit centres. In addition to lowering costs, MTRS will decrease and availability will increase. When accomplished, they are direct contributors to company revenue and profit (Smith & Hinchcliffe, 2006).

Although analysis of MTRS has been done in the past, and has been valuable, hardware downtime may no longer dominate system downtime, especially in software application intensive businesses. The analysis of trouble tickets by Bauer and Franklin (2006) offers a holistic view of outage duration information, including data ordinarily excluded when using specific quality management and quality improvement tools to undertake such analysis. Their canonical outage model includes restoration data from unplanned outages that were recovered manually, as well as unplanned outages recovered automatically, using immature

and mature restoration activities of both the manual and automated types. This canonical model allows the analyst to include outage duration data in a way that reflects actual customer usage of the system that experienced the unplanned outage(s).

Indeed, it is customer usage and, more importantly, customer perception, which makes MTRS from an unplanned outage an important IT service support metric (Xie, Sun, Cao, & Trivedi, 2003). The use of the Markov regenerative process models was among the first to analyse the server-user interaction and its effects on user-perception of MTRS that allowed future research to assess whether failure to use a server successfully was more likely the result of behaviour by the user or behaviour of the server, itself (Song, Tobagus, Raymakers, & Fox, 2004). While their research results support the human behaviour contribution to perception established by Xie, Sun, Cao and Trivedi (2003), these results are considered preliminary, having used a simulation study where the control of the servers used were within the control of the researchers and manipulated by them to trigger human responses. Figure 2-14 is modelled from their research and demonstrates the simulation format of their work.

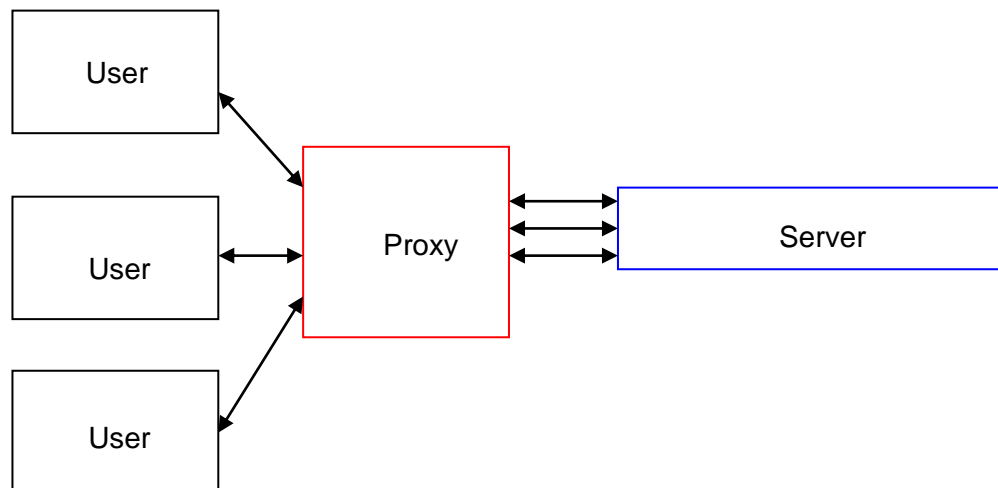


Figure 2-14. Model Used to Test User Perception to MTRS (Song et al., 2004)

The model presented (and the findings delivered) indicate that MTRS is both an actual measurement to be used by IT departments and a value that causes a perception by system users that can be manipulated in order to minimise any negative perception, while actually taking technical action to restore service to its normal performance. The research of Song, Tobagus, Raymakers and Fox (2004) have broadened the perspective of having a measurement. They note that there exists an end user response to that measurement and that the measurement and the response thereto are both important. Song, Tobagus, Raymakers and Fox (2004) have begun to determine how one measures MTRS, given that the perception of the user on its actual, mathematical value may influence its importance and (potential lack of) any concern associated with the unplanned outage that resulted in its effect as well as its duration.

Chapter 3 : Pilot Study

A pilot study was performed to undertake research into the characteristics displayed by incident managers and the approaches they use to solve problems while working to restore service when unplanned outages occur. This pilot study was performed in order to determine the practicability of a main study on these topics and to optimise the design of the main study in a manner that would provide enough information to obtain statistically valid information from incident managers in IT environments. The pilot study was undertaken in two sections. First, it was necessary to gather preliminary information about incident managers, from incident managers and technical and managerial professionals with whom they work. Second, it was necessary to design, develop, and validate two questionnaires to measure characteristics displayed and approaches used by incident managers to solve problems when unplanned outages occur. The first section would reveal information about the characteristics displayed by incident managers while working to restore service when unplanned outages occur. The second section would reveal information about the approaches incident managers use to solve problems while working to restore service when unplanned outages occur.

The goals of the pilot study were twofold. First, it was necessary to understand the role of the incident manager from the perspective of individuals in the role as well as those with whom they work closely. A focus group was used to gather this information. Secondly, two questionnaires were developed to confirm that the characteristics identified by incident managers as key to their ability to perform their role successfully, and the approaches they use to solve problems to perform their role. Presented here is work done and conclusions drawn from the results of the pilot study, allowing the undertaking of the main study.

3.1. Focus Group

Qualitative methods, including focus groups, enable one to get a deep understanding of human behaviour and the reasons why individuals perform in different ways. They focus on the actual experiences of the research participants and their critical voices. The pilot study included two distinct methods of data collection. The first was hosting a focus group. In this study, the focus group was used to identify characteristics displayed by incident managers while working to restore service when unplanned outages occur. Additionally, the focus group was used to identify the approaches incident managers use to solve problems while working to restore service when unplanned outages occur.

3.1.1. Method

Because unplanned outages occur, professional incident managers are needed to provide IT service support to corporations to restore the services lost when unplanned

outages occur. In order to obtain a first-hand perspective on the work of incident managers, from incident managers and from individuals with whom they work closely, a focus group was hosted to identify key themes important to this role. Much has been written about focus groups, their purpose, effective ways of hosting them, and the value of the data they provide (Creswell, 2009; Kitzinger, 1994; Webb & Kevern, 2001). Krueger and Casey (2000) state that focus group discussions tap into human tendencies. Attitudes and perceptions about a topic are developed, in part, with other people. The literature review performed during this research identified a variety of sources citing the importance of avoiding unplanned outages; however, throughout the research, there were minimal sources found that addressed the reality that unplanned outages occur and what actions should be taken to restore service. Hosting a focus group of incident managers, technical support specialists, and corporate managers—each with a particular interest in unplanned outages, and, not always the same interest—allowed the researcher to explore both the characteristics displayed by effective incident managers and the approaches used by incident managers to solve problems while working to restore service when unplanned outages occur.

3.1.2. Participants

It is necessary to have the correct types of participants engage in a focus group. Sampling and data collection processes are critical to the quality of a study and the ability to generalise its findings. These processes should operate within the parameters of the research goal, be guided by emerging theoretical considerations, and cover a range of relevant participant perspectives (Gibbs, Kealy, Willis, Green, Welch & Daly, 2007). In this research, the perspectives sought were from the focus group participants who were directly impacted by an unplanned outage. These individuals were not users of the failed system, but are the individuals required to restore the service that was lost when the unplanned outage occurred. The perspectives of individuals sought to participate in the focus group included non-technical individuals who were given technical information by technically knowledgeable colleagues. These individuals were identified as corporate managers. The perspective of the technically astute and responsible for the technical restoration of service was also sought. These individuals were identified as technical support specialists. Finally, the perspective of individuals, whose responsibility includes the actual restoration of service, with experience of providing IT support 24-by-7-by-365, was sought. These individuals were identified as incident managers. This entire group would allow an exploration of the impact of working to keep IT systems available to users at all hours of the day. Each of these aspects was considered when selecting candidates to participate in the focus group. Selected by stratified convenience sampling, the focus group participants were chosen with the acknowledgement that the larger population which the sample represented had its one *a priori* being IT employees who work to restore service when unplanned outages occur. That

larger sample group includes all incident managers; however, the focus group participants were drawn from incident managers and their colleagues from one division of one multinational organisation, referred to by a pseudonym, PyruX. The participants held job roles as corporate managers (N = 2), technical support specialists (N = 4), or incident managers (N = 4) and were all employed within the IT department of the organisation. The focus group's composition is cited in Table 3-1.

Table 3-1.
Composition of Focus Group

Professional Role	N	Representing
Corporate Manager	2	Individuals who are responsible for the corporate financial losses (both visible and invisible) resulting because the unplanned outage occurred. These individuals are also responsible for the communication of the estimate of the loss(es) to all interested executive managers and the duration of time expected to be required for the unplanned outage to be restored.
Incident Manager	4	Individuals responsible for the restoration of services degraded or lost when unplanned outages occur.
Technical Support Specialist	4	Individuals with technical knowledge of the system that failed which is both comprehensive enough to identify the fault and broad enough to determine a manner in which the lost service can be restored.

This combination and number of participants ensured that the sample would accurately reflect the population at large. As a result of the researcher belonging to a professional organisation in which some of the focus group participants also belonged, the researcher considered the potential of introducing bias into the focus group or into the analysis of its output. Statistically, bias is the tendency for a given experiential design or implementation to skew the results, unintentionally (Wienclaw, 2008). A professional moderator was engaged by the researcher to minimise the likelihood of introducing bias or any other compromises that are inherent in most qualitative focus group research, including sample, location, or approach (Harris, 2008).

Finally, participants in the focus group only worked on unplanned outages that are referred to in the IT industry as Severity 1 and Severity 2 incidents. These are incidents considered so significant to the business affected by them that immediate, or as close to immediate as possible restoration time is required. The perspective of the focus group participants on the role of incident managers is framed by their experience in only working on unplanned outages that cause the business devastating, critical or otherwise significant

impact to the day-to-day operations of the organisation and its ability to sell products or services to its customers. That the participants in the focus group were available to participate in the discussion, without being preoccupied by short message services (SMS) or mobile phone calls is directly related to the fact that at the time the focus group interview was held, there were no new or in-need-of-immediate-attention Severity 1 or Severity 2 unplanned outages requiring attention. Had such an unplanned outage occurred during the time the focus group met, the restoration of service lost caused by that unplanned outage would have taken precedence over participation by the incident managers, as well as other participants, in the focus group discussion.

3.1.3. Procedure

The University's Research Ethics Committee approved the researcher's hosting of a focus group and informed consent was obtained from the corporation that employed the focus group participants and from the participants themselves. The focus group hosted in the pilot study was of the type known as an exploratory approach focus group, designed NOT for the participants, but for the researcher, to stimulate thinking and for the formation of future research to be undertaken, based on outcomes from the focus group (Calder, 1977). The information obtained is pre-scientific—as it is not designed to obtain quantitative data upon which statistical analysis can be performed—but to use everyday speech and knowledge and apply them in a manner to allow further work to be done by the researcher.

After obtaining approval from the University to proceed, it was necessary to identify a corporation that was large enough that the number of incident managers it employed was likely to provide the *a priori* sought by the researcher. The company selected was PyruX. PyruX is a pseudonym for an international data management business with its world headquarters in Australia. PyruX Corporation has its main office in Melbourne, Victoria and employs more than 20,000 people. It has sales and support offices across Australia, New Zealand, Asia, England and the United States. PyruX has an IT organisation that is among the largest in the southern hemisphere. It had annual revenues of more than ten billion Australian dollars in 2008 (its fiscal year ends in June) and has been in business for more than a century. Its combination of mainframe computers, midrange servers, and more than 25,000 desktops, coupled with its excess of 1,200 software applications (including Commercial Off The Shelf (COTS)) applications, vendor-built custom applications and some developed internally) led the researcher to conclude that its IT Service Management organisation would have an incident management team that would be large enough to have candidates with a broad spectrum of incident management experience and significant enough unplanned outages that members of its organisation would agree to participate in the focus group. The researcher met with three of the senior corporate executives at PyruX, who, in turn, met with the corporation's legal representatives to obtain approval to extend

invitations to a subset of its employees to participate in the focus group. Those individuals who did participate provided their written consent to be included. Complete anonymity was assured to both the corporation whose employees participated in the focus group and to each individual participant.

Prior to hosting the focus group, the researcher outlined a set of questions to ask the focus group members. An initial set of questions was developed that asked about individual experiences of, by, and with incident managers, specifically regarding the actions of incident managers when an unplanned outage occurs. Questions were selected within the ITIL incident management framework, allowing a broad incident management discussion to occur. Allowing a broad discussion provided the moderator and researcher with the ability to contain the discussion solely to incident management and not allow it to broaden to other functions in the service support environment. The questions were pilot tested in the form of a verbal discussion held prior to the date on which the focus group was hosted with academics at the University, the researcher, and the professional moderator. Some questions were modified to extract specific citations about personal and professional experiences from the participants concerning their work with, or as, incident managers.

The focus group was held as a two-hour discussion with participation of all members, with one fifteen-minute break. The event was held in a private conference room at the Pyrux headquarters; all participants worked in or near that building, so face-to-face participation (rather than by telephone or via video conferencing) was assured. The event was professionally recorded and transcribed. The questions asked of the focus group were specifically designed to ensure active participation and broad input about the characteristics displayed by incident managers, as well as the approaches incident managers use to solve problems and restore service when unplanned outages occur. A sample of the questions raised by the researcher to the focus group participants about behavioural characteristics displayed by incident managers is presented in Table 3-2.

Table 3-2.
*Sample Questions Concerning Behavioural Characteristics Raised
with Focus Group Participants*

Sample Question 1:

*Okay . . . what other abilities, do incident managers need?
Attitudes or traits. You said decisive. Are there others?*

Sample Question 2:

*Incident Manager 2 used a term, competent. Can anyone
say, what are the competencies you expect from an effective
incident manager?*

Sample Question 3:

*So can we just think of just personality? What sort of a
personality strikes you when you see someone whom you
would say is a best leader and their personality
characteristics.*

Sample Question 4:

*We talked from incident manager's perspective what are the
administrative roles they perform in their task, in their role.
Now, you from a client perspective, what do you think is, what
do you think in terms of an administrative role?*

Sample Question 5:

*What do you think? How do you build that trust in this sort of
a confronting situation? Is it that people are so aware that this
is only a situation which makes you behave like that and so
the next minute once a situation or incident is done you are
back to normal and you behave as normal and concerned
about others? Is that how it happens?*

In addition to raising questions with the focus group concerning the characteristics that incident managers display while working to restore service, questions were also raised about the approaches incident managers use to solve problems. A sample of the questions raised by the researcher to the focus group participants about approaches-to-solving-problems is presented in Table 3-3.

Table 3-3.
*Sample Questions Concerning Approaches-to-Solving-Problems
Raised with Focus Group Participants*

Sample Question 1:

*. . . what do you think would be the most important thing to
restore services . . . ?*

Sample Question 2:

So, what is the duty of care involved in restoring service?

Sample Question 3:

*You are saying you must understand the nature of the
problem before you can start to solve it, is that right?*

3.1.4. Results

The focus group data was investigated to determine the information the focus group provided. The data was analysed to identify it as relative to the characteristics incident managers display while working to restore service when unplanned outages occur. It was also interrogated to determine its revelation, if any, to the approaches incident managers use to solve problems while working to restore service when unplanned outages occur. The data was investigated in three ways. A thematic analysis of the data identified themes that were revealed as important to the actual description of incident management. A content analysis of the data was also performed. Both the thematic analysis and content analysis were performed using Nvivo™, version 7, qualitative coding software that supports data display and data analysis. The analyses and results of each analysis are discussed in the following sections.

3.1.4.1. Thematic Analysis – Characteristics

Thematic analysis revealed that effective incident managers are decisive and firm; they have the confidence and the courage to make decisions quickly; they benefit from investing time with others with whom they frequently work. The following extracts from focus group participants highlight the themes identified when analysis was completed. For ease of reference, incident managers who participated in the focus group are identified as IM_n (where n is an identification number of the participant), Technical Support Specialists who participated in the focus group are identified as TSS_n, Corporate Managers who participated in the focus group are identified as CM_n.

Thematic analysis revealed that effective incident managers require information about who to engage for assistance, as well as to whom the event of the unplanned outage, and its impact, must be communicated. Effective communication is their greatest asset.

[CM₁]: Well, sure, because what it says is the incident manager has to be able to talk to the propeller heads with enough technical knowledge to convince them that you're not a blooming idiot and then you have to go back to business and talk to them about either dollars lost or time to restore. So, I've got to be able to take what the technical problem is and see what the impact is on the business and then communicate to each group and that's a very different framework.

Incident managers need to have both a strong technical understanding, and an understanding of the needs of non-technical people, so they are able to translate a technical issue into an assessment of user impact, and accurately estimate the duration of an unplanned outage. The focus group cited the importance for effective incident managers to build relationships, maintain focus, be organised, coordinate different teams, delegate, demonstrate leadership, listen, use intuition, have a sense of urgency, and have a customer focus. Three themes that were identified are Communication, Leadership and Relationship Management. They need to spend time building relationships and finding out "who's who in the zoo", so when a crisis occurs they know exactly with whom to speak. In terms of abilities, communication skills are key. Incident managers need to have both a good technical understanding, and an understanding of the needs of non-technical stakeholders, so they are able to translate a technical issue into an evaluation of the user impact, and an approximation of "how long" an outage will last. This was discussed as an unusual characteristic of an IT person as they are not known for their people skills.

[TSS₂]: . . . I normally find you need to take a leadership role and lead them through it. They have the answers but they're not going to step forward as an individual representing their [company] . . . and take on a PyruX-related incident because they don't have the authority or they've been instructed not to. . . . So you need to lead them through. They have the answers but you just need to bring the pieces together and you need to be decisive. You need to make a decision and not all decisions are going to be right but making decisions is better than sitting there just staring at the roof . . .

[IM₃]: What I discovered is it took me a long time to get an answer from an Australian. Because I would ask a binary question and they would read me War and Peace. Or they would answer a question that was a really interesting answer, but it wasn't to the question I had asked . . . it took me six months to finally figure out why I was so ineffective at getting done what I was being paid to do and once I cottoned onto the fact that, by definition, Australians won't answer the question you asked, I started to give them the choices of yes and no because it helped a lot. And now it just speeds stuff up.

[CM₂] And the role that I'm in now, you would put the most responsibility on to develop that relationship.

The focus group participants revealed that communication and leadership were two significant characteristics that must be displayed by incident managers during unplanned outages. Moreover, the high-pressure nature of the role—being purely reactive to an unplanned event that causes negative impact to the company—was perceived as simply part of the job and not a noteworthy characteristic of the role.

The importance of the role of incident managers was expressed by those with whom they work more frequently than by incident managers, themselves. The corporate managers and the technical support specialists with whom the incident managers work through unplanned outages to restore service both viewed incident managers as vital to the restoration of service, more for their ability to facilitate the work that needed to be done by others and keeping working groups engaged through long outages than by any other manner.

3.1.4.2. Thematic Analysis – Approaches to Solving Problems

Thematic analysis revealed that incident managers sought either the root cause of the unplanned outage in order to eliminate it permanently or investigated alternative ways to restore service. Citations extracted directly from the focus group transcript are provided, each indicative of the thinking used by focus group members when discussing how they perceive the goal they need to achieve and the approaches they use to do so.

[IM₃]: It's good about how you ask questions. Because, for example, I know, technically, I know very little about ACD switch technology. But I know a lot about mainframe technology. So if somebody talks to me about mainframes, lpars, swapping memory, db2 upgrades, table locks, I'm with them 100%. You tell me about the call routing and the switches over in the network and how the billing gets done, I'm just not that strong, but I ask the same question. Pretend I'm your great grandmother. And just, like, really, really picture her. Now, tell me what the problem is.

[IM₁]: . . . if that outcome's not put on the table to say we're all in this teleconference or all in this meeting to come up with a solution of getting the service back on line, then we'll all work our separate agendas and we'll all be putting in bits of irrelevant info or bits of useless . . .

TSS₃. . . keep track of the various threads or trains of thought that are going on, because as you begin working on an incident there could be possibly several different root causes.

[TSS₂]: I must convince my team that we're making progress. And twenty hours in and if you still have no idea what the root

cause is, it's just human nature, they just start to lose enthusiasm, lose interest, and just say, "I give up." Everything we achieve is a win. If that is getting hold of a log file and sending it over the US that's good. We've got acknowledgement that they've received it and they're looking at it. You must keep them "we are still" no matter how bad the situation, no longer how long we've been at it, we're making progress. You've gotta make the team realise we are moving forward, we're not moving back.

The thematic analysis did not indicate that a combination of the two approaches was ever used or that neither approach was ever used. Additionally, whether incident managers opted to identify a root cause or opted to eliminate the unplanned outage without concern of its root cause, specific steps were followed to attain their respective goals. As well, specific types of questions were asked of parties engaged to restore service.

3.1.4.3. Summary from Thematic Analysis

Thematic analysis revealed that effective incident managers displayed three specific types of characteristics. These were being communicative, having strong relationship management abilities, and having effective leadership abilities. These characteristics were revealed through their repeated citation by most members of the focus group as to their importance and their use in the success achieved by incident managers. Additionally, whether incident managers opted to identify a root cause or opted to eliminate the unplanned outage without concern of its root cause, specific steps were followed.

Furthermore, thematic analysis revealed that part of the role of an incident manager includes solving problems and helping others solve problems. It is through effective problem solving that service restoration is attained. Only two approaches to solving problems were revealed in the thematic analysis. These include the use of a problem-focused approach to solving problems, in which permanently eliminating the root cause of the failure that caused the unplanned outage would restore service. Alternately, there was the use of a solution-focused approach to solving problems, in which any avenue through which progress could be made was acknowledged and that the restoration of service was the only requirement of the incident manager who used this approach to solve problems and restore service. The analysis did not indicate that a combination of the two approaches was ever used or that neither approach was ever used.

3.1.4.4. Content Analysis – Characteristics

Content analysis—the summarizing, quantitative analysis of messages that relies on the scientific method and is not limited as to the types of variables that may be measured or the context in which the messages are created or presented (Neuendorf, 2002)—verified the themes revealed in the thematic analysis. It also revealed additional characteristics of

effective incident managers—Administration, Decision Making, and Entrepreneurship. The occurrences of characteristics, by use of a noun or adjective (or a diminutive) used by participants in the focus group are cited in Table 3-4.

Table 3-4.
Content Analysis Results from Focus Group Transcript – Behavioural Characteristics

Characteristic	Citations	Percentage of Use in Relation to all Characteristics
Communicative	44	27.33
Leadership	34	21.12
Decisive	30	18.63
Administrative	22	13.66
Entrepreneurial	8	04.97
Relationship Management	8	04.97
Authoritative	4	02.48
Credible	3	01.86
Motivating	3	01.86
Facilitative	2	01.24
Offensive	2	01.24
Pleasant	1	00.62

It was revealed through the content analysis that administration, decision-making, and being entrepreneurial were important characteristics displayed by successful incident managers. The results were confirmed by counting the frequency of use of each of these words (and their derivatives and diminutives).

The focus group successfully laid a foundation to investigate questions that could be answered by many incident managers to understand the characteristics displayed that would result in success. By using the textual data from the focus group transcript and identifying the characteristics that were revealed in the thematic and content analysis, it was found that there was a varying degree of frequency in which six characteristics (as well as their diminutives and derivatives) were cited. The count revealed the frequency of the specific characteristics cited by the focus group participants as important to the success of incident managers. All were revealed by the focus group as important characteristics displayed by successful incident managers.

3.1.4.5. Content Analysis – Approach to Solving Problems

Identifying only two approaches-to-solving problems in the thematic analysis, a content analysis was performed to determine if other approaches could be identified. Content analysis was performed on the approaches content of the focus group transcript; however, this analysis confirmed the problem-focused approach to solving problems and the solution-focused approach to solving problem that were revealed in the thematic analysis. The focus

group identified a problem-focused approach as the more common used to restore service (91 percent versus eight percent).

Table 3-5.
*Content Analysis Results from Focus Group Transcript –
Approaches to Solving Problems*

Approach to Solving Problems	Citations
Problem Focused	31
Solution Focused	3

3.1.4.6. Summary from Content Analysis

Content analysis revealed that effective incident managers displayed three specific types of characteristics. These were being administrative, being decisive, and being entrepreneurial. None of these had been revealed in prior analysis of the focus group transcripts. Additionally, the approaches to problem solving that are used by incident managers confirmed the findings in the thematic analysis, insofar as only two types of problem-solving approaches are used. These are the use of a problem-focused approach or a solution-focused approach.

3.1.5. Summary from Focus Group

Krueger and Casey (2000) state that focus group discussions tap into human tendencies. Attitudes and perceptions about a topic are developed, in part, with other people. The literature review performed during this research identified a variety of sources citing the importance of avoiding unplanned outages; however, throughout the research, minimal research was found that addressed the reality that unplanned outages occur and the actions that should be taken when the service disrupted during those unplanned outages must be restored. Hosting a focus group of incident managers, technical support specialists, and corporate managers—each with a particular interest in unplanned outage and, not always the same interest—produced a discussion among an optimum group of individuals to explore both the characteristics displayed by effective incident managers and the approaches to solve problems used by incident managers to restore service when unplanned outages occur.

Finally, both the thematic and content analyses confirmed only two types of approaches to solving problems are used by incident managers. One approach is that of being problem-focused and working with others to identify the fundamental reason an unplanned outage occurred and to eliminate that reason, permanently. These individuals focus on permanently removing the problem. The second approach used is that of being solution-focused and working with others to restore service.

3.2. Questionnaires

Upon completion of the analyses of the transcript from the focus group, two questionnaires were developed to progress this research. These were a behavioural characteristics questionnaire and a questionnaire on incident managers' approach-to-solving-problems. The behavioural characteristic questionnaire had six dimensions and the approach-to-solving-problems questionnaire had two dimensions. Ten items were drafted for each of the characteristics and approaches from the themes of the pilot study focus group and from specific references found in the literature, including, but not limited to works of Cater-Steel, Toleman, and Tan (2006) for ITIL-related questions, Cauffman and Berg (2002) for approaches-to-problem-solving questions, and Fox and Patterson (2003) for high availability of services questions. The intention was to give the questionnaire to incident managers, analyse the responses provided and assess the validity and reliability of the questionnaires. If validated and confirmed reliable, it was expected they would be used in the main study.

3.2.1. Method

The behavioural characteristics questionnaire was designed to include items to obtain information about the six characteristics identified by the focus group as being displayed by incident managers when working to restore service when an unplanned outage occurred. These behavioural characteristics include being communicative, relationship management, being administrative, being decisive, having leadership and being entrepreneurial. The behavioural characteristics questionnaire contained a total of 60 items. The approach-to-solving-problems questionnaire included items to obtain information about the approaches used by incident managers to solve problems while working to restore service when unplanned outages occur. The approach-to-solving-problems questionnaire contained a total of 20 items. In each of the two questionnaires, a 5-point Likert scale was used to measure answers which were presented using the following range: 1 = never, 2 = rarely, 3 = sometimes, 4 = often, and 5 = always. The Likert scale was designed in 1932 to improve levels of measurement in social research. In 2006, a group of market researchers reviewed the five-point and six-point Likert scale and most modern researchers agree that the neutral rating in a five-point Likert scale is needed when conducting survey research in order to capture unbiased sentiments of survey respondents (Gwinner, 2006). For this reason, the five-point Likert scale was selected as the scale for measurement in this research.

3.2.1.1. Content Validity

Prior to distributing the questionnaires to a group of incident managers in order to collect research data, seven incident managers, selected by convenience sampling, evaluated the two questionnaires. This group was referred to as the Review Team (N = 7). No members

of the Review Team had participated in the focus group. To perform content validity on the questionnaires prior to their distribution, each member of the Review Team assessed each of the 60 items in the behavioural characteristics questionnaire and each of the 20 items in the approach-to-solving-problems questionnaire using the widely-used method of measuring content validity developed by Lawshe (1975). Lawshe's conclusion is that content validity is affirmed if the summary output provided by the respondents when $N = 7$ is 0.99 or greater, using the results as the Content Validity Ratio (CVR). For each item, in each questionnaire, the Review Team members, Subject Matter Experts in incident management, were asked to identify the items in each questionnaire as 1 = Essential, 2 = Useful, but Not Essential or 3 = Not Necessary. When the CVR of the behavioural characteristics questionnaire was calculated, a value of 0.75 was returned; additionally, the CVR of the approach-to-solving-problems questionnaire was calculated, a value of 0.73 was returned. Although neither CVR indicated a reliable questionnaire had been developed, the data did reveal that 84 percent of the responses to the behavioural characteristics questionnaire returned a CVR of 1.00 and 50 percent of the responses to the approach-to-solving-problems returned a CVR of 1.00. Eliminating the items the Review Team identified as either 2 = Useful, but Not Essential or 3 = Not Necessary resulted in two questionnaires that each had content validity of 1.00. The updated questionnaires were again sent to the Review Team for assessment. A test for content validity was performed using data from the Review Team. Both the behavioural characteristics questionnaire and the response-to-solving-questionnaire returned a CVR of 0.100, indicating both pilot study questionnaires demonstrated content validity.

3.2.1.2. Reliability

The assessment for reliability of the behavioural characteristics questionnaire and the approach-to-solving-problems questionnaire was not undertaken until the validity of each was established. The questionnaires were distributed to the Review Team ($N = 7$) and the results were calculated to identify a value for Cronbach's alpha to identify reliability. The Cronbach's alpha value for the behavioural characteristics questionnaire from results provided by the Review Team was 0.892; the Cronbach's alpha from the approach-to-solving-problems questionnaire from results provided by the Review Team was 0.794. The fundamental information had been obtained to warrant distributing the questionnaires and assessing the Cronbach's alpha values obtained from the final responses of participants to each of the questionnaires.

3.2.2. Participants Replying to the Pilot Study Questionnaires

PyruX employed all individuals who volunteered to provide responses to the behavioural characteristics questionnaire and the approach-to-solving-problems questionnaire, in one of four of its Australian divisions (A, B, C, and D, for ease of reference). Individuals from

Divisions A, B, and C were hand delivered both questionnaires at the same time by the researcher; the total distributed was 43, 48, and 45 respectively. Both questionnaires were delivered to a single individual in Division D who served as the PyruX liaison between the Division D incident managers and the researcher. The liaison distributed the questionnaires on the researcher's behalf. This was due to the requirements of the Division D senior manager for whom all Division D incident managers worked. That senior manager would allow the incident managers in Division D to participate only if PyruX retained control of who received the questionnaires. The researcher was advised that all managers working in Division D would be given the questionnaires, and, in fact, 47 questionnaires were distributed. It cannot be confirmed that due to illness or holiday all eligible incident managers actually received the questionnaires; however, the Division D liaison did confirm that 47 individuals received the questionnaires.

The total number of incident managers who completed the pilot study questionnaires were given is 118. The participation rate was 64 percent. Table 3-6 identifies the number of incident managers who were invited to participate and the number of questionnaires completed and returned.

Table 3-6.

Distribution and Collection of Pilot Study Questionnaires and Responses

Participants	Number of Distributed Questionnaires	Returned Questionnaires with all Items Completed
Division A	43	24
Division B	48	32
Division C	45	30
Division D	47	32

3.2.3. Procedure

Having had success engaging PyruX management and its legal team to obtain authorisation for some PyruX employees to participate in the focus group, the researcher again approached PyruX to allow its incident managers to reply to the pilot study questionnaires. As noted in Section 3.2.2, the questionnaires were submitted to incident managers working at four divisions of PyruX. All participants were located at Australian offices. All participants provide incident management services for the same corporation, but were employed across different divisions. The incident management groups do not work together on the same incidents on any unplanned outages.

Both PyruX and its incident managers who participated by responding to the questionnaires were guaranteed anonymity. This anonymity included both the fact that they had responded to the questionnaires and the answers they provided to the items in the questionnaires. The corporation provided written approval to notify direct line managers of

the prospective participants of the corporation's approval of the study and of the participation of their employees. All participants answered the questionnaires voluntarily and there was no negative impact as to how they were perceived by their management team if they chose to participate or chose not to do so.

The questionnaires were distributed on paper and each page was single-sided. They were distributed to four groups of incident managers. The questionnaires were distributed to and collected from participants, in person, by the researcher at Divisions A, B, and C. Each participant was given two weeks to complete the questionnaires, at which time the researcher returned to the participants and collected the completed questionnaires. A representative for Division D received the questionnaires electronically and, after reviewing them, invited the researcher to make a formal presentation to the group of line managers whose employees were to be given the questionnaires and invited to complete them. The PyruX liaison provided printed copies of the questionnaires to each of the line managers who attended the formal presentation; each line manager agreed to provide one copy of both questionnaires to every incident manager who worked for that line manager. The line managers in Division D were given two weeks to distribute and collect the completed pilot study questionnaires, after which they were returned to the PyruX liaison in Division D, who sent the completed questionnaires to the researcher by courier. Upon collection of all responses from all four divisions, only fully completed questionnaires were included in those analysed

3.2.4. Results

The data from the results of the two questionnaires designed and distributed in the pilot study were analysed using SPSS™ Version 15. The analysis of the results from each is presented in the following sections. Factor analysis was performed on the data using the oblique rotation extraction method. Results from the behavioural characteristics questionnaire were followed by the results from the approach-to-solving-problems questionnaire analysis.

3.2.4.1. Behavioural Characteristics Questionnaire Results

Preliminary information was obtained concerning the data collected, identifying characteristics included in the behavioural characteristics questionnaire, prior to factor analysis being performed. Descriptive statistics are provided in Table 3-7.

Table 3-7.
Descriptive Statistics for Characteristics of Incident Managers

Characteristic	N	Mean	Standard Deviation	Min	Max
Communicative	118	2.834	1.178	1.00	5.00
Relationship Management	118	2.957	1.013	1.00	5.00
Administrative	118	3.855	0.93	1.00	5.00
Decisive	118	3.448	0.833	1.00	5.00
Leadership	118	3.531	0.869	1.00	5.00
Entrepreneurial	118	3.145	1.009	1.00	5.00

All data was entered and assessed to determine if it was suitable to factor analysis. The Kaiser-Meyer-Olkin (KMO) result indicated a satisfactory factor analysis could be performed, given its sampling adequacy of 0.699. A score of 0.50 is necessary for the use of factor analysis to be reliable (Loas, Noisette, Legrand & Boyer, 2000). As shown in Table 3-8, Factor 1 is significantly negatively associated with Factor 2, yet all other factors are predominantly positively associated to one another. Of the 28 pairings in the correlation matrix, seven, by virtue of being correlated to themselves have a value of 1.00, five are negatively associated (ranging from -0.009 to -0.99), and 16 are positively associated (ranging from 0.004 to 0.205).

Table 3-8.
Correlation Matrix for Characteristics of Incident Managers

Factor	1	2	3	4	5	6	7
1	1.000						
2	-0.990	1.000					
3	-0.133	0.004	1.000				
4	0.094	-0.117	0.005	1.000			
5	0.136	0.133	-0.009	0.046	1.000		
6	-0.067	0.027	0.024	0.071	0.006	1.000	
7	0.205	0.048	0.042	0.148	0.142	0.064	1.000

After reviewing the Correlation Matrix, the Communalities and Variances were analysed. Communalities values indicate the amount of variance in each factor. Principal component extraction with oblique rotation extraction method was used to produce the communalities table (see Table 3-9); those items with values of less than 0.50 were eliminated from the table.

Table 3-9.

Communalities for Characteristics of Incident Managers

	Initial	Extraction
I work well with people who are polite and trusting.	1.00	0.582
When I socialize, I spend most of the time talking about my work.	1.00	0.746
I would rather be 100% wrong than only 99% right.	1.00	0.771
Technical teams involved in restoring service share information . . . willingly and honestly.	1.00	0.552
When an unplanned outage takes an unexpectedly long time . . . the technical team leader explains why ,... .	1.00	0.585
I decide what tasks should be taken to restore service.	1.00	0.687
The rules and regulations to succeed within my work group are clearly specified.	1.00	0.721
I would be willing to take a pay cut now if there was a career opportunity . . . increase my future earning power.	1.00	0.579
The amount of effort someone must put into restoring service is not of interest to me.	1.00	0.623
I ensure I follow the process and policies established for my team to perform my role.	1.00	0.589
I insist that the technical teams present very detailed and specific information during teleconferences.	1.00	0.520
Clear lines of authority and responsibility exist when I manage an unplanned outage.	1.00	0.647
I follow a written script during teleconferences so I remember to ask the right questions.	1.00	0.570
When time is important, I refuse to be pressured.	1.00	0.510
If the impacted users won't assist in restoring service by doing testing, I assume there really isn't an issue.	1.00	0.683
Information overload is a by-product of having an unplanned.	1.00	0.658
I allow the technical teams working to restore service a great deal of independence.	1.00	0.523
I often organise casual meetings . . . to review the work we do together.	1.00	0.636
I prefer to manage incidents that are duplicates of previous unplanned outages . . .	1.00	0.649
When I am done at the office, I spend time at the gym or with my family and leave work behind.	1.00	0.599
The longer it takes to restore service, the more I demand from the people trying to restore it.	1.00	0.618
The more clearly a problem can be described, the more likely the unplanned outage will be restored quickly.	1.00	0.529
Information about unplanned outages I manage is always provided to me in a timely manner.	1.00	0.719
Most of the time, I enjoy my job, not because of my salary, but because it is interesting work.	1.00	0.861
Information flows through a clearly defined chain of command.	1.00	0.577
I use teleconferences to work through the technical details so that the right actions are taken to restore service.	1.00	0.700
It is more effective to restore service by cutting corners than it is to "do it by the book".	1.00	0.596
Technical teams do a good job of keeping me informed about matters that indicate when service will be restored.	1.00	0.683
When faced with an unplanned outage, I apply careful analysis to all of the information provided.	1.00	0.659
I hold the technical support group accountable for their actions in efforts to restore service.	1.00	0.744

Table 3-9.
Communalities for Characteristics of Incident Managers

	Initial	Extraction
My decisions are usually wide-ranging for and accommodating to all impacted parties.	1.00	0.563
Significant outages usually only need simple solutions to restore service.	1.00	0.679
When I manage an unplanned outage, I make decisions quickly and take action.	1.00	0.658
The management team is responsible for obtaining all required resources to restore service . . .	1.00	0.619
I am technically astute enough to challenge the technical teams when they provide . . . information.	1.00	0.604

For Bartlett's test of sphericity, the approximate chi-square is 149.833, degrees of freedom is 28, and the significance is zero. Two items with absolute values of less than 0.45 were eliminated. Rotation converged in 27 iterations (eliminating six of the items). The seven factors identified explained 61.638 percent of the variance revealed. A loading factor of 0.45 was used to optimise the factor analysis, resulting in all components numerically greater than seven being eliminated from explaining variance, as the contribution to that variance was considered by the researcher to be too low. An Eigenvalues greater than one was used and seven factors were identified. (See Table 3-10.)

Table 3-10.
Total Variance Explained from Pilot Study: Characteristics

Factors ^a	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings ^b
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	5.888	15.096	15.096	5.888	15.096	15.096	4.205
2	5.413	13.879	28.976	5.413	13.879	28.976	4.973
3	3.717	9.531	38.506	3.717	9.531	38.506	3.412
4	2.748	7.046	45.552	2.748	7.046	45.552	3.917
5	2.264	5.805	51.358	2.264	5.805	51.358	3.574
6	2.243	5.750	57.108	2.243	5.750	57.108	2.378
7	1.767	4.530	61.638	1.767	4.530	61.638	3.712

^a Also referred to in the Total Variance Explained as Components. ^b When components are correlated, sums of squared loadings cannot be added to obtain a total variance.

A Cronbach's alpha value of 0.729 was calculated on the items in the behavioural characteristics of incident managers questionnaire. A Cronbach's alpha score of greater than 0.70 is recommended (Nunnally, 1978) to confirm internal consistency reliability. This quantitative analysis of the data reported from the results of the pilot study behavioural characteristics questionnaire divided the items into seven factors. The seven factors selected from the items identified through the factor analysis had absolute value loadings of no lower than 0.45. The results were normally distributed. Descriptive statistics are provided in Table 3-11. The items and factor analysis loadings obtained for the behavioural characteristics of incident managers are provided in Table 3-12.

Table 3-11.
Descriptive Statistics from Factor Analysis of Pilot Study Data: Characteristics

Factor	N	Mean	Standard Deviation	Min	Max
1	118	3.150	0.719	1.00	5.00
2	118	3.196	1.064	1.00	5.00
3	118	3.023	1.073	1.00	5.00
4	118	3.251	0.909	1.00	5.00
5	118	4.291	0.981	1.00	5.00
6	118	3.119	1.201	1.00	5.00
7	118	3.192	0.884	1.00	5.00

Table 3-12.

Items and Factor Analysis of Behavioural Characteristics of Incident Managers

Item	STATEMENT	FACTOR	1	2	3	4	5	6	7
26	When I am done at the office, I spend time at the gym or with my family and leave work behind.		-.69						
28	The more clearly a problem can be described, the more likely the unplanned outage will be restored quickly.		-.66						
41	I am technically astute enough to challenge the technical teams when they provide questionable or inaccurate information.		-.64						
19	Others think I am aggressive.		-.60						
16	I follow a written script during teleconferences so I remember to ask the right questions.		.56						
2	When I socialize, I spend most of the time talking about my work.		-.54						
3	I would rather be 100% wrong than only 99% right			.85					
10	The amount of effort someone must put into restoring service is not of interest to me.			.75					
27	The longer it takes to restore service, the more I demand from the people trying to restore it.			.70					
30	Most of the time, I enjoy my job, not because of my salary, but because it is interesting work.			-.69					
13	I insist that the technical teams present very detailed and specific information during teleconferences.			.60					
20	If I won the lottery, I would stop working.			.53					
24	I often organize casual meetings (coffee, etc) with support teams and management teams to review the work we do together.			-.51					
1	I work well with people who are polite and trusting.			-.51					
34	Technical teams do a good job of keeping me informed about matters that indicate when service will be restored.				.80				
7	The rules and regulations to succeed within my work group are clearly specified.				.80				
29	Information about unplanned outages I manage is always provided to me in a timely manner.				.55				
23	I allow the technical teams working to restore service a great deal of independence.				.52				
4	Technical teams involved in restoring service share information with me as they progress and they do it willingly and honestly.				.50				
8	I would be willing to take a pay cut now if there was a career opportunity that could increase my future earning power.				-.46				
18	If the impacted users won't assist in restoring service by doing testing, I assume there really isn't an						.76		

Table 3-12.

Items and Factor Analysis of Behavioural Characteristics of Incident Managers

Item	STATEMENT	FACTOR	1	2	3	4	5	6	7
	issue.								
25	I prefer to manage incidents that are duplicates of previous unplanned outages, rather than new and unknown outages.					.67			
22	Information overload is a by-product of having an unplanned outage.					.65			
32	I use teleconferences to work through the technical details so that the right actions are taken to restore service.					-.64			
5	When an unplanned outage takes an unexpectedly long time to restore, I have the technical team leader explain the reasons why to my manager.					.54			
31	Information flows through a clearly defined chain of command.					.52			
38	Significant outages usually only need simple solutions to restore service.					.46			
36	I hold the technical support group accountable for their actions in efforts to restore service.						.74		
40	The management team is responsible for obtaining all required resources to restore service when an unplanned outage occurs.						.67		
21	One of my first tasks to perform is to notify my manager an unplanned outage has been reported.						.63		
14	Clear lines of authority and responsibility exist when I manage an unplanned outage.						.49		
33	It is more effective to restore service by cutting corners than it is to "do it by the book".							.74	
6	I decide what tasks should be taken to restore service.							.74	
39	When I manage an unplanned outage, I make decisions quickly and take action.								.81
35	When faced with an unplanned outage, I apply careful analysis to all of the information provided.								.69
11	I ensure I follow the process and policies established for my team to perform my role.								.50
43	A new incident has been reported. My first thought is to figure out who will assist me in getting service restored.								
42	I provide all information to all interested parties when an unplanned outage is being restored.								
15	I remind the technical teams how long their previous outage took to restore.								
17	I wait for the results from the technical team's work before directing them on what next to do.								
9	Identifying what has stopped working, or what has begun to work differently than expected, is the first step to restoring service from an unplanned outage.								
12	It is often necessary to intimidate people to get the correct actions performed.								

Having completed the factor analysis, labeling the identified factors required a review of not only the data output, but also the literature, to ensure alignment with the data obtained and the relationship between specific characteristics displayed by managers and the importance of their being displayed. The selection of factor labels and reasons for their selection are discussed in the following sections.

3.2.4.1.1. *Being Entrepreneurial*

Factor analysis revealed that questionnaire items number 26, 28, 41, 19, 16 and 2 identify one characteristic, cited as Factor 1, as shown in Table 3-12. Collectively, it can be stated that individuals displaying the characteristic identified as Factor 1 can be said to have a passion for parts of their lives, whether in employment or personal relationships. These features contributed more than 15 percent of the total variance of the factors identified through factor analysis. Factor 1 was labeled Being Entrepreneurial. Being entrepreneurial allows incident managers flexibility under pressure. Inherently encouraging a management of uncertainty, incident managers, by virtue of the job they perform, are confronted with uncertainty and must direct the actions of others to restore service without, necessarily, being able to articulate all of the risks associated with decisions made. The incident manager must demonstrate confidence in the technical teams in order to have them assume some of that confidence so that they are empowered to take action that would, otherwise, be counterintuitive. Recent research (Schjoedt, 2009) performed surveying top managers and Chief Executive Officers of organisations in the southwestern United States (N = 547) reports that there is a distinct relationship between having an entrepreneurial satisfaction with work and the autonomy, variety, and feedback obtained from the performance of that work. Moreover, work by Hatch and Zweig (2000) concludes that entrepreneurial exercise requires the ability to demonstrate risk tolerance, a desire to control, a desire to succeed, and the abilities of perseverance and decisiveness. The results from the factor analysis aligned with the pilot study statements; the label conferred on Factor 1 is being entrepreneurial.

3.2.4.1.2. *Being Demanding*

Factor analysis revealed that questionnaire items number 3, 10, 27, 30, 13, 20, 24 and 1 identify one characteristic, cited as Factor 2, as shown in Table 3-12. Collectively, it can be stated that individuals displaying the characteristic identified as Factor 2 are individuals who have a requirement to have their needs met; however, there is no indication that they comprehend the needs of others, including those who meet their needs. Intolerance and manipulation are words that can be used to identify some of the statements that contributed nearly 14 percent of the total variance of the factors identified through factor analysis. Factor 2 was labeled Being Demanding. Being demanding is a characteristic of incident managers who engage technical support teams and corporate managers to ensure that attention is

given to priority unplanned outages and that the skills required to create and deploy technical changes are available. Research indicates that how a demand is made is designed and presented with the intention of obtaining a particular action or reaction (Boon, Moors, Kuhlmann, & Smits, 2008). Incident managers benefit from displaying a demanding characteristic because of its ability to communicate clearly to others “I’m in charge” (Pinto & Pisco, 2009). This view complements two pieces of work done in 2002 (Caughlin; Eldridge & Christensen) in which demanding individuals often obtained what they wanted by virtue of complaining to others either so often or so intensely that the others found meeting the needs easier than listening to the continuing verbal onslaught. The results from the factor analysis align the pilot study statements; the label conferred on Factor 2 is being demanding.

3.2.4.1.3. *Being Authoritative*

Factor analysis revealed that questionnaire items number 34, 7, 29, 23, 4 and 8 identify one characteristic, cited as Factor 3, as shown in Table 3-12. Individuals who displayed the characteristics identified in Factor 3 could be said to have an understanding for the importance of not only giving direction to others, but also having others follow that direction. Factor 3 was labeled Being Authoritative. Being authoritative provides incident managers the ability needed to follow rules and enforce company policies. Such well-framed structure allows the incident manager, and those with whom that person is engaged, to understand the rules to follow to achieve goals. This structure is complemented by control. By maintaining a high degree of control over subordinates and associates, incident managers are able to direct the actions of many participants in highly complex situations. As identified by Yeung (2004) features common in authoritative control include the use of questions and rephrasing statements heard. Additionally, this control affords the incident manager the opportunity to make non-productive participants in the unplanned outage able to contribute by ensuring the roles of all participants are understood and necessary. As is true for all tripods, the two pillars of structure and control will not stand without the third, sensitivity. Used in an authoritative context, sensitivity acknowledges the individuals involved in an unplanned outage as individuals, with needs and desires that may be dissimilar to the needs and desires of others impacted by the unplanned outage. Expressing sensitivity allows the authoritative incident manager the ability to convey appreciation and respect for those working to restore service. The authoritative characteristic of an incident manager combines the three necessary pillars of structure, control, and sensitivity cited by Bielous (1994) in his assessment of authoritative managers. The results from the factor analysis align the pilot study statements; the label conferred on Factor 3 is being authoritative.

3.2.4.1.4. *Being Communicative*

Factor analysis revealed that questionnaire items numbers 18, 25, 22, 32, 5, 31, and 38 identify one characteristic, cited as Factor 4, as shown in Table 3-12. Collectively, it can be stated that individuals displaying the characteristic identified as Factor 4 can be said to have an understanding for the importance of ensuring that all interested parties impacted by unplanned outages are given the information each needs about those unplanned outages. Technically, it is true that being communicative means having skills to process some set of inputs from another source and understand the outputs successfully; being communicative is a vital tool of incident managers. In business, being communicative is not an isolated activity, and its significance, as concluded by Shockley-Zalabak (2001), is in its use as a flexible tool for managers and members of an organisation to motivate workers towards productive ends. For incident managers, that productive end is service restoration. Factor 4 was labeled Being Communicative. Being communicative is the formal and informal sharing of relevant, reliable, and timely information in a process through which individuals share and create information in order to reach their common goal (Anderson & Narus, 1990; Johnson & Lederer, 2005; Walczuch et al., 2001). The results from the factor analysis align the pilot study statements; the label conferred on Factor 4 is being communicative.

3.2.4.1.5. *Being Facilitative*

Factor analysis revealed that questionnaire items numbers 36, 40, 21 and 14 identify one characteristic, cited as Factor 5, as shown in Table 3-12. Individuals who displayed the characteristics identified in Factor 5 could be said to have genuine respect for the parties impacted by an unplanned outage and actively work to ensure the needs of all parties are met. Factor 5 was labeled Being Facilitative. Being facilitative occurs because individuals exploit available means to achieve intrinsic propensities toward higher levels of complexity (Grzwacz & Butler, 2005). Although being facilitative suggests a willingness to deliver a solution that meets the requirements of all parties, it is, in fact, used to meet the needs of the parties actually impacted. It requires engagement with many of the impacted parties. This complements the work of Kesby (2002) who cited that isolation caused difficulty in finding solutions, while working in a facilitative manner provides greater ease to identify solutions. The results from the factor analysis aligned with the pilot study statements; the label conferred on Factor 5 is being facilitative.

3.2.4.1.6. *Being Pragmatic*

Factor analysis revealed that questionnaire items numbers 33 and 6 identify one characteristic, cited as Factor 6, as shown in Table 3-12. Individuals who displayed the characteristics identified in Factor 6 could be said to have the ability to use common sense. Factor 6 was labeled Being Pragmatic. Being pragmatic includes the unemotional

acceptance and processing of data provided, founded on principles of the person overseeing the work of others. As cited by Emison (2004), being pragmatic is not having a simple view of pursuing an easy course of action; wise courses of action are sought. McGovern (1997) cited three characteristics that align specifically with managers who demonstrate the ability to display being pragmatic. These characteristics are control, steps, and authorisation. This trio ensures that the manager who displays the characteristic of being pragmatic does so, when successful, using common sense to ensure he understands who has control, what steps need to be taken and what authorisation is required, and from whom, to move to finding solutions. The results from the factor analysis aligned with the pilot study statements; the label conferred on Factor 6 is being pragmatic.

3.2.4.1.7. *Being Decisive*

Factor analysis revealed that questionnaire items numbers 39, 35, and 11 identify one characteristic, cited as Factor 7, as shown in Table 3-12. Individuals who displayed the characteristics identified in Factor 7 could be said to benefit from not worrying about being wrong. Factor 7 was labeled Being Decisive. Researchers (Caulkins, Morrison, & Weidemann, 2007) report that decision makers consider the quality control of the data used to make decisions is more important than the actual accuracy of the data. The time to worry about a decision is before it is made (Syverud, 2006). Additionally, Yukl (1998) determined that effective leaders are those whose qualities include the ability to act decisively, yet there is no indication that deciding correctly influences the view that the leaders are effective. Indeed, decision-makers knowingly make significant decisions using data that is knowingly flawed (Caulkins, Morrison, & Weidemann, 2007). Individuals who are decisive are so with the full knowledge that some decisions made will be wrong, not out of intent, but due to bad or incomplete data being used to make the decision. However, being decisive means making decisions with whatever data is available and chosen for use. The results from the factor analysis aligned with the pilot study statements; the label conferred on Factor 7 is being decisive.

3.2.4.2. *Approach-to-Solving-Problems Questionnaire Results*

Preliminary information was obtained concerning the data collected from responses to the approaches-to-solving-problems questionnaire, prior to factor analysis being performed. Factor analysis was performed on the data using the oblique rotation extraction method. Results from the factor analysis of the approaches-to-solving-problems questionnaire are provided in the following sections. Descriptive statistics are provided in Table 3-13.

Table 3-13.
Descriptive Statistics of Approaches-to-Solving-Problems by Incident Managers

Approach to Solving Problems	N	Mean	Standard Deviation	Min	Max
Factor 1	118	3.493	0.990	1.00	5.00
Factor 2	118	3.779	0.996	1.00	5.00

All data was entered and assessed to determine if it was suitable to factor analysis. The Kaiser-Meyer-Olkin (KMO) result indicated a satisfactory factor analysis could be performed, given its sampling adequacy of 0.699. A score of 0.50 is necessary for the use of factor analysis to be reliable (Loas, Noisette, Legrand & Boyer, 2000). The correlation matrix, produced using principal axis factoring and the oblimin with Kaiser Normalization rotation method (see Table 3-14), revealed that Factor 1 is significantly positively associated with Factor 2.

Table 3-14.
Correlation Matrix of Approaches-to-Solving-Problems by Incident Managers

Factor	1	2
1	1.00	
2	0.91	1.00

After reviewing the correlation matrix, the communalities and variances were analysed. Given that communalities values indicate the amount of variance in each factor, it is recommended that those with a value of less than 0.50 indicate that the variables associated may not fit well with the factor solution and should be considered for excluding from the analysis (Field, 2005). The principal component oblique extraction method was used to produce the communalities table (see Table 3-15); those items with values of less than 0.50 were eliminated from the table.

Table 3-15.

Communalities of Approaches-to-Solving-Problems by Incident Managers

	Initial	Extraction
Understanding the root cause of an unplanned outage is important.	1.00	0.544
Introducing a permanent fix must occur in order to restore service.	1.00	0.672
The best solution to a problem should almost always be implemented.	1.00	0.749
A new incident has been reported. My first thought is to figure out who will assist me in getting service restored.	1.00	0.684
Identifying what has stopped working, or what has begun to work differently than expected, is the first step to restoring service from an unplanned outage.	1.00	0.684
Identifying and testing possible solutions is necessary before restoring service.	1.00	0.726
An unplanned outage is restored only when the root cause is known and a permanent solution is deployed.	1.00	0.622
It is as important to know when the problem did not exist as when it started.	1.00	0.501

The two items identified from the output from the factor analysis provided a cumulative percentage of variance of 46.62 percent. A loading factor of 0.45 was used to optimise the factor analysis, resulting in all components, numerically greater than two in this output, being eliminated from explaining variance, as the contribution to that variance was considered by the researcher to be too low. As was done to produce the communalities table, principal component extraction with oblique rotation extraction method was used to produce the total variance explained (see Table 3-16).

Table 3-16.

Total Variance Explained from Approaches-to-Solving-Problems by Incident Managers

Factors ^a	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings ^b
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	3.048	30.484	30.484	2.481	24.806	24.806	2.459
2	1.613	16.133	46.617	1.095	10.952	35.758	1.158

^a Also referred to in the total variance explained as Components. ^b When components are correlated, sums of squared loadings cannot be added to obtain a total variance.

This quantitative analysis of the data reported from the results of the pilot study approach-to-solving-problems questionnaire divided the items into two factors. All items had absolute value loadings no lower than 0.450; in fact, all items actually had loadings no lower

than 0.524. The results were normally distributed. Bartlett's Test of Sphericity was also produced for sampling adequacy. Its approximate chi-squared value was 274.603 with degrees of freedom equal to 22 and a significance of .000. The Cronbach's alpha value was 0.703. To identify expressed factors, the researcher assessed the intercorrelation matrix of the questionnaire statements using the factor analysis function in the SPSS™ statistical-analysis software, and used oblimin with Kaiser Normalization rotation to obtain correlated factors. Three items with absolute values of less than 0.45 were eliminated. The remaining items actually had loadings no lower than 0.524. The results were normally distributed. The means of the questionnaire items varied from 2.51 to 4.29 (on a scale of 1.0 to 5.0) and the standard deviations from 0.990 to 0.996. Rotation converged in 11 iterations (eliminating none of the items).

Having completed the factor analysis, labeling the identified factors was required to be completed. The research items and factor analysis from the approaches-to-problem-solving are presented in Table 3-17.

Table 3-17.
Research Items and Factor Analysis of Approaches-to-Solving-Problems of Incident Managers

Item	Statement	Factor	1	2
3	Introducing a permanent fix must occur to restore service		.732	
5	Identifying and testing possible solutions is necessary before restoring service.		.696	
2	Understanding the root cause of an unplanned outage is important.		.663	
7	An unplanned outage is restored only when the root cause is known and a permanent solution is deployed.		.524	
9	It is as important to know when the problem did not exist as when it started.			.768
6	Even when little progress is being made, I appraise the technical team as it works to restore service.			.729
10	I rarely take risks because doing so could exacerbate the duration of the unplanned outage.			.688
1	The best solution to a problem should almost always be implemented.			
4	Progress is interesting, but only the restoration of service matters.			
8	If the impacted users won't assist in restoring service by doing testing, I assume there really isn't an issue.			

The approach-to-problem-solving questionnaire investigated the prominent approaches used by incident managers to solving problems encountered while working to restore service when unplanned outages occur. Having completed the factor analysis, labeling the identified factors to provide an accurate citation that ensured alignment with the data obtained and the relationship between specific approaches-to-solving-problems used by incident managers

and the importance of their being used. The selection of factor labels and reasons for their selection are discussed in the following sections.

3.2.4.2.1. *Problem-Focused Approach-to-Solving-Problems*

Factor analysis revealed that questionnaire items number 5, 4, 7, and 1 identify one problem-solving approach, cited as Factor 1. Individuals who use an approach to solving problems as identified in Factor 1 could be said to be interested in why an unplanned outage occurred. They are methodical in the manner in which they perform their work; however, they are focused on why. Beginning with the identification of all components as either failing or not failing, users of this problem-focused approach attempt to explain symptoms observed (de Kleer et al., 1990; Miettinen & Flegel, 2003). Specifically identified as being a more viable problem-solving approach to incident managers than the use hunches, instinct, or intuition (Marquis, 2006), a problem-focused approach to solving problems affords incident managers a luxury of time to determine, and eliminate, the root cause of an unplanned outage so that it does not recur. The results from the factor analysis aligned with the pilot study statements; the label conferred on Factor 1 is a problem-focused approach.

3.2.4.2.2. *Solution-Focused Approach-to-Solving-Problems*

Factor analysis revealed that questionnaire items numbers 6, 2, and 1 identify one problem-solving approach, cited as Factor 2. Individuals who use the problem-solving approach identified in Factor 2 could be said to be interested in how to restore service impacted from the occurrence of an unplanned outage. They are methodical in the manner in which they perform their work; however, they are focused on the attainment of a particular result—the restoration of service—above all other avenues of investigation, technical anomalies, or other areas of interest to parties impacted by the unplanned outage. This confirms the work of Watzlawick, Weakland, and Fisch (1974) who found that problems were often perpetuated when time was taken to understand their origins; problems were lessened when actions were taken to find their solutions. Founded on the framework of Solution Based Brief Therapy, established at the end of the 20th century, users of solution-focused approach to problem solving ask questions that identify solutions based on the removing of problems, not necessarily understanding them and by repeatedly giving verbal rewards to those making the smallest steps forward in removing the problems (Bannink, 2007). Focusing on a desired state, rather than on the current state (Cepeda & Davenport, 2006), users of a solution-focused approach to problem solving recognise and acknowledge progress as it is made. In all cases, progress leads to the attainment of service restoration.

The results from the factor analysis aligned with the pilot study statements; the label conferred on Factor 2 is a solution-focused approach.

3.3. Discussion of the Pilot Study

The research design used in the pilot study included both qualitative and quantitative research methods and allowed the researcher to develop questionnaires for use in the main study. The qualitative research included the hosting of a focus group and a qualitative data analysis of the focus group transcript. The quantitative analysis in the pilot study included the establishment, tests for validity and reliability of the two questionnaires. The first questionnaire investigated the behavioural characteristics displayed by incident managers; the second questionnaire investigated the approaches-to-solving-problems used by incident managers while working to restore service from unplanned outages.

From the analysis of the focus group transcript, six characteristics were identified as being important to the success of incident managers. These were being communicative, showing relationship management, being administrative, being decisive, having leadership, and being entrepreneurial. The factor analysis from the completed behavioural characteristics questionnaire, however, revealed that the key characteristics of incident managers are being entrepreneurial, being decisive, being demanding, being authoritative, being facilitative, being communicative, and being pragmatic. This supported key characteristics identified in research performed by de Pillis and Meilich (2006), Schein (1973, 1975), Shucksmith, Hendry, & Glendinning (1995), among others.

Information from the focus group transcript about the approach-to-solving-problems complemented information found in the literature (Bannink, 2007; Calabrese, Foo & Ramsay, 2007; Cepeda & Davenport, 2006; Froerer et al., 2009; Kepner & Tregoe, 2005; Maze-Emery, 2008; Miettinen & Flegel, 2003; Taylor, 2007) that indicates either a problem-focused approach or a solution-focused approach is used by incident managers while working to restore service from unplanned outages. The two pilot study questionnaires were successfully developed, validated, and found to be statistically reliable based on the responses received from incident managers (N = 118) in Australia. These two questionnaires were then used as two sections of a single questionnaire in the main study. That questionnaire is henceforth referred to as the KOZADAR Questionnaire (whose naming origin aligns with that of the KOZADAR Research Model) and can be found in Appendix C.

Chapter 4 : Main Study

The main study has two distinct components. Component 1 was designed to identify the characteristics displayed by incident managers and to identify the approaches they use to solve problems while working to restore service when unplanned outages occur. To achieve this, the researcher distributed the KOZADAR Questionnaire to 247 incident managers working in Australia, India, and Europe through their employing companies, Pyrox and Pyrite. Component 2 was designed to investigate two further aspects. The first was to determine if there is a significant difference in the amount of time taken to restore different types of unplanned outages. The second was to determine, given the characteristics displayed by incident managers, if the approaches incident managers use to solve the problem caused by the unplanned outages moderate the time required to restore service lost when the unplanned outages occur. To achieve these components of work, the researcher analysed the responses from the KOZADAR Questionnaire in conjunction with an analysis of unplanned outage observations with data provided by Pyrite.

These two components of the main study were designed to answer the questions raised at the beginning of this research. Those research questions are (1) What are the dominant characteristics displayed by incident managers when they work to restore service that has occurred due to an unplanned outage? (2) What are the different approaches used by incident managers when they work to restore service that has been lost due to an unplanned outage? and (3) What relationship exists, if any, between the dominant characteristics displayed by incident managers when an unplanned outage occurs, taking into account the problem solving approaches they use, and the time to restore service they attain? Accepting that unplanned failures will occur (Dashofy et al., 2002), the value of answering these research questions lies in the prospective cost savings that businesses will experience by minimising the time taken to restore services after an unplanned outage occurs. This research broadens the available literature in IT Service Management and incident management. Reviewing these research questions and analysing the results from the pilot study, hypotheses were postulated to determine their answers. Those hypotheses, along with the work undertaken in Component 1 and Component 2 of the main study, are described in the following sections.

4.1. Hypotheses

The hypotheses in this research can be divided into two parts, each part addressed in Component 1 and Component 2 of the main study, respectively. The first addresses the characteristics displayed and the approaches-to-solving-problems that are used by incident

managers while they work to restore service when unplanned outages occur. The second addresses the MTRS attained given different types of unplanned outages as well as the impact of those problem-solving approaches on the MTRS incident managers attain in the restoration of service when unplanned outages occur. The associated hypotheses for each are presented in the following sections.

4.1.1. Characteristics and Approaches to Solving Problems

To determine if there is a significant difference in the characteristics displayed by incident managers requires the ability to identify those characteristics displayed. The KOZADAR Questionnaire provided that set of characteristics and allowed an analysis to be performed on the responses to the questionnaire. Kozak and Uca (2008) successfully identified leadership in managers and found it to be a strong and positive managerial characteristic. Dorio (2005) identified 50 characteristics that impacted the work of business managers. Schein (1973, 1975) tested for 92 characteristics in relation to gender and the perception of those characteristics by others who witnessed their displays. In all cases, the display of specific characteristics was required before an assessment of the impact of those characteristics could be quantified. Hypothesis 1 (H_1) will be an extension of those studies insofar as it tested if specific characteristics of incident managers can be identified. Good incident managers live on adrenalin, and quick wits, among other skills, combined with resourcefulness (Waschke, 2006). Published work (O'Callaghan & Mariappanadar, 2006[a]) identified the key skills of good incident managers from output and qualitative analysis of data from a focus group. Key skills and characteristics of incident managers were identified and include the ability to build relationships, maintain focus, be organised, coordinate different teams, delegate, demonstrate leadership, listen, use intuition and have a customer focus. Davis (1953) suggested that the neglect of the corporate grapevine disadvantages managers in effectively being communicative in their organisation. Beasley (2005) cited leadership as an important characteristic of managers. Sheehan & Ojano (2006) coupled the characteristics of organisational skill, a vision of public policy, cognitive style and emotional intelligence as all being assessed to determine the leadership of past and future presidents of the United States. H_1 tests if characteristics of incident managers can be identified and, in their identification, be noted as being displayed.

The objective of Hypothesis 2 (H_2) was to test if the two approaches to solving problems are aligned to the displayed characteristics identified in Hypothesis 1. Hence, H_2 states that when an incident manager is engaged to restore service when unplanned outages occur, there is a significant relationship between the characteristics the incident manager displays and the approach to solving problems the incident manager uses. Determining if there is or is not a significant relationship, therefore, allows the exploration of any relationships between

those characteristics that are dominant in incident managers who use a problem-focused approach to solving problems, and those characteristics that are dominant in incident managers who use a solution-focused approach to solving problems while restoring service when an unplanned outage occurs.

The ability to identify if a relationship between the characteristics displayed by an incident manager and the approach to solving problems that the incident manager uses can be determined establishes information for further research to be performed. There is a further need to determine what relationship exists between the specific characteristics displayed and the specific approach to solving problems that is used. Incident managers often restore service with a common use of hunches, instinct, and intuition to restore service (Marquis, 2006). ITIL purports that the use of the Kepner-Tregoe problem-solving method is beneficial to finding the root cause of a problem (Taylor, 2007) and encourages its use in problem management, not in incident management. Alternately, Trepper, Dolan, McCollum and Nelson (2006) have reported that although problems do occur, they do not occur all the time, at every moment. In fact, there are times during which the problem does not exist at all. By focusing on a solution to the problem, rather than focusing on the problem, they report that problems can be solved. Bannink (2007) cites that when the continual giving of compliments occurs as steps are taken to finding a solution, the attainment of a solution progresses. These lead to the third and fourth hypotheses in this research. Given that decisions are made based on the communication used to provide information with which to make them, Hypothesis 3 (H₃) states there will be a significant relationship between the characteristics displayed by an incident manager and the use of a solution-focused approach while working to restore service when unplanned outages occur. Hypothesis 4 (H₄) states that there will be a significant relationship between the characteristics displayed by an incident manager and the use of a problem-focused approach while working to restore service when unplanned outages occur.

Caughlin (2002) states that the communication of demand/withdraw in marital relationships predicts the future of the relationship. Caulkins, Morrison, and Weidemann (2007) identified that decisions are made with available information, even when that information is neither accurate nor appropriate. Whether the approach used to solve problems is solution-focused or problem-focused, it is the approach used that allows the senior executive team data—converted into information—to make decisions.

4.1.2. Unplanned Outages and MTRS

Although symptoms and root cause(s) may vary when unplanned outages occur, unplanned outages happen due to changes made in the technology environment (Marquis, 2009). Although Morrill, Beard, and Clitherow (2008) identified only six causes of unplanned

outages, this researcher confirms (O’Callaghan & Mariappanadar, 2006; O’Callaghan & Mariappanadar, 2008) the work of Enriquez, Brown, and Patterson (2002) who reported there are, in fact, seven causes of unplanned outages. For a comparison of the two lists, see Table 4-1.

Table 4-1.
Lists of Unplanned Outages

Morrill, Beard, and Clitherow (2008)	Enriquez, Brown, and Patterson (2002)
Design Error In Hardware or Software	Acts of Nature
Environmental Events.	Hardware
Human-Caused Disasters	Humans Inside a Corporation
Natural Disasters and Accidents	Humans Outside a Corporation
User/Operator Accident, Inexperience, Malice	Software
Physical Breakage	System Overload
	Vandalism

Though evident that both lists attempt to identify causes of unplanned outages, Enriquez, Brown, and Patterson (2002) cite clear and distinct categories. These seven types of unplanned outages can occur in any combination; therefore, any unplanned outage may be the result of any combination of the seven types of unplanned outages. This can be validated by using Kramp’s factorial expression, $n!$ (Hayes, 2007). See Figure 4-1.

$$n! = \prod_{k=1}^n k \quad \forall n \in \mathbb{N}$$

Figure 4-1. Factorial equation

Applying the factorial equation where $N = 7$, $7!$ equals 5,040. In all instances, the factorial of a non-negative number is the product of all positive integers equal to and less than n . In the case of the seven types of unplanned IT outages, therefore, $n!$ is equivalent to 5,040 different unplanned outage combinations. Although unplanned outages should be avoided, or minimised, through appropriate duplication and redundancy (Wang, 2007), restoring service from an excess of 5,000 root causes can be time consuming. There is a direct relationship between an unplanned outage and the time taken to restore the service lost. Lowering MTRS directly improves the user experience of system availability and directly reduces the cost to the company that experiences the unplanned outage (Fox, 2002). Computers will always crash (Fox, 2003). This leads to Hypothesis 5 (H_5), which states there will be a significant difference between unplanned outage types and their respective MTRS.

Although research has been performed focusing on continuous availability and high availability of computer systems (Fox & Patterson, 2002; Radhakrishnan et al., 2008), limited research exists on determining avenues to minimise the amount of time required to restore service when an unplanned outage occurs. The researcher argues that the characteristics displayed by incident managers are moderated by the incident managers' approach to solving problems to attain an MTRS for unplanned outages. Hypothesis 6 (H₆) states that the use of a problem-focused approach or a solution-focused approach to restore service moderates the relationship between characteristics displayed by incident managers and the attained MTRS from an unplanned outage.

A review of the pilot study results, along with the research questions initiated when this work was undertaken led to establishing six hypotheses in this research. For ease of reference, both the hypotheses and the research questions from which they were derived are provided here:

Research Question 1

What are the dominant characteristics displayed by incident managers when they work to restore service that has occurred due to an unplanned outage?

Hypothesis₁

Incident managers will display significantly different characteristics when they restore service from an unplanned outage.

Research Question 2

What are the different problem-solving approaches used by incident managers when they work to restore service that has been lost due to an unplanned outage?

Hypothesis₂

There will be a significant difference in the approaches used by incident managers to solve problems when unplanned outages occur.

Hypothesis₃

There will be a significant relationship between the characteristics displayed by an incident manager and the use of a solution-focused approach while working to restore service when unplanned outages occur.

Hypothesis₄

That there will be a significant relationship between the characteristics displayed by an incident manager and the use of a problem-focused approach while working to restore service when unplanned outages occur.

Research Question 3

What relationship exists, if any, between the dominant characteristics displayed by incident managers when an unplanned outage occurs, taking into account the problem-solving approaches they use, and the time to restore service they attain?

Hypothesis₅

There will be a significant difference between unplanned outage types and their MTRS.

Hypothesis₆

The use of a problem-focused approach or a solution-focused approach to restore service will moderate the relationship between characteristics displayed by incident managers and their attained MTRS from an unplanned outage.

These hypotheses were tested in the main study and allowed a review of the relationships between the independent variable (characteristics displayed), the dependent variable (MTRS) and the moderating variable (approach-to-solving-problems). The analyses performed in the main study are presented in the following sections.

4.2. Main Study

The seven characteristics examined and the two approaches-to-solving-problems examined, investigated in the main study, are shown in Figure 4-2, the KOZADAR Research Model, which purports that there is a relationship not only between the characteristics displayed by incident managers and the attained MTRS, but that this relationship is moderated by on the problem-solving approach they use that allows them to attain an MTRS.

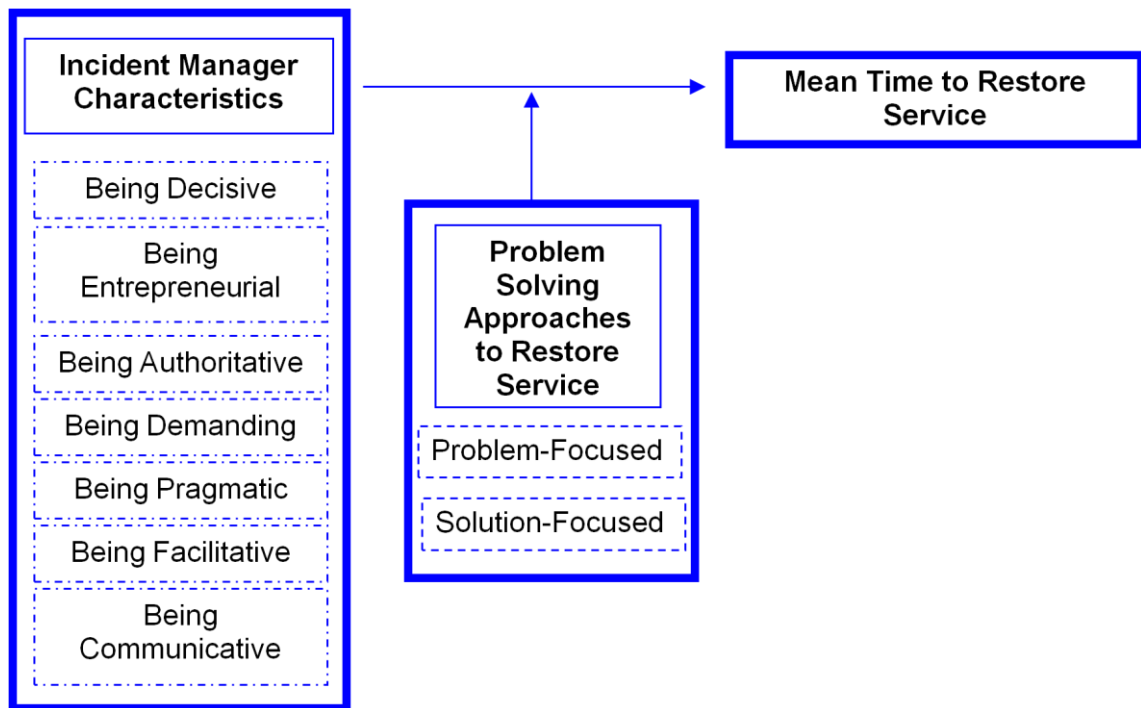


Figure 4-2. The KOZADAR Research Model, Detailed

Using the characteristics as the independent variable in the research and the MTRS attained as the dependent variable, the core of this research is determining if the approaches-to-solving-problems, used by incident managers, moderate the value of the attained MTRS. These characteristics and approaches-to-solving-problems were identified in the responses obtained from the KOZADAR Questionnaire. Applying the KOZADAR Research Model to investigate data obtained from the responses to the KOZADAR Questionnaire allowed the researcher to identify the characteristics displayed by incident managers and the approaches-to-solving-problems that incident managers use while working to restore service when unplanned outages occur.

4.3. Component 1—Characteristics and Approaches to Solving Problems

Component 1 of the main study was designed to investigate the characteristics displayed by, and the approaches-to-solving-problems used by incident managers while working to restore service when unplanned outages occur. Though some research has been completed that identifies alternatives that can be taken to avoid or minimise the impact of an unplanned outage (Allen, 2004; Brewer, 2001; Das & Das, 2008; Fox & Patterson, 2003), none focuses on the moderating effect of the variable “approach” used by incident managers to restore service when unplanned outages actually occur. The research presented here expands the boundaries of avoiding and minimising unplanned outages through the use and manipulation of technology, which has been richly investigated (Al-Ekram, Holt, Hobbs, & Sim, 2007;

Brooks et al., 2007; Candea & Fox, 2003; Shah, Hellerstein, & Brewer, 2004). Instead, the research presented here investigated the behavioural characteristics of incident managers and their contributions to the restoration of service when unplanned outages occur. Component 1 of the main study tests the first four of the six hypotheses reviewed in previous sections of this document. For ease of reference, they are included here.

H₁ Incident managers display significantly different characteristics when they restore service from an unplanned outage.

H₂ There will be a significant difference in the approaches used by incident managers to solve problems while they work to restore service when unplanned outages occurs,

H₃ There will be a significant relationship between the characteristics displayed by an incident manager and the use of a Solution-Focused Approach while working to restore service when unplanned outages occur.

H₄ There will be a significant relationship between the characteristics displayed by an incident manager and the use of a Problem-Focused Approach while working to restore service when unplanned outages occur.

Component 1 of the main study explores the relationships between the characteristics displayed by incident managers during the restoration of unplanned outages and the identification of the approaches-to-solving-problems that incident managers use. Data analysed in Component 1 of the main study was obtained from incident managers' responses to the KOZADAR Questionnaire.

4.3.1. Method

An analysis of the responses to the KOZADAR Questionnaire that were provided by incident managers from two large corporations was performed to identify demographic information, characteristics displayed, and the approaches-to-solving-problems used by incident managers while working to restore service when unplanned outages occur. This data was used to accept or reject Hypotheses one through four. The results of these analyses are presented in the following sections.

4.3.2. Participants and Tools

Invitations to participate in the main study of this research were extended to seven organisations, of which two accepted. These companies were the same as the companies

invited to participate in the pilot study. The first of the two organisations to accept the invitation, Pyrux, made the questionnaire available to 136 incident managers across its participating divisions; the second of the two organisations to accept the invitation, Pyrite, made the questionnaire available to 111 incident managers across its participating divisions. Data was collected from participants between January and March 2008. The total number of incident managers who completed the online questionnaire was 154. (See Table 4-2.)

Table 4-2.
Distribution and Collection of KOZADAR Questionnaires and Responses

Participants	Number of Distributed Questionnaires	Returned Completed Questionnaires	Percentage Returned
Pyrux	136	70	51.15%
Pyrite	111	84	75.75%
TOTAL	247	154	62.35%

To ensure complete sets of data were provided by KOZADAR respondents only those questionnaires with a response to every item were used in the analysis. This ensured no considerations needed to be made, using Bayesian or other techniques, to accommodate for missing data. A brief overview of the two organisations is provided in the following sections.

4.3.2.1. Pyrux

Having agreed to allow a subset of its staff to participate in the pilot study, Pyrux management requested that the researcher extend the company an invitation to participate in the main study. Pyrux was described in Section 3.1.3. A Pyrux representative was selected as the sole interface between the researcher and the organisation. The representative, in turn, identified the incident-manager employees in the Pyrux human resource job description inventory and provided the participants an electronic link to a secure website where they could access the KOZADAR Questionnaire. Both the organisation and the individuals were advised that their participation and their responses would be held in complete anonymity. Participants were based in Australia, Asia-Pacific, and Europe.

4.3.2.2. Pyrite

Pyrite is the pseudonym for an international data technology corporation with headquarters in the United States. It has sales and service offices in the United States, throughout South America, Australia, New Zealand, and multiple cities in Europe. With 2008 annual revenues in excess of \$US 50,000 million dollars and a worldwide workforce of more than one quarter of a million employees, Pyrite has been in business for more than fifty years. This has allowed it to build an international presence in the IT service and IT parts

market sectors, delivering IT goods and services to customers around the world. Pyrite employs incident management teams that provide service to internal portions of its own organisation, as well as teams that provide incident management services at customer sites. Pyrix senior managers signed consent forms to have its incident managers respond to the KOZADAR Questionnaire on-line. Both the organisation and the individuals were advised that their participation and their responses would be held in complete anonymity. Participants were based in Australia, England, and India.

4.3.3. Procedure

Invitations to participate in the main study of this research were extended to seven organisations, by phone, in calls placed to the CIO of each of the seven companies. Two of the organisations accepted the invitation to participate. The companies invited were asked to participate by means of judgment sampling on the part of the researcher. In their respective 2007-2008 annual reports, all organisations stated that the number of employees was greater than 40,000. Additionally, the IT footprint of each organisation – the extent of hardware, software, support, and applications in use – required the services of no fewer than 50 incident managers. Participants were asked to respond to the KOZADAR Questionnaire online. The data obtained from the responding incident managers was divided into two sections. The first was demographic information. The second was hypotheses testing information.

Each of the two companies that agreed to have its employees respond to the online version of the KOZADAR Questionnaire selected a single representative to serve as the companies' liaison to the researcher. It was to those representatives that the researcher provided the electronic link to the online questionnaire. Those representatives sent an invitation to the employees, identified as incident managers through their organisations' human resource job description inventory, and provided the electronic link to the secure website. Because one of the two companies participated in both the pilot study and in the main study, the researcher is unable to identify who, if any, of the respondents to the KOZADAR Questionnaire had also responded to the pilot study questionnaires. The responses were sent directly to the researcher for analysis.

In Component 1 of the main study, the KOZADAR Questionnaire was used to obtain information about incident managers, the characteristics they display while working to restore service from an unplanned outage, as well as the approaches they use to solve problems. At the beginning of the questionnaire, which can be found in Appendix B, participants were informed the reason the questionnaire data was being collected and why they were invited to participate. This ensured that the individuals who responded understood why the research was being conducted and why the individual had been invited to respond to the

questionnaire. Although no participants made use of them, the contact details of the researcher were also provided so that any participants interested in making direct contact with either the researcher or the sponsoring university could easily do so. (Both e-mail addresses as well as telephone numbers were provided to participants.) Finally written confirmation, via email, of the participants' anonymity, as well as anonymity of the actual responses submitted, was provided. A sample of the invitation sent to individuals from the corporate liaison can be found in Appendix B.

The KOZADAR Questionnaire is composed of three sections. Section 1 collects demographic information; Section 2 investigates approaches to solving problems; Section 3 investigates characteristics displayed by incident managers when restoring service from unplanned outages. There were five items that identified demographic information about the respondent; there were seven items related to the problem-solving approaches used by the respondents; there were 35 items related to characteristics investigated. With the exception of the demographic items, a Likert scale of one-to-five was used as a rating scale for all responses. The Likert scale ranged from 1 = never, 2 = rarely, 3 = sometimes, 4 = often, and 5 = always. The demographic items included gender, age, years working as an incident manager, marital status, and level of education completed.

The distribution of the questionnaire occurred electronically. In this research, the KOZADAR Questionnaire was hosted at surveymonkey.com, a secure website that provides anonymous and authorised-only access to custom surveys to individuals granted access by the individual or group that pays for the surveymonkey.com services. With its offices physically located in the northwestern United States, surveymonkey.com was established in 1999. It is an online service that enables people to create their own surveys quickly and is used by more than 80 percent of the Fortune 100 (The Monkeys, 2008). The researcher posted the KOZADAR Questionnaire onto the website and provided access to each of the two corporate liaisons with whom she worked; representatives from PyruX and Pyrite sent email invitations to prospective participants with an explanation of the research and a link to the questionnaire. The KOZADAR Questionnaire was available to be accessed for one month, after which participants were no longer able to submit responses. Surveys with incomplete data were deleted from the analyses. When the website was no longer active, the researcher collected responses to the KOZADAR Questionnaire electronically. The raw data of the participants' responses were downloaded into a Microsoft Excel™ spreadsheet to perform data analysis.

4.4. Component 2—Characteristics, Approaches and MTRS

Component 2 of the main study was designed to investigate the characteristics displayed by incident managers and if the MTRS service attained by incident managers is moderated in

any way by the approaches used by incident managers to solve problems. Component 2 of the main study tests the last two hypotheses reviewed in previous sections of this document. For ease of reference, they are included here.

H₅ There will be a significant difference between unplanned outage types and their MTRS.

H₆ The use of a Problem-Focused Approach or a Solution-Focused Approach to restore service will moderate the relationship between characteristics displayed by incident managers and their attained MTRS from an unplanned outage.

This work was undertaken using the results obtained from the KOZADAR Questionnaire, an analysis of unplanned outage data provided by Pyrite, and an alignment of the incident management rosters provided by Pyrite. Unlike Component 1 of the main study, which interrogated the responses of individuals to items in the KOZADAR Questionnaire, Component 2 of the main study was performed on the observations of actual unplanned outages, the duration of time required to restore service, and the alignment of incident managers responsible for the restoration of that service and their responses to the KOZADAR Questionnaire.

4.4.1. Method

Component 2 of the main study required additional data to augment Component 1 of the research. Component 2 tested two hypotheses. The first tested the MTRS service from unplanned outages. The second tested if any relationship between the characteristics displayed by incident managers, moderated by the approach used to solving problems, affected the MTRS attained by those incident managers. To test these hypotheses, data was collected from Pyrite.

An interrogation of three months' of unplanned outage data was provided to the researcher by Pyrite, described in Section 4.3.2.2, above. Additionally, the roster of the incident managers that worked during the months for which the unplanned outage data had been given was also analysed. Finally, some of the responses from the KOZADAR Questionnaire were also used in Component 2 of the main study. A discussion of the collection and interrogation of this data is provided in the following sections.

4.4.2. Observations

It is the number and type of observations of unplanned outages that allowed this research to be completed. Pyrite provided 2,122 unplanned outage observations, with complete descriptions of the outages and the work done to restore service. Upon request, Pyrite

agreed to submit all Severity 1 and Severity 2 incident dockets that had been managed by its incident managers during the months of August, September, and October of 2007 for analysis. This data was submitted from two divisions of Pyrite. The first was received from work performed in Asia-Pacific; the second was received from work performed in Europe. This set of data was the Severity 1 and Severity 2 incidents reported by Pyrite itself, to its internal incident management team, about its own unplanned outages. Pyrite did not release any unplanned outage data (or any other data) from any IT environment other than its own. By using only its own data, none of its customers had to be contacted or asked to release any of its own confidential data. Additionally, no further confidentiality agreements between Pyrite, the researcher, the academic institution overseeing the research, or any Pyrite customer were required.

Of the 2,122 unplanned Severity 1 and Severity 2 outages provided, 2,036 were interrogated to investigate Hypothesis 5 (there will be a significant difference between unplanned outage types and their MTRS). Each unplanned outage was categorised into one of seven types of unplanned outages (see Section 2.2.2.2), classifying each of the 2,036 interrogated unplanned outages as one of those seven types. The unplanned outage data provided by Pyrite allowed the MTRS to be calculated. The observations provided include those unique fields identified in Table 4-3:

Table 4-3.
Fields in Unplanned Outage Data Sent by Pyrite

Unique incident number	Time unplanned outage ended
Date unplanned outage began	Severity of the unplanned outage
Time unplanned outage began	Description of the unplanned outage
Date unplanned outage ended	Description of the restoration

4.4.3. Participants—Matching Incident Managers to the Unplanned Outages They Restored

As only unplanned outages from Pyrite were analysed to test Hypothesis 5, only the unplanned outages managed by Pyrite incident managers were considered to test Hypothesis 6 (the use of a problem-focused approach or a solution-focused approach to restore service will moderate the relationship between characteristics displayed by incident managers and their attained MTRS from an unplanned outage). To determine the specific incident manager who handled a particular unplanned outage, a multi-step process was followed to identify specific incident managers as “owners” of unplanned outages.

Step 1 identified the responses from the KOZADAR Questionnaire that were submitted by employees of Pyrite. In addition to collecting responses to the KOZADAR Questionnaire, the Internet Protocol (IP) addresses from which the responses were sent were also collected.

This allowed the IP address to be interrogated using a software tool that lists the owning company of the IP address, identifying the response from every participant as being from a PyruX or Pyrite IP address, indicating the company for which the individual worked. Because all unplanned outage data was from Pyrite, all KOZADAR Questionnaire results received from Pyrite were identified by the IP address associated with the response.

An IP address is presented to its viewer as four digits, in the following format: $a_1.a_2.a_3.a_4$, where the values of any a must be between zero and 255 and can be identical to or different from the value of any other a . An IP address is the network address used to identify the source of data transmitted across a network. Effectively, if the IP address was equivalent to the mailing address of an individual at his or her home, the values of n equal the name-of-person-to-whom-the-letter-is-being-mailed (a_1), the street-address-of-that-person (a_2), the city-in-which-that-person-lives (a_3), the state-in-which-that-city-exists (a_4). When KOZADAR Questionnaires from Pyrite were identified, those responses from PyruX were eliminated from any further analysis.

Step 2 required the timestamps of the submitted Pyrite KOZADAR Questionnaire results to be aligned with the Pyrite incident management roster. Each shift worked by an incident manager was a 12-hour shift, beginning at either 0600 or 1800 and ending at 1815 or 0615, respectively. The roster data identified each incident manager by first name only and the shifts the incident manager worked during the three months for which the unplanned outage data was provided. The roster included information relative to leave taken, overlaps in shifts covered, and other details that confirmed which unplanned outage mapped to specific incident managers working the shift during which the unplanned outage occurred. The shift overlap times allowed a handover between shifts so that incoming incident managers received current information on incidents not yet restored and other important information that related to activities performed during the shift just ending. The incident managers' rosters were aligned to the timestamps of the KOZADAR Questionnaire responses, as it was assumed that incident managers completed their responses online during their work hours.

Step 3 excluded all unplanned outages of greater than 12 hours, as all unplanned outages of greater than 12 hours required restoration to occur during more than one roster-shift, indicating that more than one incident manager was involved in their restoration. There were 1,336 incidents interrogated that met the duration requirements and a single incident manager could be identified as being the restoring incident manager.

Step 4, performed to ensure participant anonymity, coded the individuals listed on the roster. To protect the anonymity of the respondents, each was coded as Im_n so that all data obtained about the restoring incident manager was coded and the actual names of the incident managers were held in confidence by the researcher.

Step 5 was the coding of the gender of the incident managers who answered the KOZADAR Questionnaire during their shifts. From that information, gender assignments were made, allowing a complete alignment of KOZADAR Questionnaire respondents and unplanned outages to be matched.

It is recognized that the research presented addresses only the 1:1 relationships, vis-à-vis outage-and-owning-incident-manager, acknowledging that every outage on which conclusions are drawn are those for which only one incident manager was assigned. Moreover, it is acknowledged that, in many cases, there have been provided to the researcher outages which required greater than 12 hours to restore and that more than only one incident manager had responsibility and accountability for the restoration of its service. The exception of drawing conclusions about or otherwise providing investigative detail concerning the work and related causalities of any unplanned IT outage which equals X and number of involved incident managers equals Y is not addressed.

4.4.4. Tools

Completing the five steps detailed in Section 4.4.3, 1,336 incidents (63 percent of the number of unplanned outages provided by Pyrite) and their restoration times were analysed. Aligning the incident manager responsible for restoring service from specific unplanned outages, hierarchical moderated multiple regression testing was performed with MTRS as the dependent variable, the characteristics displayed as the independent variable and the approach-to-solving-problems used by incident managers who restored service from an unplanned outage as the moderating variable. The demographic data of age, tenure in the role of incident management, and education levels obtained from incident managers who completed the online survey were used as control variables.

The hierarchical moderated multiple regression test was performed in three steps. In Step One the control variables (age, tenure in role and education) were entered. In Step Two all the main effects represented by the independent variable (incident manager characteristics) and the moderator variables (problem-focused approach and solution-focused approach) were also submitted for analysis. In Step Three, all interaction effects were entered and the analysis performed. The interaction effects are referred to as moderation effects. The moderator function of the variable partitions a focal independent variable into subgroups that identify the areas of maximal effectiveness in regard to a given dependent variable. It is calculated by the independent variable and the moderator variable (the mathematical factors) being multiplied to provide a product (the mathematical output of multiplication) and then used to draw conclusions. Generally, a moderator variable affects the direction and/or strength of the relationship between an independent variable (the

characteristics, in this research) and a dependent variable (MTRS, in this research) (Baron & Kenny, 1986).

4.4.5. Method

This research was designed to determine if an incident manager can reduce the time taken to restore service when unplanned outages occur by the use of particular approaches to problem solving when displaying characteristics determined as important to individuals in the role. The following sections provide detail on how incident managers, their displayed characteristics, their use of particular problem solving approaches, and their attained MTRS values were analysed to test Hypothesis 6 (the use of a problem-focused approach or a solution-focused approach to restore service moderates the relationship between characteristics displayed by incident managers and their attained MTRS from an unplanned outage).

Reviewing all available data was necessary to align the unplanned outages and the incident manager responsible for restoring service from them. To determine the specific incident manager who handled a particular unplanned outage, a multi-step process was followed and data from three sources were used to establish incident managers as “owners” of unplanned outages. These sources include the Pyrite rosters, the unplanned outage investigated, and the responses to the KOZADAR Questionnaire.

The roster data was coded, as described in Section 4.3.3 and assignments were made identifying a specific, though anonymous, “owner” of each unplanned IT outage and the MTRS for those individuals, for each unplanned outage type. In all, 1,336 incidents were interrogated for which the restoration time was less than 12 hours, indicating a single incident manager was responsible for restoring service.

4.4.6. Procedure

In addition to unplanned outage data, the researcher was also provided the incident management roster used during the three-month period the unplanned outage data represented. The roster data provided the researcher the single piece of data that aligned responses to the KOZADAR Questionnaire to particular incident managers and particular incident managers to specific unplanned outages for which they attained the restoration of service.

Over the course of the four weeks that the questionnaire was available for completion, daily snapshots of the responses were taken to ensure that each new entry was assessed and a determination was made that the rostered incident manager was, or was not, the incident manager who submitted responses to the KOZADAR Questionnaire.

4.5. Summary

The main study was undertaken in two distinct components, each designed to test specific hypotheses. Component 1 tested hypotheses that addressed the characteristics displayed by incident managers, as well as the approaches they use to solve problems while working to restore service when unplanned outages occur. Component 2 aligned the characteristics and approach to solving problem solving information obtained and assessed the impact of the approach used to solve problems on the attained MTRS values attained by incident managers responsible for actually restoring service from the unplanned outage. Additionally, the available data allowed the study to be done on different types of unplanned outages that were reported and assess any impact the actual type has on the MTRS value attained.

Generous participation by two large, international organisations allowed data to be collected from professional incident managers and production unplanned outage data to be evaluated, ensuring the unplanned outages were experienced in a production environment and not in either a test or development environment. This ensured the unplanned outages were treated in a manner that accurately reflected their impact to the business that experienced them.

Chapter 5 : Main Study Results

The data obtained in the main study of this research included responses (N = 154) to the KOZADAR Questionnaire and is significant because it is the first study of its kind that presents findings about incident managers on data provided by incident managers, combined with data provided about the work those incident managers perform. In addition to demographic information, the data collected and analysed provided insights and answers to the research questions that prompted the instantiation of this work and the hypotheses explored during its execution. The results from the main study are presented here.

5.1 Demographic Information

A minimal set of demographic information was captured from respondents who participated in this research. This data was collected for two purposes. The first was to understand basic demographics information about the respondents. The second was to use this data as control variables in the hierarchical moderated multiple regression testing performed to accept or reject H₆, which states that the use of a problem-focused approach or a solution-focused approach to restore service moderates the relationship between characteristics displayed by incident managers and their attained MTRS from an unplanned outage. Findings from the investigations undertaken to accept or reject the six hypotheses tested in this research are discussed in the following sections.

Demographic information, including gender, age, marital status, level of education and tenure in the role of an incident manager were collected. It is noted that the data provided concerning marital status was eliminated from analysis, as the data provided proved to be insignificant. No summary of that data is provided in the demographic data reported here. All other demographic data is provided in the following sections.

5.1.1. Gender

The information provided in Table 5-1 indicates that 87% of the respondents are male. Females represent 13% of the respondents. Tests of homogeneity were performed on the data obtained, indicating the distribution of incident managers is equal across gender is accepted (Chi-square is 84.39; the p-value is 0.001).

Table 5-1.
Frequency: Gender

Gender	Frequency	Percentage
Male	134	87.0
Female	20	13.0
Total	154	100.0

5.1.2. Age

The information provided in Table 5-2 denotes that 38.3% of the respondents are at least 41 years of age, or older, suggesting greater than one third of the participants, likely, have many years of work experience in a professional work environment. Tests of homogeneity were performed on the data obtained, indicating the distribution of incident managers is equal across age is accepted (Chi-square is 41.89; the p-value is 0.001).

Table 5-2.
Frequency: Age

Age	Frequency	Percentage	Cumulative Percentage
21-30	34	22.0	22.0
31-40	61	39.6	61.6
41-50	51	33.1	94.7
51-60	8	5.2	99.9
Total	154	99.9	

5.1.3 Education Level Obtained

The information provided in Table 5-3 indicates that 48% of the respondents obtained, at least, undergraduate qualifications at university, indicating that nearly half of the respondents demonstrated the discipline required to complete a formal university program. Tests of homogeneity were performed on the data obtained, indicating the distribution of incident managers is equal across education levels is accepted (Chi-square is 87.09; the p-value is 0.001).

Table 5-3.
Frequency: Education

Education	Frequency	Percentage	Cumulative Percentage
Attended High School	12	7.8	7.8
Graduated High School	47	30.5	38.3
Attended University	21	13.6	51.9
Graduated University	57	37.0	88.9
Attended Post Graduate School	8	5.2	94.1
Graduated Post Graduate School	9	5.8	99.9
Total	154	99.9	

5.1.4 Tenure Working as an Incident Manager

The information provided in Table 5-4, denotes that 42.2% (N = 65) of the respondents have worked as incident managers for fewer than five years. Tests of homogeneity were performed on the data obtained indicating the distribution of incident managers is equal across Tenure Working as an Incident Manager is accepted (Chi-square is 23.71; the p-value is 0.001).

Table 5-4.
Frequency: Tenure Working as an Incident Manager

Tenure Working as an Incident Manager	Frequency	Percentage	Cumulative Percentage
Less than one year	26	16.9	16.9
1-5 years	63	40.9	57.8
6-10 years	39	25.3	83.1
11-15 years	26	16.9	100.0
Total	154	100.0	

5.3 Hypothesis Testing

Hypotheses were postulated by dividing the analyses in the main study into two components. Component 1 investigated the characteristics displayed by and the problem-solving approaches used by incident managers while working to restore service when unplanned outages occur. Component 2 investigated the characteristics displayed by and the MTRS attained by incident managers and any moderation of the MTRS due to the problem-solving approach used by incident managers. The results of both components investigated are described in the following sections.

5.3.1 Results from Component 1 of the Main Study

Four of the six hypotheses investigated in the main study were addressed in Component 1. The first four are cited here for ease of reference for the reader. H₁ states that incident managers display significantly different characteristics when they restore service from an unplanned outage. H₂ states that incident managers use different approaches to solving problems while they work to restore service when unplanned outages occur. H₃ states that there will be a significant relationship between the characteristics displayed by an incident manager and the use of a Solution-Focused Approach while working to restore service when unplanned outages occur. H₄ states that there will be a significant relationship between the characteristics displayed by an incident manager and the use of a Problem-Focused Approach while working to restore service when unplanned outages occur. Findings from the investigations undertaken to accept or reject these hypotheses are discussed in the following sections.

5.3.2.1. Characteristics Displayed

Weighted means testing and descriptive analysis, along with t-tests, were performed to examine Hypothesis 1 (incident managers display different characteristics when they restore service from an unplanned outage). The restoration of service from an unplanned outage is the core job function of an incident manager and this hypothesis tests whether a distinct characteristic, or set of characteristics, can be identified as being most likely to be displayed

by incident managers. Weighted means testing accounted for the different number of items presented in the KOZADAR Questionnaire for the seven characteristics investigated. Weighted means testing allowed a valid analysis to be performed on the responses from participants who submitted complete responses to the KOZADAR Questionnaire. Analysis indicated that although all seven characteristics were used, not all seven were always used or even likely to be used. Being facilitative and being decisive were identified as being most frequently used. Additionally, being pragmatic was identified as being least often used and, among characteristics cited as being preferred, was least preferred.

The results of an ANOVA analysis, based on means, rather than by, for example, pair wise comparison, presented in Table 5-5 aligns with the frequency results obtained and both confirm that Hypothesis 1 is accepted, as $p < 0.01$.

Table 5-5.
ANOVA Results of Incident Manager Characteristics

	Sum of Squares	DF	Mean Square	F-Value	P-Value
Between Groups	187.21	6.00	31.20	111.34	0.00
Within Groups	300.12	1071.00	0.28		
Total	487.33	1077.00			

Descriptive statistics provide a summary of the data obtained from the responses to the characteristics displayed by incident managers, collected from respondents to the items in the KOZADAR Questionnaire. See Table 5-6.

Table 5-6.
Descriptive Statistics: Characteristics Displayed

	N	Mean	Standard Deviation	Standard Error of Mean	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
Being Decisive	154	4.03	0.57	0.05	3.94	4.12	2.67	5.00
Being Entrepreneurial	154	3.25	0.48	0.04	3.17	3.32	2.17	4.50
Being Authoritative	154	3.03	0.51	0.04	2.95	3.11	2.00	4.67
Being Demanding	154	3.21	0.41	0.03	3.15	3.28	2.13	4.38
Being Pragmatic	154	2.97	0.64	0.05	2.87	3.07	1.00	5.00
Being Facilitative	154	4.05	0.57	0.05	3.96	4.14	2.75	5.00
Being Communicative	154	3.58	0.49	0.04	3.50	3.65	2.50	5.00

Figure 5-1, a box plot generated using SPSS™ Version 15, depicts that the means for the characteristics displayed by incident managers when restoring service from unplanned IT

outages are different. The rectangles in the middle of the box plot identify the mean of each characteristic and the two horizontal bars show the variation expected in that mean. The 95 percent confidence interval for mean confirms the means are different for each of the seven characteristics identified as significant characteristics displayed by incident managers.

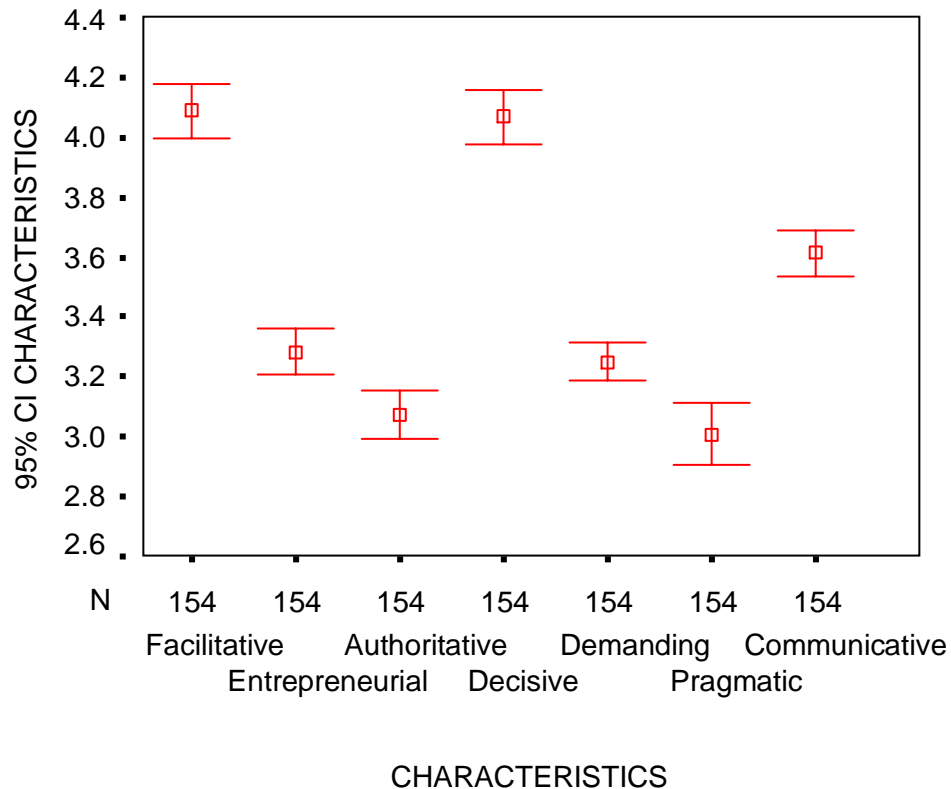


Figure 5-1. Ninety-five Percent Confidence Interval (Mean) for Characteristics Displayed by Incident Managers

5.3.2.2. Approaches Used by Incident Managers

Weighted means testing and descriptive analysis, along with independent samples t-tests were performed to examine Hypothesis 2 (incident managers use different approaches to solving problems while they work to restore service when unplanned outages occur) and identify whether incident managers use different types of problem-solving approaches when restoring service from an unplanned outage. Among the results from this research includes the finding that incident managers use either a problem-focused approach to solving problems or a solution-focused approach to solving problems (O’Callaghan & Mariappanadar, 2008).

The KOZADAR Questionnaire responses were subjected to analysis. The results of the ANOVA analysis, based on means, rather than by, for example, pair wise comparison, confirm that H₂, incident managers use different approaches to solving problems while they work to restore service when unplanned outages occur, is accepted, as p < 0.01. See Table 5-7.

Table 5-7.
ANOVA Results of Approaches-to-Solving-Problems Used by Incident Managers

	Sum of Squares	DF	Mean Square	F-Value	P-Value
Between Groups	54.843	4.00	13.711	15.223	0.00
Within Groups	134.202	149.00	0.901		
Total	189.045	153.00			

There are two approaches-to-problem-solving that could be identified as being used by incident managers when restoring unplanned outages. Incident managers reported using a problem-focused approach to problem solving more frequently than using a solution-focused approach to solving problems. Descriptive statistics provide a summary of the data obtained from the responses to the approach-to-solving-problems items in the KOZADAR Questionnaire. (See Table 5-8.)

Table 5-8.
Descriptive Statistics: Approaches-to-Solving-Problems

Problem Solving Approach	N	Mean	Standard Deviation	Standard Error of Mean	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
Problem-Focused	154	3.240	0.55	0.04	3.235	3.245	1.00	5.00
Solution-Focused	154	3.659	0.75	0.06	3.656	3.662	1.00	5.00

Analysis of the data from incident managers clearly identifies two different and distinct problem-solving approaches used when restoring service from an unplanned outage. These are the use of a problem-focused approach (N = 116) or a solution-focused approach (N = 38). Results from the t-test for Equality of Means (see Table 5-9) also confirm Hypothesis 2, incident managers use different approaches to solving problems while they work to restore service when unplanned outages occur, is accepted, as $p < 0.01$.

Table 5-9.
T-Test for Equality of Means

t-Value	DF	P-Value	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
					Lower	Upper
-5.60	306.00	0.00	-0.42	0.07	-0.57	-0.27

Figure 5-2, a box plot generated using SPSS™ Version 15, clearly depicts that the mean for a problem-focused approach to solving problems and that of a solution-focused approach to solving problems used by incident managers when restoring service from an unplanned IT outage is different. The rectangles in the middle of the box plot identify the mean of each approach and the two horizontal bars shows the variation expected in the mean. The 95% confidence interval for mean confirms the means for a problem-focus approach and a solution-focus approach are different.

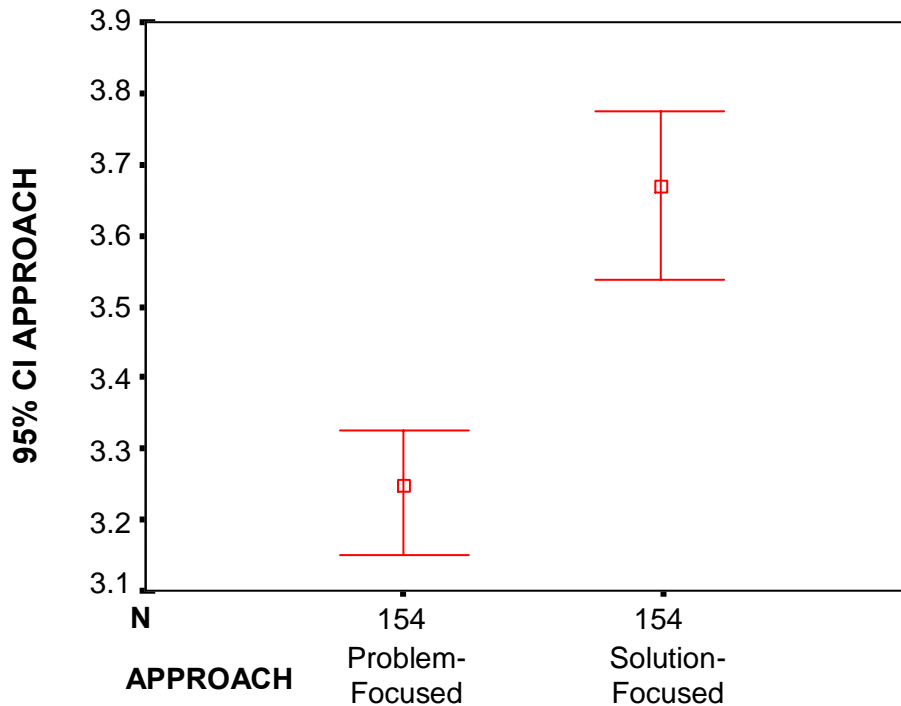


Figure 5-2. Ninety-five Percent Confidence Interval (Mean) for Types of Problem-Solving Approaches Preferred to Restore Service

5.3.2.3. *Characteristics and Solution-Focused Approach to Solving Problems*

H₃ states that there will be a significant relationship between the characteristics displayed by an incident manager and the use of a solution-focused approach to solving problems while working to restore service when unplanned outages occur. A hierarchical multiple regression analysis was performed to test this hypothesis. An ANOVA test was performed, run as part of the suite of tests processed when executing a hierarchical multiple regression test, using SPSS™ Version 15, to determine if there is a linear relationship between the characteristics displayed and the use of a solution-focused approach to restoring service when unplanned outages occur. It predicts that an individual using a solution-focused approach would display all investigated characteristics. The model summary, detailed in Table 5-10, identifies the

relationships between the various characteristics and a solution-focused approach to restoring service when unplanned outages occur. Ninety-one percent (R Square equals 0.915) of the variance in the solution-focused approach displayed can be predicted from the characteristics displayed.

Table 5-10.
Model Summary Output for Solution-Focused Approach

Model	N	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
						R Square Change	F Change	df1	df2	Sig. F Change
1 ^a	154	.957 ^b	.915	.866	.3543	.915	18.536	7	12	0.000

^a Model summary using data from all respondents. ^b Predictors: (constant), Being Communicative, Being Authoritative, Being Pragmatic, Being Facilitative, Being Demanding, Being Entrepreneurial, Being Decisive

Descriptive data (See Table 5-11) describes the basic features associated with incident managers who use a solution-focused approach to solving problems and the characteristics they display obtained during this study. The results show a mean of 15.79, with a range of 5.94 through 25.69.

Table 5-11.
Characteristics and the Use of a Solution-Focused Approach to Problem Solving

	N	Mean	Standard Deviation
Solution-Focused Approach	154	07.31	1.493
Being Decisive	154	12.09	1.708
Being Entrepreneurial	154	19.47	2.899
Being Authoritative	154	18.19	3.057
Being Demanding	154	25.69	3.284
Being Pragmatic	154	05.94	1.274
Being Facilitative	154	16.20	2.299
Being Communicative	154	21.45	2.933

A univariate analysis (N = 154) shows that the characteristics Being Communicative, Being Authoritative and Being Decisive are significant predictors of the use of a solution-focused approach to solving problems. Of these, however, Being Communicative accounts for 96.6 percent of variation (β is 0.966, significance is .001), Being Authoritative accounts for 77.3 percent of variation (β is .0773, significance is .001) and Being Decisive accounts for 71.7 percent of variation (β is 0.717, significance is .001). Being Communicative (significance is .000) is identified as the most highly predicted characteristic to be displayed when using a solution-focused approach to problem solving. Moreover, one additional

characteristic is identified as being significant (with $p \leq 0.05$), that is, Being Facilitative (significance is .000). The significance of each of these four characteristics, therefore, indicates that they are not identified by chance as predictors of the use of a solution-focused approach to solving problems by incident managers. Hypothesis 3, there is a relationship between the characteristics displayed by an incident manager and the use of a solution-focused approach while working to restore service when unplanned outages occur, is accepted with $p \leq 0.001$. (See Table 5-12.)

Table 5-12.
Characteristic (DEAD PFC) Coefficients Solution-Focused Approach

	Unstandardised Coefficients		Standardised Coefficients	t	Sig.
	B	Std. Error	(β) Beta		
(Constant)	17.300	1.558		11.106	0.000
Being Decisive	0.548	0.132	0.717	1.143	0.001**
Being Entrepreneurial	-0.006	0.048	-0.019	-0.122	0.905
Being Authoritative	-0.228	0.050	-0.773	-4.575	0.001**
Being Demanding	-0.108	0.052	-0.273	-2.081	0.059
Being Pragmatic	0.206	0.096	0.262	2.146	0.053
Being Facilitative	-0.415	0.082	-0.549	-5.031	0.000***
Being Communicative	0.420	0.051	0.966	8.245	0.000***

** $p \leq 0.001$

*** $p = 0.000$

5.3.2.4. Characteristics and Problem-Focused Approach to Solving Problems

H₄ states that there is a significant relationship between the characteristics displayed by an incident manager and the use of a problem-focused approach to problem solving while working to restore service when unplanned outages occur. A hierarchical multiple regression analysis was performed to test this hypothesis. ANOVA was used to examine if there is a linear relationship between the characteristics displayed and the use of a problem-focused approach to restoring service when unplanned outages occur. It predicts that an individual using a problem-focused approach displays all investigated characteristics. The model summary identifies the relationships between the various characteristics and a problem-focused approach to restoring service when unplanned outages occur. Twenty-four percent (R^2 equals 0.240) of the variance in the problem-focused approach displayed was predicted from the characteristics displayed. (See Table 5-13.)

Table 5-13.
Model Summary Output for Problem-Focused Approach

Change Statistics										
Model	N	R	R ²	Adjusted R ²	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change
1 ^a	154	.490 ^b	.240	.203	2.45446	.240	6.573	7	146	0.000

^a Model summary using data from all respondents. ^b Predictors: (constant), Being Communicative, Being Demanding, Being Pragmatic, Being Decisive, Being Facilitative, Being Authoritative, Being Entrepreneurial

Descriptive data (see Table 5-14) depicts the basic features associated with incident managers who use a problem-focused approach to solving problems and the characteristics they displayed in this study. The results show a mean of 16.90, with a range of 5.94 through 25.69.

Table 5-14.
Characteristics and the Use of a Problem-Focused Approach

	N	Mean	Standard Deviation
Problem-Focused Approach	154	16.20	2.749
Being Decisive	154	12.09	1.708
Being Entrepreneurial	154	19.47	2.899
Being Authoritative	154	18.19	3.057
Being Demanding	154	25.69	3.284
Being Pragmatic	154	5.94	1.274
Being Facilitative	154	16.20	2.299
Being Communicative	154	21.45	2.933

The results from the ANOVA (N = 154) showed that the characteristic Being Pragmatic is a significant predictor of the use of a problem-focused approach to solving problems. Being Pragmatic accounted for 36 percent of the variance seen (β 0.360, significance is 0.000). This indicates Being Pragmatic and using a problem-focused approach to solving problems is not identified by chance (with $p < 0.001$). Hypothesis 4, which postulated that there is a relationship between the characteristics displayed by an incident manager and the use of a problem-focused approach while working to restore service when unplanned outages occur, is accepted with $p < 0.001$. (See Table 5-15.)

Table 5-15.
Characteristic (DEAD PFC) Coefficients Problem-Focused Approach

	Unstandardised Coefficients		Standardised Coefficients	t	Sig.
	B	Std. Error	(β) Beta		
(Constant)	8.584	2.595		3.308	0.001**
Being Decisive	0.139	0.092	0.116	1.510	0.133
Being Entrepreneurial	0.013	0.080	0.014	0.167	0.867
Being Authoritative	-0.192	0.071	-0.213	-2.688	0.008
Being Demanding	-0.352	0.129	-0.218	-2.735	0.007
Being Pragmatic	0.302	0.071	0.360	4.255	0.000***
Being Facilitative	0.164	0.168	0.076	0.978	0.330
Being Communicative	0.192	0.076	0.205	2.521	0.013

** p < = 0.001 *** p = 0.000

5.3.2 Results from Component 2 of the Main Study

Two of the six hypotheses investigated in the main study were addressed in Component 2. These are cited here for ease of reference for the reader. H₅ states that there will be a significant difference between unplanned outage types and their MTRS. H₆ states that the use of a Problem-Focused Approach or a Solution-Focused Approach to restore service will moderate the relationship between characteristics displayed by incident managers and their attained MTRS from an unplanned outage. Findings from the investigations undertaken to accept or reject these hypotheses are discussed in the following sections.

5.3.2.1. Outage Types and MTRS

Pyrite provided data on a total of 2,122 unplanned outage incidents to the researcher. Of these, a total of 85 incidents (four percent of those provided) were eliminated from the total analysed for one of four reasons. One reason incidents were eliminated was when the incident number provided was not unique. This indicated that duplicate instances of the same incident were sent. A review of each of those items for which duplicate incident numbers were identified confirmed that the data associated with duplicate incident numbers were, in fact, duplicate instances of the same incident. Only the duplicate incidents were eliminated. A single instance of the incident was retained and the duplicate incidents (N = 42) were eliminated from the data analysed. A second reason incidents were eliminated was because the severity of the incident was not identified (N = 26). The severity of the incident was a required field (as indicated in Table 4-3). Thirdly, incidents that were not completed or not closed and had no valid “close date” or no valid “close time” were eliminated (N = 16) from data analysis because the incident had not been reported as restored. Given that no restoration date or restoration time was provided, no valuable restoration data could be obtained from the incident information provided. The final reason an unplanned outage

provided by Pyrite was not included in the analysis performed was that, although it met all the criteria required for analysis, there was only one report of a Systems Overload unplanned outage. It was eliminated because of inadequate data. Although a total of 85 of the incidents provided by Pyrite were eliminated from those analysed, 95.99 percent (N = 2,036) of the unplanned outage data provided by Pyrite was used and analysed.

Of those 2,036 unplanned outages, all were viable and used in the data analysis performed on the unplanned outage data provided by Pyrite. In total, there were 950 unplanned Hardware outages (46.6 percent of those incidents analysed), 139 unplanned Humans Inside the Affected Company outages (6.8 percent of those incidents analysed), and 947 unplanned Software outages (46.5 percent of those incidents analysed).

Of the seven possible types of outages (Acts of Nature, Hardware, Humans Inside the Affected Company, Humans Outside the Affected Company, Software, System Overload, and Vandalism) that could have been included in the inventory of unplanned outages analysed, only four types of those outages were actually included. There were no reports of unplanned outages due to Acts of Nature; there were no reports of unplanned outages due to Humans Outside the Affected Company; there were no reports of unplanned outages due to Vandalism. Moreover, there was only one System Overload unplanned outage reported, representing only 0.0005 percent of the unplanned outages provided by Pyrite; it was eliminated from the data analysed. A descriptive analysis performed on the unplanned outage data that was included in the researcher's analysis to establish initial information about the data is depicted in Table 5-16.

Table 5-16.
Descriptive Analysis – Unplanned Outage Types

	N	Mean (in mins)	Standard Deviation	Min	Max	Median	MTRS (in days)
Hardware	950	1624.33	6603.90	0.77	108068.00	98.92	1.13
Humans Inside Affected Company	139	1214.77	3941.71	1.00	29523.48	13.00	0.84
Software	947	3037.63	7500.79	1.15	65110.80	285.40	2.11
Total Unplanned Outages	2036	2253.73	6934.70	0.77	108068.00	136.83	1.56

To determine the acceptability of Hypothesis 5, that there will be a significant difference between unplanned outage types and their Mean Times to Restore Service, further analysis was undertaken. A Kruskal-Wallis test was performed on the unplanned outage data

provided by Pyrite to determine if statistically significant differences could be found between the unplanned outage types and the MTRS attained. This non-parametric test is based on the assumption that the population tested is not normally distributed; however, it does assume an identically shaped and scaled distribution for each group. It is, effectively, ANOVA for testing the equality of population medians among groups (with data replaced by ranks). Results of the Kruskal-Wallis test are shown in Table 5-17.

Table 5-17.
Kruskal-Wallis Test: Unplanned Outage Types and Associated MTRS

Unplanned Outage Type		N	Mean Rank
MTRS	Hardware	950	930.81
	Humans Inside the Affected Company	139	643.04
	Software	947	1161.58
	Total Number of Unplanned Outages	2036	
Chi-Square	133.92		
DF	2.00		
P-Value	0.00		

Hypothesis 5, there is a significant difference between unplanned outage types and their Mean Times to Restore service, with a p value of < 0.01, is accepted.

Further testing was conducted to determine the relationships between individual outage types and their respective Mean Times to Restore Service. The Kolmogorov-Smirnov test was performed for the pairs Hardware-Software, Hardware-Humans Inside the Affected Company, and Software-Humans Inside the Affected Company. Hypothesis 5 is accepted, as each of the p values is < 0.01. (See Tables 5-18, 5-19, and 5-20, respectively.)

Table 5-18.
Kolmogorov-Smirnov Test: Unplanned Hardware-Software Outages and Associated MTRS

Unplanned Outage ^a Type		N
MTRS	Hardware	950
	Software	947
	Total Number of Unplanned Outages of these types	1897
TEST	Kolmogorov-Smirnov	3.85
P-Value		0.00

^a Grouping Variable: Unplanned Outage Type

Table 5-19.

Kolmogorov-Smirnov Test: Unplanned Hardware-Humans-In-the-Affected-Company Outages and Associated MTRS

Unplanned Outage ^a Type		N
MTRS	Hardware	950
	Human Inside Affected Company	139
	Total Number of Unplanned Outages of these types	1089
TEST	Kolmogorov-Smirnov	4.44
P-Value		0.00

^a Grouping Variable: Unplanned Outage Type

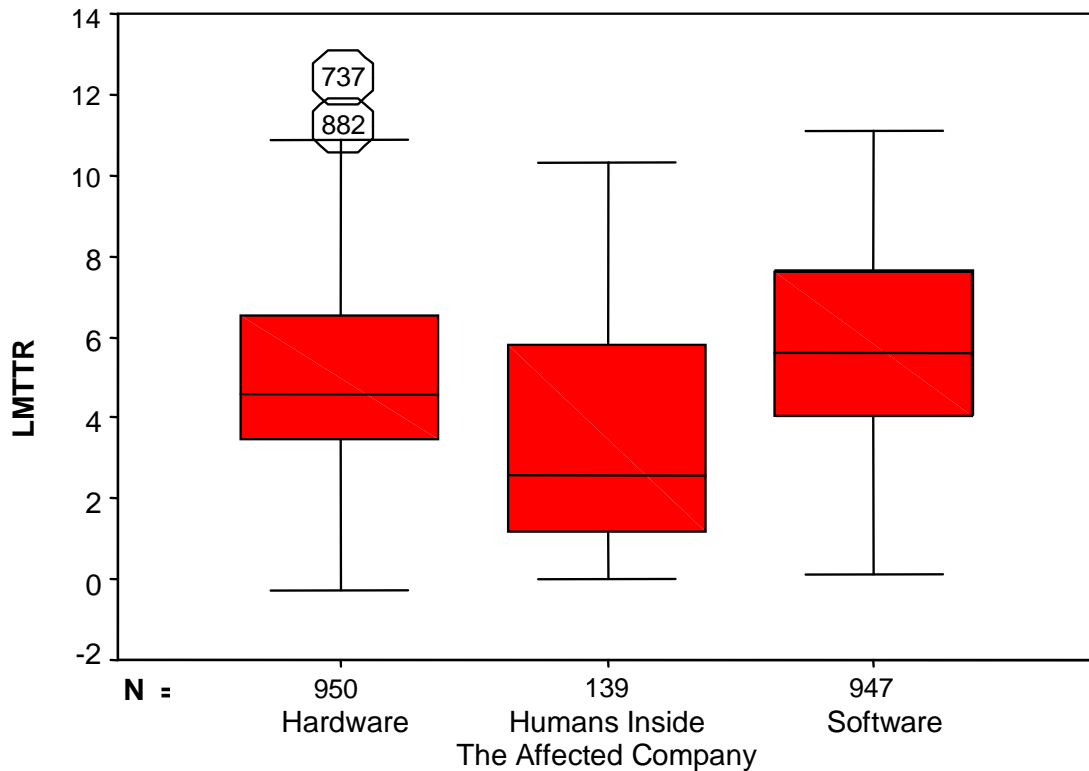
Table 5-20.

Kolmogorov-Smirnov Test: Unplanned Software- Humans-Inside-the-Affected-Company Outages and Associated MTRS

Unplanned Outage ^a Type		N
MTRS	Software	947
	Human Inside Affected Company	139
	Total Number of Unplanned Outages of these types	1086
TEST	Kolmogorov-Smirnov	5.08
P-Value		0.00

^a Grouping Variable: Unplanned Outage Type

Figure 5-3, a box plot generated using SPSS™ Version 15, displaying a five-value summary of the distribution, depicts the horizontal line in each box as the median value of the attained MTRS value. The horizontal lines below and above the medians are the 25th and 75th percentile values, respectively. The two whiskers at the bottom and top are the minimum and maximum values of the distribution. The extreme outliers are shown above the top whisker. An analysis of the box and whisker plot clearly demonstrates that the median values of the MTRS for different types of unplanned outages analysed in this research were different from one another.



UNPLANNED OUTAGE TYPES REPORTED IN THIS RESEARCH

Figure 5-3. Box and Whisker Plots Display the Relationship Between Unplanned Outage Types and Their Associated Mean Times to Restore Service. (The Natural Logarithm of the MTRS is shown in the Y-Axis of the scale.)

5.3.2.2. Characteristics, Approaches, Hardware, MTRS

Prior to undertaking an analysis intended to provide information to know whether to accept or reject H_6 , which states that the use of a problem-focused approach or a solution-focused approach to restore service will moderate the relationship between characteristics displayed by incident managers and their attained MTRS from an unplanned outage, an analysis of each unplanned outage type was performed in relation to the characteristics displayed by incident managers and the approach to solving problems that they use. In this section, the association with unplanned hardware outages is presented.

Analysis of the available unplanned hardware outages reported (N = 950 outages) showed that 10 distinct subsets were identified. A descriptive analysis of the data of hardware unplanned outage subsets is shown in Table 5-21.

Table 5-21.
Unplanned Hardware Outage Subsets and Respective MTRS

Hardware Unplanned Outage Subset	Number of Reported Occurrences	Percentage of Reported Occurrences	MTRS (days)	MTRS (hours)
Cable Failure	1	0.11	7.88	189.12
Hardware Error	65	6.84	3.22	77.28
Network Error	10	1.05	19.20	460.80
Power Failure	9	0.95	1.06	25.44
Printer Error	10	1.05	0.35	8.40
Router Failure	83	8.74	1.32	31.40
Server Down	18	1.89	25.14	603.36
Server Error	365	38.42	1.70	40.80
Storage Device Error	208	21.89	1.70	40.80
Switch Failure	181	19.05	0.52	12.48
TOTAL	950			

It is noted that the superset Hardware Outages has within its subsets, among others, Hardware Error. This subset is included because the specific nature of the hardware error reported could not be further delineated as to being an alternate subset of hardware outage or, if it was, details were not provided to the researcher in the information provided by Pyrite. The data clearly indicated the outage type was hardware and that the subset type was also hardware; however, no data was available to identify further the type of hardware to which the error could be aligned. Insofar as the subset hardware error represents nearly seven percent of the hardware outages included, it was decided not to eliminate it, but include it and refer to hardware outages as the superset and hardware errors as a subset of that superset.

The combined subsets of cable failure, network error, power failure, and printer errors total less than three percent (N = 60) of the total number of unplanned hardware outages reported (N = 950 outages). Additionally, the hardware outage subsets of MTRS values range from 0.35 days to 25.14 days; the overall hardware outage MTRS is 1.13 days.

Moreover, server down unplanned outages caused fewer than two percent (N = 18) of the actual number of unplanned hardware outages (N = 950 outages), yet, the MTRS to recover server down unplanned outages required 40% of all MTRS service restoration times for hardware outages. MTRS values for each of the unplanned server down unplanned outages that were reported are listed in Table 5-22.

Table 5-22.
MTRS for Individual Server Down Unplanned Hardware Outages

Server Down Incident #	MTRS (days)	MTRS (hours)
1	0.002	0.048
2	0.010	0.240
3	0.073	1.752
4	0.085	2.040
5	0.098	2.352
6	0.419	10.056
7	7.855	188.520
8	12.061	289.464
9	13.697	328.728
10	14.177	340.248
11	16.187	388.488
12	24.774	594.576
13	34.961	839.064
14	38.922	934.128
15	48.684	1,168.416
16	57.928	1,390.272
17	68.091	1,634.184
18	114.517	2,748.408

Of the 18 server-down unplanned outages reported, 33 percent (six) were restored in less than one day; all others took from in excess of seven days to greater than three months to restore. The data shows that the hardware subset of server down unplanned outages requires significant durations of time to restore service. The data indicates server down unplanned outages can be quickly restored (from less than 30 minutes to just greater than ten hours) or can require months to restore.

Of the total unplanned hardware outages (N = 950 outages) provided to the researcher by Pyrite for analysis, 75 percent (N = 709 outages) had three common traits. First, the 709 had a restoration time of less than 12 hours; second, the 709 had only a single incident manager responsible for the restoration of service (indicating that the outage did not extend so significantly across the boundary of two 12-hour shifts that more than one incident manager ever handled the restoration of service from the unplanned outage); and third, the 709 outages could be successfully identified as having been worked by a specific incident manager whose responses to the KOZADAR Questionnaire were available and able to be identified as the response from the restoring incident manager. This allowed for an analysis of nearly 75 percent of the unplanned hardware outages reported and the relationship to be established between the owning incident managers, the characteristics displayed, the preferred approach to solving problems, and the duration of the outage. Of the ten subsets of unplanned outages that belong to the superset Hardware, only six subsets existed within the 709 unplanned hardware outages analysed for which an owning incident manager could be

identified. Those omitted include cable failures, router failures, switch failures and server down (as opposed to server errors). Table 5-23 identifies the number of hardware outage subset incidents for which the owning incident manager's responses to the KOZADAR Questionnaire could be paired.

Table 5-23.
Unplanned Hardware Outage Subsets for Which the Owing Incident Managers Could Be Identified

Hardware Outage Subset	Number of Reported Occurrences
Cable Failure	0
Hardware Error	35
Network Error	197
Power Failure	4
Printer Error	9
Router Failure	0
Server Down	0
Server Error	308
Storage	156
Switch Failure	0
TOTAL	709

5.3.2.3. Characteristics, Approaches, Humans, MTRS

Prior to undertaking an analysis that would provide information to know whether to accept or reject H_6 , the use of a Problem-Focused Approach or a Solution-Focused Approach to restore service will moderate the relationship between characteristics displayed by incident managers and their attained MTRS from an unplanned outage, an investigation into each unplanned outage type needed to be performed in relation to the characteristics displayed by incident managers and the approach to solving problems that they use. In this section, their association with unplanned Humans Inside the Affected Company outages was investigated.

Analysis of the available unplanned outages that were caused by human beings within the corporation that experienced the unplanned outage reported (N = 139 outages) revealed distinct occurrences of this outage type. Analysis of the data showed that five distinct subsets were identified; these included Documentation, No Error Found, Process Failure, Security Failure, and User Error.

While the total of documentation errors are attributed to only three percent (N = 4 outages) of the unplanned outages caused by human beings inside the affected company (N = 139 outages), they are included as one of the five subsets of outage types that, combined, are identified as outages caused by human beings inside the affected company. The alternative to combine them with errors of the subset User Error was rejected, as the documentation errors were clearly identified as the specific issue that caused the unplanned

outage, whereas, the subset User Error was unable to be further broken down into identifiable components of outage subsets. A descriptive analysis of the data of these unplanned outage human-beings-inside-the-affected-company types is shown in Table 5-24:

Table 5-24.
Unplanned Outage Subsets When Human Beings Inside the Affected Company are Identified as Causing the Unplanned Outage and Respective MTRS Values Attained

Humans Inside Unplanned Outage Subset	Number of Reported Occurrences	Percentage of Reported Occurrences	MTRS (days)	MTRS (hours)
Documentation	4	2.87	4.20	100.80
No Error Found	35	25.18	0.23	5.52
Process Failure	17	12.23	32.06	769.44
Security	65	46.76	8.87	212.88
User Error	18	12.95	2.25	54.00
TOTAL	139			

Although process errors caused a greater number of unplanned outages than any other of the type human-beings-inside-the-affected-company reported, their duration was approximately one-fourth (1/4) the duration of those caused by the subset “security”. Moreover, while MTRS attainment for the subsets of outages caused by human-beings-inside-the-affected-company ranges from 0.23 days to 32.06 days; the overall MTRS for the outage type human-beings-inside-the-affected-company is 0.84 days.

Of the 139 unplanned outages (determined to have been the result of errors performed by human-beings-inside-the-affected-company) that were provided to the researcher by Pyrite for analysis, 30 had three significant characteristics. Firstly, the 30 had a restoration time of less than 12 hours; secondly, the 30 had only a single incident manager responsible for the restoration of service (indicating that the outage did not extend so significantly across the boundary of two 12-hour shifts that more than one incident manager ever handled the restoration of service from the unplanned outage); and thirdly, the 30 outages could be successfully identified as having been worked by a specific incident manager whose survey results were available and able to be identified as the response from the restoring incident manager. This allowed for further analysis of 21 percent of the unplanned outages reported that were the result of human-beings-inside-the-affected-company.

Of the five subsets of unplanned outages that belong to the superset, henceforth referred to, simply, as ‘Humans Inside’, only two subsets existed within the 30 unplanned Humans Inside outages that were available to be analysed. Those omitted include documentation, no error found, and process failures. Of the two subsets reported for which specific incident managers could be associated as having restored the service for them, 46 percent were of

the subset security and 54 percent were of the subset user errors. The quantity of the Humans Inside unplanned outage subsets incidents analysed is provided in Table 5-25.

Table 5-25.
Unplanned Humans-In Outage Subsets and Occurrences of Each

Humans Inside Unplanned Outage Subset	Number of Reported Occurrences
Documentation	0
No Error Found	0
Process Failure	0
Security	16
User Error	14
TOTAL	30

5.3.2.4. **Characteristics, Approaches, Software, MTRS**

Prior to undertaking an analysis that would provide information to know whether to accept or reject H_6 , which states that the use of a Problem-Focused Approach or a Solution-Focused Approach to restore service will moderate the relationship between characteristics displayed by incident managers and their attained MTRS from an unplanned outage, an investigation into each unplanned outage type needed to be performed in relation to the characteristics displayed by incident managers and the approach to solving problems that they use. In this section, their association with unplanned Software outages was investigated.

Analysis of the available unplanned software outages reported (N = 947 outages) showed that four distinct subsets were identified. The four subsets, and the number of occurrences of each, which were provided by Pyrite for the researcher to analyse are presented in Table 5-26:

Table 5-26.
Unplanned Software Outage Subsets and Occurrences of Each

Subset of Unplanned Software Outages	N
Application	477
Database	84
Operating System	13
Software Error	373
TOTAL	947

It is noted that the superset Software Unplanned Outages has within its subsets Software Error. This subset is included because the specific nature of the software error reported could not be further delineated as to being a particular type of software error or, if it was, that detail was not provided to the researcher in the information provided by Pyrite. The data clearly indicated the outage type was software and that the subset type was software error;

however, no data was available to identify further the type of software outage to which the error could be aligned. Insofar as the subset software error represents nearly 40 percent of the software outages included, it was decided not to eliminate it, but include it and refer to software outages as the superset and software errors as a subset of that superset.

While the total of operating system unplanned outages total only one percent (1%) of the unplanned software outages reported, they are included as one of the four subsets of outage types that, combined, total all reported unplanned software outages. The alternative to combine them with errors of the subset software errors was rejected, as the operating system errors were clearly identified as the issue that caused the unplanned outage. Alternately, the subset software error was unable to be further broken down into identifiable components of outage subsets.

Each unplanned software outage subset has a calculated MTRS. Each is detailed in Table 5-27.

Table 5-27.
Unplanned Software Outage Subsets and Respective MTRS

Software Unplanned Outage Subset	Number of Reported Occurrences	Percentage of Reported Occurrences	MTRS (days)	MTRS (hours)
Application	477	50.37	23.87	572.88
Database	84	8.87	2.77	66.48
Operating System	13	1.37	6.57	157.68
Software Error	373	39.39	1.25	30.00

Though the software subset MTRS values range from 1.25 days to 23.87 days, the overall software MTRS is 2.11 days. Of the 947 unplanned software outages that were provided to the researcher by Pyrite for analysis, 597 had three significant characteristics. Firstly, the 597 had a restoration time of less than 12 hours; secondly, the 597 had only a single incident manager responsible for the restoration of service (indicating that the outage did not extend so significantly across the boundary of two 12-hour shifts that more than one incident manager ever handled the restoration of service from the unplanned outage); and thirdly, the 597 outages could be successfully identified as having been worked by a specific incident manager whose survey results were available and able to be identified as the response from the restoring incident manager. This allowed for an analysis of 63 percent of the unplanned software outages provided to the researcher for analysis.

Of the four subsets of unplanned outages that belong to the superset, Software, instances of all four exist among the 597 unplanned software outages that were available to be analysed. The MTRS attained for each of the four subsets of software outages indicates that the maximum difference in the time taken to restore the service lost when the unplanned

software outage occurred is only nine percent. The quantity of the software unplanned outage subsets incidents are provided in Table 5-28.

Table 5-28.
Unplanned Software Outage Subsets and Quantity of Outages

Software Unplanned Outage Subset	Number of Reported Occurrences
Application	263
Database	54
Operating System	12
Software Error	268
TOTAL	597

5.3.2.5. Moderating Effect of Approach

In order to test Hypothesis 6 (the use of a Problem-Focused Approach or a Solution-Focused Approach to restore service will moderate the relationship between characteristics displayed by incident managers and their attained MTRS from an unplanned outage), hierarchical moderated multiple regression testing was performed with MTRS as the dependent variable, the characteristics displayed as the independent variable and the approach-to-solving-problems used by incident managers who restore service from an unplanned outage as the moderating variable. The demographic data of Age, Tenure in the Role of Incident Management, and Education were used as control variables.

The hierarchical moderated multiple regression test was performed in three steps. In Step One the control variables (Age, Tenure in Role and Education) were entered. In Step Two all the main effects represented by the Independent Variable (Incident Manager Characteristics) and the Moderator Variables (Problem-Focused Approach and Solution-Focused Approach) were also submitted for analysis. In Step Three, all interaction effects were entered and the analysis performed. The interaction effects are referred to as moderation effects. The moderator function of the variable separates a focal independent variable into subgroups that identify the areas of maximal effectiveness in regard to a given dependent variable. It is calculated by the independent variable and the moderator variable (the mathematical factors) being multiplied to provide a product (the mathematical output of multiplication) and then used to draw conclusions. Generally, a moderator variable affects the direction and/or strength of the relationship between an independent variable (the characteristics, in this research) and the dependent variable (MTRS, in this research) (Baron & Kenny, 1986). The model of the moderator variable's affect on the dependent variable is shown in Figure 5-4:

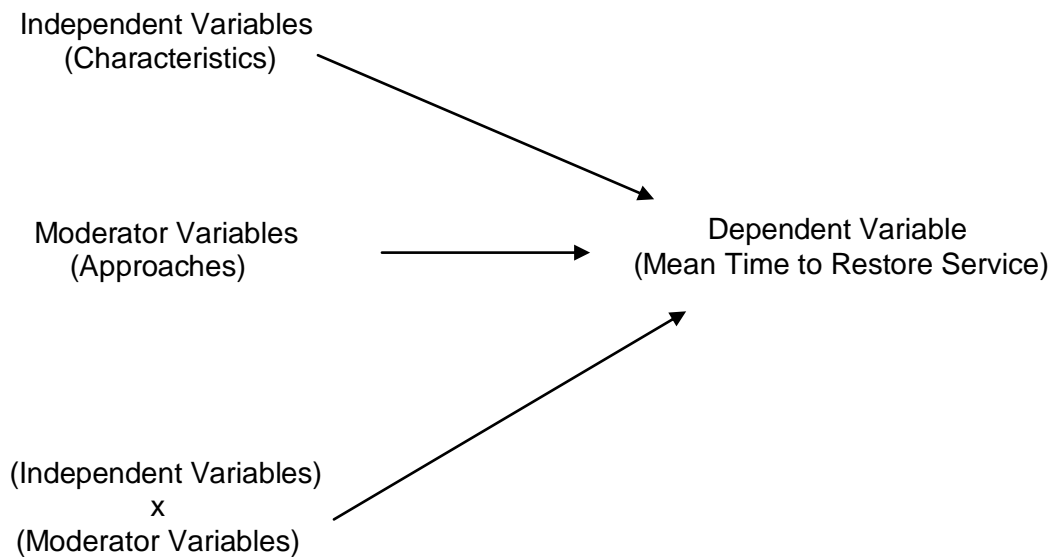


Figure 5-4. Moderator Variables Model (Baron & Kenny, 1986)

Using SPSS™ Version 15, descriptive statistics were produced and are listed in Table 5-29. This data includes the mean and standard deviations for each demographic variable, each characteristic, the approach used to restore service, and the dependent variable. The moderation effects have been computed as products of the independent variable (characteristics) and the moderator variable (approach-to-solving-problems).

Table 5-29.
Descriptive Statistics

	Mean	Standard Deviation	
MTRS	133.963	61.91847	
Age	27.65 years	0.7769	
Time in Role	14.2 years	0.9075	
Education where:			
1 = Attended High School			
2 = Graduated High School			
3 = Attended University	3.167	1.3112	
4 = Graduated University			
5 = Attend Post Graduate School			
6 = Graduated Post Graduate School			
Decisive	3.9420	0.62692	
Entrepreneurial	3.1546	0.48390	
Authoritative	2.9882	0.46453	
Demanding	3.1469	0.40817	
Pragmatic	2.9740	0.58656	
Facilitative	3.9219	0.55880	
Communicative	3.4185	0.44461	
Problem-Focused Approach	3.3271	0.54916	
Solution-Focused Approach	3.5313	0.71012	
(Decisive) *	(Problem Focused)	0.0129	0.34935
(Entrepreneurial) *	(Problem Focused)	0.5980	0.29798
(Authoritative) *	(Problem Focused)	0.0289	0.32174
(Demanding) *	(Problem Focused)	0.0991	0.17859
(Pragmatic) *	(Problem Focused)	-0.0099	0.32329
(Facilitative) *	(Problem Focused)	0.0038	0.33324
(Communicative) *	(Problem Focused)	0.0636	0.26698
(Decisive) *	(Solution Focused)	0.2407	0.51805
(Entrepreneurial) *	(Solution Focused)	-0.0513	0.47356
(Authoritative) *	(Solution Focused)	0.1056	0.36565
(Demanding) *	(Solution Focused)	-0.0243	0.25961
(Pragmatic) *	(Solution Focused)	0.0069	0.53212
(Facilitative) *	(Solution Focused)	-0.0018	0.35624
(Communicative) *	(Solution Focused)	0.0605	0.26061

After completing Steps 1, 2, and 3, cited previously, the moderation effects (Baron & Kenny, 1986) were computed as products of the independent and moderator variables. The F-value in the third step illustrates the significance of the regression model that represents the moderation effects. A significant increase of R² (Cohen & Cohen, 1983) in the third step indicates the presence of moderation effects (Youndt, Snell, Dean, & Lepak, 1996). The results from the hierarchical moderated multiple regression tests, detailed in Table 5-30, confirm that the approach used by incident managers when restoring service from an

unplanned outage can have a positive moderating effect on the MTRS attained. Additionally, the combination of displaying an authoritative characteristic and using a solution-focused approach provides the only statistically significant decrease in the MTRS attained by incident managers. The moderating effect identified in the summary model is found in both the significant increment of R² (Cohen & Cohen, 1983) identified in Step 3, which, in turn, indicates the presence of moderation effects (Youndt et al., 1996), with a p-value < 0.01 and statistical significance.

Table 5-30.

Characteristics, Approaches, and MTRS → Being Authoritative and Solution-Focused Approach Provide the Best Results

Predictors	MTRS Dependent Variable								
	Step 1			Step 2			Step 3		
	Beta	t-value	P-value	Beta	t-value	P-value	Beta	t-value	P-value
Age	-0.08	-0.59	0.55	-0.13	-0.86	0.39	-0.14	-0.60	0.55
Time in Role	0.00	0.02	0.99	0.05	0.28	0.78	-0.13	-0.55	0.58
Education	0.21	2.02	0.05	0.23	1.90	0.06	0.29	1.60	0.11
Being Facilitative				-0.11	-0.87	0.39	-0.07	-0.51	0.61
Being Entrepreneurial				-0.03	-0.19	0.85	0.04	0.25	0.80
Being Authoritative				-0.01	-0.06	0.95	-0.17	-1.28	0.21
Being Decisive				0.00	-0.03	0.98	0.15	0.81	0.42
Being Demanding				0.03	0.24	0.81	0.04	0.16	0.88
Being Pragmatic				0.10	0.84	0.41	0.07	0.37	0.71
Being Communicative				-0.04	-0.32	0.75	0.06	0.35	0.73
Problem-Focused Approach				0.07	0.55	0.59	0.33	1.85	0.07
Solution-Focused Approach				-0.01	-0.06	0.95	-0.23	-0.80	0.43
Being Facilitative			* Problem-Focused Approach				-0.07	-0.34	0.74
Being Entrepreneurial			* Problem-Focused Approach				-0.41	-1.17	0.25
Being Authoritative			* Problem-Focused Approach				-0.41	-1.45	0.15
Being Decisive			* Problem-Focused Approach				0.32	1.46	0.15
Being Demanding			* Problem-Focused Approach				0.31	1.34	0.18
Being Pragmatic			* Problem-Focused Approach				0.15	0.57	0.57
Being Communicative			* Problem-Focused Approach				0.02	0.07	0.94
Being Facilitative			* Solution-Focused Approach				0.18	0.71	0.48

Table 5-30.

Characteristics, Approaches, and MTRS → Being Authoritative and Solution-Focused Approach Provide the Best Results

Predictors	MTRS Dependent Variable								
	Step 1			Step 2			Step 3		
	Beta	t-value	P-value	Beta	t-value	P-value	Beta	t-value	P-value
Being Entrepreneurial * Solution-Focused Approach							0.04	0.10	0.92
Being Authoritative * Solution-Focused Approach							-0.63	-2.56	0.01*
Being Decisive * Solution-Focused Approach							0.26	0.89	0.38
Being Demanding * Solution-Focused Approach							-0.42	-1.30	0.20
Being Pragmatic * Solution-Focused Approach							0.41	1.52	0.13
Being Communicative * Solution-Focused Approach							-0.31	-1.23	0.22
R ²		0.053			0.081			0.393	
R ² Change					0.028			0.312	
F-Value		1.718			0.281			2.530	
P-Value		0.169			0.978			0.006*	

* value is <= 0.01 and is statistically significant

The conclusion to be drawn, therefore, is that the characteristics displayed by incident managers when restoring service from an unplanned outage is significantly moderated by the approach they use to solve problems. The common use of a problem-focused approach to problem solving is less significant; in fact, the display of an authoritative characteristic moderated by the use of a solution-focused approach to solving problems is the most effective manner in which to restore service from unplanned outages.

5.4 Summary

This research was undertaken to investigate the relationships between the characteristics displayed by incident managers, the MTRS attained by incident managers, and the impact, if any, of the approach incident managers use to solve problems while working to restore service when unplanned outages occur. A review of the literature in business and information technology reveals that there has been limited research conducted on the work of incident managers labouring to restore service. Though much has been written about the prevention of unplanned outages, little exists to indicate that the individuals charged with the restoration of service, as immediately as possible, have been analysed, either through the exploration of how incident managers restore service or how they engage others to restore service. While unplanned outages are accepted as events that will occur, little work has been done in researching how to restore those outages in the shortest possible time. Unplanned outages are accepted as events that, in fact, will occur. This research investigated not only the types of unplanned outages that occur at corporations by analysing actual, production unplanned outages (as opposed to those unplanned outages that may occur in test or development environments), but also by interrogating the characteristics displayed and the approaches to solve problems used by incident managers as they work to restore service.

The demographic data analysed in this research included tests of homogeneity for gender, age, level of education, and tenure working as an incident manager, independently from another. It also evaluated the characteristics displayed by incident managers while working to restore service from an unplanned outage, confirming that the seven characteristics tested for are displayed by incident managers. These include being decisive, being entrepreneurial, being authoritative, being demanding, being pragmatic, being facilitative and being communicative.

This research analysed unplanned outage observations belonging to three of the seven types of unplanned outages. These unplanned outages analysed were of the type hardware, human beings inside the affected company, and software. Each type was further segregated into subtypes. Unplanned hardware outages include the subtypes cable failures, hardware

errors that could not be further defined, network errors, power failures, printer errors, router errors, server errors, servers down, and switch failures. Unplanned outages with a subtype of documentation error, no error found, process failures, security failures, and user errors were assigned to unplanned outages of the type human beings inside the affected company. Unplanned software outages include the subtype application errors, database errors, operating system errors and software errors that could not be further defined. Each type and subtype was analysed.

The types of approaches used by incident managers to solve problems was also analysed in this research. It was confirmed that the only types of approaches to solving problems includes a problem-focused approach to solving problems and a solution-focused approach to solving problems.

Finally, this research analysed the duration of unplanned outages by type through the investigation of the observations of unplanned outages provided for review. The MTRS for each type was calculated and an analysis as to the relationship between the duration of each type of unplanned outage was compared to each other type, using the Kolmogorov-Smirnov test, in available combinations to determine if there is a significant difference in the duration of MTRS attained for each unplanned outage superset. Finally, using hierarchical moderated multiple regression testing, the combination of characteristics displayed approach to solve problems and the attained MTRS values were examined to determine if the MTRS value attained was moderated by the approach to solving problems used by incident managers. A discussion of these tests and their results, along with a review of the limitations of this study is provided in the following chapter.

Chapter 6 : Discussion and Conclusions

Computers are ubiquitous in businesses across the world. The goods and services sold and shipped, worldwide, due to the ease with which shoppers can purchase those goods and services via the Internet will only increase the ongoing need for computers and their applications to be available, on demand, to users. Modern living, in the developed world, is characterised by the technology revolution, which has changed the way people work, live, play, and otherwise engage with one another (Döckel, 2003). This technology revolution allows data to be converted into information; that information allows businesses to operate. This research is designed to identify how it is that an incident manager's combination of characteristics and approaches-to-solving-problems affect the MTRS values attained when restoring service from unplanned outages.

This exploratory study describes the relationships between the characteristics displayed by incident managers in an IT environment and the moderating effect of problem-solving approaches on the MTRS incident managers attain when service is restored. This chapter discusses this research, and the KOZADAR Questionnaire that was developed specifically to undertake this work. The KOZADAR Questionnaire met all validity and reliability requirements to recognise it as a new questionnaire. The importance of this contribution is significant in that it provides IT managers an incident-management-specific tool to assess the performance of individuals in the role of incident manager. It can be used by IT support organisations to identify the specific characteristics their own incident managers display and the likelihood of their ability to minimise MTRS. This research is the first to determine the combination of displayed characteristics and approach to problem-solving that minimise the MTRS attained when an unplanned IT outage occurs.

Findings include how the role of each characteristic studied predicts the problem-solving approach likely to be used; they also include how the moderating effect of the problem-solving approach impacts the MTRS values attained. In this chapter, a discussion of how the research has answered the questions raised at its origin is presented, along with the findings from the work performed. Conclusions are drawn and the limitations of the research are identified. Recommendations for future research to be considered are also presented.

The answers to each of the questions raised in this research were answered through the testing of multiple hypotheses. Although answers were sought for all of the seven types of unplanned outages, the questions were answered for only three of those seven, including unplanned hardware outages, unplanned software outages, and unplanned outages caused by human beings inside the affected company. Question 1 asked "What are the dominant

characteristics displayed by incident managers when they work to restore service that has occurred due to an unplanned outage?” Answers provided from responses to the KOZADAR Questionnaire identify them as Being Decisive, Being Entrepreneurial, Being Authoritative, Being Demanding, Being Pragmatic, Being Facilitative, and Being Communicative. Question 2 asked “What are the different problem-solving approaches used by incident managers when they work to restore service that has been lost due to an unplanned outage?” Answers provided from responses to the KOZADAR Questionnaire identify them as being either a problem-focused approach to solving problems or a solution-focused approach to solving problems. There is no indication that a combination of the two are used or that an alternate approach to solving problems is used.

Question 3 asked “What relationship exists, if any, between the dominant characteristics displayed by incident managers when an unplanned outage occurs, taking into account the problem-solving approaches they use, and the time to restore service they attain?” Through the use of data from the KOZADAR Questionnaire responses, the unplanned outage data provided by Pyrite and the incident management roster provided by Pyrite, conclusions are drawn. Significantly, the display of the characteristic Being Authoritative, moderated by the use of a solution-focused approach to problem solving, will result in a lower MTRS than will either the use of only a problem-focused approach to solving problems, a solution-focused approach to solving problems, or any other combination of displayed characteristics and approaches to solving problems that was investigated.

6.1. Discussion

Results from this study contribute findings that are important to the current literature. First, this study adds to the very small body of literature about the role that incident managers perform and how it is their work is measured. A comprehensive review of the current literature in both business management and information technology confirmed that there is limited work that analyzes unplanned IT outages and their restoration. Significant and extensive research has been produced that investigates and discusses the avoidance of unplanned IT outages (McLaughlin et al., 2008; Pelleg et al., 2008; Qi et al., 2008; Zhong et al., 2008). Published works by Cartlidge, Hanna, Rudd, Macfarlane, Windebank and Rance (2007) and Marquis (2006) contain much of the written literature on what happens when an unplanned outage occurs, as opposed to the previous authors cited who investigated avoiding unplanned outages. As a result of this research, new contributions have been added to the body of literature that focuses on the role of incident managers and the restoration of unplanned IT outages (O’Callaghan, 2008, 2009; O’Callaghan & Mariappanadar, 2006, 2008, 2010; O’Callaghan, Mariappanadar & Thomas, 2010).

Throughout the literature, and from the researcher's first-hand experience of working in IT Service Management for nearly twenty years, all organisations accept that unplanned outages will occur and that restoring service in as effective and least-impacting manner as possible is sought by all impacted parties, not the least of whom are the users of the IT system that has experienced the unplanned outage.

6.1.1. Characteristics

This research provides a thorough investigation into the relationship between the characteristics displayed by incident managers when unplanned outages occur and how those characteristics, moderated by the problem-solving approach an incident manager uses, can decrease the MTRS values attained by the incident manager. The analysis of this research confirms that incident managers are able to decrease the attained MTRS by combining their display of Being Authoritative with the use of a solution-focused approach to solving problems. This is the most important contribution of this research to the literature on problem-solving, unplanned IT outages, and the need for corporations to minimise the duration of unplanned IT outages.

The first question raised when this research was conceived was "What are the dominant characteristics displayed by incident managers when they work to restore service that has occurred due to an unplanned outage?" The literature review suggested that any of the 92 characteristics identified by Schein (1973, 1975) provide an abundance of choices for study and was used in research performed by Bosner (2008), Dorio (2005), Kunkel, Dennis and Waters (2003), and others. Four characteristics from Schein's Descriptive Index were selected for interrogation in this research. These included being authoritative, being competitive, being decisive, and having leadership. From the list of 13 key characteristics developed by de Pillis and Meilich (2006), the only item selected for investigation was being compassionate. This sole selection was the result of the other characteristics in their list being what this author considers negative characteristics, including being passive, being weak, and being unreliable, among others. The richer version of characteristics established by Schein, coupled with items from the focus group, provided a plentiful set of characteristics to investigate. The five characteristics identified by the focus group during the pilot study and included in this research were being communicative, being demanding, being entrepreneurial, being facilitative and being pragmatic.

The literature suggests that each characteristic makes important contributions to the management of an organisation and how its members perceive themselves (Bosner, 2008) and others. The results from the pilot study identified seven of these characteristics being

perceived by incident managers as key to their success. Those seven characteristics include Being Decisive, Being Entrepreneurial, Being Authoritative, Being Demanding, Being Pragmatic, Being Facilitative, and Being Communicative.

Incident managers display significantly different characteristics when they restore service from an unplanned outage. Research performed by Burke and Hutchins (2007) on the characteristics displayed by employees involved in knowledge-transfer-training cite none of the seven characteristics investigated in this study; however, they identified six others as dominant and having a direct effect on the results of the effectiveness of the training obtained. This research, however, does support the work of Perillin (2005) in concluding that being authoritative includes the firm enforcement of rules, high levels of open communication, and respectfulness for the developmental needs of the parties with whom the incident manager interacts. It also supports the findings of Yeung (2004) insofar as identifying the positive value of questioning when used to obtain information and confirm information obtained.

Applying the findings from the research of Lamborn, Mounts, Steinberg and Dornbusch (1991) and Shucksmith, Hendry, and Glendinning (1995) to incident managers, displaying an authoritative characteristic affords incident managers the ability to achieve the required goal (restoring service) while positively engaging the technical support groups and corporate managers with whom they need to work. They insist on structure, yet are flexible in their decision-making processes and their management of personnel. The authoritative characteristic of an incident manager combines the three necessary pillars of structure, control, and sensitivity cited by Bielous (1994) in his assessment of authoritative managers. Moreover, this research finds the communication model established at Bell Labs and described by Deglar and Lewis (2004) is unchanged. Incident managers display the characteristic of being communicative in the same process as do others, with an input-process-output framework. Further, respondents to the KOZADAR Questionnaire provided confirmation that, as was found by Shockley-Zalabak (2001), being communicative is significant in its use as a flexible, strategic tool for the organisation to orient and motivate employees towards a productive end. For incident managers, that productive end is always the restoration of service when an unplanned outage occurs.

Neutral in its support of the work of Caulkins, Morrison, and Weidemann (2007), this research does not explicitly address the recognition that some decisions are made with incomplete data or incorrect data; instead, this research finds that by making decisions that provide solutions are, simply, made. Investigation into the support of the 2007 work of

Caulkins, Morrison, and Weidemann should be considered in future studies of incident managers.

Reade (2003), Thompson (2006), and Silva (2007) all investigated the characteristic of being demanding, perceived from a perspective of having oneself put upon, as opposed to demonstrating demanding behaviours. All three reported that being demanding was, thus, perceived as a negative characteristic and was unwelcome; however, both this research and that of Pinto and Piso (2009) investigated the characteristic of being demanding from the perspective of self-identification and of displaying the characteristic. In both their 2009 study and in this study, displaying the characteristic of being demanding was desired. Unlike being demanding, being entrepreneurial was identified by other researchers as being associated with being passionate and tenacious (Baum & Locke, 2004). Timmons (2000) cited it as encouraging individuals to face extreme uncertainty and resource shortages. This research must be said to have a neutral relationship to those cited, as being entrepreneurial, though able to be identified, was done so with no association of passion, tenacity, or uncertainty, as these characteristics were not investigated.

Studying the characteristic of being pragmatic, Greatbatch and Clark (2002), McGovern (1997), and Huczynski (1993) all cite the appeal of practical solutions to business problems. Though not explicitly extracted from this research, support for their perspective must be cited as neutral from this research and its findings on the display of being pragmatic as a characteristic. Finally, this work supports the findings of Kesby (2002) in that the being facilitative is provided within support of one's team, across professional boundaries, a key characteristic displayed by incident managers.

This research adds to the literature by identifying characteristics displayed by incident managers. The results of this research confirm that incident managers display all seven studied characteristics, including being decisive, being entrepreneurial, being authoritative, being demanding, being pragmatic, being facilitative, and being communicative. This research identified that incident managers most frequently display the characteristics of being facilitative and being decisive. Additionally, being pragmatic is least often used and, among characteristics cited as being preferred, is the characteristic least preferred to be displayed. Although research on all aspects of this professional role is limited, the contribution of this study aligns with the work of the authors of the ITIL tomes, confirming the role of incident managers as being accountable for the restoration of service from unplanned IT outages.

This exploration of the characteristics displayed by incident managers provides evidence of the ability to attain a lower MTRS by use of a solution-focused approach to problem-

solving, rather than a problem-focused approach to problem-solving. The combination of the display of being authoritative with the use of a solution-focused approach to problem-solving results in one's ability to attain lower MTRS values than will be attained with the use of a problem-focused approach alone or with any other characteristic displayed. ITIL instills the importance of aligning the IT department to the business (Carr, 2006; Steinberg & Goodwin, 2006). The output from this research aligns directly with the needs of the business, insofar as lower MTRS values cost less money to the company that experiences an unplanned IT outage than it incurs when a higher MTRS is attained. This research contributes to the literature through the development of a new and validated incident management questionnaire, the KOZADAR Questionnaire, that allows respondents to be assessed relative to the characteristics they display while restoring service from unplanned IT outages and the approach to problem-solving that they use to restore service.

6.1.2. Approaches to Solving Problems

In addition to identifying the characteristics displayed by incident managers when working to restore service from unplanned IT outages, this research also identified the approach to solving problems that each respondent to the KOZADAR Questionnaire preferred to use. The second question raised at the beginning of this research was "What are the different problem-solving approaches used by incident managers when they work to restore service that has been lost due to an unplanned outage?" The literature leans heavily on problem-focused problem solving and includes the work of Coppola (1997), Rooney, Kubiak, Westcott, Reid, Wagoner, Pylipowe, et al. (2009), Kepner and Tregoe (1965, 1997), and Marquis (2006). In each review of problem-focused problem solving, authors propose that understanding and eliminating the root cause of a problem will solve the problem. This research confirms their work; however, and more importantly, this research found that the elimination of the root cause of a problem is not necessary to obtain a solution to a given problem. Importantly, it is not necessary to find the root cause of a problem that caused an unplanned IT outage when finding a solution to that problem can restore service more expeditiously than finding out why the problem occurred. This research supports Visser's (2009) view that the impact of a problem can be lessened by taking action to provide a solution rather than focus on a given problem. Problem-focused problem solving is not required by incident managers; solution-focused problem solving, alternately, is found in this research to be valuable to incident managers and, in concert with the display of being authoritative, contributes to lower MTRS values being attained.

With a nearly 50-year head start held by those who proselytise problem-focused problem solving, solution-focused problem solving literature is less bulky, but no less important. Based on the psychological therapy introduced in the late 20th century, Solution Focused Brief Therapy, the introduction of solution-focused management and solution-focused problem solving led to the adoption of its structure in business (McKergow & Clarke, 2007). Solution Focused Brief Therapy proposed that the problems trying to be solved were often perpetuated when time was taken to understand their origins. Moreover, problems, and their impacts, were lessened when actions were taken to find solutions to the problems. Rather than focusing on the problem to remove it, solution-focused practitioners focus on solutions to remove the impact of the problem. Furthermore, it includes the giving of verbal rewards—compliments—to reinforce thought processes and actions that result in a desired state (Bannink, 2007). This research confirms Bannink's work, as well as that of other solution-focused practitioners and promoters (Jackson & McKergow, 2007; McKergow & Clarke, 2007) by confirming that the use of a solution-focused approach to solving problems, when used by incident managers, can reduce the time taken to restore service from an unplanned outage.

This research has expanded the literature to include the application of solution-focused problem solving by incident managers, operating in high stress environments and working to restore service from unplanned IT outages. Cepeda and Davenport (2006) align person-centred therapy with its focus on now, and Solution Focused Brief Therapy with its focus on future, as two therapeutic techniques that raise awareness of the ability, skills, and resources available to the individual experiencing a problem. Use of a solution-focused approach builds on the resources of the individuals needing help to obtain a state they desire. In the case of incident managers, that desired state is the restoration of service. It is uniquely suited to facilitating positive outcomes (Froerer, Smock, & Seedall, 2009). As well, this research contributes to the literature through the development of a new and validated incident management questionnaire that identifies the characteristics displayed by incident managers and also identifies the preferred approach to problem-solving that incident managers use. The questionnaire allows respondents to be assessed relative to the problem-solving approaches they use to restore service, moderating the characteristics they display to attain an MTRS value. When a solution-focused approach to solving problems moderates the display of being authoritative, MTRS is reduced.

The goal of incident managers is to restore service lost when unplanned outages occur. It is uniquely aligned with the goals of solution-focused problem solving, in that attention is focused on the restoration of service, not the cause of the loss of service. Though ITIL, the

de facto standard in IT Service Management, promotes the use of Kepner-Tregoe problem solving for problem managers, it offers no preference for how the work done by incident managers is to be performed. This research has confirmed that the use of a solution-focused approach to problem solving by incident managers could minimise the duration of time unplanned outages endure. This finding is not only statistically significant, but can be used as a guide and a goal for organisations wanting to take action to minimise the MTRS values attained by those currently providing service in IT incident management.

The research presented here identifies the benefits of the use of a solution-focused approach to solving problems when time is of the essence to obtain a viable and effective solution and costs are being experienced that cannot be recovered and may, in fact, need to be defended. Whether that defence is presented to senior managers in a corporation or to an interested media pool, the costs experienced by the unplanned outage can be minimised, and possibly avoided, by minimising the MTRS values attained. When service has been restored to an acceptable operating level, IT applications and associated data are available for use.

The identification of characteristics displayed by incident managers and their preferred approach to problem solving, both identified through the use of the KOZADAR Questionnaire, affords organisations an opportunity to identify the performance of their current incident managers and take actions to improve their performance. The displayed characteristics of Being Decisive, Being Facilitative, Being Authoritative, and Being Communicative, each in combination with a solution-focused approach to problem solving was found to be statistically significant in attaining a lower MTRS than attained with other combinations of characteristics displayed and problem-solving approach used. Additionally, the display of Being Pragmatic was found to be significant when a problem-focused approach to problem solving was used. The contribution of this research establishes the literature for the display of specific characteristics by incident managers and the impact of their use of problem-solving approaches on the minimisation of MTRS values. This study clearly identifies the strength of relationship of the use of a solution-focused problem solving approach with the display of being decisive, being facilitative, being authoritative, and being communicative. It also clearly identifies the strength of the relationship of the use of a problem-focused problem solving approach and the display of being pragmatic.

There is nothing in this research to suggest that there is no need for a problem-focused approach to solving problems. Though not referred to as a solution-focused approach when it was used, NASA's focus on the return to earth of its stranded astronauts on the Apollo XIII mission was an explicit use of a solution-focused problem solving approach to solving its

problem. Subsequent to the astronauts' return to earth, NASA did use a problem-focused problem solving approach to identify the root cause of the famous explosion onboard the spaceship. Though Kepner and Tregoe (1997) refer to the use of an abbreviated use of problem analysis, in fact, NASA engineers did not focus, during the time its crew was wayward in space, on anything other than the safe return to earth of the crew of Apollo XIII. To achieve this, they needed a solution-focused approach and, as this research confirms, the ability to moderate an output is optimised by the use of a solution-focused approach to solving problems. It is in the same manner that incident managers use a solution-focused approach when displaying the characteristic of being authoritative that allows them the ability to expedite the return to service a system failure that results in an unplanned IT outage.

6.1.3. MTRS

The third question raised at the beginning of this research was “What relationship exists, if any, between the dominant characteristics displayed by incident managers when an unplanned outage occurs, taking into account the problem-solving approaches they use, and the time to restore service they attain?” Minimal literature exists that suggests an answer to this question. This research demonstrates that there are significant differences in the MTRS values of the unplanned IT outages examined. All unplanned outage data provided by Pyrite was analysed, determined to be of one of the seven types of unplanned outages, and then further divided into subsets of those types. Only three (hardware, software, and unplanned outages caused by human beings inside the affected corporation) of the seven types of unplanned outages were included in the provided data. Results of a Kruskal-Wallis test confirmed that there were statistically significant differences between the unplanned outage type and the MTRS attained to return service from unplanned outages. This confirms that the three unplanned outage types assessed (hardware, humans inside the affected company, and software) each result in different MTRS values attained. Future researchers may choose to investigate the MTRS values attained when unplanned IT outages are due to acts of nature, humans outside a company, system overload, or vandalism.

There is limited literature on the importance of specific types of unplanned outages and the attained MTRS. That which exists cites the growing importance of networks and access to the Internet as forces that incite corporate leadership into seeking high availability and avoid and/or minimise unplanned outages (Arai, Yoshihara, & Idoue, 2008; Garg, Kintala, & Stotts, 2006; Jews et al., 2008; Lumpp et al., 2008; McLaughlin et al., 2008). This research successfully identified the significant relationships between the MTRS attained when restoring service—from unplanned hardware outages, unplanned software outages, and

unplanned outages caused by human beings within the affected company—when incident managers display the characteristic of being authoritative and use the problem-solving approach of being solution-focused. In all cases there was a significant relationship across these three types of unplanned outages. This research supports the work of Smith and Hinchcliffe (2006), confirming that the lower the MTRS attained, the higher system availability and the lower the cost of the unplanned outage, contributing to company revenue and profit. This association is established through the costs of unplanned outages researched or reviewed by Alonso (2002), Brown (2004), Fordahl (2001), Hartley (2005), Hitch and Sullivan (2006), IBM (2008), Orbitz (2003), Scott (1999) and Tsuruoka (2008). Unplanned outages cost companies money.

The use of a problem-focused approach or a solution-focused approach to restore service will moderate the relationship between characteristics displayed by incident managers and their attained MTRS values from an unplanned outage. Minimal literature exists that discusses the relationship between characteristics displayed and problem-solving approaches used. A three-step hierarchical moderated multiple regression test, with MTRS as the dependent variable, the characteristics displayed as the independent variable and the approach-to-solving-problems used by incident managers who restored service from an unplanned outage as the moderating variable was performed to determine the relationship between the moderating variable (approach to problem solving) and the independent variable (displayed characteristics). This provided information vis-à-vis the MTRS values attained for the type of unplanned outage identified. The demographic data of Age, Tenure in the Role of Incident Management, and Education Levels obtained from incident managers who completed the KOZADAR Questionnaire were used as control variables.

The research presented here confirms that the use of a solution-focused approach, coupled with the display of the characteristic Being Authoritative, contribute to a lower MTRS than can be attained by any other combination of characteristics displayed and problem solving approach used. Additionally, this pairing is more effective to attain a lowered MTRS than a problem-focused problem solving approach is with any characteristics or, indeed, used alone. The contribution of discovering the most effective manner to lower MTRS is the most significant contribution to the literature that this study presents. It provides scholars a platform to continue researching the restoration of service from unplanned outages. Importantly, it affords corporations with incident managers a model to optimise the work those individuals perform.

The importance of this finding is significant from not only a research perspective, but from its prospective application within corporations and incident management organisations.

Knowing that the display of being authoritative, moderated by a solution-focused approach to problem solving, will result in a lower MTRS, thereby lowering the costs associated with unplanned IT outages, has the potential to revolutionise the work done by all users of the ITIL framework. Companies that have invested in ITIL expect a return on that investment, particularly when they invest in a framework, rather than a set of process steps that will ensure them lower MTRS values. The goals of ITIL, in part, are to reduce costs and to manage more effectively the delivery of IT services within an organisation. This research complements the writings in the ITIL framework (Cartlidge, et al., 2007) and allows the stated goal of reducing costs to be achieved. This work confirms that MTRS values can be reduced with the combination of being authoritative and using a solution-focused approach to problem solving while working to restore service from an unplanned outage. The “abbreviated use of the problem analysis” (Kepner & Tregoe, 1997) acknowledges the need for speedy solutions, not root causes. Indeed, this is what solution-focused problem solving provides; it also offers structure and discipline in its delivery.

6.2. Limitations

There are a number of limitations that should be considered in the review of this research. The first limitation is that the use of the KOZADAR Questionnaire required individual responders to self-identify their displayed characteristics and approaches to problem solving. Though the items identifying specific characteristics and approaches were randomly distributed throughout sections of the questionnaire, self-identification may be the result of the responder considering what a “correct” answer might be, although advised in the introduction of the questionnaire that there were no right or wrong answers.

A second limitation in Phase One (Pilot Study) was the use of convenience sampling to identify participants in the focus group (N = 10) and to validate the questionnaires (N = 118). Additionally, all participants in Phase One were employed by the same organisation, in the same country of that multinational organisation. Organisational corporate cultural alignment may be considered a possible limitation. A third limitation, in Phase Two (Main Study) of this research, was being unable to identify every respondent by detail and associate every respondent with specific outage data provided. All outage-specific data required the responding participant to be employed by Pyrite, thereby limiting the contribution of the incident managers at Pyrox to being respondents to the KOZADAR Questionnaire. It was not possible to determine the contribution of an attained MTRS value made by more than just one incident manager. A fourth limitation, as well, is that the unplanned IT outages

investigated in this research were obtained from a single organisation; hence, the generalisation of the research findings is limited.

Not all types of unplanned IT outages were available to investigate. Four of the seven types of unplanned outages are candidates for further research, relative to incident managers and MTRS values. These include acts of nature, human beings outside the affected company, system overload and vandalism. This simple framework ignores the complexity of IT systems, but provides a starting point for future researchers who may want to study incident management activities, characteristics and problem-solving approaches, as this is the first framework found for research into incident management.

These limitations, however, do not diminish the value of this study. Significant research was completed that confirms the characteristics displayed by incident managers can be identified, the preference of a particular approach to solving problems can be identified, and that the MTRS values attained can be assessed based on those displayed characteristics and problem solving approaches. Additionally, although MTRS service level agreements seek restoration times for Severity 1 and Severity 2 unplanned outages in the range of less-than-one-hour to as-many-as-four hours (Hartley, 2005; Orbitz, 2003), the data analysed here indicates that many unplanned outages require days to restore, not hours.

6.3. Recommendations for Future Research

Recommendations for future research are based on discoveries from both the pilot study and the main study performed in this research. They are included with proviso that businesses that can benefit from future research about minimising MTRS will be required to participate fully and allow researchers access to more unplanned IT outage data, shift rosters, and more incident managers. Moreover, the relationship between the responses of incident managers and the unplanned outages restored by those incident managers must be able to be easily identified.

This research has introduced a different approach to the study of how unplanned IT outages can be managed. Other researchers have investigated the value of technology solutions to maintain working systems by minimising downtime, increasing hardware and application redundancy, and otherwise taking actions that attempt to prevent unplanned outages (Allen, 2004; Brewer, 2001; Das & Das, 2008; Fox & Patterson, 2003). This research accepts that unplanned IT outages will occur and that the individuals in the IT Service Management (ITSM) part of an IT organisation have a significant contribution to make to restore lost services.

In addition to the continued study of the relationship between the characteristics displayed by incident managers and the MTRS they attain, moderated by the problem-solving approach they use, there are several opportunities for other researchers to explore in the world of IT Service Management and in the world of incident management. Recommendations for future research include an investigation into the relationship between the dollars saved by effective and efficient incident managers and the salary modeling used by corporations to pay these individuals who are able to save companies millions of dollars. In addition, the application of a fully disciplined ITIL organisation should be investigated to determine if the greater allegiance and disciplines demonstrated to the ITIL framework results in a relationship to attained MTRS by its incident managers. Finally, the characteristic of being pragmatic was identified as not being valuable to incident managers; yet, the statistical analysis indicates its use can be beneficial to achieving a lessened MTRS value. A future researcher may consider investigating why this characteristic, not preferred by incident managers, shows benefit to the business.

This research focused on the role of incident managers without regard to complementing systems that can be used to minimise restoration time. A future researcher may seek to investigate how the incident manager role interacts with other unplanned outage actions to restore service or avoid an unplanned outage altogether. Consideration may be given to automatic diagnosis techniques, preventative measures and testing activities, and the change and problem activities performed that are specifically designed to avoid unplanned outages.

In conclusion, this research on the moderating approach of problem solving on the MTRS values attained when unplanned outages are restored identified key characteristics of incident managers. The researcher found that the reduced MTRS values are attained when displaying an authoritative characteristic, moderated by a solution-focused approach to restoring service. From an academic perspective, the literature is enriched with data from genuine, production IT unplanned outages, as opposed to studying those which occur in a test or development environment. The field of IT Service Management is open to new opportunities to investigate the unplanned outage types not included in this study. From a corporate perspective, given that unplanned outages are expected, it is recommended that the application of these findings, put into practice, will result in lower MTRS attainment and the dollar savings associated thereto.

6.4. Conclusion

Overall, the objectives outlined in the beginning of this research have been achieved successfully. This research established the value of using a solution-focused approach to problem solving by incident managers within an IT organisation, noting the complementing impact it has when incident managers display the characteristics of being decisive, being facilitative, being authoritative or being entrepreneurial. It also established a positive relationship between problem-focused problem solving and the displayed characteristic of being pragmatic. The literature has gained by the introduction of solution-focused problem solving by incident managers. Also, this research introduces a new and validated questionnaire that can be used by incident managers to identify the characteristics they display and the problem-solving approach they use when restoring service when an unplanned outage occurs. The final results provide corporations the ability to apply the learnings from this research in their own IT organisations and undertake the required steps to improve their contribution to the success of the businesses for which they work.

The most important contribution this research makes to the literature, to academia, and to the industry is that there is now the ability to conclude, with documented research, that there is a significant relationship between the types of characteristics displayed by incident managers, moderated by specific problem-solving approaches on the MTRS values attained in day-to-day business (see Figure 6-1).

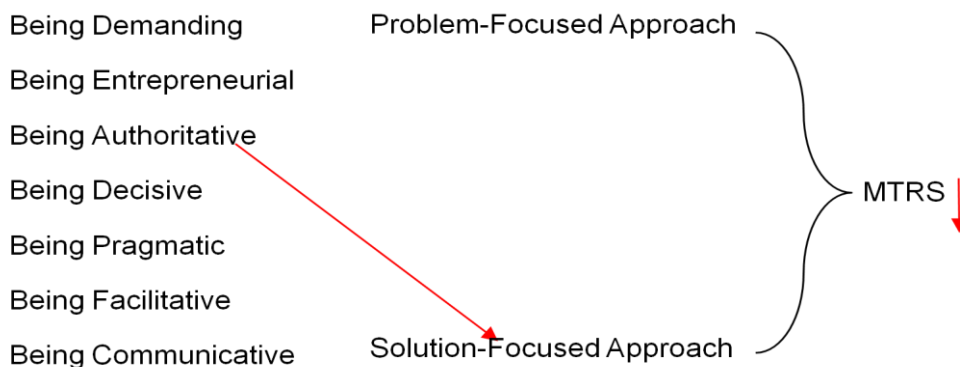


Figure 6-1.

This research concludes with the finding that displaying the characteristic of Being Authoritative, moderated by the use of a solution-focused approach to solve problems, results in the lowest MTRS that can be attained by incident managers.

This study contributes to the literature and to the professional practice of IT Service Management and to the professional delivery of incident management. It provides a framework to explain the relationship between unplanned outages in a corporation, the

characteristics displayed, as well as the approach to solve problem used by incident managers working to restore service and the time in which the unplanned outages are restored.

Academically, this study investigates the approaches incident managers use to entice, demand, direct, and otherwise entice the actions of the technical support specialists who contribute to the restoration of service when an unplanned outage occurs. The unplanned outages in this research are of the type considered to be greatly important or critical to the business that experiences them. This research identifies specific problem-solving approaches to the restoration of service used by incident managers. It identifies the characteristics displayed by incident managers during the restoration of unplanned outages. These findings are all new contributions to the literature in the fields of IT Service Management, incident management, and business. The study has determined the impact specific problem-solving approaches have on the speed with which service from unplanned outages is restored. Additionally, it provides a foundation on which future research can be undertaken.

This study contributes to the literature by its review of the types of problem-solving approaches used by incident managers when unplanned outages occur. Additionally, this research introduces two validated research questionnaires that, respectively, capture information on the characteristics displayed and the problem-solving approaches used by incident managers in their professional roles. This research has also introduced the KOZADAR Research Model, which presents a framework for analysing the characteristics displayed by incident managers, the approaches used by incident managers to solve problems, and the resulting MTRS attained when each is displayed or used, respectively. Future researchers may benefit from its creation, easing future investigations in IT Service Management. The contribution to the literature is such that this study has expanded the literature in the areas of IT Service Management, IT Service Support, and Incident Management (O'Callaghan, 2009; O'Callaghan, 2008; O'Callaghan & Mariappanadar, 2008, O'Callaghan & Mariappanadar, 2006[b]; O'Callaghan, Mariappanadar & Thomas, 2010). It acknowledges the value to large corporations of having effective incident managers who can save companies time and money when unplanned outages occur.

Appendix A – Bass-Avolio Leadership Steps

The five Bass-Avolio leadership steps transition individuals through the three types of leadership styles proposed by Bass and Avolio (2005). These types and their associated steps are presented here. The labels and abbreviations noted in Figure A-1 are from the Management Leadership Questionnaire (MLQ) and an analysis of the results from those questionnaires.

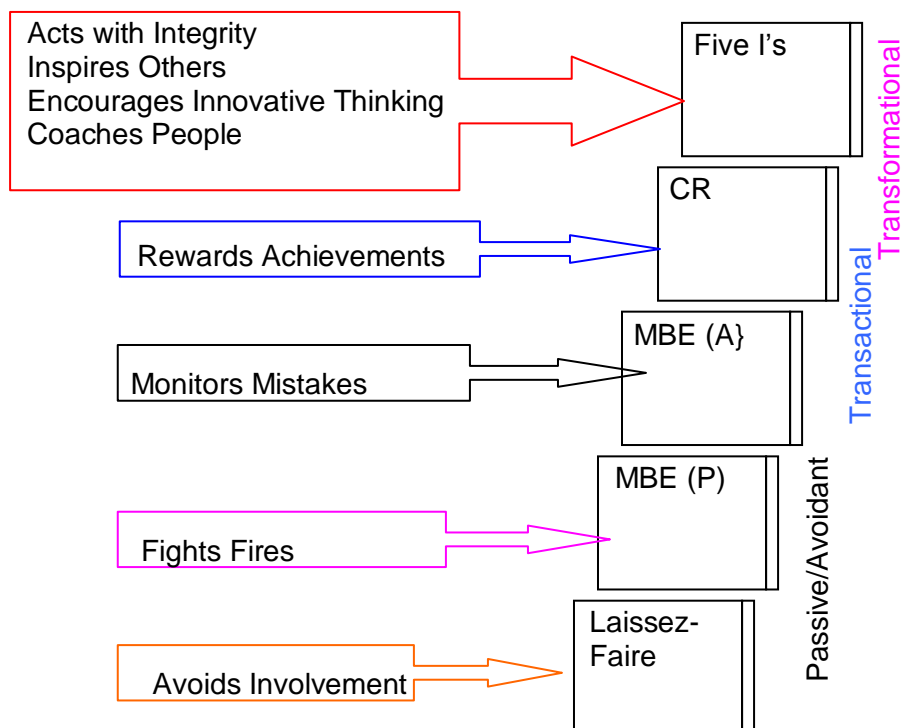


Figure A-1. The Steps Required to Achieve Superior Leadership (Bass-Avolio, 2005)

The laissez-faire style of leadership is also referred to as a non-leadership style. This leader avoids clarifying expectations, avoids addressing conflicts, and avoids making decisions. These leaders do not get involved when important issues arise or there is a need for them to make a decision (Muenjohn, 2009). Leaders with this style who develop stronger leadership skills develop into a transactional leadership style, starting with showing passive-avoidant tendencies, rather than, simply, avoidance. It is acknowledged that some researchers consider passive-avoidance to belong completely to the laissez-faire style of leadership (Toor & Ofori, 2009); however, the display of passive-avoidant leadership is considered minimally effective in leading teams of people (Muenjohn, 2009; Toor & Ofori,

2009). When engaged, the actions of passive-avoidant leaders include participating in fire-fighting when events require extraordinary action.

The professional development of a leader from a fire-fighting posture (Management-by-Exception-Passive (MBE-P)) is the leadership demonstrated through Management-by-Exception-Active (MBE-A), the step from passive-avoidant to active engagement as a leader. The display of transactional leadership (MBE-A) spans behaviours intended to prevent potential problems prior to them arising (Xirasagar, 2008). It also introduces the leader to the effective use of contingent reward (CR), wherein demonstrated behaviours are designed to clarify performance expectations and to establish follower credibility that value those rewards (Xirasagar, 2008).

Finally, transformational leadership is the attainment by a leader to optimise the work performed by the leader and by the followers. This leadership style describes an individual who earns trust and respect from followers by being a good role model, by encouraging others to share a common vision, and by providing both a clear vision and a strong sense of purpose (Muenjohn, 2009). From the MLQ reports provided, this leadership style is identified closely with the five “Is”—idealized influence behaviour, idealized influence attributed, inspirational motivation, individual consideration and intellectual stimulation.

Appendix B – Sample Participation Invitation

Dear Incident Manager,

[Name of company] is participating with a student researcher who is investigating the role of Incident Managers in large organisations.

You are invited to provide information about your job, and the manner in which you perform it, by clicking on the following link and responding to the survey to which this link will take you.

[monkeysurvey.com link to the KOZADAR Questionnaire inserted here]

This research is being conducted by Ms. Katherine O'Callaghan, a doctoral student at Australian National Catholic University (Melbourne campus). You may choose to respond to the survey or not respond to it. If you choose to respond to it, your responses will be sent directly to the researcher and [name of company here] will not see or being given the responses you submit. Additionally, your responses will not be identified as being sent by you, so your anonymity is assured. Both the company and each individual participant have been committed complete anonymity. Any future publications in which the results of this work are published, including Ms. O'Callaghan's doctoral dissertation, will use a pseudonym for the company and will not cite the individuals who replied by name.

This URL will be valid for four weeks, so please take work time to participate. All items must have a response or the survey will not be submitted successfully.

[Name of company here] strongly supports this research and encourages you to participate. If you have questions or would like further information, please contact the researcher directly at kozinoz@yahoo.com.au or at 0409 520 703. Alternately, you may contact me directly.

[Name of Corporate Liaison]

Appendix C – The KOZADAR Questionnaire

CONFIDENTIAL QUESTIONNAIRE

What Makes Incident Managers Successful?

Why this survey?

Most importantly: your responses to this survey are confidential.

Incident Managers, sometimes called “Problem Managers”, “Critical Situation Managers”, or “Service Restoration Managers” or “Duty Managers” are hired by organisations to manage the restoration of services when unplanned outages occur. In this survey, they will be called “Incident Managers”. This survey is designed to identify two areas of interest. Although basic demographic information is captured in Section 1, Section 2 includes statements about the approach(es) used by incident managers in the performance of their tasks. Section 2 includes statements about how those tasks are performed.

No one “always” undertakes the actions described in these statements; however, most use a preferred style when dealing with other people. Choose the answer that reflects how you see yourself and how you really perform—not how you “wish” you perform. There is no “correct” or “incorrect” answer. Consider the statements as reading “Most often, . . . “

This survey and the responses provided are confidential. Your identity is also confidential. This survey is part of a study currently being done at a university in Australia.

Why you?

You have been identified as currently performing a role equivalent to that of an incident manager in your organisation. Fundamentally, you assist technical support and management teams in restoring service to key software applications and/or hardware systems and/or network components.

You do not need to complete the survey in one sitting, but answering every statement is requested. When you have completed it, please hit the “submit” key and it will be sent directly to the researchers. Your organisation will not have access to the raw data; all replies are completely anonymous.

Directions

For each of the following statements, please select the radio button that best indicates your response to the statement. There are no right or wrong responses.

SECTION 1:

My gender is: Male Female

My age is:

- 20-25 26-30 31-35 36-40 41-45
 46-50 51-55 55-60 Older than 60

I have been in my current job role for:

- Less than one year 1-5 years 6-10 years
 11-15 years 16-20 years More than 20 years

I am currently:

- Single Married in a 2nd Marriage
 Married Married in a 3rd Marriage
 Separated Married in a 4th Marriage
 Divorced

The highest level of schooling I attended was:

- High School (attended) High School (graduated)
 University (attended) University (graduated)
 Master's (attended) Master's (graduated)
 Doctorate (attended) Doctorate (graduated)

Continue now or save your responses and finish later?

- Continue Save my answers and I will finish this later

SECTION 2:

1. An unplanned outage is restored only when the root cause is known and a permanent solution is deployed.

- Never Rarely Sometimes Often Always

2. Even when little progress is being made, I praise the technical team members engaged as they work to restore service.

- Never Rarely Sometimes Often Always

3. I rarely take risks because doing so could exacerbate the duration of the unplanned outage

- Never Rarely Sometimes Often Always

4. Identifying and testing possible solutions is necessary before restoring service.

- Never Rarely Sometimes Often Always

5. Introducing a permanent fix must occur in order to restore service.

- Never Rarely Sometimes Often Always

6. It is as important to know when the problem did not exist as when it started.

- Never Rarely Sometimes Often Always

7. Understanding the root cause of an unplanned outage is important.

- Never Rarely Sometimes Often Always

Continue now or save your responses and finish later?

- Continue Save my answers and I will finish this later

SECTION 3:

1. Clear lines of authority and responsibility exist when I manage an unplanned outage.

- Never** **Rarely** **Sometimes** **Often** **Always**

2. I allow the technical teams working to restore service a great deal of independence.

- Never** **Rarely** **Sometimes** **Often** **Always**

3. I am technically astute enough to challenge the technical teams when they provide questionable or inaccurate information.

- Never** **Rarely** **Sometimes** **Often** **Always**

4. I decide what tasks should be taken to restore service.

- Never** **Rarely** **Sometimes** **Often** **Always**

5. I ensure I follow the process and policies established for my team to perform my role.

- Never** **Rarely** **Sometimes** **Often** **Always**

6. I follow a written script during teleconferences so I remember to ask the right questions.

- Never** **Rarely** **Sometimes** **Often** **Always**

7. I hold the technical support group accountable for their actions in efforts to restore service.

- Never** **Rarely** **Sometimes** **Often** **Always**

8. I insist that the technical teams present very detailed and specific information during teleconferences.

- Never** **Rarely** **Sometimes** **Often** **Always**

Continue now or save your responses and finish later?

- Continue** **Save my answers and I will finish this later**

9. I often organise casual meetings (coffee, etc) with support teams and management teams to review the work we do together.

Never Rarely Sometimes Often Always

10. I prefer to manage incidents that are duplicates of previous unplanned outages, rather than new and unknown outages.

Never Rarely Sometimes Often Always

11. I use teleconferences to work through the technical details so that the right actions are taken to restore service.

Never Rarely Sometimes Often Always

12. I work well with people who are polite and trusting.

Never Rarely Sometimes Often Always

13. I would be willing to take a pay cut now if there was a career opportunity that could increase my future earning power.

Never Rarely Sometimes Often Always

14. I would rather be 100% wrong than only 99% right.

Never Rarely Sometimes Often Always

15. If I won the lottery, I would stop working.

Never Rarely Sometimes Often Always

16. If the impacted users won't assist in restoring service by doing testing, I assume there really isn't an issue.

Never Rarely Sometimes Often Always

Continue now or save your responses and finish later?

Continue Save my answers and I will finish this later

17. Information about unplanned outages I manage is always provided to me in a timely manner.

- Never Rarely Sometimes Often Always

18. Information flows through a clearly defined chain of command.

- Never Rarely Sometimes Often Always

19. Information overload is a by-product of having an unplanned outage.

- Never Rarely Sometimes Often Always

20. It is more effective to restore service by cutting corners, short-cutting processes as necessary, than it is to “do it by the book”.

- Never Rarely Sometimes Often Always

21. Most of the time, I enjoy my job, not because of my salary, but because it is interesting work.

- Never Rarely Sometimes Often Always

22. One of my first tasks to perform is to notify my manager an unplanned outage has been reported.

- Never Rarely Sometimes Often Always

23. Others think I am aggressive.

- Never Rarely Sometimes Often Always

24. Significant outages usually only need simple solutions to restore service.

- Never Rarely Sometimes Often Always

Continue now or save your responses and finish later?

- Continue Save my answers and I will finish this later

25. Technical teams do a good job of keeping me informed about matters that indicate when service will be restored.

- Never Rarely Sometimes Often Always

26. Technical teams involved in restoring service share information with me as they progress and they do it willingly and honestly.

- Never Rarely Sometimes Often Always

27. The amount of effort someone must put into restoring service is not of interest to me.

- Never Rarely Sometimes Often Always

28. The longer it takes to restore service, the more I demand from the people trying to restore it.

- Never Rarely Sometimes Often Always

29. The management team is responsible for obtaining all required resources to restore service when an unplanned outage occurs.

- Never Rarely Sometimes Often Always

30. The more clearly a problem can be described, the more likely the unplanned outage will be restored quickly.

- Never Rarely Sometimes Often Always

31. The rules and regulations to succeed within my work group are clearly specified.

- Never Rarely Sometimes Often Always

32. When faced with an unplanned outage, I apply careful analysis to all of the information provided.

- Never Rarely Sometimes Often Always

Continue now or save your responses and finish later?

- Continue Save my answers and I will finish this later

33. When I am done at the office, I spend time at the gym or with my family and leave work behind.

Never Rarely Sometimes Often Always

34. When I manage an unplanned outage, I make decisions quickly and take action.

Never Rarely Sometimes Often Always

35. When I socialize, I spend most of the time talking about my work.

Never Rarely Sometimes Often Always

You're Done!!!

Submit

Save my answers and I will finish this later

Appendix D –Author’s Conference Publications

The following papers were presented at conferences during the course of this research. Copies can be obtained from the sponsoring organisation.

O’Callaghan, K., Mariappanadar, S. PhD, and Thomas, T., PhD (2009). Incident Management—Reality. In *Proceedings of the Summer 2009 Information Technology Service Management Forum (itSMF)–Australian Capital Territory Chapter, Canberra, Victoria*.

O’Callaghan, K. (2008)[a]. Fundamentals of Incident Management. In *Proceedings of the Autumn 2008 Information Technology Service Management Forum (itSMF)–Victorian Chapter, Melbourne, Victoria*.

O’Callaghan, K. and Mariappanadar, S. (2006)[b]. Solution Focused Management of Unplanned IT Outages. In *Proceedings of the 7th International We-B (Working for e-Business) Conference*, ISBN 178-1-86272-670-3, Melbourne, Victoria, Australia.

O’Callaghan, K. and Mariappanadar, S. (2006) [a]. Unplanned IT Outages. In *Proceedings of the 2006 Pacific Internet and Information and Communication Technologies (PacINet) Conference*, Apia, Samoa.

Appendix E – Author’s Journal and other Publications

The following papers were published during the course of this research. Copies can be obtained from the publishing organisation.

O’Callaghan, K., Mariappanadar, S. (2010). Incident Manager? Meet PHIL CROSS. IT Service Management Forum Australia, *Informed Intelligence*, Summer, p. 7.

O’Callaghan, K., Mariappanadar, S., and Thomas, T. (2010). Managing Unplanned IT Outages. *CIO Magazine (New Zealand)*.

O’Callaghan, K. (2009). There are only Seven Types of Unplanned Outages IT Service Management Forum Australia, *Informed Intelligence*, Summer, p. 10.

O’Callaghan, K. (2008)[b]. Characteristics of Incident Managers, IT Service Management Forum Australia, *Bulletin*, Winter, p. 20.

O’Callaghan, K. and Mariappanadar, S. (2008). Approaches Used by Incident Managers to Restore Service When Unplanned IT Outages Occur, *IT Professional (10)*, 3, pp. 40-45.

Appendix F – Ethics Approval

Australian Catholic University
Brisbane Sydney Canberra Ballarat Melbourne



Human Research Ethics Committee

Committee Approval Form

Principal Investigator/Supervisor: Dr Sugumar mariappanadar Melbourne Campus
Co-Investigators: Melbourne Campus
Student Researcher: Katherine O'Callaghan Melbourne Campus

Ethics approval has been granted for the following project:
Decreasing mean time to restore service when an unplanned outage occurs.
for the period: 06.06.06 to 06.10.06
Human Research Ethics Committee (HREC) Register Number: V200506 73


The following standard conditions as stipulated in the *National Statement on Ethical Conduct in Research Involving Humans* (1999) apply:

- (i) that Principal Investigators / Supervisors provide, on the form supplied by the Human Research Ethics Committee, annual reports on matters such as:
 - security of records
 - compliance with approved consent procedures and documentation
 - compliance with special conditions, and
- (ii) that researchers report to the HREC immediately any matter that might affect the ethical acceptability of the protocol, such as:
 - proposed changes to the protocol
 - unforeseen circumstances or events
 - adverse effects on participants

The HREC will conduct an audit each year of all projects deemed to be of more than minimum risk. There will also be random audits of a sample of projects considered to be of minimum risk on all campuses each year.

Within one month of the conclusion of the project, researchers are required to complete a *Final Report Form* and submit it to the local Research Services Officer.

If the project continues for more than one year, researchers are required to complete an *Annual Progress Report Form* and submit it to the local Research Services Officer within one month of the anniversary date of the ethics approval.

Signed:  Date: 06.06.06
(Research Services Officer, Melbourne Campus)

References

- Aggarwal, A. K., & Adlakha, V. G. (2006). Quality management applied to web-based courses. *Total Quality Management & Business Excellence*, 17(1), 1-19.
- Al-Ekram, R., Holt, R., Hobbs, C., & Sim, S. (2007). Automating Service Quality with TOMCAD (Tradeoff Model with Capacity and Demand). In *ACM ISBN: 978-1-59593-878-7* (pp. 4-9). Atlanta, GA: U.S.A.: ASE Workshop on Automating Service Quality.
- Allen, D. (2004). Back IT up. *Chartered Accountants Journal*, November, 13-16.
- Aloisio, M. (2004). The Calculation of Easter Day, and the Origin and Use of the Word Computer. *IEEE Annals of the History of Computing*, 26(3), 42-49.
- Alonso, F. (2002). Managing Business Continuity: Part 1 The cost of unplanned downtime is growing. *Data Based Advisor* 1-6.
- An 811 'Call-Before-You-Dig' Ring Can Save a 911 Call. (2007). *ENR: Engineering News-Record*, 258(5), 31-31.
- Anderson, J. C., & Narus, J. A. (1990). A Model of Distributor Firm and Manufacturer Firm Working Partnerships. *Journal of Marketing*, 54(January), 42-58.
- Anonymous. (2005). Leveraging ITIL to Better Manage Outsourcing Relationships. *Computer Economics Report*, 27(12), 11-15.
- Anonymous. (2009[a]). Interpreting the future: A wider perspective through anticipatory leadership. *Strategic Direction*, 25(2), 9-11.
- Anonymous. (2009[b]). Unbalanced [Review of the *1-Click Payroll*]. *Accounting Today*, 23.
- Apple Corporation. (2008, June). What is Firmware. *apple.com*, HT1471. Retrieved February 3, 2009, from http://support.apple.com/kb/HT1471?viewlocale=en_US.
- Arai, D., Yoshihara, K., & Idoue, A. (2008). Network-Wide Rollback Scheme for Fast Recovery from Operator Errors Toward Dependable Network. In *Lecture Notes in Computer Science, Challenges for Next Generation Network Operations and Service Management*.
- Armenakis, A. A., Harris, S. G., Cole, M. S., Fillmer, J. L., & Self, D. R. (2007). A Top Management Team's reactions to Organizational Transformation: The Diagnostic Benefits of Five Key Change Sentiments. *Journal of Change Management*, 7(3-4), 273-290.
- Arthur, L. J. (1997). Quantum Improvements in Software System Quality. *Communications of the ACM*, 40(6), 46-52.
- Baden-Fuller, C. & Stopford, J.M. (1994). Creating corporate entrepreneurship. *Strategic Management Journal*, 15(7), 521-536.

- Bailey, D., Frank-Schultz, E., Lindeque, P., & Temple, J. L., III. (2008). Three reliability-engineering techniques and their application to evaluating the availability of IT systems: An introduction. *IBM Systems Journal*, 47(4), 577-589.
- Bannink, F. P. (2007). Solution-Focused Brief Therapy. *Journal of Contemporary Psychotherapy*, 37(2), 87-94.
- Bardoel, E. A., De Cieri, H., & Mayson, S. (2008). Bridging the research-practice gap: Developing a measurement framework for work-life initiatives. *Journal of Management & Organization*, 14, 239-258.
- Baron, R. D., & Kenny, D. A. (1986). The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic and Statistical Consideration. *Journal of Personality and Social Psychology*, 51, 1173-1182.
- Bass, B. M. (1985). *Leadership and performance beyond expectations*. New York, N.Y.: U.S.A.: Free Press.
- Bass, B. M., & Avolio, B. J. (1993). Transformational leadership: a response to critiques. In M. M. Chemers & R. Ayman (Eds.), *Leadership Theory and Research: Perspectives and Directions* (pp. 49-80). San Diego, CA: U.S.A.: Academic Press.
- Bass, B. M., Avolio, B. J. (Authors), & Moss, S., Dr (Engineer). (2005). *Pre-Post Comparative Longitudinal Feedback Report: Sample Company 2004-2005. Sample Company Leaders* (pp. 1-8) [Group & De-identified Individual MLQ360 Assessment Data]. Melbourne, VIC: Australia: MLQ Pty Ltd.
- Bauer, E. J., & Franklin, P. H. (2006). Framework for Availability Characterization by Analyzing Outage Durations. *Bell Labs Technical Journal*, 11(3), 39-46.
- Baum, J. R., & Locke, E. A. (2004). The Relationship of Entrepreneurial Traits, Skill, and Motivation to Subsequent Venture Growth. *Journal of Applied Psychology*, 89(4), 589-598.
- Beasley, A. L. (2005). The style split: good communication has no gender. *Journal of Accountancy*, 200(3), 91-92.
- Behr, K., Kim, G., & Spafford, G. (2005). *The Visible Ops Handbook: Implementing ITIL in 4 Practical and Auditable Steps*. Eugene, OR: U.S.A.: IT Process Institute.
- Bellowin, S. M. (2008). The Physical World and the Real World. *Communications of the ACM*, 51(5), 104.
- Berne, E. (1964). *Games People Play*. New York, NY: U.S.A.: Grove.
- Bielous, G. (1994). Why We Should Become an Authoritative Manager and Not an Authoritarian One. *Supervision*, 55(5), 11-13.
- Bierck, R. (2000). How to handle a media crisis. *Harvard Management Communication Letter*, 3(3).
- Biles, G. E., Bolton, A. A., & DiRe, B. M. (1998). Herman Hollerith: His 100 Year Legacy. *Academy of Management Proceedings*, AN 4980212, 127-132.

- Bingermann, M. (2008, July 28). New Qantas system causes delays. *The Australian, Australian IT*.
- Bird, B.J. (1989). *Entrepreneurial Behavior*. Glenview, IL: Scott Foresman & Company.
- Boam, M. M., Gilbert, J., Mathew, T. K., Rasovsky, K., & Sistla, R. (2003). Modular Communications Platform. *Intel Technology Journal*, 74, 7-16.
- Boon, W. P., Moors, E. H., Kuhlmann, S., & Smits, R. E. (2008). Demand articulation in intermediary organisations: The case of orphan drugs in the Netherlands. *Technological Forecasting and Social Change*, 75(5), 644-671.
- Bosner, K. C. (2008). Gender stereotypes and self-perceptions among college students. *Journal of Diversity Management*, 3(3), 41-52.
- Brancaccio, D. (Host). (2001). Marketplace, *NYSE Officials say new software loaded . . . all trading was stopped*. June 8, 2001. Saint Paul, MN: American Public Media.
- Brewer, E. A. (July/August, 2001). Lessons from Giant-Scale Services [Special issue]. *IEEE Internet Computing*, 05(4), 46-55.
- Brooks, C., Leung, C., Mirza, A., Neal, C., Qiu, Y., Sing, J., et al. (2007, February). *IBM System Storage Business Continuity Solutions Overview: SG24-6684-01*. Redbooks (2nd ed., pp. 1-172) Armonk, NY: U.S.A.: IBM International Technical Support Organization.
- Brown, A. B. (2004). Oops! Coping with Human Error in IT Systems. *QUEUE Focus: Error Recovery*, 28, 34-41.
- Brown, W. J., Hockey, R., & Dobson, A. (2007). Rose revisited: a "middle road" prevention strategy to reduce non-communicable chronic disease risk. *Bulletin of the World Health Organization*, 85(11), 886-887.
- Brunninge, O., & Nordqvist, M. (2004). Ownership structure, board composition and entrepreneurship. *International Journal of Entrepreneurial Behaviour & Research*, 10(1/2), 85-105.
- Bryman, A. (2006). Paradigm Peace and the Implications for Quality. *International Journal of Social Research Methodology*, 9(2), 111-126.
- Buckingham, M., & Clifton, D. O., PhD. (2001). *Now, Discover Your Strengths*. New York, NY: U.S.A.: The Free Press: A Division of Simon & Schuster, Inc.
- Burke, L. A., & Hutchins, H. M. (2007). Training transfer: An integrative literature review. *Human Resource Development Review*, 6, 263-296.
- Burstin, H. R., MD, MPH. (2008). Achieving the Potential of Health Information Technology. *Journal of General Internal Medicine*, 23(4), 502-504.

- Butler, J. G. (1997). Concepts in New Media. Unpublished raw data, University of Arizona.
- Calabrese, R., Foo, L., & Ramsay, O. (2007). Reducing Variance. *Drug Discovery & Development, 10*(8), 31-33.
- Calder, B. J. (1977). Focus groups and the Nature of Qualitative Marketing Research. *Journal of Marketing Research, 353-364*.
- Caminer, D. T., OBE. (1997). LEO and its Applications: The Beginning of Business Computing. *The Computer Journal, 40*(10), 585-597.
- Canali, C., Colajanni, M., & Lancellotti, R. (2009). Performance Evolution of Mobile Web-Based Services. *IEEE Internet Computing, March/April*, 60-68.
- Candea, G., & Fox, A. (2003). Crash-Only Software. *9th Workshop on Hot Topics in Operating Systems (HotOS-IX)*, 1-6.
- Carr, D. F. (2006). I.T. Infrastructure Library. *Baseline, June*(60), 91-91.
- Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J., & Rance, S. (2007). Cartlidge & M. Lillycrop (Eds.), *An Introductory Overview of ITIL ® V3*. Berkshire, United Kingdom: The UK Chapter of the itSMF.
- Casey, D., & Pike, D. (2007). Fit for Purpose: working with the Community to Strengthen Policing in Victoria, Australia. *Flinders Journal of Law Reform, 3*(2), 373-401.
- Cater-Steel, A., Toleman, M., & Tan, W. (2006). Transforming IT Service Management -- The ITIL Impact. In *Proceedings of the ACIS 17th Australasian Conference on Information Systems: Thought, Leadership in IS*. Adelaide, SA: Australia.
- Cauffman, L., & Berg, I. K. (2002). Solution-focused Corporate Coaching. *LERNENDE ORGANISATION*, January/February.
- Caughlin, J. P. (2002). The demand/withdraw pattern of communication as a predictor of marital satisfaction over time: Unresolved issues and future directions. *Human Communication Research, 28*, 49-85.
- Caulkins, J. P., Morrison, E. L., & Weidemann, T. (2007). Spreadsheet Errors and Decision Making: Evidence from Field Interview. *Journal of Organizational and End User Computing, 19*(3), 2-23.
- Cepeda, L. M., & Davenport, D. S. (2006). Person-centered therapy and solution-focused brief therapy: An integration of present and future awareness. *Psychotherapy: Theory, Research, Practice, Training, 43*(1), 1-12.
- Chadwick, S. (2009). From outside lane to inside track: sport management research in the twenty-first century. *Management Decision, 47*(1), 191-203.
- Chang, R. C. (2004, October 30). *Time Motion Study for Modular Caustic Solvent Extraction Unit* (OSTI ID: 835552nd ed., WSRC-MS-2004-00703, pp. 1-6) [DOE Contract Number AC09-06SR18500]. Savannah River Site (US): US Department of Energy.

- Clampitt, P. G. (1991). *Communicating for Managerial Effectiveness*. Thousand Oaks, CA, U.S.A.: Sage.
- Clarke, W. J., Alves, L. C., Dell, T. J., Elfering, H., Kubala, J. P., Lin, C., et al. (2009). IBM System z10 design for RAS. *IBM Journal of Research & Development*, 53(1), 11:1-11:11.
- Cocchiara, R., Davis, H., & Kinnaird, D. (2008). Data center topologies for mission-critical business systems. *IBM Systems Journal*, 47(4), 695-706.
- Cohen, J., & Cohen, P. (1983). *Applied multiple regression/correlation analysis for the behavioural sciences* (2nd ed.) Hillsdale, N.J.: U.S.A.: Lawrence Erlbaum Associates Inc. (Original work published 1975).
- Conklin, C. R., Hollenback, C. J., Mayer, C., & Winter, A. (2007). Reducing planned outages for book hardware maintenance with concurrent book replacement. *IBM Journal of Research and Development*, 51(1/2), 157-171.
- Constitution of the United States (1787). *Article I, Section 2* (Census Clause).
- Continuous Improvement Facilitators. (2006). A systematic problem solving & decision making method. In *Kepner-Tregoe* (pp. 1-26). Edmond, OK: U.S.A.: Continuous Quality Improvement Facilitator.
- Cooper, L. (2006, October 11). CSF's, KPI's, Metrics, Outcomes and Benefits – Part 1. *DITY*, 2(4), 1-6.
- Coppola, M. N., Major. (1997). The Four Horsemen of the Problem Solving Apocalypse. *U.S. Army Medical Department Journal*, 7/8, 20-27.
- Corcoran, J., & Pillai, V. (2009). A Review of the Research on Solution-Focused Therapy. *British Journal of Social Work*, 39, 234-242.
- Craig, D., Kanakamedala, K., & Tinaikar, R. (2007). *The next frontier in IT strategy: A McKinsey Survey* (Spring 2007, pp. 1-3). New York, NY: U.S.A.: McKinsey.
- Creasy, E. S., Sir. (1851). *Fifteen Decisive Battles of the World: from Marathon to Waterloo* (1st ed.) London: England: Wildside.
- Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.) Thousand Oaks, CA, U.S.A.: Sage. (Original work published 1994).
- Cummings, J. C., & Kiesler, S. (2008). Who Collaborates Successfully? Prior Experience Reduces Collaboration Barriers in Distributed Interdisciplinary Research. In *Proceedings of the 2008 ACM Conference on Computer-Supported Cooperative Work*. San Diego, CA: U.S.A., 437-446.
- Darwin, C. R. (1859). *On the Origin of Species by Means of Natural Selection, or the Preservation of Favoured Races in the Struggle for Life*. (1st ed.) London, England: John Murray.

- Das, O., & Das, A. (2008). Performability evaluation of mobile client-server systems. In *Proceedings of the 2008 ACM Symposium on Applied Computing*. Fortaleza, Ceara, Brazil, 2197-2201.
- Dashofy, E. M., van der Hoek, A., & Taylor, R. N. (2002). Towards architecture-based self-healing systems. In *Proceedings of the 2002 Workshop on Self-healing Systems WOSS '02*. Charleston, SC: U.S.A., 21-26.
- Davies, M. (2003). *IT Service Management: An Overview* [White Paper]. Retrieved September 5, 2006, from <http://www.proactiveservices.com.au/uploads/White%20Paper%20ITSM%20Overview2001.pdf>
- Davis, K. (1953). Management Communication and the Grapevine. *Harvard Business Review*, September-October(29), 43-49.
- de Kleer, J, Mackworth, A, & Reiter, R. (1990). Characterizing Diagnoses. In *Proceedings from the 8th National Conference on Artificial Intelligence (AAAI'90)*, Boston, MA: U.S.A., 324-330.
- de Pillis, E. G., & Meilich, O. (2006). V. J. Kannan (Ed.). A reduced and updated revision of the Schein Descriptive Index. In *Proceedings from the 35th Annual Meeting of Western Decision Sciences Institute*, Waikoloa, HI: U.S.A., 552.
- de Pillis, E., Kernochan, R., Meilich, O., Prosser, E., & Whiting, V. (2008). Are managerial gender stereotypes universal? The case of Hawai'i. *Cross Cultural Management: An International Journal*, 15(1), 94-102.
- De Villiers, F. (Compiler). (2006). *The Illustrated Lean Agile and World Class Manufacturing Cookbook*. San Francisco, CA: U.S.A.: Scribd.
- De Vries, P., Mulig, E. V., & Lowery, K. (2004). A useful tool for data scanning in executive information systems: schematic faces. *Industrial Management & Data Systems*, 104(8), 644-649.
- Deglar, D., & Lewis, R. (2004). Maintaining Ontology Implementations: The Value of Listening. In *Extreme Markup Languages* (August). Montreal, Quebec: CA, 1-14.
- DeMarie, S. M., & Hitt, M. A. (2000). Strategic Implications of the Information Age. *Journal of Labor Research*, XX13, 419-429.
- Demsky, A. (1996). Who Returned First-Ezra or Nehemiah? *Bible Review*, 12(02), 28-33.
- Döckel, A. (2003). *The Effect of Retention Factors on Organisational Commitment: an Investigation of High Technology Employees*. Unpublished Masters Thesis, University of Pretoria, Pretoria, South Africa.
- Dorio, J. M. (2005). *The Impact of Gender-Role Stereotypes and the Sex-Typing of the Professor Job on Performance Evaluations in Higher Education*. University of South Florida, Tampa, Florida.
- Duehr, E. E., & Bono, J. E. (2006). Men, Women, And Managers: Are Stereotypes Finally Changing? *Personnel Psychology*, 59(4), 815-846.

- Duncan, A. (2008). Sustainable risk management from the basement to the boardroom. *Keeping Good Companies, June*, 305-308.
- Eckhaus, J. (2004). Data Centre Relocation. *DM Review, 14*(5), 44-44.
- Eldridge, K. A., & Christensen, A. (2002). Demand-withdraw communication during couple conflict: A review and analysis. In P. Noller & J. A. Feeney (Eds.), *Understanding marriage: Developments in the study of couple interaction* (pp. 289–322). Cambridge, UK: Cambridge University Press.
- Emison, G. A. (2004). Pragmatism, Adaptation, and total quality Management: Philosophy and Science in the Service of Managing Continuous Improvement. *Journal of Management in Engineering, April* (2004), 56-61.
- Enriquez, P., Brown, A. B., & Patterson, D. A. (2002). Lessons from the PSTN for Dependable Computing. In *Proceedings of the 2002 Workshop on Self-Healing, Adaptive and Self-MANaged Systems (SHAMAN)*. NY, NY: U.S.A., 1-7.
- Fitchett, H. (2004, May). Data Center Relocation. *DM Review, 14*(5), 44-44.
- Fleizach, C., Liljenstam, M., Johansson, P., Voelker, G. M., & Méhes, A. (2007). Can You Infect Me Now? Malware Propagation in Mobile Phone Networks. In *Proceedings of the 5th ACM Workshop on Recurring Malcode (WORM '07)*, Alexandria, VA: U.S.A.
- Fordahl, M. (2001, January 29). Industry, academia try to kill bugs. *Eagle Tribune*. Retrieved November 23, 2005, from <http://www.eagletribune.com/news/storeis/20010129>.
- Fourali, C. (1999). Quality Assurance in Psychotherapy and Counseling. *International Journal of Psychotherapy, 4*(2), 161-177.
- Fox, A. (2002). Toward Recovery-Oriented Computing. In *Proceedings of the 28th International Conference on Very Large Data Bases, VLDB Endowment*. Hong Kong, China.
- Fox, A. (2003). Other Research Leaders [Computing]. *Scientific American, 289*(6), 55-69.
- Fox, A., & Patterson, D. (2003), Self-Repairing Computers. *Scientific American, 288*(6), pp. 54-62.
- Free, C., & Radcliffe, V. (2009). Accountability in Crisis: The Sponsorship Scandal and the Office of the Comptroller General in Canada. *Journal of Business Ethics, 84*, 189-208.
- Froerer, A. S., Smock, S. A., & Seedall, R. B. (2009). Solution-Focused Group Work: Collaborating with Clients Diagnosed with HIV/AIDS. *Journal of Family Psychotherapy, 20*(1), 13-27.
- Galup, S., Quan, J. J., Dattero, R., & Conger, S. (2007). Information technology service management: an emerging area for academic research and pedagogical development. *Computer Personnel Research Annual Conference: The Global Information Technology Workforce: IT Service Management*, 46-52. St. Louis, MI: U.S.A.: ACM SIGMIS (Nov 9-14, 2008).

- Ganesh, B., Illsley, R., Rodger, A., & Thompson, M. (Researcher). (2008). *IT Systems Management Exploiting the Infrastructure for Business Value* (RTO10408IMT, pp. 1-289). Hull, East Yorkshire, UK: Butler Direct Limited a Datamonitor Company.
- Gates, W. H., III. (2007). Great Expectation. In *Commencement address at Harvard University*. Cambridge, MA: U.S.A.: Harvard University. (Original work published June 7, 2007 Retrieved March 3, 2009, from http://humanity.org/voices/commencements/speeches/index.php?page=gates_at_harvard)
- General Accounting Office (GAO) (2009). *Federal Information System Controls Audit Manual* (GAO/AIMD-12.19.6. pp. 1-599). Washington, D.C.: U.S.A.: United States General Accounting Office.
- Ghemawat, S., Gobiuff, H., & Leung, S.-T. (2003). The Google file system. In *Proceedings of the 19th ACM Symposium on Operating Systems Principles SOSP*. Bolton Landing, NY: U.S.A.
- Gibbs, L., Kealy, M., Willis, K., Green, J., Welch, J., & Daly, J. (2007). What have sampling and data collection got to do with good qualitative research? *Australian and New Zealand Journal of Public Health*, 31(6), 540-544.
- Gillingham, D., & Noizet, J. (2007). A response model for the public relations management of a critical incident. *Disaster Prevention and Management*, 16(4), 545-550.
- Gonzalez, D. (2008). STEM Progress in Katrina's Wake. *Tech Directions*, 67(8), 23-26.
- Goss, T., Ph.D. (2004). Gettysburg's "Decisive Battle". *Military Review*, July-August, 11-16.
- Graham, S., & Sherman, L. (2003, April 23). Opinion: Windows can mean dependable uptime. *ComputerWorld*.
- Greatbatch, D., & Clark, T. (2002). Laughing with the gurus. *Business Strategy Review*, 13(3), 10-18.
- Greiner, L. (2007). ITIL: The International Repository of IT Wisdom. *NetWorker*, 11(4), 9-11.
- Grottke, M. & Trivedi, K. S. (2005[a]). A Classification of Software Faults, In *Supplemental Proceedings of the Sixteenth International Symposium on Software Reliability Engineering*, 2005, Chicago, IL: U.S.A., 4.19-4.20.
- Grottke, M. & Trivedi, K. S. (2005[b]). Software Faults, Software Aging and Software Rejuvenation, *Journal of the Reliability Engineering Association of Japan* 27(7), 425-438.
- Grover, V., Henry, R., & Thatcher, J. (2007). "Fix IT-Business Relationships through Better Decision Rights," *Communications of the ACM*, 50(12), 80-86.
- Guida, M., Longo, M., & Postiglione, F. (2008). Reliability and Survivability Methodologies for Next Generation Networks. In *Proceedings of the 6th International Conference on Advances in Mobile Computing and Multimedia*, Linz, Austria, 326-331.

- Grzywacz, J. G., & Butler, A. B. (2005). The Impact of Job Characteristics on Work-to-Family Facilitation: Testing a Theory and Distinguishing a Construct. *Journal of Occupational Health Psychology, 10*(2), 97-109.
- Gupta, H. V. & Shoshan, S. (2003). MTTR. i Six Sigma. Abstract retrieved November 13, 2005 from <http://www.isixsigma.com/dictionary/MTTR-429.htm>.
- Gwinner, C. (2006). *Infosurv white paper: 5-point vs. 6-point Likert scales*. Retrieved September 4, 2006, from http://www.infosurv.com/images/Likert_Scale_Debate.pdf
- Hallinger, P., & Kantamara, P. (2001). Learning to lead global changes in local cultures: Designing a computer based simulation for Thai school teachers. *Journal of Educational Administration, 39*(3), 197-220.
- Harding, J. (2008). Information literacy and the public library: we've talked the talk, but are we walking the walk? *The Australian Library Journal, 57*(3), 274-294.
- Harris Interactive. (2009, January 21). *Is Your Boss Presidential* [Survey on behalf of Randstad US]. Retrieved May 12, 2009, from <http://www.thefreelibrary.com/Is+Your+Boss+Presidential%3f-a0193389270>
- Harris, K. (2008). Qualitative research: Quo vadis? *B & T Magazine, 58*(2660), 15.
- Hart, G. (2006). The Information Literacy Education Readiness of Public Libraries in Mpumalanga Province (South Africa). *Libri: International Journal of Libraries and Information Services, 56*, 48-62.
- Hartley, K. L. (2005). Defining Effective Service Level Agreements for Network Operation and Maintenance. *Bell Labs Technical Journal, 9*(4), 139-143.
- Hatch, J., & Zweig, J. (2000). What is the stuff of an entrepreneur? *IVEY Business Journal, (65) 2*, 68-72.
- Hayes, B. (2007). Fat Tails: Sometimes the average is anything but average. *American Scientist, 95*(3), 200-204.
- Hayes, F. (2005, December 15). IT Heroes. *Computerworld, 86*.
- HCI. (2009). Cause and effect diagrams. *Cause and effect diagrams*. Abstract retrieved April 7, 2009, from <http://www.hci.com.au/hcisite5/library/materials/Cause%20and%20effect%20diagrams.htm>.
- Hershey Foods Corporation. (1999). Hershey Foods Corporation (Annual Report), Hershey, PA: Hershey Foods Corporation.
- Hinson, G. (Author), & Neumann, P. G. (Moderator). (2008). Computerised anti-aircraft gun kills 9. In *ACM SIGSOFT Software Engineering Notes* (1st ed., Vol. 33, p. 18). Atlanta, GA: U.S.A.: ACM SIGSOFT (Nov 9-14, 2008).
- Hisrich, R.D. (Ed.) (1986). *Entrepreneurship, Intrapreneurship and Venture Capital*, Lexington Books, Lexington, MA: U.S.A.

- Hitch, L., & Sullivan, B-A. (2006). Higher ed 101 - teaching techies higher ed culture. In *Proceedings of the 34th annual ACM SIGUCCS Conference on User Services* (pp. 143-148). Edmonton, Alberta: Canada.
- Hochmuth, P. (2004, October 4). Winning over skeptics, VoiP support builds. *NetworkWorld*, 22-22.
- Holden, J., & Thompson, M. (Researcher). (2006). *IT Service Management: Provision of IT with Organisational Benefits: RT010606ISM. Technology Management and Strategy Report* (pp. 1-164). Hull, East Yorkshire, UK: Butler Group a Datamonitor Company.
- Hollerith, H. (1914). Tabulating Machine. U.S. Patent 1,087,061. Washington, DC: U.S. Patent and Trademark Office.
- Hopper, G. M. (1981). The First Bug. *IEEE Annals of the History of Computing*, 3(3), 285-286.
- Houck, D.J., Kim, E., O'Reilly, G. P., Picklesimer, D. D., & Uzunalioglu, H. (2004). A Network Survivability Model for Critical National Infrastructures. *Bell Labs Technical Journal*, (8), 4, 153-172.
- How to ctrl, alt, delete \$48 billion. (2007, March 2). *The Age*. Retrieved March 5, 2007, from <http://www.theage.com.au/news/technology/ctrl-alt-delete-what-happend-to-the48bn/2007/03/22/1174153207365.html>.
- Huczynski, A. (1993). *Management Gurus*. London: Routledge.
- Hunt, J., & McCollom, M. (1994). Using Psychoanalytic Approaches in Organizational Consulting. *Consulting Psychology Journal*, 46(2), 1-11.
- Hurst, D., Rush, J., & White, R. (1989). Top Management Teams and Organisational Renewal. *Strategic Management Journal*, 10 (SI), 87-105.
- IBM Corporation. (2008, September). *IBM IT Facilities Consolidation and Relocation Services - data center consolidation and relocation* (SFD03011-USEN-00, pp. 1-4). Somers, NY: U.S.A.: IBM Global Services.
- ILX Group PLC. (2007, November 12). UK Businesses not ready for ITIL Version Three [Independent survey shows UK IT managers are ill equipped to meet ITIL standards]. *M2 Presswire*, 1.
- Im, G. P., & Baskerville, R. L. (2005). A Longitudinal Study of Information System Threat Categories: the Enduring Problem of Human Error. *The DATA BASE for Advances in Information Systems*, 36(4), 68-79.
- Industry Leaders. [SAF Corporate Leaders]. (2009). *Service Availability Forum*. Abstract retrieved September 7, 2009, from <http://www.saforum.org/Industry-Leaders~214708~16627.htm>
- Iqbal, A. (2008). Evaluation of Economy in a Zero-sum Perfect Information Game. *The Computer Journal*, 51(4), 408-418.

- Jackson, P. Z., & McKergow, M. (2007). *The Solutions Focus: Making coaching and change SIMPLE* (2nd ed.) London, U.K.: Nicholas Brealey Publishing. (Original work published 2002).
- Jamieson, L., & Williams, L. M. (2003). Focus group methodology: Explanatory notes for the novice nurse researcher. *Contemporary Nursing*, 14(3), 271-280.
- Jews, C., Ahmad, R., & Surman, D. H. (2008). IBM Parallel Sysplex Clustering: Technology options for continuous availability. *IBM Systems Journal*, 47(4), 505-517.
- Johannisson, B. (1998). Personal networks in emerging knowledge-based firms: spatial and functional patterns. *Entrepreneurship & Regional Development*, 10, 297-312.
- Johnson, A. M., & Lederer, A. L. (2005). The Effect of Communication Frequency and Channel Richness on the Convergence Between Chief Executive and Chief Information Officers. *Journal of Management Information Systems*, 22(2), 227-252.
- Jones, K. A., Smith, N. C., & Holmes, P. S. (2004). Anxiety Symptom Interpretation and performance Predictions in High-Anxious, Low-Anxious and Repressor Sport Performers. *Anxiety, Stress & Coping*, 17(2), 187-199.
- Joyce, A. (Ed.). (2008). *World Almanac & Book of Facts: 2008 Edition. Computer Milestones*. New York, NY: U.S.A. Simon & Schuster, Inc.
- Junelle, P. (Author), & Neumann, P. G. (Moderator). (2007, October 29). Gatwick Airport screens display wrong local time (88th ed., Vol. 24). Message posted to <http://catless.ncl.ac.uk/Risks/24.88.html#subj13>.
- Kepner, C. H., & likubo, H. (1996). A. Hickey (Ed.), *Managing Beyond the Ordinary*. NY, NY: USA: Amacom.
- Kepner, C. H., & Tregoe, B. B., PhD. (1965). *The Rational Manager: A Systematic Approach to problem Solving and Decision Making*. Princeton, NJ: Princeton Research Press.
- Kepner, C. H., & Tregoe, B. B., PhD. (1997). *The New Rational Manager*. Princeton, NJ: U.S.A.: Princeton Research Press.
- Kesby, S. G. (2002). Nursing care and collaborative practice. *Journal of Clinical Nursing*, 11, 357-366.
- Kiciman, E. & Fox, A. (2005). Detecting Application-Level Failures in Component-based Internet Services. *IEEE Transactions on Neural Networks*, 16(5), 1027-1041.
- Kim, G. (2006, June). Beyond Checklists: How to Effectively Audit Change Controls. In *Information Systems Audit and Control Association*. Symposium conducted at the meeting of the ISACA 2006, San Diego, CA: U.S.A.
- Kim, Y., Lau, W. C., Chuah, M. C., & Chao, H. J. (2006). PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks. *IEEE Transactions on Dependable and Secure Computing*, 3(2), 141-155.

- Kimber, D. A., Zhang, X., Franklin, P. H., & Bauer, E.J. (2006). Modeling Planned Downtime. *Bell Labs Technical Journal*, 11(3), 7-19.
- Kirby, M. (1997). Intranets & Information empowerment: the Ascendance of a New Information Architecture. *Strategic Communication Management*, February/March, 14-17.
- Kitzinger, J. (1994). The Methodology of focus groups: The Importance of Interaction Between Research Participants, *Sociology of Health*, 16(1): 103-121.
- Klenke, K., PhD. (1993). Changing roles of information systems professionals: From Technical Managers to Strategic Leaders. In *Special Interest Group on Computer Personnel Research Annual Conference* (pp. 214-225). St. Louis, Missouri: U.S.A.: 1993 Annual Association of Computer Machinery/Computer Personnel Research.
- Kotler, P., & Keller, K. (2006). *Marketing Management* (12th ed.) Upper Saddle River, NJ: U.S.A.: Pearson/Prentice-Hall.
- Kotter, J. P. (2001). What Leaders Really Do. *Harvard Business Review*, 79(11), 85-96.
- Kouzes, J., & Posner, B. (2003). Character Development. *Executive Excellence*, 20(9), 3-4.
- Kozak, M. A., & Uca, S. (2008). Effective Factors in the Constitution of Leadership Styles: A Study of Turkish Hotel Managers. *Anatolia: An International Journal of Tourism and Hospitality Research*, 19(1), 117-134.
- Krueger, R. A., & Casey, M. (2000). *Focus Groups: a Practical Guide for Applied Research* (4th ed.) Thousand Oaks, CA: U.S.A.: Sage. (Original work published 1962).
- Kunkel, A., Dennis, M. R., & Waters, E. (2003). Contemporary university students' ratings of characteristics of men, women, and CEOs. *Psychological Reports*, 93(3), 119-136.
- Lamborn, S. D., Mounts, N., Steinberg, L., & Dornbusch, S. (1991). Patterns of competence and adjustment among adolescents from authoritative, authoritarian, indulgent, and neglectful families. *Child Development*, 62, 1049-1065.
- Langer, S. M., PhD. (2006). Solution-Focused Management. *Northwest Brief Therapy Training Center*. Abstract retrieved September 17, 2009, from <http://www.nwbttc.com/sfmd.html>.
- Laraudogoitia, J. P. (2008). The Comic as a Binary Language: An Hypothesis on Comic Structure. *Journal of Quantitative Linguistics*, 15(2), 111-135.
- Larsen, J. A., Maundrill, R., Morgan, J., & Moulard, L. (2005). Practice development facilitation: An integrated strategic and clinical approach. *Practice Development in Health Care*, 4(3), 142-149.
- Lawshe, C. H. (1975). A Quantitative Approach to Content Validity. *Personnel Psychology*, 4(28), 563-575.

- Leithwood, K., & Slegers, P. (2006). Transformational School Leadership: Introduction. *School Effectiveness and School Improvement*, 17(2), 143-144.
- Lorge, A. (2007, November 8). Timing Glitch Affected Thousands in Marathon [Sports Desk]. *New York Times*, p. D5.
- Loveland, S., Dow, E. M., LeFevre, F., Beyer, D., & Chan, P. F. (2008). Leveraging virtualization to optimize high-availability system configurations. *IBM Systems Journal*, 47(4), 591-604.
- Lumpp, T., Schneider, J., Holtz, J., Mueller, M., Lenz, N., Biazetti, A., et al. (2008). From high availability and disaster recovery to business continuity solutions. *IBM Systems Journal*, 74(4), 605-619.
- Lumsdaine, E., Dr., & Lumsdaine, M. (1994). Team thinking that measures up to the task. *IEEE Potentials*, December '94/January '95, 4-9.
- Maguad, B. A. (2006). The Modern Quality Movement: Origins, Development and Trends. *Total Quality Management*, 17(2), 179-203.
- Malhotra, D., Ku, G., & Murnighan, J. K. (2008). When Winning is Everything. *Harvard Business Review*, 86(5), 78-86.
- Malis, R. S., & Roloff, M. E. (2006). Demand/Withdraw Patterns in Serial Arguments: Implications for Well-Being. *Human Communication Research*, 32, 198-216.
- Manafy, M. (2005). Shout it Out Loud. *EContent*, 28(3), p.6.
- Mankowski, M. (2007). *SaaS/Hosting Case Studies -- Interviews with SaaS Providers: Mass Market Quarterly Series* (4Q06 ed., pp. 1-6) Minneapolis, MN: U.S.A.: Tier1Research.
- Mann, S., & Janzen, R. (2007). Fluid Samplers: Sampling music keyboards having fluidly continuous action and sound, without being electrophones. In *ACM Multimedia 2007* (pp. 912-921). Augsburg, Bavaria: Germany: MultiMedia 2007.
- Margeson, B. (2003). The Human Side of Data Loss. *Disaster Recovery Journal*, 16(2), 48-48.
- Marquis, H. (2006, June 21). Thinking About Kepner-Tregoe. *DITY*, 2(24), 1-4.
- Marquis, H. (2009, February 12). Impact Assessment in 5 Simple Steps. *DITY*, 5(6), 1-4.
- Maslow, A. H. (1943). A Theory of Human Motivation. *Psychological Review*, 50(4), 370-396.
- Materna Information & Communications. (2007). *IT Service Management Executive Survey: IT Service Management Survey 2007. Standardisation Before Customisation*. Germany.
- Materna Information & Communications. (2008). *IT Service Management Executive Survey: IT Service Management Survey 2008*. Germany and Austria.

- Mayer, P. (2005). How to lower your storage costs. *Communications News*, 42(5), 18-22.
- Mayfield, J. (2009). Motivating language: a meaningful guide for leader communications. *Development and Learning in Organizations*, 23(1), 9-11.
- Maze-Emery, E. (2008). Seven quality tools can help supervisors roll a winner. *Tooling & Production*, 74(9), 23-23.
- McGovern, P. (1997). Management Gurus: The Secret of Their Success? *Business Strategy Review*, 8(3), 52-60.
- McKee, A., & Massimilian, D. (2006). Resonant leadership: a new kind of leadership for the digital age. *Journal of Business Strategy*, 27(5), 45-49.
- McKergow, M., PhD, & Clarke, J. (2007). *Solutions Focus Working: 80 real-life lessons for successful organizational change*. United Kingdom: SolutionsBooks.
- McKinney, M. (2007). What Happens When the IT System Goes Down? *Hospitals & Health Networks*, 81(12), 14-14.
- McLaughlin, G. T., Liu, L. Y., DeGroff, D. J., & Fleck, K. W. (2008). IBM Power Systems platform: Advancements in the state of the art in IT availability. *IBM Systems Journal*, 47(4), 519-533.
- McLaughlin, K. A., & Damiano, F. (2007) American ITIL. In *Proceedings of the 35th Annual ACM SIGUCCS Conference on User Services*. ISGUCCS'07, Orlando, FL: U.S.A., 251-254.
- Meletta, L.-B. C. (2008). Non-Enforcement by a Local Executive: Limitations of Judicial Review and Considerations to Restrain the Use of Executive Power. *New York University Annual Survey of American Law*, 63(3), 511-546.
- Miettinen, O. S., MD, & Flegel, K. M., MD. (2003). Elementary concepts of medicine: VIII. Knowing about a client's health: gnosis. *Journal of Evaluation n Clinical Practice*, 9(3), 333-335.
- Miller, D. (1983). The Correlates of Entrepreneurship in Three Types of Firms. *Management Science*, 29(7), 770-791.
- Mills, E. (2009, March 30). Melissa Virus Turns 10. Message posted to <http://www.cbsnews.com/stories/2009/03/30/tech/cnettechnews/main4903386.shtml>.
- Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics*, 38(8), 114-117.
- Morrill, H., Beard, M., & Clitherow, D. (2008). Achieving continuous availability of IBM systems infrastructures. *IBM Systems Journal*, 47(4), 493-503.
- Morris, M. H., Allen, J., Schindehutte, M., & Avila, R. (2006). Balanced management Control Systems as a mechanism for Achieving Corporate Entrepreneurship. *Journal of Managerial Issues*, XVIII(4), 468-493.

- Muenjohn, N. (2009). Expatriates_ Leadership Behaviours and Local Subordinates Extra Effort, Satisfaction, and Effectiveness. *The Business Review, Cambridge, 13(2)*, 260-266.
- Mulier, T. (2008, June 19). Nestle Says Jenny Craig Weight-Loss Sales Slowing. *Bloomberg*. Retrieved June 13, 2009, from http://www.bloomberg.com/apps/news?pid=20601085&sid=aFExE7O_Phmw&refer=europe
- Nahrstadt, B. C. (2009). Former Employee Sabotage? Invoke the Computer Fraud and Abuse Act. *Journal of Internet Law, February*, 17-26.
- Neuendorf, K. A. (2002). *The Content Analysis Guidebook*. Thousand Oaks, CA: U.S.A.: Sage.
- New York Road Runners (2009). Prize Money. Retrieved November 28, 2009 from <http://www.nyrr.org/races/procedures/prizemoney.asp>.
- Loas, G., Noisette, C., Legrand, A., & Boyer, P. (2000). Is Anhedonia a Specific Dimension in Chronic Schizophrenia? *Schizophrenia Bulletin, 26(2)*, 495-506.
- Nordstrom, C., Ph.D., & Thomas, S. L. (2007). *North American Journal of Psychology, 9(2)*, 359-376.
- Northrop, R. (2003, April 22). The Sleeping Bag Solution. *Intelligent Enterprise, 6(7)*, 44-46.
- Norton, R. W. (1978) Foundation of a Communicator Style Construct. *Human Communication Research. 4(2)*, 99-112.
- Nunnally J.C. (1978). *Psychometric Theory*, 2nd edition. McGraw-Hill, New York.
- O'Callaghan, K. (2008). Characteristics of Incident Managers, *itSMF Australia Bulletin*, Winter, p. 20.
- O'Callaghan, K. (2009). There are only Seven Types of Unplanned Outages, *itSMF Australia Bulletin*, Summer, p. 10.
- O'Callaghan, K. & Mariappanadar, S. (2006[a]). Solution-Focused Management of Unplanned IT Outages, In *Proceedings of the 7th International We-B working for e- Business Conference*, ISBN 178-1-86272-670-3, Melbourne, Victoria, Australia.
- O'Callaghan, K. & Mariappanadar, S. (2006[b]). Unplanned IT Outages, In *Proceedings of the 2006 Pacific Internet and Information and Communication Technologies PacINet Conference*, Apia, Samoa.
- O'Callaghan, K. & Mariappanadar, S. (2008). Approaches Used by Incident Managers to Restore Service When Unplanned IT Outages Occur, *IT Professional (10)3*, 40-45.
- O'Callaghan, K., Mariappanadar, S. (2010). Incident Manager? Meet PHIL CROSS. IT Service Management Forum Australia, *Informed Intelligence*, Summer, p. 7.

- O'Callaghan, K., Mariappanadar, S., and Thomas, T. (2010). Managing Unplanned IT Outages. *CIO Magazine (New Zealand)*.
- Okpara, J. O., Dr. (2006). The Relationship of Personal Characteristics and Job Satisfaction: A Study of Nigerian Managers in the Oil Industry. *The Journal of American Academy of Business, Cambridge, 10(1)*, 49-58.
- Orbitz, LLC. (2003). SEC File 333-88646. *Software Maintenance, Data Services and Operations Service Level Agreement* (Accession Number 1047469-3-39912).
- Orr, C. (2008, November). Seven Practical Steps to Mitigate Virtualization Security Risks. In *Virtualization Today*. Symposium conducted at the meeting of the Cloud Computing Expo 2008, San Jose, CA: U.S.A.
- Pelleg, D., Ben-Yehuda, M., Harper, R., Spainhower, L., & Adeshiyani, T. (2008). Systems work at IBM Research. *ACM SIGOPS Operating Systems Review: Vol. 42. Vigilant: out-of-band detection of failures in virtual machines, 42(1)*, 26-31.
- Perillin, L. A. (2005). Student Disengagement and the Socialization Styles of High Schools. *Social Forces, 84(2)*, 1159-1179.
- Pfleeger, S. L., & Rue, R. (2008). Cybersecurity Economic Issues: Clearing the Path to Good Practice. *IEEE Software, 2008(January/February)*, 35-42.
- Pichot, L., Pierre, J., & Burlot, F. (2009). Management practices in companies through sport. *Management Decisions, 47(1)*, 137-150.
- Pinto, J. B., & Piso, C. N., PhD. (2009). Gaining insight into the ophthalmic personality. *Ocular Surgery News - U.S. Edition, March 10*, 18-22.
- Prabhakar, G., Rastogi, R., & Thottan, M. (2005). OSS Architecture and Requirements for VoIP Networks. *Bell Labs Technical Journal, 10(1)*, 31-45.
- Praeg, C.-P., & Schnabel, U. (2006). IT-Service Cachet -managing IT-service performance and IT-service quality. In *Proceedings from the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*. Kuai, HI: U.S.A., Volume 2, 34.1.
- Qi, L., Jin, H., Foster, I., & Gawor, J. (2008). Provisioning for Dynamic Instantiation of Community Services. *Virtual Organizations, 12(2)*, 29-36.
- Radhakrishnan, R., Mark, K., & Powell, B. (2008). IT service management for high availability. *IBM Systems Journal, 47(4)*, 549-561.
- Ramakrishnan, K. K., Shenoy, P., & Van der Merwe, J. (2007). Live Data Center Migration across WANs: A Robust Cooperative Context Aware Approach. In *Applications, Technologies, Architectures, and Protocols for Computer Communication* (pp. 262-267). Kyoto, Japan: SIGCOMM workshop on Internet network management.
- Ramanathan, J., Ramnath, R., & Glassgow, R. (2009). *The People, the Process or the Technology? Using the ACE framework to make tradeoffs in service delivery improvement*. In Proceedings of the 2009 ACM Symposium on Applied Computing. Organizational Engineering Track, 259-264.

- Ritchie, G. (2008). *Incident Management – Do's and Don'ts* (Version 3 ed., pp. 1-10) [White Paper] Livingston EH54 6QF Scotland, UK: Serio Limited.
- Robinson, R., & Polozoff, A. (2003). Planning for Availability in the Enterprise. *IBM WebSphere Developer Technical Journal*, December(6.9).
- Roeber, J. & Locsin, D. (2004). NSI Software, Inc. Educates Attendees at Contingency Planning Expo with Methods for Maintaining Business Continuity and Measuring ROI. Media Alert, November 3, Retrieved on October 29, 2005 from <http://www.nsi.Software.com/NR/rdonlyres/DEB1AEE5-11F4-462D-9FD8-BOBE6F0D7649/12/CPMExpoAlertFINAL2.pdf> on October 29, 2005.
- Rollag, K. (2007). Defining the term 'new' in new employee. *Journal of Occupational and Organisational Psychology*, 80, 63-75.
- Rooney, J.J., Kubiak, T.M., Westcott, R., Reid, R.D., Wagoner, K., Pylipowe, P. E., et al. (2009). Building from the Basics: Master these quality tools and do your job better. *Journal for Quality and Participation*, 31(4), 18-29.
- Royse, D., Thyer, B., Padgett, D., & Logan, T. (2006). *Program Evaluation: An Introduction* (4th ed.) Belmont, CA: U.S.A.: Thomson Brooks/Cole. (Original work published 2001).
- Rust, R. T., & Miu, C. (2006). What Academic Research Tells Us About Service. *Communications of the ACM*, 49(7), 49-54.
- Sallé, M. (2004). IT Service Management and IT Governance: review, comparative analysis and their impact on utility computing. Hewlett-Packard Company.
- Schein, V. E. (1973). The relationship between sex role stereotypes and requisite management characteristics. *Journal of Applied Psychology*, 57, 95-100.
- Schein, V. E. (1975). Relationships between sex role stereotypes and requisite management characteristics among female managers. *Journal of Applied Psychology*, 60, 340-344.
- Schenk, K. D., Vitalari, N. P. & Davis, K. S. (1998), Differences Between Novice and Expert Systems Analysts: What Do We Know and What Do We Do? *Journal of Management Information Systems*, 15(1), 9-50.
- Schjoedt, L. (2009). Entrepreneurial job characteristics: an examination of their effect on entrepreneurial satisfaction. *Entrepreneurship: Theory and Practice*, 33(3), 619-645.
- Schroeder, B., & Gibson, G. A. (2007). Understanding disk failure rates: What does an MTTF of 1,000,000 hours mean to you? *ACM Transactions on Storage*, 3(3), 8:1-8:31.
- Schumpeter, J. A. (1982). *The Theory of Economic Development: An Inquiry into Profits, Capital, Credit, Interest, and the Business Cycle*. Cambridge, MA: U.S.A.: Harvard University Press. (Original work published 1949).

- Schwartz, G. (2008, April 2). *Confirmit drives service improvement program for Serco Solutions*. Retrieved May 20, 2008, from http://www.responsesource.com/releases/rel_display.php?relid=37932&export=pdf
- Scott, D. (1999). *Making Smart Investments to Reduce Unplanned Downtime: TG-07-4033. Tactical Guidelines, pp. 1-2. Stamford, CT: GartnerGroup.*
- Scott-Morgan, P. (1994). *The Unwritten Rules of the Game: Master Them, Shatter Them, and Break Through the Barriers to Organisational Change*. New York: McGraw-Hill.
- Shah, M. A., Hellerstein, J. M., & Brewer, E. (2004). Highly Available, Fault Tolerant, Parallel Dataflows. In *Proceedings of the 2004 Association for Computing Machinery's Special Interest Group on Management of Data*. Paris, France, 827-838.
- Sharma, P., & Chrisman, J. (1999). Toward a reconciliation of the definitional issues in the field of corporate entrepreneurship. *Entrepreneurship Theory & Practice*, 23 (3), 11-27.
- Sheehan, J. J., & Ojano, O. T. (2006). The American Presidency: Categorizing and Assessing Leadership Qualities. *Journal of Social Studies Research*, 30(1), 9-14.
- Shockley-Zalabak, P. (2001) *Fundamentals of Organisational Communication: Knowledge, Sensitivity, Skills, and Values (5th Edition)* Allyn & Bacon.
- Shortell, S. M., & Kalunzy, A. D. (2000). *Health Care Management Organization Design and Behavior (4th ed.)* Albany, NY: Delmar Publications.
- Shucksmith, J., Hendry, L. & Glendinning, A. (1995). Models of parenting: Implications for adolescent well-being within different types of family contexts. *Journal of Adolescence*, 18, 253-270.
- Silva, A. S. (2007). the relationship between personality traits and eating pathology in adolescent girls. *Archive of Women's Mental Health*, 10, 285-292.
- Singer, E. (2007). Raising Consciousness. *Technology Review, January/February*, 50-54.
- Smilor, R. (1997). Entrepreneurship: Reflections on a Subversive Activity, *Journal of Business Venturing*, 12(5): 341–345.
- Smith, A. M., & Hinchcliffe, G. R. (2006). Calculating availability to develop preventative maintenance plan. *Plant Engineering*, 60(3), 41-42.
- Smith, G. S., & Amoruso, A. J. (2006). Using real options to value losses from cyber attacks. *Journal of Digital Asset Management*, 2(3/4), 150-162.
- Smock, S. A., Trepper, T. S., Wetchler, J. L., McCollum, E. E., Ray, R., & Pierce, K. (2008). Solution-focused group therapy for level 1 substance abusers. *Journal of Marital and Family Therapy*, 34(1), 107-120.

- Song, Y. J., Tobagus, W., Raymakers, J., & Fox, A. (2004). *Is MTTR More Important Than MTTF For Improving User-Perceived Availability?* Manuscript submitted for publication, Stanford University.
- Spangler, T. (2006, July). Don't Spring a Data Leak. *Baseline*, 15-18.
- Spector, L. (2008, July). Answer Line. *PC World*, 26(7), 116.
- Stanford, L. G. (2007). Welcome Address [Keynote Address]. In *itSMF - Thailand*. Bangkok, Thailand: The IT Service Management Forum - Thailand.
- Steinberg, R. A. & Goodwin, M. (2006, October 23). Getting a head start on ITIL - To survive in the 21st century, IT must manage itself based on the services it delivers. *InfoWorld*, 28(43), 10-15.
- Stevenson, H. H. & Jarillo, J. C. (1990). A Paradigm of Entrepreneurship: Entrepreneurial Management. *Strategic Management Journal (Summer Special)*, 11(4), 17-27.
- Strechay, R., & White, J. (2007). Storage Management and ITIL: Where To Begin? *Business Communications Review*, April, 54-59.
- Stump, J. (2007, February 13). State Won't Bear Cost of Weight Watchers for Medicaid Recipients. *Charleston Daily News*.
- Sunrise Software Ltd. (2008). *The ITIL Maturity Report* (pp. 1-15). Surrey, United Kingdom: Sunrise Software, Ltd.
- Syverud, K. D. (2006). Lessons from Working for Sandra Day O'Connor. *Stanford Law Review*, 58(6), 1731-1733.
- Tanner, J. C. (2005). The true value of communication. *Telecom Asia*, 16(2), 4.
- Taylor, L. A., & Skjei, S. M., P.E. (2002). A Disaster-Recovery Plan For Local Municipalities Using Currently Available Communication Satellite Facilities and Services. In *Proceedings from the National Conference on Digital Government*. Los Angeles, CA: U.S.A., 1-11.
- Taylor, S. (Chief Architect). (2007). *Service Operations*. Norwich, U.K.: Controller of Her Majesty's Stationery Office.
- The Monkeys Behind the Scenes. (2008). Retrieved March 3, 2008, from http://www.surveymonkey.com/Home_CompanyInfo.aspx.
- The World's OnLine Marketplace* (2008) [Data file]. California: U.S.A.: e-Bay. Retrieved November 23, 2005, from <http://pages.ebay.com/aboutebay/thecompany/companyoverview.html>.
- Thompson, E. H., Jr. (2006). Images of Old Men's Masculinity: Still a Man? *Sex Roles*, 55, 633-648.
- Timmons, J. A. (2000). *New venture creation: Entrepreneurship 2000* (5th ed.) Homewood, IL: U.S.A.: Irwin Publishing.

- Toor, S.-U., & Ofori, G. (2009). Ethical Leadership: Examining the Relationships with Full Range Leadership Model, Employee Outcomes, and Organizational Culture. *Journal of Business Ethics*, 90(4), 533-547.
- Trepper, T. S., Dolan, Y., McCollum, E. E., & Nelson, T. (2006). Steve de Shazer and the Future of Solution-Focused Therapy. *Journal of Marital and Family Therapy*, 36(2), 133-139.
- Tsuruoka, D. (2008). Amazon.com Web Site Has More Problems On Monday, Following Its Outage On Friday; Shares Fall For A Second Day; Performance tracker says e-tailer's outage on Friday lasted more than two hours. *Investor's Business Daily, Section A*, 4.
- Turner, C. (2002). *Lead to Succeed*. US: Texere Publishing.
- Umarji, M., & Seaman, C. (2008). Why Do Programmers Avoid Metrics? In *Proceedings in the International Symposium on Empirical Software Engineering and Measurement (ESEM)*, Kaiserslautern, Germany: 129-138.
- Useem, J. (1999, November 11). Can These Marriages Be Saved? *Fortune*, 102-114.
- Verlag, R. H. (2006). G. Lueger & H. Korn (Eds.), *Solution Focused Management*. Mering, Germany: Deutsche Nationalbibliothek.
- Virzi, A. (2006). A Better Way to Manage Problems. *Baseline*, July (Case 217), 51-55.
- Visser, C., & Bodien, G. S. (2005). The 4 Step Method of Solution-Focused Management. *Solution Focused Change in Organizations*. Retrieved June 23, 2007, from http://www.m-cc.nl/solution_focused_change_in_organizations2.htm?the_4_step_method_of_solution-focused_management.htm.
- Visser, C.F. (2009). Doen wat werkt. Oplossingsgericht werken, coachen en managen. Van Duuren Management, 2e druk.
- Volkema, R. J. (2006). Problem formulation as a purposive activity. *Strategic Management Journal*, 7(3), 267-279.
- Volynkin, A. S. (2007). *Advanced Methods for Detecting Malicious Software*. Retrieved from ProQuest Digital Dissertations. (AAT 3285803).
- Walczuch, R., Seelen, J., & Lundgren, H. (2001). Psychological Determinants for Consumer Trust in E-Retailing. In *Proceedings from the 8th Research Symposium on Emerging Electronic Markets*, Maastricht, The Netherlands, 1-21.
- Wang, Y. (2007). Recent Database Challenges in China on Data Consolidation and Integration. In *Proceedings of the 2007 ACM Special Interest Group on Management of Data International Conference on Management of Data*, Beijing, China, 898-898.
- Waschke, M. (2006). ITIL Spurs New Generation of Service Desk Technicians. *SupportWorld*, 38-40.
- Watzlawick, P., Weakland, J., & Fisch, R. (1974). *Change: Principles of problem formation and problem resolution*. New York, NY: U.S.A.: Norton.

- Webb C. & Kevern J. (2001). Focus groups as a research method: a critique of some aspects of their use in nursing research. *Journal of Advanced Nursing*, 33(6), 798–805.
- Weight Watchers. (2009). We're with you, every step of the way, every week of the year. *History & Philosophy: Our philosophy*. Abstract retrieved September 8, 2009, from <http://www.weightwatchers.com.au/about/his/board.aspx>.
- Wickham, P. A. (2004). *Strategic Entrepreneurship*. Harlow: Financial Times Prentice Hall.
- Wienclaw, R. A. (2008). *Research Starters Academic Topic Overview: EBSCO Research Starters. Sample Survey Design*, 1-5. Great Neck, NY: U.S.A.: Great Neck Publishing.
- Wilkinson, S. (2007). What Was Old Is New Again: A century-old idea gives wireless mics new life. *Electronic Musician*, 23(9), 5.
- Wituk, S., Bomhoff, K., Commer, A., Warren, M., & Meissen, G. (2003). Using a focus group methodology to gain input from people who use home and community based services. *Home Health Care Services Quarterly*, 22(4), 27-41.
- Wong, C. A., MSc, RN, & Cummings, G. G., PhD, RN. (2007). The relationship between nursing leadership and patient outcomes: a systematic review. *Journal of Nursing Management*, 15, 508-521.
- Xie, W., Sun, Y., Cao, Y., & Trivedi, K. S. (2003). Modeling of user perceived webserver availability. In *Proceedings of the IEEE International Conference on Communications*. Anchorage, AK: U.S.A.
- Xirasagar, S. (2008). Transformational, transactional and *laissez-faire* leadership among physician executives. *Journal of Health Organization and Management*, 22(6), 599-613.
- Yeung, L. (2004). The paradox of control in participative decision-making: Facilitative discourse in banks. *TEXT*, 1, 113-146.
- Youndt, M. A., Snell, S. A., Dean, J. W., & Lepak, D. P. (1996). Human resource management, manufacturing strategy, and firm performance. *Academy of Management Journal*, 39(4), 836-866.
- Yukl, G. (1998). *Leadership in organisations* (4th ed). Upper Saddle River, NJ: Prentice Hall.
- Zain, A. (2008, February 5). Cable damage hits 1.7m Internet users in UAE. *Khaleej Times Online, News(Nation)*. Retrieved February 13, 2008, from http://www.khaleejtimes.com/DisplayArticleNew.asp?section = theuae&xfile = data/theuae/2008/february/theuae_february155.xml
- Zeng, J. (2007). Improving IT Service Delivery Quality: A Case Investigation. *Journal of American Academy of Business*, 12(1), 24-30.

- Zhang, X., Sharma, M., & Franklin, P. H. (2005). Evaluating system reliability from the customer perspective to improve availability predictions. In *Proceedings of Reliability and Maintainability Symposium (RAMS '05)*. Alexandria, VA, U.S.A., 126-132.
- Zhong, M., Shen, K., & Seiferas, J. (2008). Replication Degree Customization for High Availability. In *Proceedings of the European Conference on Computer Systems*. Glasgow, Scotland: U.K.: 55-68.