

**UNIVERSITY OF SOUTHERN QUEENSLAND**

**AN ANALYSIS OF INFORMATION SECURITY IN SELECTED  
AUSTRALIAN ORGANISATIONS**

A dissertation submitted by

Warren J Darragh, BIT, Grad Dip CIS Mgt

For the award of

Master of Information Technology (Research)

2009

## ABSTRACT

Previous, mainly quantitative, research has indicated that information security threats and incidents are having a significant impact on the conduct of electronic business - and office automation in general - both nationally and internationally. However, as revealed by this study's extensive review of the relevant literature, our understanding of the information security situation in Australian organisations has been quite limited. There has been very little detailed research into security threats and incidents and, equally importantly, the strategies the Australian IT industry is using to deal with them.

In addressing that deficiency, this study used a qualitative, case-based research methodology involving a variety of Australian organisations. The case based approach, using in-depth interviews, facilitated a thorough examination of the information security risks (threats and incidents) and enabled assessment and analysis of management actions (countermeasures) to mitigate the identified risks.

The major findings with regard to this study's research issues are:

- The case-study organisations are generally highly reliant on IT for the conduct of their business and therefore would be heavily impacted if it was unavailable
- They face a variety of information security threats with viruses being the most prevalent threat. The hacking threat was not as evident as reported in the literature
- There are some differences between the Australian information security experience and that reported in the literature for international organisations in particular many of the very large business overseas operate on a much larger scale than those in Australia
- The organisations do not believe that they are specific targets for security attacks; rather they believe that are 'targets of opportunity'
- A wide range of countermeasures are employed; generally, the larger the organisation the greater the diversity and complexity of countermeasures. However, the majority do not have a clear link between risks and countermeasures
- The majority of the organisations do not have a specific security budget.

Whilst Australian organisations were generally well prepared and versed on security issues, the findings indicate the need for the application of best practice across the industry as a whole. A degree of cynicism regarding the nature of the hacking threat was evident – with many participants believing that the threat is overstated. Indeed this study uncovered little direct evidence of the organisations involved being subjected to actual hacker attacks.

The framework developed for this study and its findings are readily adaptable for use by industry. By following the process specified in the framework, organisations will be better able to identify both likely and unlikely threats and incidents and deploy appropriate countermeasures.

## **CERTIFICATION OF DISSERTATION**

I certify that the ideas, experimental work, results, analyses, software and conclusions reported in this dissertation are entirely my own effort, except where otherwise acknowledged. I also certify that the work is original and has not been previously submitted for any other award, except where otherwise acknowledged.

---

Signature of Candidate

---

Date

## **ENDORSEMENT**

---

Signature of Supervisor/s

---

Date

---

## ACKNOWLEDGEMENTS

The completion of this body of work has been an academic and personal journey that dates back to the year 2000, when I was serving with the Australian Army in the Former Yugoslavia – Bosnia – Herzegovina. It was during my spare moments, whilst finalising course work that I first proposed the topic of this dissertation. It was at this time that Professor Edmond Fitzgerald took me under his wing to help guide me through the pitfalls of post graduate research. For his professionalism, patience, and the sacrifice of his own time - long after his departure from the University of Southern Queensland – I owe a debt of gratitude that cannot be repaid.

It was Professor Fitzgerald that helped me to realise that the light at the end of the tunnel was not a train and encouraged and motivated me over eight long years.

I would also like to acknowledge Professor Andy Koronios for his work at the commencement of this research

My family has supported me throughout. The good grace and understanding of my wife and children cannot be under estimated. The gentle encouragement and competitiveness of my siblings who have encouraged and cajoled along the way. They have helped ensure that I complete my ‘masterpiece’.

Thanks go to my father for instilling in me self discipline and patience as well as a love of reading. To my mother, who we lost upon the way, I dedicate this work – your greatest achievements continue to be the children that you pushed to do more.

## TABLE OF CONTENTS AND NOTATION

<b>AN ANALYSIS OF INFORMATION SECURITY IN SELECTED AUSTRALIAN ORGANISATIONS .....</b>	<b>i</b>
<b>ABSTRACT .....</b>	<b>i</b>
<b>ACKNOWLEDGEMENTS.....</b>	<b>iii</b>
<b>TABLE OF CONTENTS AND NOTATION .....</b>	<b>iv</b>
<b>LIST OF FIGURES .....</b>	<b>viii</b>
<b>CHAPTER 1 - INTRODUCTION.....</b>	<b>1</b>
1.1 Background and Significance of the Study .....	1
1.1.1 Significance of Information Security .....	2
1.2 Research Problem.....	2
1.3 Justification for research .....	2
1.3.1 Contribution of the research (contribution to theory/contribution to practice) .....	3
1.4 Methodology .....	3
1.5 Structure of dissertation .....	4
1.6 Delimitations of scope and key assumptions .....	4
1.6 Conclusion .....	4
<b>CHAPTER 2 - LITERATURE REVIEW.....</b>	<b>5</b>
2.1 Risk Management.....	5
2.1.1 Simple Risk Management Model.....	5
2.1.2 Security vs Functionality .....	6
2.1.3 Qualitative Risk Analysis.....	7
2.1.4 Quantitative Risk Analysis.....	8
2.2 Information Security .....	8
2.2.1 Information security components.....	8
2.2.1.1 Confidentiality .....	9
2.2.1.2 Integrity .....	9
2.2.1.3 Availability.....	10
2.2.1.4 Authentication .....	10
2.2.1.5 Non-repudiation .....	10
2.3 The information security in Australia immediate discipline.....	11
2.3.1 Threats to information security in Australian business.....	11
2.3.1.1 Viruses .....	12
2.3.1.2 The internal threat - Disgruntled employees.....	13
2.3.1.3 Hackers and Hacking .....	15
2.3.1.4 Espionage and other threats .....	18
2.3.2 Australian businesses are targets.....	19
2.3.3 Countermeasures .....	20
2.3.3.1 Anti - Virus protection .....	21
2.3.3.2 Intrusion detection.....	23
2.3.3.3 Firewalls.....	25
2.3.3.4 Encryption .....	27
2.3.3.5 Security Policies and Standards .....	29
2.3.3.7 Incident response.....	30
2.3.4 Resource expenditure .....	32
2.3.5 Reliance on Information Technology .....	32
2.4 Development of a theoretical framework.....	34
2.5 Research question.....	36

2.5.1 Research issues.....	36
<b>CHAPTER 3 - METHODOLOGY.....</b>	<b>38</b>
3.1 Research design.....	38
3.1.1 Research purpose .....	38
3.1.2 Research strategy .....	39
Internal validity .....	52
External validity .....	52
Construct validity .....	52
Reliability .....	53
<b>CHAPTER 4 - DATA ANALYSIS .....</b>	<b>58</b>
4.1 Background Information on case studies .....	58
4.2 Overview of within-case analysis method .....	59
4.3. Case A – Small wholesale food business .....	61
4.3.1 Risks.....	62
4.3.2 Management.....	65
4.3.3 Differentiators .....	66
4.3.4 Case A – Security assessment framework .....	67
4.3.5 Summary and recommendations .....	69
4.4 Case B – Commonwealth Government agency .....	69
4.4.1 Risks.....	70
4.4.2 Management.....	76
4.4.3 Differentiators .....	78
4.4.4 Security Framework .....	79
4.4.5 Summary and recommendations .....	81
4.5 Case C – Large Commonwealth agency .....	81
4.5.1 Risks.....	81
4.5.2 Management.....	87
4.5.3 Differentiators .....	89
4.5.4 Security Framework .....	90
4.5.5 Summary and recommendations .....	93
4.6 Case D – Resort/Hospitality Company .....	93
4.6.1 Risks.....	94
4.6.2 Management.....	97
4.6.3 Differentiators .....	98
4.6.4 Security Framework .....	99
4.6.5 Summary and recommendations .....	101
4.7 Case E – Software Company.....	101
4.7.1 Risks.....	102
4.7.2 Management.....	104
4.7.3 Differentiators .....	105
4.7.4 Security Framework .....	106
4.7.5 Summary and recommendations .....	108
4.8 Case F – Small Commonwealth Government Agency .....	108
4.8.1 Risks.....	108
4.8.2 Management.....	112
4.8.3 Differentiators .....	112
4.8.4 Security Framework .....	113
4.8.5 Summary and recommendations .....	115
4.9 Case G – Medium Sized Utility Company.....	115
4.9.1 Risks.....	116

4.9.2 Management.....	121
4.9.3 Differentiators .....	122
4.9.4 Security Framework .....	123
4.9.5 Summary and recommendations .....	125
4.10 Case H – Small Sized Local Council .....	125
4.10.1 Risks.....	125
4.10.2 Management.....	128
4.10.3 Differentiators .....	129
4.10.4 Security Framework .....	129
4.10.5 Summary and recommendations .....	131
4.11 Case I – Small sized State Government Department .....	131
4.11.1 Risks.....	131
4.11.2 Management.....	135
4.11.3 Differentiators .....	137
4.11.4 Security Framework .....	138
4.11.5 Summary and recommendations .....	140
4.12 Case J – Large State Government Department .....	140
4.12.1 Risks.....	141
4.12.2 Management.....	145
4.12.3 Differentiators .....	147
4.12.4 Security Framework .....	147
4.12.5 Summary and recommendations .....	150
4.13 Cross – case analysis.....	150
4.13.1 Risks – Reliance on IT .....	150
4.13.2 Risks - Threats .....	152
4.13.3 Risks – Incidents .....	153
4.13.4 Risks - Australian business as targets .....	154
4.13.5 Management – Countermeasures .....	155
4.13.6 Management – Level of security budget.....	156
4.13.7 Differentiators .....	157
4.14 Summary .....	159
<b>CHAPTER 5 - CONCLUSIONS AND IMPLICATIONS.....</b>	<b>160</b>
5.1 Conclusions about IT reliance.....	160
5.2 Conclusions about threats .....	164
5.2.1 Potential security threats .....	164
5.2.2 Perceived security threats.....	166
(i) Viruses.....	167
(ii) System users .....	167
(iii) Hackers and Hacking .....	168
5.2.3 Actual security incidents .....	168
5.3 Conclusions about Australian businesses as targets.....	170
5.3.1 Information security incidents: Australia vs. overseas .....	170
5.3.2 Differentiators .....	172
5.4 Conclusions about countermeasures .....	174
5.5 Conclusions about security budgets .....	177
5.6 Implications for theory .....	178
5.6.1 Qualitative based research.....	179
5.6.2 Innovative use of technology .....	179
5.6.3 Broad approach .....	179
5.6.4 Use of existing theories.....	180

5.6.5 Appropriateness of case study research .....	180
5.7 Implications for practice .....	180
5.8 Implications for future research .....	181
5.9 Limitations of this study .....	182
5.10 Concluding remarks .....	182
<b>REFERENCES .....</b>	<b>184</b>
<b>APPENDIX A – INTERVIEW PROTOCOL.....</b>	<b>190</b>
Preliminary Information.....	190
Section A - Use of IT within your organisation.....	191
Section B - Threats to computers, data, and networks.....	191
Section C - Computer, data, and network security incidents.....	192
Section D - Security Practices and Procedures .....	192
Section E - Your Organisation .....	193
Conclusion of interview .....	193
<b>APPENDIX B – SURVEY INSTRUMENT.....</b>	<b>194</b>
<b>APPENDIX C - VIRTUAL INTERVIEW .....</b>	<b>207</b>
Virtual Interview Protocol.....	208
Introduction.....	208
Conduct.....	208
General Instructions.....	209
Use of IT within your organisation.....	209
Threats to computers, data, and networks .....	210
Computer, data, and network security incidents.....	211
Security Practices and Procedures .....	213
Your Organisation .....	214
Conclusion of interview .....	215
<b>APPENDIX D – LETTER TO PARTICIPANTS .....</b>	<b>216</b>
<b>APPENDIX E – EXAMPLE INTERVIEW TRANSCRIPT.....</b>	<b>218</b>
<b>APPENDIX F – THANK YOU E-MAIL TO PARTICIPANTS .....</b>	<b>226</b>



## LIST OF FIGURES

Figure 2-1: Simple Risk Management Model.....	6
Figure 2-2: Security v Functionality Trade Off .....	7
Figure 2-3: Information Security Concepts.....	9
Figure 2-4: Simple Intrusion Detection Concept Model.....	23
Figure 2-5: A typical depiction of a firewall.....	26
Figure 2-6: Basic encryption process .....	28
Figure 2-7: IT use and reliance framework.....	34
Figure 2-8: Theoretical Framework of Research Problem.....	35
Figure 3-1: Case Selection Matrix .....	43
Figure 4-1 Strategic Grid .....	61
Figure 4-2 Case A Strategic Grid.....	63
Figure 4-3 Case B Strategic Grid .....	72
Figure 4-4 Case C Strategic Grid .....	83
Figure 4-5 Case D Strategic Grid.....	95
Figure 4-6 Case E Strategic Grid .....	103
Figure 4-7 Case F Strategic Grid .....	110
Figure 4-8 Case G Strategic Grid.....	117
Figure 4-9 Case H Strategic Grid.....	126
Figure 4-10 Case I Strategic Grid .....	133
Figure 4-11 Case J Strategic Grid .....	143

## **CHAPTER 1 - INTRODUCTION**

This chapter introduces the dissertation topic and the specific project described and analysed in a later chapter. This chapter begins with an overview of the relevant parent disciplines for an investigation into IT security in the Australian business environment. This study attempts to identify the IT security threats, the actual number and type of incidents and the counter measures that organisations are employing to protect their systems. For the purpose of this thesis:

- Information security is basically about the examination of threats and risks to information and the application of technical sciences and procedures to counter those threats (Hancock 2000; Dhillon 2007).
- Risk management is essentially a process designed to study and identify risks, investigate risk reduction methods and the implementation of the risk reduction methods and the subsequent management of the residual risk (Caelli, Longley, and Shain 1989; Conrow and Shishido 1997; Hassler 2001).

These terms are more fully discussed in chapter 2.

### **1.1 Background and Significance of the Study**

The electronic economy and the Internet economy in Australia is booming with Australian organisations estimating that Internet business tools generated \$28 billion in 2000 to 2001 (Brown 2001). In the five years to 2006-07 Internet Service Providers (ISP) in Australia have achieved growth of over 152.6% (Baker 2007). With large amounts of money at stake chief executives and IT managers alike must be aware of the actual risk to their organisations in order to deploy the appropriate counter measures. Australian companies do suffer financial losses from computer crime and security related incidents (Thompson 1998; Lichtenstein 1998). Therefore, the Australian business community would benefit from a comprehensive study into information security in the Australian business environment.

Section 3.0 will demonstrate that there is a gap in the literature in regards to nature of threats to IT resources in Australia. One previous study used a case based methodology to conduct an in-depth review of the information security problems of one particular organisation (Lichtenstein 1998). This research confirms that there are security threats worthy of further investigation. As the Lichtenstein study involved a single organisation a more comprehensive study may provide additional information.

Much of today's economy relies on the use of IT. Until recently only a few managers were fully aware of how their day-to-day operations and basic business administration was dependant on the availability and integrity of computing and network resources (Caelli et al 1989; Withers 2002). Organisations and society in general are increasingly more dependent on the use of technology and organisations are becoming even more reliant on computer technology and the interconnection of computing resources (Furnell and Warren 1999; McNurlin and Sprague 1998; Ward and Griffiths 1998).

The success or failure of an organisation now rests with its ability to maintain and leverage their IT resources. Hence the importance of ensuring that computing and network resources remain available and that the integrity of organisational data is assured (Caelli et al 1989; Fisher 1984; Westwood 1997).

### **1.1.1 Significance of Information Security**

The information economy is now a significant part of our way of life with more organisations turning to e-commerce and the Internet to either create or extend their business (Brown 2001; Hassler 2001). It is therefore somewhat ironic that the technology being used to develop business can also be used to conduct cyber crime against businesses (Caelli, Gaskell, Longley 2005). Businesses are suffering verifiable financial losses from cyber crime. In 1998 for example one study indicated losses to business were in the order US \$266 million dollars (Harrison 1999).

There is evidence that instances of cyber crime are increasing. The US Federal Bureau of Investigations (FBI) and the Computer Security Institute (CSI) have teamed together over the last 12 years to conduct a number of surveys on information security. Their findings show that the number of reported attacks is increasing and the amount of money being lost to cyber criminals is growing at an equally alarming rate (Power 2000). In the year 2000 survey 90% of respondents had suffered from an attack or misuse of their systems (Power 2000). This figure was up from 78% in 1999. Overtime however, the year 2000 peak had reduced to 46% in 2007 (Richardson 2007).

## **1.2 Research Problem**

The business research problem for the proposed study is stated in general terms (Zikmund 1997) and focuses on the general area of the problem (McPhail 2000). The proposed research problem for the study is as follows:

*The phenomenon of information security incidents, and concerns over data security are having a significant impact on the conduct of electronic business and office automation in general. Little is known of the impact, costs, or what strategies the Australian IT industry is using to deal with information security incidents.*

## **1.3 Justification for research**

The research as proposed is justified on the basis that it is unique in the depth that it intends to cover information security in the Australian context. There is a gap in the current literature in regards to both detail and availability of qualitative data and quantitative data in Australia. The majority of past research deals with quantitative data for example Briney (1998) and Harrison (1999). Qualitative studies in Australia about cyber crime and information security are limited in the number of cases that they contain, for example Lichtenstein (1998) details a single case. The 1997 Information Security Survey (Thompson 1998) is the most detailed study found that was conducted in the Australian environment, however, it focused on law enforcement issues and makes few inferences.

The findings of this research will be highly relevant to many Australian organisations that rely heavily on interconnected computer systems and the Internet. Qualitative data on how threats are being realized, why certain companies are being targeted, and what companies are doing to protect themselves would be highly valuable information. Industry value alone provides sufficient justification for the pursuit of the proposed research question (Varadarjan 1996). Analytical generalizations made from the research finding will enable industry to make more informed IT security decisions.

### **1.3.1 Contribution of the research (contribution to theory/contribution to practice)**

The expected outcome of this research is to increase Australian industry's understanding of the nature of information security issues that they face. Importantly it will better enable Australian business to identify information security risks. Armed with a more complete picture of the relevant risks IT managers will be able to make more informed decisions about how they attempt to manage the risks to their organisations.

## **1.4 Methodology**

The research was aimed at in-depth and detailed investigation of the how and why of information security in Australia. Based on the framework provided by Yin (1994) for choosing an appropriate research strategy, case study was chosen as the most appropriate method. Data collection was done in two ways: a pilot study and in-depth interviews. Each data collection method is briefly described below.

**In-depth Interviews.** A case study matrix was developed in order to get a reasonable cross section of large/small to medium enterprise and both public and private organisations. Two informants from each organisation were chosen from the IT management area. Where possible, a general IT manager was chosen as one informant and an IT security specialist was chosen as the other in order to gain a different perspective on information security. A 45-minute interview was scheduled for each participant. An interview guide was developed to provide a basic structure to the interviews. In some cases the interviews could not be conducted face to face and had to be conducted via a combination of telephone and electronic correspondence.

**Pilot study.** As much of the previous research had been conducted using quantitative research techniques that had proved less than scientific due to poor response rates a small pilot study was conducted to test the validity of quantitative and qualitative techniques. The pilot study consisted of a single case interview and the distribution of a survey instrument to a number of well-frequented information security newsgroups on the Internet. The pilot was also used to validate assumptions and gather feedback on the focus and usefulness of the research.

## 1.5 Structure of dissertation

This MIT dissertation is structured as follows:

**Chapter 2 - Literature Review.** This chapter provides a review of the literature surrounding information security and presents a research framework by which information security in the Australian business context can be investigated. Specific research questions are also presented which will be addressed in the data collection stage.

**Chapter 3 - Methodology.** This chapter identifies, describes and justifies the methodology used to explore the research problem and answers the research questions. Data collection procedures and the interview guide are also presented.

**Chapter 4 - Data Analysis.** This chapter reports on the finding from the in-depth interviews in the context of Australian business.

**Chapter 5 - Conclusions and Implications.** This chapter answers the research questions and provides conclusions about the research problem. The implications for theory and practice are also presented. Finally, the limitations of the study, and implications for future research are discussed.

## 1.6 Delimitations of scope and key assumptions

Information security can potentially impact on all organisations that use computing or information resources. Due to potentially global nature of the interconnected information systems this research has focused only on information security in the Australian context. Its focus is on the collection of qualitative data gathered from IT managers about how information security impacts on their business.

A key assumption that has been made is that organisations will be reluctant to participate in the study due to the potentially sensitive nature of the information being dealt with. In some cases the informants are being asked to identify system vulnerabilities or are inferring information about potential systemic problems with their organisations. The data collected will be primarily relevant to the time frame in which it was collected 2002 – 2003.

## 1.6 Conclusion

This chapter laid the foundation for the dissertation. It provided a background on information security and the significance of information security to business. The study was justified as a significant contribution to both theory and practice of information security in Australia. The method by which the research was conducted was presented. Following which the delimitations of scope and key assumptions were presented. Finally, an overview of the dissertation chapter was given.

The next chapter is a review of literature regarding information security in Australia.

## **CHAPTER 2 - LITERATURE REVIEW**

This chapter provides an overview of the published literature and research on information security. It also provides a research framework for studying information security in Australia. Specific research questions are also presented which will be addressed in the next stage of the study. The chapter provides an introduction to IT academics who are interested in information security issues whilst also being of relevance to information security practitioners as it provides a unique and objective approach to the subject matter. The chapter starts with an introduction to the disciplines that are applicable to the study; risk management and information security. Throughout the discussion of the literature references are made to the international context and findings and the equivalent research results in the Australian context. Then a research framework that could be used to investigate information security in Australia is presented. Finally, the research questions that cover the issues of the research question are presented.

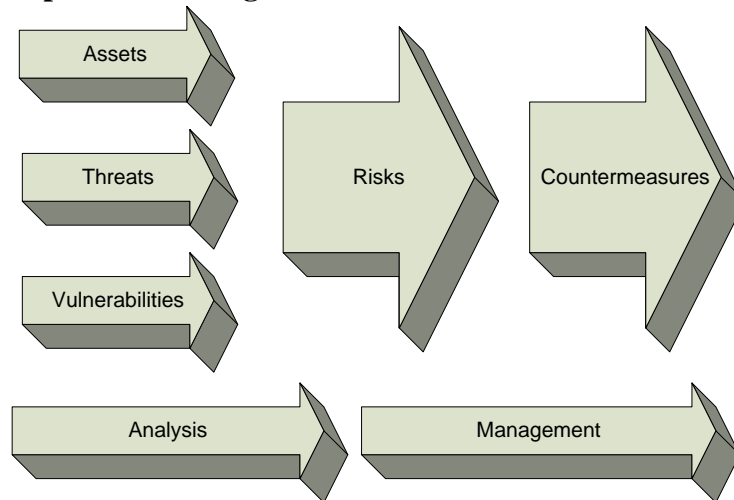
### **2.1 Risk Management**

Risk management and analysis are commonly used terms and methodologies employed in business. Risk management is an element of management science, which has provided the basis of underwriting decisions in the insurance industry (Caelli et al 2005). For the purpose of this research we are primarily interested in the application of risk management methodologies as they relate to information systems and information security. Risk management methodologies may use qualitative, quantitative or combination of both methodologies in order to estimate the level and nature of risk (Halliday, Badenhorst, von Solms 1996)

#### **2.1.1 Simple Risk Management Model**

A simple risk management model is depicted in Figure 2-1 below. Risk analysis is the key component of the risk management methodology. Risk analysis evaluates the relationship between the seriousness of a threat, the frequency of occurrence (probability), and the cost of implementing a suitable protection mechanism (Hassler 2001).

**Figure 2-1: Simple Risk Management Model**



*Source: Caelli et al 1996*

The risk analysis process involves the analysis and study of:

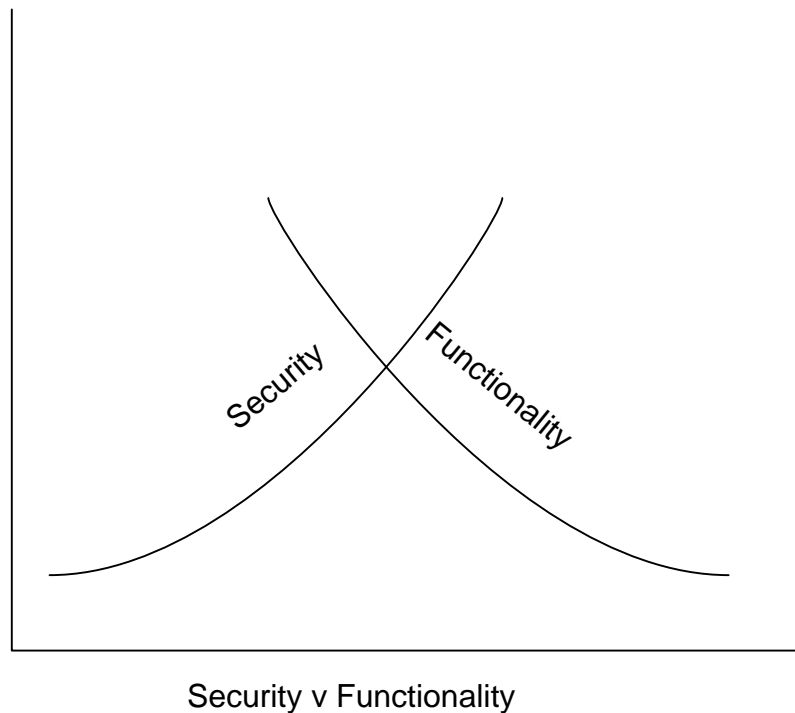
- The assets to be protected
- The threats in the assets environment
- The vulnerabilities to these threats
- The types of impact to be reduced
- The safeguards used to mitigate the risk

*Source: Caelli, Longley, and Shain 1994*

### **2.1.2 Security vs Functionality**

Security procedures are costly and often involve some form of compromise for a company's profits, user convenience, and turn around times. (Risk free information security or any other business activity is never attainable.) Acceptable levels of risk must be postulated (Caelli et al 2005). Essentially, a decision must be made in regard to the amount of security to employ in relation to an acceptable level of system functionality. Risk analysis aims to ensure that the decisions made are based on accurate information. Figure 2-2 (below) illustrates that as functionality in a system increases the amount of security that is generally capable of being applied drops. This is the essence of how risk management applies to information security.

**Figure 2-2: Security v Functionality Trade Off**



*Source: Developed for this research*

### **2.1.3 Qualitative Risk Analysis**

Qualitative risk analysis, according to Peltier cited by Power (2000, p.281) “is a technique that can be used to determine the level of protection required for applications, systems, facilities, and other enterprise assets. It is a systematic examination of assets, threats, and vulnerabilities.” The qualitative methodology attempts to prioritise the various risk elements in subjective terms. Qualitative methodologies usually relate to variables that are intangible, descriptive, or subjective in nature. Qualitative matrixes are expressed in terms of a ranking from high to low or using numbers to rank threats, vulnerabilities or assets.

The twelve steps in qualitative risk analysis identified by Power (2000) are:

1. Develop a plan
2. Develop an application priority
3. Identify and evaluate assets
4. Identify threats
5. Evaluate threats
6. Estimate potential losses
7. Calculate risk factors
8. Analyse vulnerabilities
9. Identify safeguards
10. Perform cost/benefit analysis of safeguards
11. Rank safeguards in priority order
12. Write risk-analysis report



### **2.1.4 Quantitative Risk Analysis**

Quantitative risk analysis uses mathematical formula to determine in tangible form the monetary costs and potential losses involved in a risk. A popular quantitative technique is Annualised Loss Exposure (ALE) (Bandyopadhyay, Mykytyn. P, Mykytyn. K 2000; Caelli et al 2005). This technique attempts to assess risk based on the Risk = Probability of occurrence x one time loss produced by the occurrence of a threat (Caelli et al 2005; Fisher 1984). Quantitative techniques allow businesses to compare the value of their information assets to the amount of money they can or should spend protecting those systems.

## **2.2 Information Security**

It is somewhat ironic that one of the first uses of the computer was to break codes and ciphers used to protect information during World War II. The allied effort was greatly assisted by the use of the first computer to break the German Enigma code, which subsequently helped stop the German U-Boat Wolf-Packs from savaging allied shipping. Now the security of all information, particularly that stored and transmitted using computers or other electronic devices is subject to potential compromise (Caelli et al 1996).

Security is a broad concept, which has its own language, which focuses on the processes of attacks on information, and in preventing, detecting and recovering from attacks (Caelli et al 1996). Information security is defined as procedures and actions designed to prevent the unauthorised disclosure, transfer, modification, or destruction, whether accidental or intentional, of information in a network. Information includes data, voice, video, images, and fax (Ghosh and Schumacher 1997).

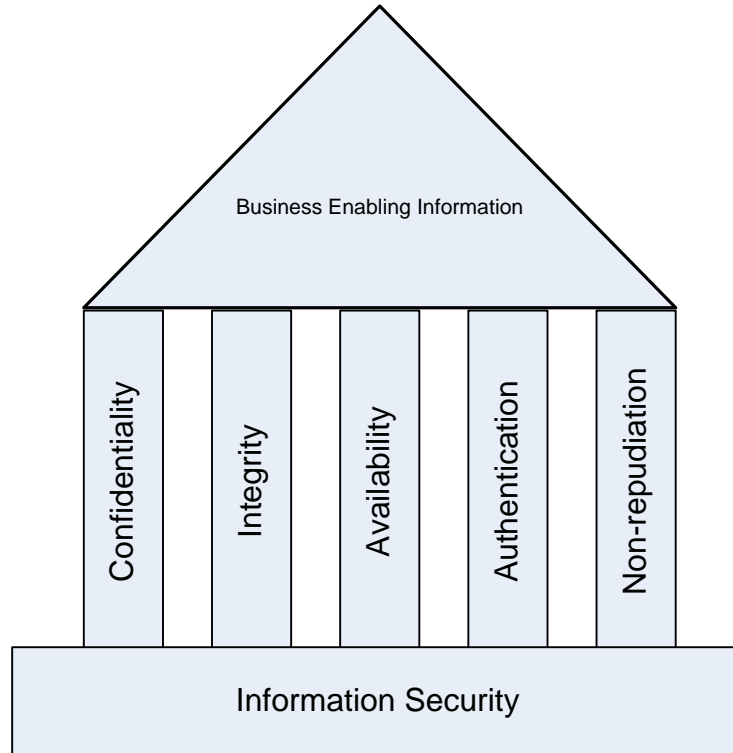
### **2.2.1 Information security components**

Information security consists of three main system components:

- Confidentiality
- Integrity
- Availability

*Source: Caelli et al 1996*

Another two components that are sometimes added to the main three are non-repudiation and authentication (Hassler 2001;Escamilla 1998). Figure 2-3 below depicts the relationship between information security requirements and business enabling information.

**Figure 2-3: Information Security Concepts**

*Source: Developed for this research*

### 2.2.1.1 Confidentiality

Confidentiality refers to the protection of data so that it cannot be disclosed in an unauthorised fashion, also referred to as privacy or secrecy (Escamilla 1998; Hassler 2001; Caelli 1996). Most IT users recognise the need to ensure that the information that they transmit to a recipient should arrive without being read by a third party. Encryption is the most widely used technique or process used to provide confidentiality to data and systems. Whilst it is one of the most widely employed mechanisms, encryption alone will not protect all systems from being destroyed or modified, therefore it is usually combined with other protection tools.

### 2.2.1.2 Integrity

The data integrity component of information security aims at ensuring that data is not modified or altered by unauthorised system users (Hassler 2001; Escamilla 1998). It is possible that damages could be sustained if users of systems make business decisions based on faulty information. A systems' integrity relates to the assurance of accuracy, completeness, and performance according to defined specifications (Khadraoui and Herrman 2007).

Integrity is normally provided on a computing system through a number of approaches. Encryption can assist in providing data integrity by ensuring that data packets are not intercepted, modified and then re-transmitted to an unsuspecting recipient. Access control, which involves ensuring that only authorised users can

gain access to data is another mechanism that be used to provide or to ensure data integrity (Escamilla 1998; Khadraoui et al 2007; Hassler 2001). By restricting access to a particular system it makes it potentially harder for an outsider to access and then modify the data.

### **2.2.1.3 Availability**

The availability goal in information security is to protect network services and data from unauthorised attempts to withhold information or computer resources (Escamilla 1998). Lack of access to information can be a critical concern. If patients' medical records become unavailable due to a network security problem the consequences could be fatal.

Statements about the availability of network and data services cannot be made with the same level of confidence as can be given for confidentiality and integrity (Escamilla 1998). A hardware failure resulting in a network traffic congestion problem could deny users access to resources. Either of which could be a result of equipment failure, poor network planning or some other reason and therefore not the result of security incident per se. A number of controls may, however be implemented to increase availability. Network design, access control, and prioritising services and users can all promote enhanced resource availability.

### **2.2.1.4 Authentication**

Authentication ensures that a users' identity or data origin are genuine and that they have access rights and privileges to computer resources (Hassler 2001). Authentication systems determine what IT resources any given user has the right to use on a system. Most network operating systems have some form of built-in authentication system that associates a particular user with a list of resources that the user is allowed to access. Encryption techniques can also be employed in more sophisticated authentication systems.

### **2.2.1.5 Non-repudiation**

Non-repudiation is the process of proving that a message or data could not have come from anyone other than a stated author (Escamilla 1998). Non-repudiation is a valuable concept in military systems. For example, before ordering an attack on an enemy, generals would want to be certain that the message they received was from the appropriate and authorised source (Arquilla and Ronfeldt 1997). This concept is also important to business. Any organisation that wants to guarantee that the other party in a conversation, message, or other data transfer is the person or organisation that they claim to be may be interested in non-repudiation services. The common technique used for non-repudiation in public key cryptography.

## **2.3 The information security in Australia immediate discipline**

In the Information Security in Australia immediate discipline, five research issues will be addressed.

### **2.3.1 Threats to information security in Australian business**

As this study is based on information security in Australia it is important to determine what information security threats are faced by Australian industry. International literature and research findings will be used to provide a preliminary list of threats. This will allow for the comparison between threats in the Australian environment and those identified overseas.

As mentioned in previous sections of this thesis data in the Australian context is limited in comparison to studies that have been conducted overseas. A basic list of information security threats that Australian business face are as follows:

- Disgruntled employees
- Independent hackers or information brokers
- Australian owned corporate competitor
- Foreign corporate competitor
- Customers
- Suppliers
- Foreign government intelligence activity
- Criminals
- Authorised users

*Source: Thompson 1997*

In one international study, in which, 114 Australian businesses participated, 53% of all the participating businesses stated that they were more concerned about external threats, 53% by hackers, unauthorised users 49% are rated as a greater threat than current employees/authorised users 31% (Dinnie 1999). Whilst there were Australian participants in the survey no breakdown of the threats perceived in each country has been given. This study could not therefore shine any light on the situation in Australia. It would be desirable to establish whether, the threats in Australia are indeed similar to those experienced internationally.

The increasing threat of viruses should be added to Thompson's list. Viruses are a known threat to Australian businesses Lichtenstein (1998). The problem of definitions of what a threat is; is an issue that could cause difficulty in either compiling a list of threats or attempting to make comparisons between international studies. The definitions for threats, types of incidents and vulnerabilities are often used interchangeably (Caelli et al 1996). For the purpose of this research a threat is

defined as ‘...the active agent in a potentially loss causing event’ (Caelli et al 1996 p.84).

Each of the major threats will be discussed in the sections below.

### **2.3.1.1 Viruses**

The threat of computer viruses has become headline news over the last few years. A few years ago many people were unaware of the potential threat that viruses posed to computer systems and that data that resides on those systems (Richardson 2007; Baker, Hylender, and Valentine 2008). Computer viruses are now commonplace. They pose real and credible threats to virtually all computer-based networks. Not only are the threats of computers viruses’ real the number of incidence and the numbers of viruses in circulation are on the increase (Caelli et al 1996; Khadraoui et al 2007; Kearvell-White 1996; Bissett and Shipton 1999; Hanson 2000).

The virus was defined by Cohen as a program that can infect other programs by modifying themselves to include a (possibly evolved) copy of itself (Caelli et al 1996). The National Computer Security Centre has recently defined the term virus as a ‘self propagating ‘Trojan Horse’, composed of a mission component, a trigger component, and a self propagating component. A more complete definition of the term virus is given by Pipkin (2000), who defines a virus as a program that infects another program by replicating itself into the host program. A virus has three phases:

1. The infection phase where the host is infected from previously existing virus.
2. The activation phase, where this new copy is triggered to find a new host to infect.
3. The replication phase, where the virus finds a suitable host and copies itself to the host.

Most researchers in the area of information security investigate viruses as threats to computer systems to some extent. A number of international surveys have indicated that viruses are the common type of information security incident that an organisation is likely to face (Richardson 2007; Baker et al 2008; Rapalus 2000; Dinnie 1999; Bisset et al 1996). The research does show that there is some difference in the quantitative figure for the rate of incidents. According to one study, conducted by Ernst and Young, the global rate of business exposed to viruses was 52 %, with 49 % of Australian organisations indicating that they had suffered from virus attacks (Dinnie 1999). This survey also reported that the incident of viruses in the United States was 63%. The Computer Security Institute and US Federal Bureau of Investigation figures for the same year are vastly different. The CSI/FBI research indicates that in the same year 90% of respondents had been subject to virus attacks (Power 2000).

The CSI/FBI survey only considers United States respondents but the wide variation between the Ernst and Young research and the CSI/FBI results highlight one of the significant issues relating to research in the information security field. According to

the Ernst and Young research they included the comments of 4 254 IT managers in 29 countries. The report does not indicate response rates. The CSI/FBI report, which is considered an authoritative source of statistics in the field, had a 14% response rate. A 1996 study conducted by KPMG in the UK had a response rate of 9.6% (Kearvell-White 1996), while an industry wide survey conducted by Information Security Journal in 1998 had 9.9% response rate. Given the extremely low response rates it is difficult to know the true rate of virus incidents or any other type of information security incident.

The number of new viruses in circulation increases by between 150 – 200 per month (Kearvell-White 1996). Many of the ‘new’ viruses however, are simple modifications of an existing virus (Bissett et al 1996). For example a virus that displayed a certain message on the screen could be slightly changed to alter the spelling of a single word on the screen. The altered message would result in the virus being classified as a different virus.

Current research does not tell us the whole story of the threat and impact that viruses are having on businesses, particularly as those threats affect Australian organisations. As the current information involves mainly quantitative data it can only be implied in a limited context. Surveys conducted by KPMG, Ernst and Young, and the CSI/FBI attempt to quantify the number of virus related security incidents that are occurring and in some case they also attempt to quantify the financial losses that result from such incidents (Power 2000; Briney 1998; Dinnie 1999; Kearvell-White 1996). There is a gap in the current literature as little is known about the kinds of how, why, and when viruses incidents are occurring. More needs to be known about the nature of the virus threat to Australian organisations so a proper defence strategy can be formulated.

Quantitative surveys conducted in Australia under the auspices of the Australian Computer Emergency Response Team (AusCERT) indicate that viruses were the most common form of electronic attack reported by their respondents with 45% of respondents experiencing this type of infection (AusCERT 2006).

### **2.3.1.2 The internal threat - Disgruntled employees**

It has already been identified that there are a wide variety of potential threats to computing systems and networks. One of the more frequent or likely threats that an organisation’s systems face originate internally (Powers 2000; Denning 1999; Thompson 1997; Dinnie 1999). The internal threat has been described in a variety of ways by different researchers and authors on the subject. Essentially, the internal threat is made up disgruntled former and current employees whom take it upon themselves to seek revenge or de-fraud their employer and of authorised users who access information without proper authorisation (Denning, Caelli et al 1996; Briney 1998).

The threat of the insider ‘turned bad’ has attracted a significant amount of coverage in the media. One such example of a trusted employee who turned into a major information security threat can be seen in the well-known Tim Lloyd/Omega case. In

this case an employer became upset at the lack of respect that he was being showed by his organisation. After leaving the organisation a computer application that he had built and later modified was made to crash their file servers. The consequential damage cost Omega 10 million dollars and 80 staff were retrenched (Gaudin 2000). This case demonstrates that a significant amount of trust is given to employees especially those with network administration roles (Gaudin 2000; Ceraolo 1998, Powers 2000; Schumacher et al 1997). Insiders are more likely to have intimate knowledge of how systems internal to organisation operate and what data is most valuable to an organisation. When this knowledge is combined with access to a system a dis-affected employee or even a thrill seeking employer could cause a considerable security threat.

The American Society for Industrial Security (ASIS) survey, conducted in 1998 confirmed what information security experts have been saying for years: The single greatest threat to corporate intellectual property is trusted insiders – current and former employees, temps, onsite contractors, and consultants (Denning, 1999). Other surveys support the notion that insiders are a major threat to corporate security (Thompson 1998; Dinnie 1999; Rapalus 2000), however, there is some debate as to the exact level of threat, and whether is the most likely or simply among the more likely threats to information security and corporate information in general (Power 2000; Ernst and Young 1995 Survey 1995; NUA Internet Survey 2001). Current research also indicates that the number of incidents of insider originated security breaches are increasing, however, the percentage rise in external incidents is increasing a faster rate. The CSI/FBI research indicates that over the last five years the disgruntled or dishonest employees involved in security related incidents has topped the level of threats (Powers 2000; Rapalus 2000). In general terms the threat from insiders has remained constant in comparison to increased rate for external sources of security incidents.

The 1995 Ernst and Young Survey indicated that 88% of respondent organisations stated that internal threats were greater than external threats (Ernst and Young 1996). The CSI/FBI report show that in 1997 40% of respondents reported incidents relating to employee access abuse; in the year 2000 this figure rose to 71% (Powers 2000; Rapalus 2000). One the prominent reasons cited for the insider threat is because of the very nature of organisational networks, they are by definition designed to give people access to information. Security related incidents occur when a system is designed in such a manner that it is possible to gain access to information for which they have no right to see. Unauthorised access to information is perhaps the largest component of insider related security incidents (Powers 2000; Denning 1999; Briney 1998; Ceraolo 1998; Guadin 2000). An additional type of insider abuse of systems has also surfaced over the last few years, namely, employees abusing their access to Internet during work time (Powers 2000; Lichtenstein 1998). Organisations are keen to ensure that valuable work time is not lost while employees misuse the Internet (Briney 1998; Denning 1999; Kearvell-White 1996).

The perception of the internal threat being greater than the external threat has reduced in the years from 2000 – 2008. In fact many organisations now consider the external threat to be greater than the internal threat. This may be because of increasing maturity of organisations in the analysis of risks or due to implementation

of countermeasures that have adequately dealt with the earlier identified insider threat (Richardson 2007; Baker et al 2008, AUSCERT 2006).

Research into information security threats in the Australian context, whilst limited in scope and size in comparison to the international studies indicates that Australian organisations also believe that the internal threat is more likely in comparison to external threats (Thompson 1998; Liechtenstein 1998).

This study attempts to differentiate between ‘threats’ and ‘incidents’. A threat for example may never eventuate – whilst an incident is something that has actually occurred. This distinction is made due to the importance of perceptions on how information security is managed (hence the importance of a qualitative approach). For example the example of ‘insider’ threat mentioned above. In comparison to the findings mentioned recent Australian surveys demonstrate that the majority of incidents (83% externally compared to 29% internally launched incidents) (AusCERT 2006).

### **2.3.1.3 Hackers and Hacking**

The term hacker is generally used to describe those people who attempt to penetrate a system externally (Powers 2000). Within the hacking community however, a hacker is defined as a person who attempts to break into a system in order to learn and explore whilst a person who breaks into a system with the intent to steal or destroy is referred to as a cracker (Powers 2000; Furnell, Downland, and Sanders 1999; Westwood 1997; Khadraoui et al 2007). Regardless of their intent hackers and crackers attempt to illegally gain access to an organisation’s computing networks and therefore pose a significant threat to the information that resides on those systems (Caelli et al 1996).

The popular stereotypical hacker is a young intelligent person attempting prove their skills and to perhaps make a statement about a particular point of view. Whilst a certain percentage of hackers may fit this profile other researchers are quick to point out that there are far more serious hackers who are professional in every sense of the word; they can be sponsored by large corporations or foreign governments with intent to gather otherwise unavailable information (Powers 2000; Denning 1999; Westwood 1997; Khadraoui et al 2007; Furnell and Downland et al 1999; Furnell et al 1999; Hinde 1998; Schwartua 1994).

The term ‘White Hat’ and ‘Black Hat’ are also used to describe hackers and crackers respectively (Bishchoff 2001). Again, the white hat is driven by curiosity whilst the black hat is driven by power or for the chance at stealing or making a profit (Bishchoff 2001). It is comparing the fundamental differences where the paradigm of defending against hackers seems flawed. It is widely believed that the white hat hackers thrive on the challenging of breaking into highly secured systems whilst the black hats will generally target those with little or no security; the analogy often used is “*if my house is locked then the thief will move next door*” (Bishchoff 2001; Gouldson 2001; Caelli et al 1996; Power 2000). This theory does not account for those professional hackers who may be determined to break into a particular site for



specific reasons such as obtaining information that no other organisation has (Powers 2000; Denning 1999; Schwartua 1994).

Hacking and hackers also generate a lot of interest from the media, which has the effect of significantly raising its profile in comparison to other computer related security incidents (Powers 2000). The incidents of hacking are certainly on the increase (Powers 2000; Rapalus 2000; Kearvell-White 1998; Richardson 2007). There appear to be two major reasons for the increase in the number of hacker related security incidents; firstly as computer networks continue to expand there is an increase in the number of systems that can be potentially attacked, and secondly because of the resources available on the Internet it is becoming a simple process to obtain and use hacking tools (Schwartua 2000; Venter and Eloff 1998; Powers 2000a; Powers 2000b; van Doorn 1999).

Anecdotes abound of organisations that have been victims of hacker attacks, however, there is a general lack of willingness on the part of organisations to share information about attacks that they have encountered (Gouldson 2001; Powers 2000). The relatively poor response rate to surveys in the field can also be seen as an indication of the sensitivity of the subject (Powers 2000). Researchers on the topic are left with reviewing the cases and incidents that have been reported and investigated, many more hacking incidents are believed to go unreported or even undetected (Powers 2000; Rapalus 2001, Gouldson 2001; Caelli et al 1996). Where instances of hacking have been reported the figures show an alarming rise in instances. The Computer Emergency Response Center (CERT), at Carnegie Mellon University have been tracking reported hacking incidents for the last 13 years. In 1988 six incidents were reported, by 1995 there were 2412 incidents in that year and in year 2000 21 756 incidents were reported to the CERT (Bishchoff 2001). The CSI/FBI results indicate that in the year 2000 25 % of respondents suffered from a system penetration from outside their networks and 27 % suffered a denial of service attack (Powers 2000). In an another international survey the global average for organisations that had suffered from hacker attacks was 21 % (Dinnie 1999). Given the seemly large amount of reports that the CERT Center is receiving it would appear that many organisations are either not responding the surveys or not admitting or do not know that they have suffered from a hacker attack (Powers 2001; Bishchoff 2001).

There are a variety of reasons that an organisation may have for not reporting that they have suffered from a hacker attack. In the 1999 CSI/FBI report 84 % of respondents failed to report hacker attacks and other security incidents because they feared negative publicity. 79 % of respondents felt that they could not report the incidents in case their competitors seized upon the opportunity to take advantage of the situation. 36 % were not aware of the fact that they could report the incident to law enforcement agencies for them to investigate and resolve (Powers 2000). There is also a belief that reporting incidents to law enforcement agencies can be a double-edged sword. Whilst, law enforcement agencies have encouraged organisations to report incidents of cyber crime, information handed over to them by victim organisations under confidentiality agreements may subsequently be obtained by the media and other organisations under freedom of information arrangement (Gouldson 2001). Successful prosecution of hacking crimes has also proved to be difficult given the depth required in investigating the crimes and the limited resources available; the

successful conviction rate is very low (Gouldson 2001; Bequai 1998). This trend appears to be continuing as the 2007 CSI/FBI 2007 study indicated a 'peak' of reporting to law enforcement of incidents to 29% (Richardson 2007).

Fear of negative publicity is a genuine concern, especially for small e-commerce based companies that rely on networks such as the Internet for much of their income. In one recent case a small home based company that sold photos of animals online, had its customer credit card number database stolen after hackers discovered a flaw with the online payment software that the company used. Unknown to the company hackers were stealing credit card numbers and using them as they wished. In one instance a customer's credit card was charged 30 000 dollars. When the organisation attempted to right the situation they found it was very difficult to gain assistance from credit companies, law enforcement, or from software vendors (Fenn 2001). This case indicates why hacking can be extremely damaging to an organisation in terms of poor publicity and the difficulties that are often encountered when attempting to investigate instances of cyber crimes (Escamilla 1998; Bejtlich 2004; Khadraoui et al 2007).

A variety of techniques are used by hackers in their attempt to break into computing systems and networks. Some of these techniques are relatively straightforward and involve the use of purpose built hacking programs. These hacking programs are freely available on the Internet and require very little skill for their use (Hancock 2000; Gouldson 2001; Hind, 1998; Schwartua 1998; Powers 2000). Because of the relative ease of use of these applications and their ability to literally put powerful tools into the hands of children users of these applications and techniques are often referred to as 'Script Kiddies' (Bischoff 2001). Perhaps one of the more powerful techniques used is that of social engineering (Bischoff 2001; Khadraoui et al 2007; Escamilla 1998; Ceraolo 1998). This process involves the search for information that can be later used to uncover more sensitive information. For example, by determining who worked in an organisation's IT department a hacker may attempt to impersonate individuals, supervisors or infer to others that they have the authority of a well-known person in the organisation. Kevin Mitnick, a.k.a. the "Condor", is perhaps the most famous of hackers who served five years in prison for allegedly possessing unauthorised access codes. Mitnick would call an IT department and use his personal communications skills to convince his target that they should change the password of another person in the organisation; Mitnick's hacking spree allegedly cost his targets over 200 million dollars (Powers 2000; Bischoff 2001).

Hacking is an issue in Australia (Warren and Hutchinson 2003). The Australian IT environment, like in any country connected to a variety of global communications and information systems networks is at threat to hacker attacks. In a single week a Polish hacker using the name L4m4 attacked and defaced 47 web sites (The Australian 06 Jul 01). The hacker defaced the web sites with messages relating to the poor security of the sites and the targets ranged from legal firms, online bookstores, and television channels' web sites. These kinds of attacks show that Australian organisations are vulnerable. They also demonstrate a common hacker technique of scanning systems for vulnerabilities and then attacking opportunity targets as they arise (Denning 2001 pers. comm., 31 Dec). In the 1997 Computer Crime and Security Survey 23% of respondents indicated that they had suffered from external

hacker attacks, additionally 21% of the respondents indicated that hackers/criminals were a significant threat to their organisation (Thompson 1998).

The international experience is that hacker and security incidents in general are on the rise (Powers 2000; Rapalus 2000; Briney 1998), the same is also true in Australia. In 1999 AusCERT logged 9000 security breaches, in the year 2000 that figure had leaped to 22 000 incidents (Gliddon 2001). Hackervism, which is where hackers attack websites to make a political point have been rampant in the US since the Spy Plane incident (Johanson and Park 2001). Whilst Australia was spared from many of the incidents involved in this informal cyber war between pro-US and pro-Chinese hackers Australian sites still suffer from approximately 40 attacks per day (Johanson et al 2001). Some other differences have been seen in the Australian context of hacking as compared to that of the international experience. In one survey, which compared security incidents where actual losses could be recorded, the global rate of hacker attacks that had resulted in losses in terms of all incidents was 21%, the US rate was 30% and the Australian rate of hacker attacks that resulted in losses was 13%, less than half of that of the US (Dinnie 1999). In order to determine the impact of hackers on the use of IT in Australia it is important to determine the perceived level of threat and how this compares to the actual rate of incidents and the subsequent management decision made because of the threat of hacker attacks.

#### **2.3.1.4 Espionage and other threats**

In previous sections it has been established that businesses and governments are becoming increasingly reliant on information systems and the data stored on those systems. The collation of this data has been used as a powerful tool by organisations to better support their business objectives. This aggregation of information has also increased the potential reward for less than ethical organisations or foreign governments to undertake computer based attacks or intelligence gathering exercises or information warfare (Hutchinson and Warren 2001a; Warren 2008a; Warren 2008b; Denning 1999; Schwartau 1997).

The term information warfare or I-War is defined as a range of deliberate offensive activities that range from destroying IT equipment (hardware) to subtle perception management, and from industrial espionage to marketing (Hutchinson and Warren 2001b; Westwood 1997; Hinde 1998; Denning 1999; Schwartau 1997).

Whilst there is little doubt that I-War occurs between nation states, businesses and organisations there is little hard evidence in the published literature that can be used as comparison. Nations are unlikely to admit (at least officially or in detail) that they use information systems to intercept computer traffic, hack into computers of foreign nations. Having said that, organisations such the National Security Agency (NSA) and the Australian equivalent the Defence Signal Directorate (DSD) are known to collect signal intelligence (SIGINT) from all sources of communications – information systems included. From an internal perspective, these organisations combine with their British and Canadian counterparts to form a system known as ECHELON. This alliance attempts to constructively share information regardless of where in the world it is derived. As digital technologies combine,

telecommunications and information systems have become seamless (Westwood 1997).

Nation states may use information systems as potential weapons and so too may terrorists and criminals. These organisations may use technology to either gain access to sensitive information or deny the rightful owner access to their own system and data (Furnell and Warren 1999b). Cyber warfare and terrorism has been used in support of broader and more traditional military and terrorism campaigns.

The threat of cyber-terrorism and is relevant to Australian organisations. Any computing system connected to other computer systems offers potential points of ingress which could be used by entities intent on causing mischief or harm. There is little hard evidence as to the exact nature of this threat. It is deemed as a possible risk but there has yet to be an exhaustive study that has been able to quantify the risk in more exact terms.

### **2.3.2 Australian businesses are targets**

Australian businesses are at risk from information security related incidents (Thompson 1997; Lichtenstein 1998; Dinnie 1999; Dearne 2002Aa Dearne 2002b; AusCERT 2006). In Thompson's study he found that 37% of respondents had suffered from an information security related incident. This compares to 50% in the same year in the U.S. (Power 2000). The difference between these two figures could be due to a number of factors. Assuming that both figures are accurate reflections of their respective populations it could be possible to speculate that there are a number of differentiators that could be influencing the results.

Australian business has not adopted e-commerce as readily as their U.S. counterparts (Dinnie 1999). According to Dinnie, the touted reasons for this difference is that Australian businesses are concerned about security issues and are also unsure if they or the technology are ready for the transition to online business.

Later studies conducted by a variety of organisations clearly indicate that Australian businesses are the targets of information security attacks and incidents. In 2002 KPMG conducted its first global information security review. This study is useful as it attempts to make comparisons between the level of incidents in the Asia/Pacific region in comparison to the level of incidents experienced in the Americas or Europe. This study also differs from its peers as it uses telephone interviews as the data collection technique instead of mail out surveys. The telephone interview technique allowed the researchers to obtain a broader range of information and to better interpret responses. The study found that organisations in the Asia/Pacific region suffered from more instances of attacks than organisations in either Europe or the Americas. Also, Asia/Pacific organisations were less likely to be protected by adequate policies and procedures in comparison to their American and European counterparts (KPMG 2002).

The 2006 AusCERT survey, which represents a joint production between AusCERT and all of Australia's law enforcement agencies reports exclusively on security incidents in the Australian context. It is however, specifically designed to follow the same format as the American CSI/FBI survey so as to allow direct comparison

between the results. This research represents the latest industry accepted data on the topic of security incidents in Australia, however, like its American counterpart it suffers from a poor response rate. The Australian survey had a response rate of 17%. The report does, however, acknowledge the fact that the data is not scientifically meaningful, but asserts the point that the data is the best currently available. The results of the survey and the way that the report is presented must also be viewed in the context that commercial entities who sell security services and products often sponsor this kind of research.

Importantly, AusCERT now has a number of completed surveys that allow for year by year comparisons of trends. The AusCERT research indicates that the volume of computer crime and security incidents in Australia is declining. 67% of respondents had suffered a computer security incident in 2002, twice the level of 1999, and higher than that recorded in the USA (AusCERT 2002). More recent results reflect the downwards trend (22% 2006, 35% 2005, and 49% 2004) (AusCERT 2006). The report also found that from 2002 that in Australia, the growing threat of external attack had surpassed the threat of internal attack. This finding represents a significant shift from previous international studies as well as those findings of similar such studies previously conducted in Australia.

The study will allow for the closer examination of potential differentiators to determine if and why there are difference between the Australian information security environment in comparison to the experiences of other nations.

There is a growing amount of evidence that Australian businesses are the subject of computer security incidents, particularly as more organisations pursue e-commerce opportunities. In March of 2002 one Australian e-commerce organisation that traded goods online was attacked on at least two occasions. In the first occasion operating system files were deleted which resulted in the trading site being offline for five days. The losses from this attack were estimated to be over \$20 000 per day. The other attack involved accessing the organisation's router and deleting important configuration information that resulted in the company losing its Internet connection. With the aid of computer forensic experts, law enforcement was able to track the attacks to a broadband connection that was being used by an ex-employee of the organisation (AusCERT 2002).

### **2.3.3 Countermeasures**

For the purpose of this research countermeasures are defined as those procedures or steps that are taken as part of providing a security solution. After identifying threats to a system and any inherent vulnerabilities in that system countermeasures are employed to deal with the risk (Caelli et al 1996). The aim of information security countermeasures is to provide:

- Impact avoidance
- Impact transfer
- Impact reduction
- Reduce likelihood
- Reduce threat

These aims may be achieved by using a number of mechanisms and procedures. One way of achieving impact transfer for example, may be seeking insurance against a major catastrophe. Security technologies such as firewalls that are used to filter access to a system can be used to attempt to achieve impact avoidance, to reduce the threat and to reduce the likelihood.

Security procedures and practices that are documented and enforced are believed to be the most effective manner to protect an organisation's systems (Power 2000; Caelli et al 1996; Khadraoui et al 2007). Little is known about the specifics of how Australian businesses are protecting themselves from information security threats. In 1997 60% of Australian businesses did not have an information security policy (Thompson 1997). This is 10% worse than recorded in the U.S. (Power 2000). The study conducted by Ernst and Young, in 1999 found that 68% (of the 114 Australian companies surveyed) had security policies (Dinnie 1999). Some of the security technologies and/or methods used in Australian businesses are:

- Anti-virus protection
- Intrusion Detection
- Firewalls
- Encryption
- Security Policies and Standards
- Incident Response

A more detailed analysis of the technologies, methods and issues involved in the protection of computing systems from security related security incidents follow in the sections below.

### **2.3.3.1 Anti - Virus protection**

As discussed previously, viruses are a major threat to the security of information systems (Powers 2000; Briney 1999). When discussing the spread and detection, and the general protection against viruses it is important to distinguish between the action of a specific and that of some future theoretical virus (Caelli et al 1996). It is always possible to detect a known virus because it has specific properties and actions, thus these properties create a unique signature for the virus that can be detected (Khadraoui et al 2007; Caelli et al 1996; Pfleeger 1989). This known signature is what is used when mechanisms are constructed to defend against certain viruses, this could subsequently lead to a virus designer to produce a program that infects other programs but does not produce a unique signature that can be detected by virus scanning software (Pfleeger 1989). It is also important to stress that it is not possible to point to an attribute that must always be present in an arbitrary virus and must always be absent from an arbitrary piece of legitimate code (Pfleeger 1989; Khadraoui et al 2007; Caelli et al 1996). Therefore there is no known test or series of tests that can unambiguously identify a virus and it has been suggested that it is theoretically impossible to develop such a test (Cohen 1994).

The advent of viruses produced a spate of anti-viral software packages, some of which provided inadequate defence mechanisms for the average PC user (Caelli et al 1996). The PC is the most likely platform to succumb to a virus attack (Power 2000; Khadraoui et al 2007). The Unix operating system does provide some inbuilt features such as file check facilities that allow for the checking of file size, a checksum of the contents, when it was last modified to potentially determine if the file has been 'attacked' by a virus (Caelli et al 1996).

The most fundamental lesson of anti-viral measures is that the most vulnerable systems are those that fail to observe sensible data security measures (Caelli et al 1996; Khadraoui et al 2007), which are characterised by:

- a. inadequate backup procedures,
- b. inadequate user training,
- c. inadequate control of the introduction of software,
- d. lack of control of file transfers, and
- e. poor or absent security policies.

Anti-viral products generally fall into three categories as listed by Caelli et al (1996, p. 609):

- a. Class 1 – Infection prevention. Designed to stop the virus replication process and prevent initial infection.
- b. Class 2 – Infection detection. Designed to pick up virus attacks soon after they happen, mark the specific component(s) infected and allow remedial action to be taken.
- c. Class 3 – Infection identification. Designed for showing up specific types of strain of viruses; it will identify viruses in systems and may remove them, but only works on known viruses.

Whilst anti-virus software can be an extremely effective tool to combat the very real threat of virus incidents, anti-virus software cannot detect all viruses, particularly if they have yet to be identified (Cohen 1984; Caelli et al 1996; Pikin 2000; Power 2000; Pfleeger 1989). Virus screening or scanning software must also be kept up to date to ensure that the software can detect and eliminate new viruses as they emerge (Thomson 2009; Lowe 2002). A total virus approach must include the capability to act on a large scale, thereby eliminating the risk of spread in an entire organisation (Dojkovski, Lichtenstein and Warren 2007). Sound security policies, good backup and recovery procedures, access control on file transfer systems used in conjunction with up to date virus screening software are the best countermeasures to the virus threat (Westwood 1997; Dojkovski et al 2007; Power 2000; Nelson 1999).

Virus controls are part of the British Standard (BS7799), which specifies 10 key controls in computer security, virus control is identified as one of the key controls in the standard. In one UK study, 88% of respondents indicated that they had implemented virus controls. Of the respondents who indicated that they followed BS7799, 95% of those organisations indicated that they had implemented virus controls. In the same study 90% of respondents who had a security policy indicated that their policy mentioned virus controls and countermeasures (Kearvell-White 1996). The 1995 Ernst and Young Survey cites that 62% of organisation in US used

virus controls and 45% of UK organisations used virus controls. The use of anti-virus controls has obviously grown with the increase in incidents, a later industry survey conducted in the US states that 91% of respondents had active anti-viral software and that anti-virus software was rated the number one security product (Briney 1999).

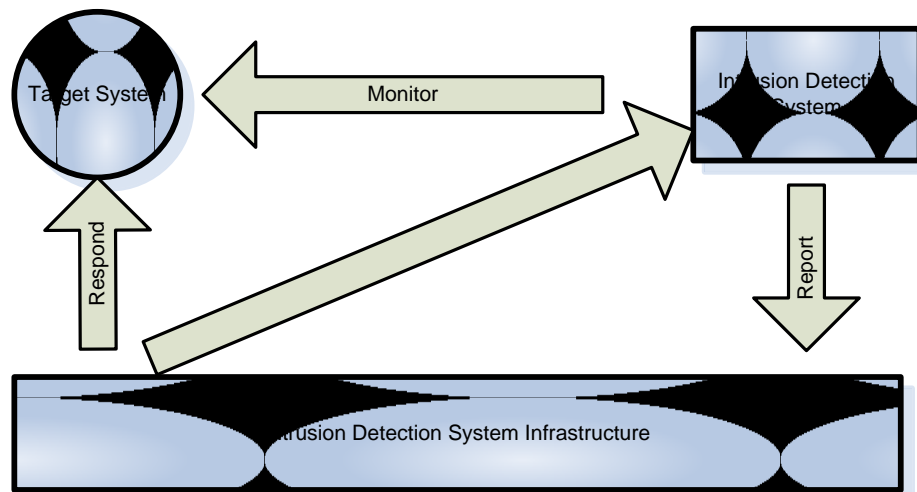
The Australian rate of use of anti-viral products is unclear. Several studies mention the threat and importance of virus countermeasures but do not quantify the extent of Australian businesses reliance of anti-viral products (Dinnie 1999; Thompson 1998). The case study into the security procedures of an Australian travel company conducted by Lichtenstein, highlights that not only are there recorded incidents of the virus threat in Australia, but Australian companies are using anti-virus measures, including scanning software, procedures and policies in an attempt to counter that threat (Lichtenstein 1998).

According to the AusCERT study reported use of anti-viral countermeasures was 98% in 2003, 100% in 2004, 99% in 2005, and 98% in 2006 (AusCERT 2006). More information is needed on the extent and the nature of anti-viral countermeasures in the Australian context.

### 2.3.3.2 Intrusion detection

The term intrusion detection has a somewhat broad definition as it is used to describe audit trail processing, firewall filtering and logging, router based access list usage, telephony toll fraud detection, operating system probes and monitors, camera surveillance at gates and fences, and even physical surveillance by law enforcers (Bejtlich 2004). For the purpose of this thesis intrusion detection is defined as the process of identifying and responding to malicious activity targeted at computing and networking resources (Bejtlich 2004; Khadraoui et al 2007; Escamilla 1998). The term intrusion basically means any misuse, intrusion, or misfeasance that is unwanted (Escamilla 1998). The basic concept of an intrusion detection system is depicted in the figure 2-4 below:

**Figure 2-4: Simple Intrusion Detection Concept Model**



Source: Developed for this research



The way in which derived information about an intrusion is processed, stored, protected, shared, and used as the basis of a risk mitigation strategy is the most challenging aspect of practical intrusion detection (Bejtlich 2004). Intrusion detection is still a relatively new field and processes, technologies and use strategies are still being developed. A number of methods are used to conduct intrusion detection (Bejtlich 2004; Escamilla 1998; Khadraoui et al 2007; Power 2000). These methods include:

- a. Audit trail processing. This is the most commonly used technique in intrusion detection. It uses existing audit logs for analysis and searching.
- b. On the fly processing. This is a form of network intrusion detection, which involves the monitoring of traffic so that real-time or near real-time analysis can be done. Specific strings are often searched for such as '/etc/passwd' or '/etc/shadow'. This technique is used to compliment audit trail processing.
- c. Profile normal behaviour. This method attempts to identify the signatures of known attacks and suspicious input strings to attempt to identify specific types of intrusions.
- d. Pattern matching. This is a special sub-set of profiling, and attempts to identify the patterns of normal network operation so that when abnormal conditions are encountered that alarms can be raised that may warrant further investigation.

Intrusion detection systems comprise of a series of common components including sensors, audit and archive mechanisms, knowledge bases that store signatures and patterns of know attacks or system operating specifications, a processing engine with associated algorithms and incorporated alarms, a systems management facility and supporting graphical user interface (Escamilla 1998; Khadraoui et al 2007). Whilst it is possible to list a series of common components of an intrusion detection system it is generally accepted that there is no 'cure all' intrusion detection product that can be purchased to provide complete security (Khadraoui et al 2007; Bejtlich 2004; Escamilla 1998). Rather, a proactive and interactive approach is required to ensure a series of complementary technologies and policies are implemented in order to have a successful intrusion detection methodology (Dojkovski et al 2007; Power 2000).

Due to the need for an integrated and comprehensive intrusion detection system host based and network based intrusion detection systems have been developed (Power 2000; Khadraoui et al 2007). Host based systems essentially rely on audit trail processing. The key advantage of host-based systems is the high quality information that can be derived from them. The disadvantages of host based systems is that they are quite often platform or operating system specific and that they can lead to performance degradation on the host due extra processing work required for logging of events (Power 2000; Khadraoui et al 2007). In network based intrusion detection systems network traffic is copied and inspected by the system. Because of this approach normal traffic flow is not affected, therefore there is zero performance impact on the system as a whole (Power 2000; Khadraoui et al 2007). The disadvantages of network-based systems are that they can lose packets in a network that has been flooded and there is a need to ensure that the system can handle the amount network traffic on a particular network (Bejtlich 2004; Escamilla 1998).

Due to the various potential advantages and disadvantages of network-based and host-based intrusion detection systems the best option is often to use an integrated approach to the implementation of an appropriate system (Powers 2000; Bejtlich 2004; Escamilla 1998; Dojkovski et al 2007). Most of the latest intrusion detection systems are classified as second-generation systems and are hybrid network and host-based systems (Eschebeck 2000). The hybrid approach has become critical in the attempt to provide real-time detection capabilities to ensure that mission critical systems are protected and monitored against cases of cyber attack (Eschebeck 2000; Power 2000; Bejtlich 2004).

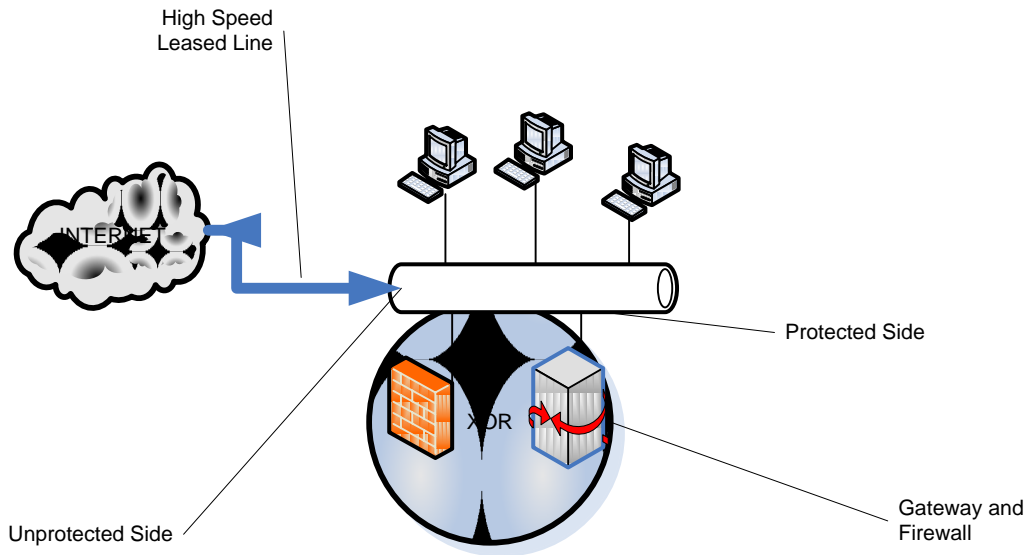
There is very little evidence to quantify or qualify the use of intrusion detection systems. The various information security surveys that have been conducted seldom mention intrusion detection systems in specific terms. The CSI/FBI surveys indicate that in 1998, 35% of respondents used some form of intrusion detection systems. Subsequent surveys in 1999 and 2000 indicated that this figure had risen to 42% and 50% respectively (Power 2000). One international survey detailed that 40% of Australian respondents used some form of security product (including intrusion detection systems) compared to 48% in the US and 49% globally (Dinnie 1999). The 2006 AusCERT survey indicates that after a peak in 2005 at 59% the use of intrusion detection systems dropped to 44% in 2006 (AusCERT 2006).

The usage rate and perceived effectiveness of the intrusion detection systems within Australia is an important fact worthy of investigation.

### **2.3.3.3 Firewalls**

The word “Firewall” when used in the context of information security can mean many different things to different people. To some, a firewall would be an entire system that acts as a gateway between your system and the outside world. To others a firewall may mean little more than a single device designed to stop unwanted data entering a network. For the purpose of this study a suitable definition for a firewall is a system (or device) that is used to control access to or from a protected network. It implements a network access policy by forcing data to pass through the firewall where it can be analysed, audited, and processed (Power 2000; Khadraoui et al 2007; Escamilla 1998). This processing could result in the information being discarded in the case of unauthorised external data or an error message being sent to an originator in the case of an unauthorised internal communications attempt. Most firewalls have auditing features that are monitored by system administrators. When unauthorised access attempts occur the systems administrators are able to examine the incident and take appropriate action (Bejtlich 2004; Khadraoui et al 2007; Escamilla 1998).

A graphical representation of a simple firewall is shown below. In this example the firewall is a system that consists of two devices a gateway and packet filter. Each of these devices will be explained in the following pages.

**Figure 2-5: A typical depiction of a firewall**

Source: Developed for this research

There are three general features that should be provided by a firewall if it is to provide adequate security for an information system (Escamilla, 1998). These purposes or features are:

- a. Restricted external access,
- b. Controlled internal use, and
- c. Audit and accountability.

The initiation of information flow from an external source should be severely restricted. In an e-commerce environment it essential that external information be allowed to flow between networks. Firewalls enable the safe transmission between two different computing environments, say from a customer's computer to a supplier's computer. Firewalls allow a system to authenticate external users to ensure that the only authorised users can access the secured domain (Caelli et al 1996; Eshchbeck 2000; Power 2000; Bejtlich 2004).

Access to external networks should also be controlled and limited to those employees who need the access for specific reasons. The amount of information that can flow into or out of an organizations computer network is usually limited and often companies pay large amounts of money to provide a basic level of capacity, referred to as bandwidth. Any use over and above the assigned bandwidth will result in delays that could cost the organization money in terms of lost revenue or the firm may need to spend additional money on expanding their bandwidth. To control network traffic and related expenses management may authorise only certain activities can occur, such as ordering from suppliers or communications to customers. Other activities such as browsing the Internet may be limited to certain sites and certain users. All of these restrictions are controlled and enforced by a firewall system.

The procedures and practices that are designed to safeguard a network must be actively monitored (Eshchbeck 2000; Power 2000; Bejtlich 2004). Any improper access to a network must be detected so that the appropriate action can be taken to rectify any security breaches or to modify security procedures. Most firewall systems

allow system managers to monitor and audit what traffic is being passed through the firewall. This information will include both internal information flowing to external networks and external information flowing to internal destinations. Armed with this information systems management can determine how effective their security procedures are and if there have been any instances of attempted breaches or any actual breaches (Escamilla 1998).

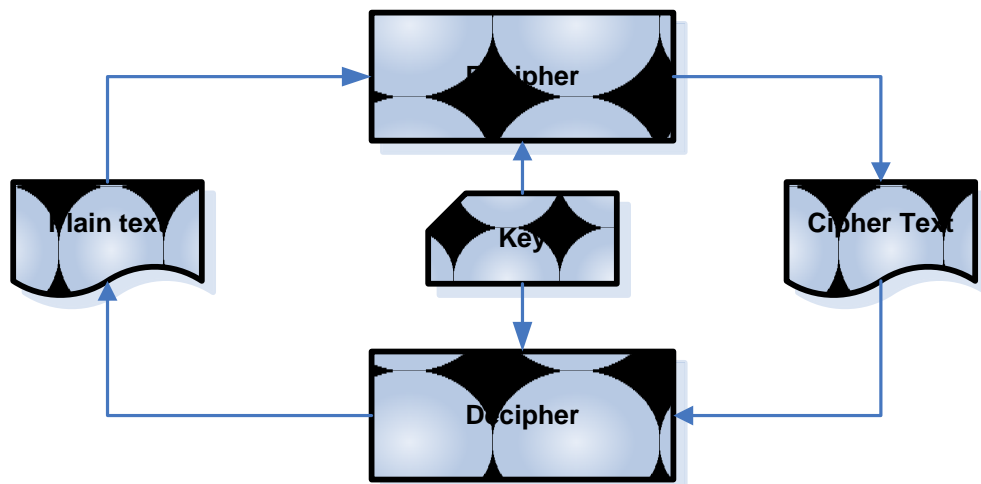
Empirical data collected on the use of firewalls indicates that they are a popular security tools (Power 2000; Briney 1998). In one study conducted in the US, which tracked security tools usage over the period 1998 to 2000, firewalls were used by 81% of respondents in 1998, 91% of respondents used firewalls, however, the number dropped to 78% in year 2000. These figures did not compare as favourably as the use of anti-viral software, physical security of systems or access control mechanisms (Power 2000). In the 1995 Ernst and Young Survey of US and UK organisations, 70% of US organisations had firewalls in comparison to 30% of UK organisations. A later international survey involving Australian businesses indicated that Australia was leading the way in terms of adoption of firewall technology with 77% of respondents indicating that they used firewalls in comparison to the US at 62% and the UK at 53% (Ginnie 1999). A different industry survey conducted in the US indicated that 76% of respondents had employed firewalls while the remaining 24% intended to employ firewalls in the near future (Briney 1998).

A case study into a typical Australian business provides some support to the notion that firewalls are an important component of information security in the Australian context (Lichtenstein 1998). In this study the organisation under study used a firewall to protect itself from Internet threats and also to monitor the activities of employees.

Most studies and authors agree that firewalls are an essential component of providing a secure computing environment (Eshehbeck 2000; Power 2000; Bejtlich 2004; Escamilla 1998; Khadraoui et al 2007), but also state that firewalls are not infallible. Without proper configuration management, monitoring, and an implementation strategy firewalls will offer little protection (Power 2000; Bejtlich 2004).

#### **2.3.3.4 Encryption**

The term encryption and cryptography are often used interchangeably, however for the purpose of this study cryptography is defined as the art or science that deals with the principles, means, and methods for rendering plaintext unintelligible and for converting encrypted messages into intelligible form. Encipherment is the *action* of converting plaintext to cipher text; encryption is often used as a synonym for encipherment, but it also covers the act of encoding a message (Caelli et al 1996; Bejtlich 2004; McClure, Scambray and Kurtz 2005). The diagram below depicts a high level view of encryption.

**Figure 2-6: Basic encryption process**

*Source: Developed for this research*

Ciphers can be categorised into two categories based on the kind of keying concept that they use, either symmetric or asymmetric (Caelli et al 1996). Symmetric encryption uses the same key to both encrypt and decrypt, or if different it is possible to derive one from the other. Where symmetric keying is used the key must be transmitted to the remote end, symmetric keying is also called Private Key encryption. Asymmetric cipher uses different keys for encryption and decryption. It is computationally infeasible to derive one key from the other. This form of encryption is often called public key cryptography (Bejtlich 2004; Khadraoui et al 2007).

Encryption mechanisms rely on keys or passwords. The longer the key the more difficult it is to break. The Data Encryption Standard (DES), which is one of the more popular encryption algorithms, relies on 56 bit key length, which is computationally feasible to break. Stronger keys may be many hundreds of bits in length. As stated earlier there are two kinds of encryption mechanisms (symmetric and asymmetric) – Private-Key and Public-Key. Private-key uses one key to encode and decode data whilst public-key encryption uses one key to encode the data and another to decode the data. The name public key comes from the unique property of this mechanism – namely, one of the keys can be made public without compromising the privacy of the message of the other key. Virtual Private Networks (VPN) employ encryption mechanisms to provide secure transmissions over public networks such as the Internet (Holbrock and Reynolds 1991; Caelli et al 1996; Bejtlich 2004).

In a recent study of security mechanisms employed by Australian organisations 47% of respondents used some form of file encryption to protect their data and 46% indicated that they used encrypted logins or sessions to ensure confidentiality (AusCERT 2006). In comparison in the USA 60% of organisations used encrypted logins and 58% used encrypted files (Power 2002).

### 2.3.3.5 Security Policies and Standards

Policies are technology independent descriptions of the security precautions that are required for different types of information and access. Quite often security policies apply more than just implementation; they apply to all corporate resources. Policies are the primary building blocks for every information security design, defining the responsibilities of the organisation, the individual, and management. Policies specify what must or must not be done to fulfil the security principles (Khadraoui et al 2007; Caelli et al 1996; Bejtlich 2004). Policies and procedures are the cornerstone of information security (Power 1996).

Policies and standards are used in organisations to provide a mechanism where directors and senior management can lay down a clear statement of direction and rules. If policy is created and implemented correctly, it will serve three main purposes for the organisation:

- a. Firstly, policy defines security requirements; without a security policy it could be argued that it isn't possible to have a security violation.
- b. Next policy allocates responsibility.
- c. Finally, the policy statement can actually contribute to control.

Security policies can contain a variety of topics and material. There is however, some agreement that policies should at the very least have a number of common components. Caelli et al (1996), Khadraoui et al (2007), and Bejtlich (2004), all recommend that a security policy include the points listed below:

- The responsibilities of owners, users, custodians, and specific departments
- Risk management, risk assessment and data classification
- Contingency planning and resilience
- Systems development/Implementation
- Access to data/systems and storage control
- Telecommunications security
- Personal computer security
- Environmental and access control
- Legal requirements
- Personnel policies

In the UK, the British Standards Organisation developed and implemented an information security standard called BS 7799 in late 1995. This standard defines 10 key controls that organisations should implement in order to adequately address information security issues. These controls include:

- Information security policy documentation
- Allocation of information security responsibilities
- Information security education and training
- Reporting of security incidents
- Virus controls
- Business continuity planning processes
- Control of proprietary software copying

- Safe guards of organisational records
- Data protection
- Compliance with security policies

A survey conducted in the UK 12 months after the introduction of BS 7799 asked respondents if they had implemented the new standard. At the time of the survey only 2% of respondent organisations had implemented the standard (Kearvell-White 1996). Many respondents were not aware of the standard (40%), whilst the remainder 'intended' to implement the standard in the near future.

In Australia, Standards Australia has followed the British Standards lead by firstly introducing AS/NZS 4444, Information Security Management, and then latter modifying the standard to be more in line the British Standard and standards in OECD nations, the new standard, introduced in 2001 was renamed AS/NZS 7799. No data on the implementation or take up rate of this standard was available. The international version of the standards, labelled as ISO 17799 indicates that approximately 41% of organisations had adopted that international standard. The financial sector recorded the highest take up rate at 25% (KPMG 2002).

In terms of general security policies and procedures to combat information security abuses, one Australian survey revealed that Australian industry, on the whole, was poorly prepared in many areas, especially in terms of the US (Thompson 1997). This study indicated nearly 60% of respondents had no policy on how to deal with systems breaches (10% worse than the US). Other data on the use of security policies vary. In one international study, use of policies in Australian organisations was at 68%, compared to the US at 61% and the global figure of 55% (Dinnie 1999). Other research indicated that the lack of policies is seen as a significant obstacle to information security (Briney 1998).

Previous research would indicate that policies, standards, and procedures are the pillars of network security (Schumacher 1997). In fact many authors and industry practitioners would argue that they are more important than having the technology (Caelli et al 1996; Power 2000; Briney 1998; Khadraoui et al 2007). Having written policies is, however, only part of the picture. The issue with any set of policies is whether they are valid and enforceable. Little is known in regards to how effective organisational policies are, and if indeed once adopted they are maintained and audited. In a case study into the security practices of one large Australian organisation it was found that polices and procedures were used to effectively coordinate and manage the application of several countermeasures, such as anti-viral protection, firewall use, and employee responsibilities (Lichtenstein 1998).

### **2.3.3.7 Incident response**

The response an organisation makes in the aftermath of a security incident will depend on a number of issues. Some organisations will simply want to press on with business while others will want to seek legal and financial recompense for any loss that may have been caused by the incident. There are three basic philosophies to responding to a security incident. They are:

**Watch and Warn.** The watch and warn method performs monitoring and notifies a key person when an incident is detected. It takes no actions by itself, except for notification. This process relies on the ability to rapidly contact a key individual about what decisions need to be made in relation to the incident and what additional warnings need to be generated. The watch and warn philosophy is the most passive method of intrusion detection and response (Khadraoui et al 2007).

**Repair and Report.** The repair and report philosophy will attempt to close the incident as quickly as possible so as to be back to business as usual as soon as practicable (Khadraoui et al 2007; Power 2000). This requires the identification of the intrusion, repairing the vulnerability that allowed the intrusion, and reporting these actions. Typically, the reporting is done through an internal mechanism such as reporting the actions to an internal manager.

**Pursue and Prosecute.** The pursue and prosecute methodology requires the monitoring of the attack, the collection and maintenance of evidence, and the involvement of law enforcement and legal counsel to prosecute the attacker (Khadraoui et al 2007; Bequai 1998). This philosophy takes an active role in fostering a protected information environment. In some instances it may include allowing the attacker to continue with the attack in a supervised way to ensure that the maximum amount of evidence is collected or to attempt to ascertain if the intruder has a specific target.

Regardless of the philosophy adopted by an organisation a incident response plan is required to coordinate efforts in a effective and efficient manner (Schumacher et al 1997; Eschelbeck 2000). A response plan will typically cover the following topics (adapted from Khadraoui et al 2007):

- a. Authority to respond
- b. Financial Limits
- c. Disabling Services
- d. Disconnection from the Network
- e. Communications
- f. Resources (People, tools, external support)
- g. Legal Review

Incident Response and Security Teams, or Computer Emergency Response Teams (CERT) have been formed in a variety of counties in order to provide organisations with expert advice and assistance in dealing with security incidents and to keep organisations informed regarding the latest information security trends and developments. Many of these specialist security organisations have formed the Forum of Incident Response and Security Teams (FIRST), with the aim to promote information sharing and greater security awareness. Organisations that subscribe to such teams often report security incidents in attempt to receive expert advice and guidance or to have vulnerabilities removed (Power 2000; Khadraoui et al 2007; Briney 1998).

In a recent survey conducted in Australia 24% of respondents reported the security incident to AusCERT (AusCERT 2002). This figure was up from 12% in 1999. More recent figures indicate that the policy of not reporting incidents outside the



organisation continues, with 69% of organisations not reporting incidents externally in both 2005 and 2006 (AusCERT 2006). The relevance of organisations such as AusCERT and the services they offer is worthy of further investigation in order to determine why organisations either use or do not use their services.

### **2.3.4 Resource expenditure**

Very little is known about the current level of expenditure or budgets on information security in Australian businesses. It has been reported that up to 45% of Australian businesses do not budget for information security at all (Dinnie 1999). A comparison between Australian information security budgets to the determined level of threat would be extremely useful to the IT industry.

A recent AusCERT survey indicated 70% of organisations indicated that they had increased their computer security related expenditure in the last 12 months as a result of computer security incidents or other perceived security concerns (AusCERT 2002). This expenditure may have involved purchasing new or upgrading network security technologies, improving personal or physical security, training and documentation. The majority of Australian organisations believed they needed to spend more money on computer security (Dearne 2002b).

The KPMG Global Security survey indicates that the average large organisation spend approximately 10.1% of their IT budget on computer security. 63% of respondents to this survey indicated that they would increase their security budgets by 19% in the upcoming year, while 10% of organisations stated that they would decrease their security expenditure. A concerning area was that 43% of respondents did not know how much money was spent on security and 30% did not know the percentage of the security budget when compared to the overall IT budget (KPMG 2002). The limitation of the KPMG study remains the global nature of this study and the nature of the population and response rates received. The KPMG study concentrated on grouping organisations in geographic regions and on larger organisations.

### **2.3.5 Reliance on Information Technology**

The use of information technology by Australian businesses has risen significantly since the early 1990s. Computer use has grown fairly steadily, rising from 49% of businesses in 1993-94 to 63% in 1997-98 and 76% in 1999-2000. Internet use grew more rapidly between 1997-98 and 1999-2000, the proportion of businesses with Internet access almost doubling from 29% to 56%. The proportion of businesses with Web sites or home pages more than doubled over the same period (from 6% to 16% of businesses) (Australian Bureau of Statistics 2000).

The Australian Bureau of Statistics (ABS), has conducted a number of studies into the impact and general use of IT by businesses. The extent to which Australian businesses use information technology is related to business size and industry. At June 2000, 100% of large businesses (those with employment of 100 or more persons) used a computer, 95% had access to the Internet and 68% had a Web site or home page. Very small businesses (those with employment of fewer than 5 employees) had much lower adoption of information technology at June 2000, with

69% using a computer, 49% having Internet access and only 9% having a Web site or homepage (ABS 2000).

Computer use and Internet access were highest in the Property and business services and Electricity, gas and water supply industries at June 2000. At least 85% of businesses in these two industries used computers and at least 76% had access to the Internet. Computer and Internet use was lowest in the personal and other services industry, where 60% of businesses used a computer and 39% had Internet access. Web site use was highest in the Electricity, gas and water supply industry, with 56% of businesses having a Web site or home page, and lowest in the Construction industry (6% of businesses) (ABS 2002).

The ABS data clearly shows that, as expected the use of IT within business is growing to meet the demands of the new information economy. As highlighted in a National Office for the Information Economy Discussion Paper (2000), the rapid growth in the use of the Internet, which is underpinning the emergence of the information economy, is transforming Australia economically and socially. Australian businesses of all sizes and industry sectors are using technology and computers in general for far more of their business (Di Gregoria and King 2000; Williamson, Lichtenstein, Sullivan, Schauder 2006). The development of the information economy and its adoption by business has opened up new markets and provided new sources of revenue. Businesses are becoming more reliant on their computing systems and therefore have more to lose should they suffer from a computer security related incident (Di Gregoria et al 2000; Dearne 2002a; Dearne 2002b).

The AusCERT research makes the linkages between the growth of the information economy and the subsequent reliance of businesses on IT clearer by identifying points of exposure to security risks. The survey found that 98% of respondents had websites, 36% had websites that were 'commercial' in that they were aimed at actually selling goods and services. Of those organisations that had commercial websites 27% earned more than 2.5 million dollars per annum, 36% earned between 1 and 2.5 million dollars and 37% earned less than 500 000 dollars, (AusCERT 2006)

It follows that the more an organisation relies on their computing technology the more they have to lose if that technology should be compromised. In an attempt to estimate the losses associated with computer security incidents AusCERT asked their respondents if their websites had suffered from a security incident and subsequently how much that incident cost their business. Of the 30% of organisations that had suffered from a loss from their commercial website 73% indicated that the losses were less than \$50 000, with 27% indicated that the losses were between \$50 000 and \$100 000 (AusCERT 2006). Where companies operate solely through an online presence if those sites were to be rendered inoperable they could lose many thousands of dollars for each hour that the site is not functioning.

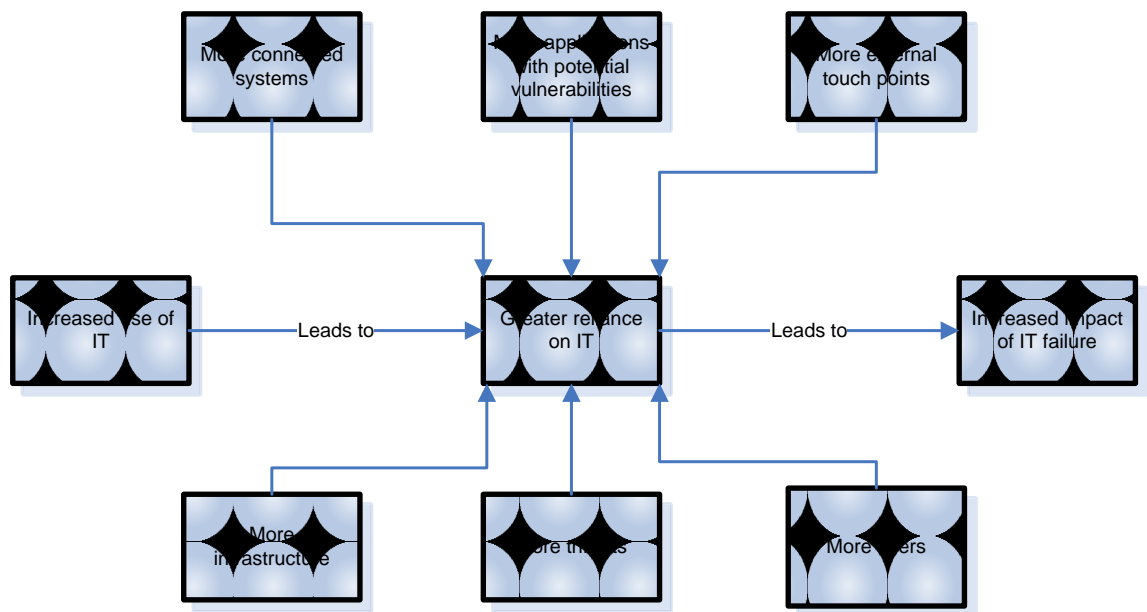
The KPMG global survey indicates the average organisation who had suffered from a website intrusion lost \$32 000 (USD). It also lists the highest recorded cost for a security incident for one organisation as \$10 million (USD) for a virus incident

(KPMG 2002). Research conducted in the USA has also found that organisations are increasingly relying on their computer technology and are suffering many millions of dollars of lost revenue due to security incidents (Rapulas 2000; Power 2000).

Of interest in the Australian business context of information security is the match between the continual expansion of the information economy, businesses of all sizes growing more dependent on the use of computers and the level of computer security incidents and the countermeasures (including funding commitments) employed to mitigate the risks.

There is a relationship between how an organisation uses IT and how reliant the operation of their business is on IT. The strength of this relationship is often not known by organisations and therefore organisations can be under prepared for the impact on their business of the unavailability of core computing systems (i.e., those that they use to perform their core business function). In some cases it has taken a catastrophic event, such as the terrorist attacks on the world trade centre to raise the level of awareness in certain businesses (Withers 2002). Figure 2-7 below depicts the relationship between use and reliance, and in particular how increased use increases organisational reliance and therefore the business continuity impact that an organisation could potentially face.

**Figure 2-7: IT use and reliance framework**

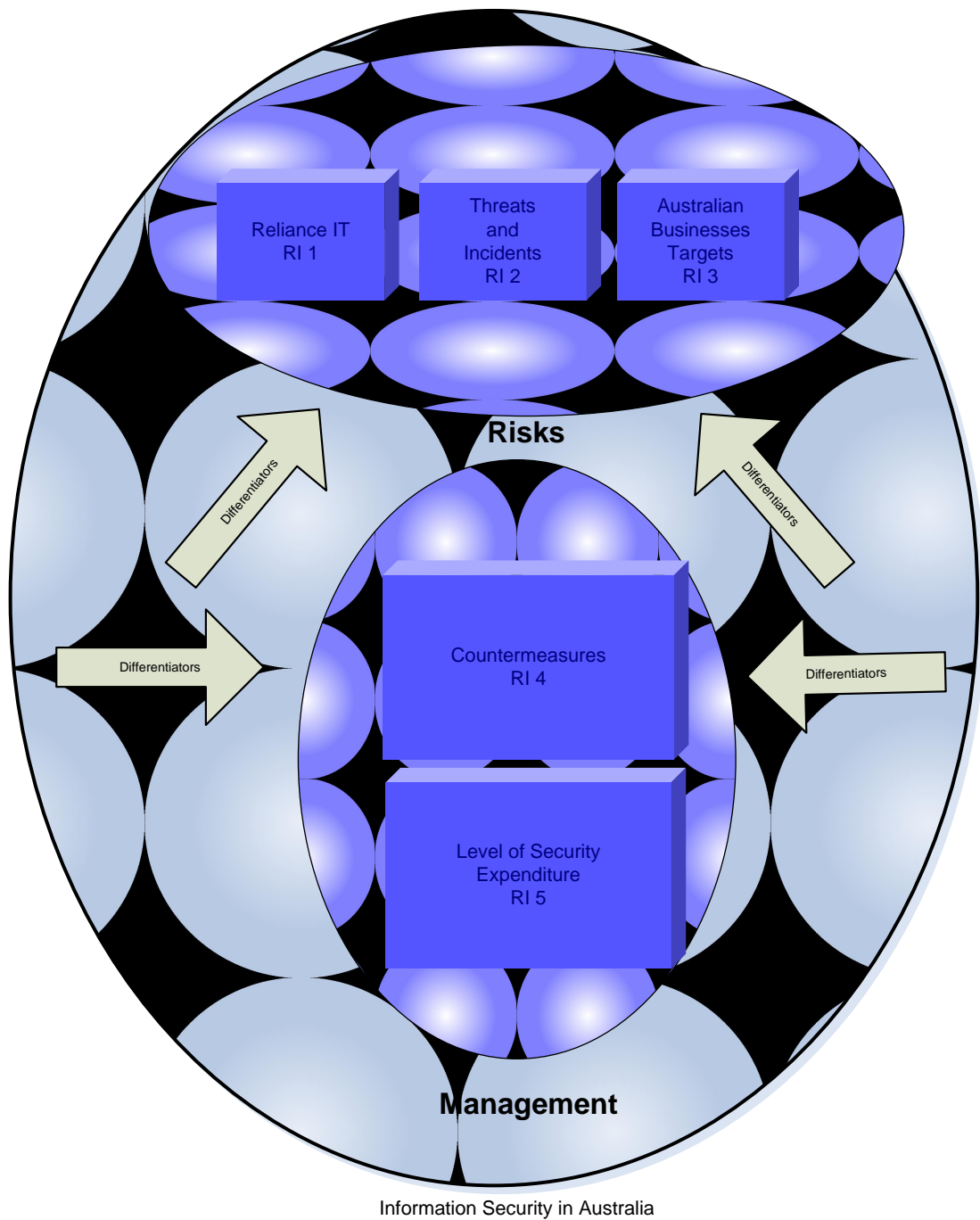


*Source: Developed for this research*

## 2.4 Development of a theoretical framework

The proposed theoretical framework for this research is depicted in Figure 2-8 below.

**Figure 2-8: Theoretical Framework of Research Problem**



*Source: Developed for this research*

The four aspects of the development of the proposed theoretical framework are:

- To study, in general terms the reliance that Australian organisations have on their information technology assets and systems.
- To study the nature and types of threats and information security incidents that are occurring in Australian businesses.

- To determine if Australian businesses are targets for people or organisations intending to perpetrate information security incidents and make a comparison between the results found in international studies.
- To investigate how Australian businesses are protecting themselves from information security incidents.
- To estimate the amount of resources that Australian businesses are committing to protecting their information assets from the identified threats and vulnerabilities.

## 2.5 Research question

The research question for the study focuses on the specifics of the enquiry at hand (Zikmund 1997; McPhail 2000; Yin 1994). The research question for the proposed study is as follows:

In an Australian business context what are the information security threats to organisations, what type of companies are being targeted, how are organisations protecting themselves from these threats, and what are the costs of the protective measures?

### 2.5.1 Research issues

Research issues have been selected to guide the research to answer the research question (Yin 1994). Research issues for the proposed study are as follows:

RI 1 – How reliant are Australian organisations on their IT?

RI 1.1 – How dependent are Australian organisations on their IT in terms of computing systems and the data that resides on those systems?

RI 1.2 – What is the likely impact of the loss of use of an organisation's IT capability?

RI 2 – How is the threat to organisations' computers, data, and networks manifesting itself in Australian industry?

RI 2.1 – What potential threats to computers, data, and networks are Australian organisations likely to face? (*Potential security threats*)

RI 2.2 – What threat(s) do Australian organisations perceive to be the most likely and prevalent/significant? – (*Perceived security threats*)

RI 2.3 – What is the level of actual information security incidents in Australian organisation? – (*Actual security incidents*)

RI 3 – Is the information security greater in Australia? If so, why?

RI 3.1. In comparison with the international experience, is there any difference in the extent to which Australian organisations are being targeted for information security related attacks?

RI 3.2. If so, what are the identifiable differentiators?

RI 4 – How are Australian organisations protecting their computer, data, and networks from information security risks?

RI 5 – What level of resource expenditure are Australian organisations committing to protect their systems and data?

The above research issues were used to explore the stated research question and to direct the research study. Each of these research issues was developed into a series of questions to be used in interviews and surveys.

## CHAPTER 3 - METHODOLOGY

This chapter describes the methodology used to provide data to investigate the research issues in chapter two, which were developed from the research question specified in chapter one. The purpose of this chapter is to identify and describe the appropriate methodology to explore the research issues and answer the research questions. This chapter provides justification for the research design and research strategy, and then explores the issues of validity and reliability. This chapter has four major sections. Firstly in section 3.1 the research purpose and commonly used strategies for collecting data to answer research problems are discussed, leading to the justification as to why the case study methodology was chosen over other potential methods. The multiple case study design for this research is then described in section 3.2. Section 3.3 outlines the process of how data was collected for the research, demonstrating how in-depth interviews were used to as the principle data collection technique. Finally, section 3.4 outlines how the data collected through interviews and other means were prepared for analysis and analysed.

### 3.1 Research design

A research design addresses the planning of inquiry for finding out something (Babbie 1995). There are three basic research designs: descriptive, causal, and exploratory.

- The major purpose of descriptive research as the term implies, is to describe characteristics of a population or phenomenon. Descriptive research seeks to determine answers to who, what, when, where, and how questions (Zikmund 1997).
- Causal research is initial research conducted to clarify and define the nature of a problem (Zikmund 1997).
- Exploratory research is initial research conducted to clarify and define the nature of the problem (Cooper and Emory 1995).

#### 3.1.1 Research purpose

The purpose of this research was to investigate information security in the Australian business context. Of the three types of aforementioned research types this research is primarily descriptive, but it also contains a small element of exploratory research in terms of the initial pilot study.

The first type of research, exploratory research, is conducted to clarify or gain a better understanding of the research topic and is typically conducted in the initial stages of the research in the form of a pilot study to assist in the clarification of the aims of the study and to confirm the research design.

The second type of research, descriptive is undertaken when the researcher seeks to describe the population or phenomenon, thus answering questions relating to who, what, when, where and how (Zikmund 1997). The purpose of this research was to *describe* the *characteristics* of the phenomena of information security in Australia and *describe how* Australian businesses are protecting themselves. The proposed

research question and associated research issues described in the earlier chapters suit a descriptive research design (Yin 1994).

### 3.1.2 Research strategy

Research strategy refers to a plan specifying the methods and procedures for collecting and analysing the needed information (Zikmund 1997). There are five types of research strategies, experiment, survey, archival analysis, history, and case study (Yin 1994). The research strategy should be aligned with the goals and characteristics of the study (Yin 1994).

Table 3-1 outlines the conditions and the type of research strategies that are suitable for each type of question.

**Table 3-1: Relevant Situations for Different Research Strategies**

Strategy	Form of research question	Requires control of behavioural events	Focuses on contemporary events
Experiment	How, why	Yes	Yes
Survey	Who, what, where, how many, how much	No	Yes
Archival analysis	Who, what, where, how many, how much	No	Yes/No
History	How, why	No	No
Case Study	How, why	No	Yes

*Source: Yin, 1994, p.6*

As the purpose of this research was to describe information security in the Australian business context, two research strategies were considered for this research: surveys and case studies. Experimental research was not considered appropriate, as there was no attempt to manipulate information security in Australia. Case studies and surveys are considered in further detail in following sections.

Surveys are a data collection technique whereby data is collected from a sample population by use of a questionnaire and they are generally considered the most common mechanism for gathering primary data (Zikmund 1997).

The greatest strength of the survey technique is its versatility. Abstract information of all types can be gathered through questioning others (McPhail 2000). In general, the major weakness of this method is that the quality of information secured depends heavily on ability and the willingness of respondents to cooperate (McPhail 2000; Zikmund 1997). As stated in chapter 2, information security research has largely concentrated on survey based research, which has historically recorded poor response rates. The 2002 AusCERT, Deloitte Touche Tohmatsu Australian Computer Crime and Security Survey for example had an 18% response rate. This figure is far below a level that would be considered sufficient to make the finding scientifically valid. Further detracting from this style of research, studies such as the one mentioned above typically target the top 300 or 500 companies in a country. This sample



completely omits a large proportion of the organisations that conduct business in any country, i.e. Small to Medium Enterprises (SME). It could also be suggested that much of this research is often sponsored or even managed by organisations offering security services and as such could be seen as a marketing strategy.

Given the historical weakness with surveys when used to conduct information security research, case study techniques were investigated due to their ability to allow the researcher to closely observe the variables under study. Results of case studies enable the researcher to expand and generalise on theories as opposed to making generalisations about populations. Generalisations about populations cannot be drawn from case study findings (Yin 1994).

The purpose of this research was to investigate information security in Australia by adopting a more thorough and scientifically valid approach in comparison to previous studies conducted both in Australia and overseas. Therefore a case study approach was chosen ahead of a survey methodology.

The primary approach to the collection of data for this research was to collect qualitative data. Qualitative data is in the form of words, or statements that can be based on observation, interviews, and documents. By being in close proximity to the variables being studied richer data and description can be obtained to improve the quality of the research results (Miles and Huberman 1994; Yin 1994).

### **3.2 Case study design**

This section describes the research design based on a multiple case study approach. As a research design includes a number of pre-requisite decisions including what concepts will be studied, how these concepts will be studied, how they will be measured, who will be studied, how data will be collected, and how the reliability and validity of the research will be maintained (Perry 1998; Yin 1994; Zikmund 1991). In addition to addressing these issues this section describes the principal instruments used for data collection for this research – namely in-depth interviews and virtual interviews.

#### **3.2.1 Unit of analysis**

The unit of analysis looks at what the ‘case’ is or what the research will focus on. Examples of units of analysis include individuals, groups, organisations or specific projects. Defining the problem requires that the researcher determine the unit of analysis for the study (McPhail 2000; Perry 1998; Yin 1994; Zikmund 1997).

The research problem can be used to determine the most appropriate unit of analysis for any particular research task (Zikmund 1997). This study investigated information security within the Australian business context; therefore the unit of analysis for this research is Australian businesses or organisations. These businesses are usually clearly defined groups of people (and assets) brought together to form an organisation with a specified purpose such as selling goods or services or providing a community service when describing some Government departments. Australian businesses come in all shapes, sizes, and sectors and have differing business objectives. The aim of using Australian businesses as the unit of analysis is to

provide an in-depth understanding of what the information security issues facing Australian businesses are. By using this unit of analysis it is also possible to make comparisons with other research in the field and to make useful comparisons to international studies.

### **3.2.2 Number of cases**

In determining the number of cases, sampling logic, as applied to survey methods in quantitative research methods, does not apply to case study research as the goal of the research is not to generalise across a population or determine the frequency of some phenomena (Perry 1998; Yin 1994). For the purpose of this study a multiple case based design has been adopted. Multiple case designs allow for within case and cross-case analysis, and are also useful in determining if findings from individual cases are replicated (Yin 1994).

When selecting the number of cases some authors advocate a minimum of two case studies, but the usual view is that, 'in practice four to six groups form a reasonable minimum for a serious project' (Hedges 1985, pp.76-7). For a maximum number of cases an upper limit of twelve cases should be set because of the high cost involved in conducting qualitative interviews, additionally large numbers of cases can make the research data collection and analysis overly complicated (Hedges 1985; Miles and Huberman, 1994; McPhail 2000). The accepted range would appear to be four to ten.

In the context of this research, having determined that multiple cases would be studied, the ideal range was set for between eight and twelve cases. The number of cases should reflect the number of case replications the researcher hopes to achieve from the research, in turn, reflecting certainty in their findings (Yin 1994). Similar results indicate literal replication and sufficient cases should be included with hope of achieving literal replication (Perry 1998; Yin 1994). Each case must be carefully selected so that it either (a) predicts similar results (a literal replication) or (b) produces contrasting results, but for predictable reasons (theoretical replication)' (Yin 1994, p.46). Due to the potentially sensitive nature of the subject matter it is important to emphasise the difficulty in attracting organisations to participate. This issue has been highlighted in numerous quantitative research studies conducted in the field of information security (Thompson 1997; Power 2000; AusCERT 2002).

It was decided that a range between eight to twelve cases would provide sufficient evidence to demonstrate replication logic and therefore address the research issues appropriately.

### **3.2.3 Number of interviewees**

After determining that between eight and twelve organisations would be included as cases for the research, it was initially determined that between two to three people would be interviewed for each organisation in order to collect data from the study. Two exploratory data collection techniques were used to derive this figure: secondary data resources (organisational charts and organisational literature), and a pilot study. Secondary data, experience surveys and pilot studies are three techniques

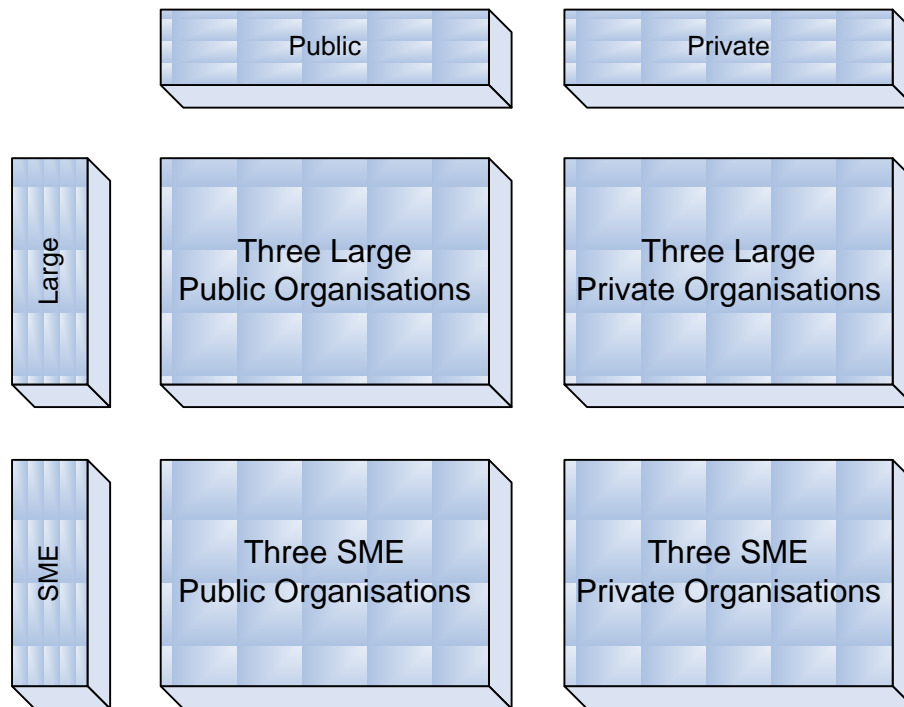
for collecting data for exploratory research (Zikmund 1997). The analysis and review of the secondary data determined that information security practitioners were generally integrated as part of the IT group or they held an advisory type role to the IT group. Regardless, of the organisational structures it was evident that there were limited numbers of people who could comment authoritatively on information security issues. Even in large organisations there may only be a single Information Security Manager as much of the 'hack work' could or is outsourced to specialist service providers. As a result of the initial secondary data analysis the interview numbers were revised to, 'as many as possible', with one or two per organisation being most likely.

The pilot case study and supporting Internet questionnaire supported the secondary data and pointed to the requirement for a more industrious and innovative method for data collection in order to encourage greater participation. At this stage a further limitation became evident that if there were limited personnel to interview in large organisations then it would be even more difficult to gain participation from smaller organisations. Due to the significant importance of SME to Australian business it was decided that even if only one interview could be secured from an IT staff member who had security responsibilities then this should be sufficient to gain a picture of the information security issues in that organisation. It could also be argued that in smaller organisations with limited numbers of IT personnel that it may easier to get a more concise view as to what the information security issues are.

#### **3.2.4 Case Selection**

After setting the number of cases and interviews, the next issue to be addressed was case selection. Using two exploratory research data collection techniques: secondary data sources (Internet newsgroups, websites, journals, and experience surveys, which included discussions with academic staff and industry practitioners), twelve organisations were selected as cases for this research. Figure 3-1 below depicts the case selection matrix. A cross section of organisations was chosen to ensure that the findings can be used to make valid inferences about information security in other organisations in Australia.

**Figure 3-1: Case Selection Matrix**



*Source: Developed for this research*

The twelve organisations were selected as cases for this research because of their ability to:

- Predict similar results for predictable reasons (that is, literal replication).
- Produce contrary results for predictable reasons (that is, theoretical replication) (Yin 1994; Stake 1994; Perry 1998)
- Provide rich-information (Perry 1998)
- Different characteristics (Perry 1998).
- The researcher’s familiarity with the organisations (Yin 1994).

Each of these issues is now addressed in turn.

### **Similar results for predictable reasons**

Cases predicted to result in similar findings (not the same) were selected to demonstrate literal replication and provide additional support for insights (Yin 1994). Organisational structures (organisational chart diagrams) and previous research findings were vital data to help select cases that could predict similar results. As all selected organisations used IT to support their business practices and all of the organisations had some form of external network connection to their own computing facilities it was determined that they would face similar information security issues.

### **Contrary results for predictable reasons**

Cases predicated to produce contrary results were selected to demonstrate theoretical replication. Exploratory research indicated that some organisations may be targeted for specific reasons, additionally larger organisations were assumed to have larger IT

budgets and would, therefore would be more likely to have dedicated IT security professionals.

### **Rich information**

Selecting information rich cases is necessary to provide valid and meaningful insights from the research (Perry 1998). Based on a number of discussions with IT practitioners and academics it was determined that the selected cases would provide rich sources of data for the research.

### **Different characteristics**

Cases with different characteristics were deliberately included in this research, as maximum variation sampling (that is, selecting extreme cases) can provide valuable insights (Perry 1998). The characteristics of organisation size (number of employees, size of IT group, size of IT budget), public or private ownership, and industry type were used to identify cases that may offer theoretical replication in relation to information security issues with Australian organisations.

### **Researcher familiarity with organisations**

The final consideration in the case selection process was selecting organisations that the researcher or the research supervisors were familiar with. The researcher had been employed by two of the organisations studied and had contacts with the IT organisations in four of the other cases. Given the sensitive nature of the subject matter it was considered important that wherever possible that contacts would be used to increase the chances of securing an interview.

Preliminary contact was made with the IT Manager in each of the twelve organisations in order to gain the commitment to participate in the research. It was immediately evident that after sending a number of letters and making follow up phone calls that many organisations were reluctant to participate in the study. As this issues was predicated at the outset of the study as a potential limiting factor it was not a surprise.

### **Scope change**

As an organisation either failed to respond or indicated their unwillingness to participate additional organisations were chosen to take their place in the research until the minimum figure of eight organisations had agreed to participate.

### **3.2.5 Time Frame**

Another important research design issue is the time frame of the research. Research can be conducted either cross-sectionally or longitudinally (Zikmund 1997). In a longitudinal study respondents are questioned at different moments in time. The purpose of longitudinal surveys is to examine continuity of response and to observe changes over time. In such a study, various segments of the population are so sampled so that relationships among variables may be investigated (Zikmund 1997).

Either cross-sectional or longitudinal approaches could have been adopted for this research, a cross-sectional study was preferred, as it was not viewed as being required to observe changes overtime to provide the requisite research data.

### **3.2.6 Data collection techniques**

Case study research often involves employing a variety of techniques to collect data from multiple sources. The use of multiple techniques improves the validity and reliability of results and also increases support for findings (McPhail 2000; Perry 1998; Yin 1994). Due to the complicated nature of information security in Australia and the difficulty in securing access to organisations willing to participate, there was a requirement to use a variety of data collection techniques; of particular importance to the collection of data was the use of interview techniques.

After the formulation and development of the research framework in section 2.4, five data collection techniques were selected for this research: in-depth interviews, a structured questionnaire, collection of data from secondary sources including the Internet and business documents, virtual interviews, and online structured questionnaires. This section details each of these five data collection techniques.

#### **In-depth interviews**

In-depth interviews are a relatively unstructured data collection technique used in the primary stages of the research process (Zikmund 1997). In-depth interviews were a primary method of data collection for this research. The in-depth interview is similar to the client interview of a clinical psychologist or a psychiatrist. The technique involves the interviewer throughout the session asking many questions and probes for elaboration after the subject answers. Unlike some other techniques the subject matter is generally undisguised (Perry 1998; Yin 1994; Zikmund 1997).

Given the nature of the subject matter it was felt that interviews would achieve a far more comprehensive set of data on information security within the Australian business context.

Interviewing provides the researcher a means to gain a deep understanding of how the participants interpret a situation or phenomenon than can be gained through other potential methodologies (Stainback 1998). It was important in the context of the research subject matter to include respondents' perceptions on the information security issues. Additionally, a basic assumption in in-depth interviewing research is that the meaning people make of their experiences affects the way they carry out that experience (Seidman 1997). Therefore, the importance that organisations place on information security should reflect their experiences in the subject area.

The use of interviews as a data collection method for qualitative research does have its weaknesses. There is the possibility of respondent errors, omissions, or misstatements. The responses generated could be subject to interpretive errors made by the researcher in the review process (Stainback 1988; Seidman 1997; Yin 1994). To overcome this potential problem data was collected in conjunction with the interview, most notably an exit survey was conducted in the form of a written questionnaire to allow for data triangulation to take place.

### In-depth interview instrument design

In-depth interviews were designed to collect data to address the research issues. The table below depicts the breakdown of the sections of the interview and how they are matched with the research issues to subsequently solve the research problem.

**Table 3-2 – Interview Protocol Design**

Research Issue	Interview Protocol Section
RI 1 - How reliant are Australian organisations on their IT?	Section A of the interview protocol, IT in your organisation deals with this RI. The aim of this section is to identify to what extent organisations are reliant on their IT networks and what happens if they fail or are subjected to information security risks.
RI 2 – How is the threat to organisations’ computers, data, and networks manifesting itself in Australian industry?	Section B, Threats to computers, data, and networks, and Section C, Computer, data, and network security incidents deal with this RI. This section aims at identifying the type and nature of information security threats and how prevalent or serious they are.
RI 3 – Is the information security greater in Australia? If so, why?	Section B, Threats to computers, data, and networks deals with this RI. This section attempts to discover if organisations perceive that they are targeted for specific reasons, i.e. due to the type of organisation. Section C, which deals with specific incidents may provide evidence that the organisation has been targeted. The comparison component of this research issue can only be answered by review previous research.
RI 4 – How are Australian organisations protecting their computer, data, and networks from information security risks?	Section D, Security Practices and Procedures addresses this RI. The aim of this section is for the organisations to describe how they deal with the threat.
RI 5 - What level of resource expenditure are Australian organisations committing to protect their systems and data?	Section D. As part of this section the respondent will be asked to estimate the amount of money and resources that they commit to information security.

*Source: Developed for this research*

The interview protocol was developed in order to meet the collection requirements for the research and to allow all respondents to provide as much information regarding information security as was practical. The interview was broken into clear sections to aid in initial note taking and later data analysis. The organisation also assisted the respondents to ‘save’ responses for the appropriate section where appropriate. The interview protocol used for the research is attached as Appendix A.

In addition to questions, a number of probing points/issues were included as part of the instrument which were developed after initial pre-testing and through reviews of previous research. The probing statements were useful in cases where the interviewee may not have fully understood the question; when further elaboration was required, or to determine if there had been any omissions in the stated response (Zikmund 1997; Gillham 2000; Seidman, 1997; Stainback 1988).

Each interview started with a personal introduction and the exchange of pleasantries. The next part of the discussion included an outline of the research, including its purpose and scope. Importantly, due to the sensitive nature of information security issues the respondents were assured that all information provided would be kept confidential and that neither respondents nor their organisations would be identified in any of the research reports or findings.

The first set of questions attempted to put the significance of information security into context. Respondents were asked about the nature of IT within their organisations, essentially how technology was used and how dependent the organisations' processes were on that technology. Subsequent questions dealt with information security specific issues such as threats, incidents, and countermeasures. Concluding questions concentrated on organisational demographics and the respondents' position within the organisation. Again, table 3-2 illustrates the linkages between the interview protocol and the research issues. The research framework depicted in chapter 2 subsequently matches both by relating the focus area of reliance on IT, threats, incidents, countermeasures, and expenditure on security to each organisation.

### **Structured written questionnaire**

Due to the nature and potential scale of the research topic it was envisaged that the research would either be a qualitative case based study, a quantitative survey based study or a combination of both. As a result lessons learnt during the review of the literature and the pilot study a case based approach was considered the optimum methodology. Therefore, the prepared survey instrument was used to compliment the in-depth interview process and to allow for triangulation of results.

In contrast to in-depth interviews, structured written questionnaires with fixed response categories (such as likert type scales) are:

- Relatively cheap to administer (Frazer et al 2000)
- A fast data collection method (Frazer et al 2000)
- Good at obtaining hard to recall data (Frazer et al 2000)
- Easy to respond to (Zikmund 1997)
- Straight forward to analyse and interpret data easily (Davis and Cosenza 1993; Frazer et al 2000; Zikmund 1997)
- Not open to different interpretations by the researcher (Davis et al 1993; Gillham 2000)

### **Structured written questionnaire design**

The structured written questionnaire designed for this research was designed to gather information across all five research issues in order to assist in solving the research problem. The questionnaire is attached as appendix B. The questionnaire is organised into five sections:

- a. Information technology in your organisation
- b. Threats to information security
- c. Information security incidents



- d. Security practices and procedures
- e. Demographics.

The questionnaire has 70 questions ranging from yes/no questions, selecting the most appropriate amount, and free text responses. Two different likert scales were used. Namely:

- a. 1 – 5 range of Strongly Agree to Strong Disagree
- b. 1 – 4 range of Least Frequent to Most Frequent.

The likert scale was selected to measure the view point of the respondents, as these scales are often used for measuring attitudes and behaviours (Zikmund 1997). As mentioned above the survey also included several areas allowing for a free text response and sections asking for any general comments of potential omissions from the previous responses. This method allowed for the respondents to give a broader range of answers and to convey perceptions about the subject matter and the survey itself.

To ensure that the designed questionnaire met the requirements of the research the questionnaire was carefully aligned with the research issues. Table 3-3 below depicts the relationship between the research issues and the questionnaire.

**Table 3-3 – Survey Instrument and Research Issue Matrix**

Research Issue	Instrument Section
RI 1	Section A, Questions 1 –16
RI 2	Section B, Questions 1 – 14 and Section C Questions 1 – 15.
RI 3	Section B, Questions 1 – 14 and Section C Questions 1 – 15.
RI 4	Section D, Questions 1 – 17 and 19
RI 5	Section D, Question 18.

*Source: Developed for this research*

There were a number of different survey instruments that were identified as part of the literature review process. These instruments were somewhat similar in their context and structure as there had been some attempts in the previous research to allow for comparisons between industry sectors and to a limited extent to allow for international comparisons. The most recent of the surveys being the CSI/FBI 2002 Survey covering security incidents (and issues) in the USA and the AusCERT 2002 Survey conducted in Australia in 2002. Whilst these surveys were used as reference points, the instrument for this research was designed well before these studies and attempts to create and illustrate linkages between the issues and the variables.

**Observation techniques**

Data collected through the interview process was triangulated with data collected through observation. Observation as a data collection technique involves witnessing and experiencing behaviours or events (Zikmund 1997), and provides the researcher

with the opportunity to collect data not possible via any other method (Yin 1994). Simply put observation has three main elements according to Gillham (p.45 2000):

- Watching what people do
- Listening to what they say
- Sometimes asking them clarifying questions

The observation technique of direct observation was used to collect data for this research. Direct observation involves witnessing events, whereas participant observation is actual participation in events (Yin 1994). Direct observation can also be called detached or structured; it involves watching from the 'outside' in a carefully timed and specified way – counting and classifying what is seen (Gillham 2000).

Wherever possible the interviews for this research were conducted at the place of business or each organisation. This allowed direct observation of information security issues including threats, incidents, and displays of information security countermeasures.

Observation techniques can be extremely useful in data collection, however, the researcher must be mindful of the techniques' limitations (Gillham 2000; Yin 1994; Zikmund 1997). Researchers may assume both action and research roles and this combination is a prime source of confusion. Observer bias is a further limitation of using observation techniques (Gillham 2000; Yin 1994; Zikmund 1997). To reduce the likelihood of observer bias notes taken as a result of observations were compared with the other data collected and some issues were discussed with academics and practitioners.

### **Virtual interview**

As indicated previously the subject matter can be very sensitive which would naturally result in potential participants being reluctant to divulge potentially compromising information. A review of previous research indicated that response rates for this kind of study were extremely low. In order to improve the quality and quantity of participant data a virtual interview system was developed.

This unorthodox method for interview collection was introduced for a number of reasons including:

- Early interview participants tended to get ahead of themselves in relation to answering subsequent questions in earlier parts of the interview
- Participants tended to wander off topic and include issues that were not as relevant as some other areas
- The potentially sensitive nature reduces the amount of potential participants therefore alternate methods are needed to increase the amount of people in the sample space
- Some individuals preferred for interviews not to be taped, which made taking of notes more important
- The design of an online interview method made use of modern technologies enabled the transcript to be actually generated by the participant. At the same

time the results were already in a format that was prepared for immediate coding and analysis

- The format reduced the potential for interviewer bias or error
- The web format made it possible to directly link the exit survey to ensure that there could still be triangulation of results
- The virtual interview also opened up other parts of the country that may have been otherwise excluded from the study due to the cost of travel
- Forms designed with long scrolling text boxes to allow respondents to type as much information as possible
- Respondents were informed that they may receive a follow up e-mail to confirm their responses. In this way a more interactive approach could be adopted

When presented with a choice the respondents preferred to take part in the virtual interview as they could:

- Complete the interview in their own time, potentially outside normal business hours
- Obtain more accurate data regarding instances
- Track down reference documents that could be later used as secondary data

A copy of the virtual interview is attached as appendix C.

### **Online written questionnaire**

The structure written questionnaire was also developed into an online survey format. This allowed the written questionnaire to be distributed to a potentially wider audience but more importantly it was the basis of a triangulation tool that could follow either an in person interview or a virtual interview.

### **Secondary data sources**

The secondary data for this research took the form of annual reports, organisational charts, strategic plans, information security strategic plans, information security policies and procedures, incident response plans, security audit documents, and vulnerability assessments. Wherever possible secondary data documents were collected prior to interviews. Documents were also collected during interviews to validate and compliment data collected through the interview process. Given the subject matter it was anticipated that some organisations would not wish to provide hard copy data. Additionally, because of the small size of some of the case participants many did not have formalised security of policy documentation to offer. Documents are an important source of data to corroborate and augment evidence derived from other sources (Gillham 2000; Stainback 1988; Yin 1994; Zikmund 1997). Documents, policies and procedures were used with some caution as they may be incomplete or they could have been out of context with the scope of the study.

### **3.2.7 Pre-testing**

After completion of the design of the in-depth interview protocol and the survey instrument pre-tests were conducted to ensure that the instruments were valid for

final data collection. Pre-testing is an important component of any research design (Zikmund 1997). Pre-testing can identify problems with data collection techniques and instruments, which could potentially compromise the validity of the research (Davis et al 1993).

Pre-testing for this research initially involved administering the in-depth interview and structured written questionnaire to four industry professionals and two academic staff members. The pre-test candidates included general IT professionals and IT security professionals who had expressed interest in the content of the study. The intent of the pre-test was to ensure that the questions being asked were relevant and easily understood by all.

After coding of the structured questionnaire in the Hyper Text Mark-up Language (HTML), the resultant hyperlink and introductory statements were posted on four Internet newsgroups that specialised in information security. Newsgroup readers were invited to take part and provide comments on the questionnaire design.

The information derived and lessons learnt from the pre-test were invaluable in modifying the questionnaire for further use in the study.

### **3.2.8 Pilot Case**

A pilot study is a collective term used to describe any small-scale exploratory research technique that uses sampling but does not necessarily apply rigorous research techniques (Zkimund, 1997). The main purpose of the pilot study for this research was to test both the interview protocol and the survey instrument. As previous studies had encountered difficulty in attracting participation the pilot study was also looked upon as an opportunity to explore alternative data collection strategies in order to maximise respondent participation. Essentially, the pilot study was aimed at validating the research approach and to confirm that respondents would be hard to find.

The draft interview protocol was tested via a single in-depth interview conducted in the manner and style as intended for the research. The survey instrument, which was intended to be a method of triangulating results, was given to the interview participant at the conclusion of the interview. To gain additional feedback and to attract future participation in the subject a web site was created and Australian IT managers were invited to participate via a number of posts to security related newsgroups on the Internet. As part of the survey participants were asked to comment on the validity, content, and style of the survey instrument.

Pilot testing is a critical part of any research design as it can potentially uncover flaws in the design of the research, therefore allowing the researcher to make the appropriate judgements before launching into the main component of the study (Seidman 1997; Yin 1994).

The organisation chosen for participation in the pilot case was chosen due to the researchers' familiarity with the organisation and the interview participant. Additionally, as the researcher was familiar with the organisation and the subject in

context with the organisation the interviewees' responses could be evaluated with a high degree of certainty, therefore allowing more time to concentrate on the design of the various instruments.

The survey instrument was tested at the conclusion of the first face to face interview and also via posting the information on a web site. A number of special IT security newsgroups were visited and Australian IT professionals were invited to take part in the survey.

As a result of the pilot study a number of minor changes were made to the structure and wording of both the interview protocol and the survey instrument.

### **3.2.9 Validity and reliability in case study research**

Validity and reliability relates to the degree of confidence researchers and academics can have in research results and are essential elements to consider in the creation of a research design (Zikmund 1997). Validity refers to minimising research errors, ensuring the accuracy of the results (Davis et al 1993). Reliability refers to achieving consistency in the results of the research, if the research was repeated (i.e., it is repeatable), (Davis et al 1993; Yin 1994). There are three types of validity namely internal, external, and construct validity (Yin 1994). Each will be addressed in regards to the conduct of this research.

#### **Internal validity**

Internal validity is not relevant to descriptive studies (Yin 1994), except to say that as many explanations as possible were considered for variable relationships to ensure that unjustified claims are not made during the research's conclusions (McPhail 2000).

#### **External validity**

The ability to make generalizations about the information security threat to Australian companies will be a useful product of the research. Comparative norms established from previous studies in the US will be used to judge the external validity of data developed in the research study (Zikmund 1997). This research, like others involving case studies will rely on analytical generalization to enable the results to be generalized to the broader area of theory on information security (Yin cited by McPhail 2000,p.5.19). By using similar questions in the survey component of the study it will be possible to identify differentiators and to validate the existing data against that previously collected.

#### **Construct validity**

Construct validity was ensured by having multiple sources of evidence (multiple cases) and having a limited group of interviewees review the case study report and interview transcripts to ensure that it is an accurate representation of reality (Healy and Perry 1999). Interview participants were also asked to complete a separate

questionnaire which was used to triangulate the results. As depicted earlier in this chapter a number of matrixes were compiled to ensure that questions could be linked to the research issues.

### **Reliability**

A case study database was built and maintained to hold transcripts of interviews and other triangulation evidence such as annual reports obtained from external sources (Perry 1998; Yin 1994). As far as possible the research was conducted in easily reconstructed steps so that other researchers could follow the steps and achieve the same results.

Other triangulation techniques that will be used in the study include the comparison of interview answers to the literature, including recent newspaper articles involving both cyber crime/warfare and the companies being studied. Audiotapes will be used to check hand written transcripts of interviews. More than one interview was conducted in each case organisation to ensure that there are fewer reporting errors introduced by the interviewee (Zikmund 1997). Additionally, interviewee's were in similar positions in each organisation.

Analysis all data will be coded using two techniques and computer applications will be used to triangulate the results of the analysis methods (Perry 1997).

#### **3.2.10 Ethical considerations**

In addition to addressing validity and reliability issues, the ethics of this research had to be addressed. Ethical considerations are important for all research activities regardless of the participants and the subject material (Zikmund 1997). The sensitive nature of the subject matter and the potential for embarrassment related to any vulnerabilities or security incidents discovered meant that all organisations wanted to keep their identities confidential anonymous. Interview participants also wanted their identities kept anonymous for similar reasons. Ethical issues in this study were addressed by:

- Reassuring the interviewees and organisations participating in the research that the information collected would remain confidential; statements regarding information would be generalised in such a way as to ensure the anonymity of the organisation.
- Assuming honest responses were provided from interviewees in relation to interview questions and responses to the survey instrument and both forms of the online versions of the data collection tools.
- Allowing participants to receive feedback from findings within the organisation. In fact, at the conclusion of the data collection respondents often asked for feedback on how their organisation compared against other organisations.
- All participants were presented with copies of transcripts firstly to ensure that notes and transcripts were accurate (triangulation) and second to assure the information recorded had not been misrepresented.

### **3.3 Data collection process**

After the research design was completed and the data collection instruments had been tested and finalised the case studies were conducted. This section outlines the process taken to collect data from each organisation, with the first step being to make contact with the case organisations.

#### **3.3.1 Contacting organisations**

A variety of methods were used to contact organisations based on discussions with academic staff and lessons learnt during the pre-tests. Additionally, the researcher's contacts as an IT Manager helped open doors to some organisations. A variety of methods and techniques were selected and required to identify participants and how to gain the appropriate permissions to ensure participation (Seidman 1997; Stainback 1988). The following approach was used for planning and conducting interviews and collecting information.

In the first instance a letter, attached as appendix D, was sent to the IT Manager of the organisation to introduce the researcher and the research topic. The letter requested permission to undertake the research, specified the required commitment from the organisation (two interviewees for one hour each), assured confidentiality of the information collected and requested the organisation contact the researcher to arrange a convenient time to conduct the interview.

In most instances the participating organisations were contacted by e-mail a week later to confirm their availability to participate in the study. The participants were again assured that the all information and organisational information would be kept confidential. Where participation was denied the organisation was struck off the list of cases. If face to face interviews were not practical or there was reluctance to participate the organisations were sent an e-mail containing the hyperlink to the virtual interview site. In some cases (where requested) the survey instrument was sent to the participants in order to finalise their participation or to help prepare them for the interview.

#### **3.3.2 Conducting interviews**

At the scheduled interview times the interviews were recorded using either a tape recorder or a mini-disc recorder. Hand written notes were taken throughout the interviews. At the completion of the interviews, the interviewees were asked to complete the written questionnaires. In some instances the interviewees indicated that they needed additional time to 'properly' complete the questionnaire. In these cases the questionnaire was left with the organisation as well as the hyperlink for the online version of the questionnaire.

After the completion of the interview secondary data (both documents and observation) was collected. This included tours of organisational IT facilities and copies of documentation. Notes were taken throughout the interviews and a request was made to each interviewee to allow for follow up or questions of clarification at a later date.

The conduct of the virtual interviews followed the same process as for the face-to-face interviews. When participants arrived at the virtual interview site they were presented with information regarding the research subject and the researcher. Again, the confidentiality of participants was re-stated and then the interviewee was guided through the process. At the conclusion of the virtual interview the respondents were automatically guided to the online questionnaire. At the completion of both components of the online data collection the participants were thanked. As the online version of the interview protocol automatically compiled the interview transcript this transcript was sent to the interviewee and they were asked to verify it for accuracy.

### **3.3.3 Post interview procedures**

Following interviews all interviewees were sent an e-mail message thanking them for their time. Additionally, the e-mail contained a copy of the interview transcript, less any notes taken by the researcher during the interview. A copy of this e-mail is attached as appendix F. An example interview transcript is attached as appendix E.

### **3.3.4 Case study database**

To organise and sort the vast quantities of data collected from various sources a case study data base was created. A database is suggested for storage of data collected from case study research (Yin 1994). The database for this research comprised of manual and electronic information and was organised as follows:

- Web newsgroup postings from relevant Internet newsgroups were stored electronically in folders sorted by topic.
- Tape and mini-disc recorded interviews were transcribed, using the online interview tool and stored in electronic text files. Separate folders (directories) were created to compartmentalise the information from each organisation.
- Surveys completed manually were converted to electronic format using the online questionnaire tool and then stored electronically with the relevant interview transcript.
- Secondary data collected in hard copy format were stored in a filing cabinet.
- Recorded observations were filed manually under the appropriate organisation's name.

The case study database provided the source data for data analysis.

## **3.4 Data analysis**

This section describes firstly how the collected data were prepared, and secondly how the data were analysed. Data analysis is the process of examining, categorising and tabulating data, providing answers to the research question (Yin 1994).

### **3.4.1 Data Preparation**

Before data can be analysed, the data must be prepared for analysis, through the process of editing and coding (Zikmund 1997). The data collected by the in-depth interviews was converted to a common format using the virtual interview tool. Tape and mini-discs were translated into the tool in order to generate an accurate



transcript. Data from the survey instrument was converted, in the case of hand-written survey responses into electronic format by the online questionnaire.

### **In-depth interviews**

The in-depth interviews were designed to gain an understanding of IT security in the Australian business environment. The format of the interview transcript allowed for the automatic coding of the interview responses. With the assistance of academic staff a list of codes was established to enable interview responses to be meaningfully coded for analysis. The codes developed were divided into the following categories:

- Risks (Threat – T, Incident – I, Target – Tg, General Risk - R)
- Management (Countermeasures – C, Budget – B, General Management - M)
- Differentiator – D
- Unknown - ? (requiring further analysis or explanation)

To prepare the in-depth interview data for analysis, the tape recorded data was transcribed. The transcripts were then verified with the original tapes (or discs) for accuracy.

### **Structured written questionnaire**

The questionnaire was designed to triangulate and provide supplementary data to that collected through the interview process. Additionally, the questionnaire data provided a point of comparison to other research that was most quantitative in form. To prepare the attitudinal responses to questionnaire statements for analysis, scores shown in the table were assigned to the Likert scale response categories.

**Table 3-4 Likert scale conversion**

<b>Likert Scale</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Neutral</b>	<b>Disagree</b>	<b>Strongly Disagree</b>	<b>Not Applicable</b>
<b>Score</b>	1	2	3	4	5	6

*Source: Developed for this research*

### **3.4.2 Data analysis**

The data collected for this research was analysed to understand information security in the Australian Business context. To understand information security in Australia the in-depth interview data were analysed first within each case and second across all cases. When a multiple case study strategy is adopted for a research design, individual-case analysis should be done before cross-case analysis (Perry 1998; Yin 1994).

### **Within-case analysis**

Qualitative analysis techniques were used to analyse the data collected from in-depth interviews. Qualitative data analysis involves examining the data for consistent patterns and summarising these patterns in relation to the research problem (Yin 1994; Zikmund 1997). The information security issues in each case were described by reviewing the themes that emerged from the in-depth interviews and searching for patterns in relation to reliance on IT, threats and incidents, Australian businesses as targets, countermeasures, and levels of expenditure on information security. The within case analysis method is further detailed in Chapter 4.

### **Cross-case analysis**

In the cross-case analysis, data was analysed and insights gained in relation to each of the research issues. The intention of cross-case analysis is to generate insights, and not to prove anything or draw any generalisations (Yin 1994). The cross-case analysis method is further detailed in Chapter 4.

### **3.5 Summary**

This chapter described and justified the use of a multiple case study methodology for researching information security in the Australian Business context. Next, the research design was detailed. The content and design of the in-depth interviews, written questionnaires, online questionnaires, and virtual interviews were described along with the procedures for their implementation. Finally, an outline was provided of how the data were prepared for analysis and then analysed within each case and the across all cases. The next chapter presents the results of the data analysis.

## CHAPTER 4 - DATA ANALYSIS

Chapter 3 described and justified the case study methodology used to collect and analyse the case study data. This chapter presents themes and patterns that emerged from the analysis of the data collected.

The first two sections of this chapter provide fundamental background information on the ten case study organisations that participated in the research.

The next part of the chapter provides an overview of how the data were analysed in each case studied followed by the within case analysis for each organisation.

The chapter concludes with the cross-case analysis, which provides the major findings for each of the research issues across all ten cases.

### 4.1 Background Information on case studies

As discussed and justified in section 3.2.2 ten Australian organisations were selected as cases for this research. The organisations represent organisation drawn from New South Wales, the Australian Capital Territory, Queensland, and Victoria. The medium to larger organisations also had entities in the other states as well as some international interests. Maintaining the privacy of the organisations and individuals that participated in this research was an ethical consideration discussed in section 3.2.10, so to protect their interests organisations or individuals have not been identified and employee numbers have been rounded. Some detail has been omitted so that easy identification of the case participants could not be achieved. The subject matter was potentially sensitive and participants were at times reluctant to provide details for fear of exposing vulnerabilities. These fears were addressed by providing generic descriptions of the organisations and their lines of business. For analysis purposes, participating organisations are referred to as case A through to case J.

Table 4-1 provides basic information about these organisations including the type of organisation, company size, and the details of when the interviews were conducted. The table illustrates how the research methodology in regards to case selection was implemented.

**Table 4-1 Participating Organisations**

Case	Description	Company Size	Interview Period
A	Small wholesale business	Small	June 2002
B	Commonwealth Government agency – Defence Information Systems	Medium	February 2002
C	Commonwealth Government Agency – Defence	Large	February 2002
D	Resort Hospitality Company	Medium	July 2002
E	Software Company –	Large	March 2002

	Security		
F	Commonwealth Government Agency – Information	Medium	March 2002
G	Private Utility Company – Electricity	Medium	April 2002
H	Local Council	Medium	August 2002
I	State Government Department – Development	Medium	August 2002
J	State Government Department - Transport	Large	September 2002

*Source: Analysis of Secondary data and interview data*

The interview process was described in chapter 3 as part of the data collection methodology and included in-depth interviews, virtual interviews, review of secondary data, exit surveys, and personal observation.

Interviewees displayed a frank and forthright attitude in their responses to the interview questions, both in the face-to-face interviews and the virtual interview. As will be demonstrated their answers provided a wealth of valuable insights into information security in their organisations.

Table 4-2 presents a list of the IT professionals interviewed for each organisation as well as a generic position title that described the individual’s role within each case organisation.

**Table 4-2 IT Professional Interviewed**

Case	IT Professional
A	Support Services Administrator
B	Manager Information Systems
	Manager Corporate Services
C	Manager Corporate Technology
	Manager Information Security
D	Manager Infrastructure
	Manager Customer Services
E	Managing Director
F	Information Strategist
G	Chief Information Officer
	Information Security Manager
H	IT Manager
I	Director Information Systems
	Information Security Manager
J	Manager Information Technology
	Information Security Manager

*Source: Developed for this research*

## 4.2 Overview of within-case analysis method

This section provides an overview of the processes undertaken in each of the ten organisations to analyse their information security issues.

Data from semi-structured interviews were analysed to gain an understanding of the information security issues facing Australian organisations. The data were analysed by reviewing interview transcripts for themes and patterns related to the research framework present in chapter 2, section 2.4. These are:

- a. **Risk.** The three elements within the sphere of risk were defined as: reliance on IT, Information Security threats and information security incidents, and Australian businesses targets
- b. **Management.** The two elements within the management sphere were defined as: countermeasures and level of security expenditure.
- c. **Differentiators.** This section of each case attempts to identify any potential differentiators that may explain the organisation's security posture as indicated in the sections on risk and management. Examples could include size, nature of the company, and connectivity to the Internet. These differentiators may help explain why there are differences between how organisations approach information security issues. They could also assist in identifying the differences in the security environments in nations that have been the focus of the research highlighted in Chapter 2, e.g., the USA and the information security environment in Australia.

Throughout the analysis extracts from interviews are used to support findings and are referenced by the case, interview number and transcription line numbers. For example, 'They are not overly reliant on IT, the main focus is on MYOB and office automation' (A:1.30) is a quotation from case A, interview number one, transcript line 30. 'Investigations are conducted for serious activities in order to identify source and implement prevention' (C:1.172-173), is a quotation from case C, interview number 1, transcript lines 172-173. To further protect the privacy of the individuals, the interview numbers do not match the order the positions are listed in table 4-2.

The within-case analysis for each of the organisations is presented next in sections 4.3 to 4.12. This within-case analysis provides an information rich analysis of the information security issues with Australian organisations. This detailed analysis was used to prepare individual reports for each organisation on the information security issues affecting their organisation. Providing feedback to participating organisations was an ethical consideration of this research, as discussed in section 3.2.10.

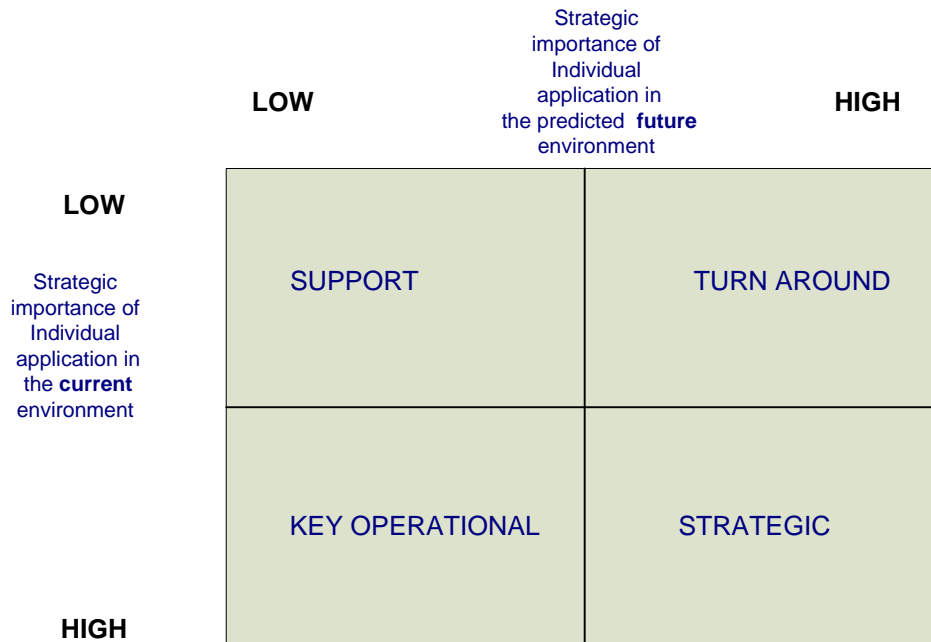
As part of the within case analysis a Strategic Grid was developed for each case in order to determine the strategic value of the IT for the case in terms of both the current systems and future developments (McFarlan, McKenny, and Pyburn 1983). The grid is demonstrated in Figure 4-1 below.

The following definitions provided for each classification:

- a. *Support role:* IT has little relevance to a firm's existing or future success.

- b. *Key operational role:* Current IT is important to the firm but future developments in IT are unlikely to improve the competitive advantage.
- c. *Strategic role:* Existing and future developments are critical to the firm's success.
- d. *Turn around:* Existing IT is unimportant but future developments are crucial to the firm's survival.

**Figure 4-1 Strategic Grid**



Source: McFarlan et al 1983

The final part of the within case analysis is the application of the information security assessment framework as defined in chapter 2. A table was created for each case listing the information security issues that each organisation faced. The assessment includes a subjective analysis (based on findings in chapter 2) as to whether the issue has a positive impact or a negative impact on the organisation's information security posture i.e. if the issue improves the posture a '+' is indicated in the table. If the issues expose the organisation to greater risk a '-' is recorded in the table.

### 4.3. Case A – Small wholesale food business

Case A is a small wholesale producer of food employing around 20 staff. They are located in the outskirts of a capital city. Their technology use could best be described as typical for a small business of this type and size (i.e. quite limited). Due to the small size and limited exploitation of technology within the organisation only one knowledgeable IT professional was available for interview.

In order to provide a more logical link to the literature, this the analysis also includes information on security deficiencies and gaps, e.g. the organisation did not have any

form of anti-viral protection in place. This appeared to be a significant shortfall in the organisation's security posture and pointed to a failure in the risk management process to identify the risk of virus incidents and the management process to implement measure despite known virus incidents.

### 4.3.1 Risks

#### Reliance on IT

Interview and observation data were analysed to gain an understanding of the reliance on IT within Case A. Overall the business reliance on IT could be considered as low.

*'They are not overly reliant on IT, the main focus is on the MYOB and office automation, there is some limited offline backup' (A:1.30-1).*

When posed the question of what would happen if the technology simply didn't work the response indicated the organisation would continue to be capable of undertaking its main function of producing food despite any technology setbacks.

*'If it didn't work, they have had problems in the past at the hardware level. It would delay the book keeping and cause some worries, but the product would still get sold' (A:1.33-5).*

The organisation appeared to use its IT (PC and servers) for the e-mail, running the business financials (MYOB accounting), access to the Internet file sharing – such as recipes and for office automation and the preparation and storage of business correspondence.

This response indicates that whilst technology clearly has a role to play in the business it is a background support tool rather than a business enabler. Due to the relatively small scale of the business and its perception of where technology fitted into the conduct of the business, security issues did not rate highly on their list of priorities.

Observational data further supported the assessment that Case A's reliance on IT was low. There were three PCs located at the company premises and one offsite – one of the PC doubled as a server. During the visit, the researcher observed that the PCs were not used by any of the employees as the staff were all involved in the production and dispatch of Case A's product. The survey instrument response also indicated the part-time nature of the IT support/security for the organisation. The staff member responsible for IT spent only 40% of his time providing IT support with the remainder being in direct support of the company's wholesale business.

The organisation's computers were networked in a rudimentary manner to allow for limited resource sharing. The ad hoc manner in which computers were used and managed within the organisation highlighted that technology was not seen as a business enabler.

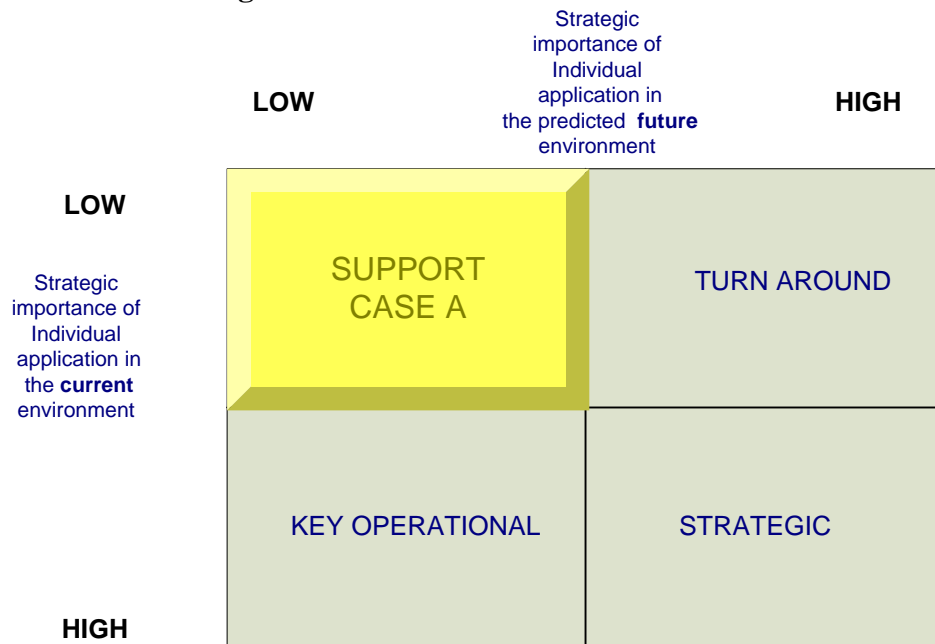
Whilst the technology is not directly related to the production of the organisation’s core product there is frequent use of the Internet.

*‘...(staff) use the Internet all the time’ (A:1. 55).*

Little of the organisation’s use of the Internet was described as being ‘business related’, although follow up questions indicated this to be the case – the organisation did not have a mechanism for logging employee Internet use. As the majority of Internet use is not business related – the organisation is potentially introducing an unnecessary risk to the organisation.

Figure 4-2 below depicts the application of the McFarlan and McKenny Strategic Grid (McFarlan et al 1983) to the organisation’s IT. Case A has been placed in the **support** category to reflect the fact that technology is used primarily for basic office automation and some limited book keeping roles – IT has little relevance to the organisation’s existing or future success. The organisations main product does not rely on technology for its creation.

**Figure 4-2 Case A Strategic Grid**



*Source: Analysis of interview and secondary data*

**Threats**

The strongest threats that emerged when identifying the threats faced by the organisation in Case A were hackers and viruses.

*‘Viruses are a big problem as they (staff) use the Internet all the time’ (A:1. 55).*



This statement highlights the fact that the virus issues faced by the organisation are related to the employee use of the Internet. After the hacker and virus threat the next greatest threat identified by the organisation was the systems internal users.

The staff member responsible for IT within Case A believed that the organisation was under threat from hackers.

*'They (employees) use the Internet all of the time. Hackers are a problem, because of the fact that the system is online 24x7. I have noticed that we have had hits almost daily. People trying to get in' (A:1. 55-7).*

The absence of a policy on Internet use in Case A resulted in a lack of control over the employees in this area. The organisation significantly increased the risk of a security related incident due to the absence of measures to inform and control staff access to the Internet.

The hacker threat was considered to be the most significant security threat that the organisation faced.

*'Probably hackers (are the most significant). If they did something to our data that would cause a big problem' (A:1. 70-1).*

The respondent in Case A indicated that the organisation had learnt about the threats the organisation faced through experience.

*'I know the threat through experience, having contact within the hacking community, plus consistent research on the net. What you do is see where the script kiddies are going, what they are doing and making sure that your system is patched appropriately' (A:1. 82-5).*

There was no evidence of a formal or informal risk management assessment.

## **Incidents**

The organisation studied in Case A had suffered from a number of computer related security incidents that had been detected and had had an impact of the way the organisation used their IT.

*'We run server logs that record attacks. They are constant, sometimes we have 50 – 60 attempts (per day) to get through' (A:1. 117-8).*

Virus incidents have also been recorded by the organisation.

*'We have also had viruses uploaded, with 15 viruses getting through. This has been due to the lack of updating virus patches' (A:1.120 – 1).*

This statement demonstrated an understanding of the cause and effect nature of managing a security environment. The organisation had not managed its system updates and security patches and the result was increased incidents of virus attacks.

The lack of a virus policy and perhaps just as importantly the lack of proper position descriptions meant that responsibility for these tasks was not clear.

The company had not noted any other type of security incident. When asked which type of incident was most prevalent the response was:

*'The most prevalent were the probes that are logged by the firewalls and then viruses' (A:1. 131).*

The organisation found it difficult to quantify the costs of any losses that had resulted from the observed incidents.

*'We have lost data because of the viruses in MYOB. They lost three weeks worth of work that had to be re-entered into the computer. It's hard to estimate (costs), basically the costs of re-entering the data' (A:1. 137-41).*

### **The business as a target**

There was clear evidence that the business was a target of information security incidents. The organisation put its 'status' as a target into the following perspective:

*'We are a target because we use servers that are connected to the Internet, but I don't believe we would be a target for a controlled attack, (we are a target) mainly because it is there. If they have the opportunity to do it. Not many people would care about our financial position' (A:1.91-5).*

The lack of a robust risk assessment process within the organisation has led to a number of threats not being recognised by the organisation. The organisation has left itself open to attack because it has not assessed the risks. Even in a small organisation such as Case A a risk assessment would have revealed the virus threat, the evidence for which would be the number of actual recorded incidents. This in turn would have pointed the organisation in the direction of where it should best devote its limited resources in order to manage the risks more effectively.

## **4.3.2 Management**

### **Countermeasures**

The organisation had a variety of countermeasures that it employed to address the threat and reduce the number of security incidents that it encountered. The company used a firewall to help protect its systems from Internet risks and had procedures (informal – not documented) to restrict access through the firewall device.

*'The server is locked down pretty tight, and so is the firewall. Only two ports are open' (A:1.170-1).*

The company also had rules that limited users' ability to install software on company systems, in particular software that may pose security problems for the company.

*'(We have) processes and procedures that don't allow users to install software such as ICQ. I then go around and make sure that this is the case.'* (A:1.173-4).

The respondent made an interesting observation that seemed to be relevant to small businesses in relation to setting rules for computing systems.

*'It's hard to tell the owners of the company not to do certain things on their own computers'* (A:1:176).

The senior management of the organisation therefore seemed to lack awareness of the potential security issues that the organisation faced. Whilst the organisation used a number of anti-viral products they were not used to their full potential by, for example, enabling features such as disk scanning.

The lack of documented security policies resulted in an uncoordinated attempt to manage the organisation's security environment. The organisation knew it should employ countermeasures but did not effectively manage the implementation or on-going maintenance of those countermeasures.

#### **Level of security expenditure**

As might be expected for a company of its size and business type, Case A did not have a large security budget. All countermeasures used existing hardware and freeware software wherever possible.

*'We spend hardly anything, we use free stuff if possible such as zoneAlarm, a free Unix firewall in an attempt to minimise cost. We do pay for our anti-virus software'* (A:1.183 – 6).

It is reasonable to expect that the organisation had little capital to invest into information security. What little funds were available were, however, allocated in a random fashion.

#### **4.3.3 Differentiators**

The data collected through the interview process, observational data, and the exit survey revealed a number of potential differentiators regarding information security within Case A. The table identifies two potentially inconsistent issues. Firstly, the nature of the business indicates that as a small wholesale producer they are not highly reliant on IT, yet they have (an unexplained) high use of the Internet. Accordingly, and they use most of their security efforts in protecting themselves from Internet based threats. The differentiators are listed in the table below.

**Table 4-3 Differentiators Case A**

<b>Differentiator Number</b>	<b>Differentiator</b>	<b>Comments</b>
1	Nature of the business	Case A was a small wholesale business that was not overly reliant on IT. This lack of reliance reduced the technology 'footprint' and reduced the significance and importance of security incidents.
2	Size	The size of the company impacted the amount of IT used, the amount of IT staff and amount of money spent on IT and IT security.
3	Role of security professional	Security was seen as a minor function of the person responsible for managing the businesses IT. It was not a stated role; it was done because the individual considered it important.
4	Use of the Internet	The company's use of the Internet largely dictated its security response and the threat that it faced. Much of the security focus was aimed at protecting the business from the Internet.

*Source: Analysis of secondary data and interview data*

#### **4.3.4 Case A – Security assessment framework**

Using the framework defined and developed in chapter 2, this study's assessment of the information security position for Case A is shown in the diagram below. The framework indicates that there are more negatives than positives. There a number of areas that require attention in order to appropriately manage information security issues.

**Table 4-4 Information Security framework Case A**

Risk						Management					
Research Issue 1 Reliance on IT		Research Issue 2				Research Issue 3 Australian Business as Targets		Research Issue 4 Countermeasures		Research Issue 5 Level of Security Expenditure	
		Threats		Incidents							
Office Automation.	-	No formal risk assessment.	-	Port Scans.	-	Small business seen as a target of opportunity only.	+	Freeware tools.	-	No security budget.	-
MYOB financials.	-	Viruses.	-	Viruses.	-			Anti-viral.	+		
Business self assessment – low.	+	Hackers.	-	System privilege abuse.	-			Software firewall.	+		
		Port Scans.	-								
		System Users.	-								

(+) Factor has a positive impact on the organisation's security posture

(-) Factor has a negative impact on the organisation's security posture

Source: Analysis of secondary and interview data

#### 4.3.5 Summary and recommendations

The organisation's security posture suffered from the lack of alignment between the risks and the management of those risks. The absence of information security policies, which are subsequently implemented by technology, resulted in the organisation suffering from excessive security incidents. The failure to conduct a risk assessment exercise resulted in an uncoordinated and less than effective implementation of countermeasures.

If Internet usage is business related then processes need to be implemented to mitigate the Internet based risks.

The following recommendations are based on a comparison of the analysis of the current state of security in Case A with best practice as uncovered by the literature review (see chapter 2). If implemented the recommendations should significantly improve the organisation's security position:

- a. **Risk assessment.** The organisation should undertake a risk assessment to determine what threats they face and what vulnerabilities their systems have. Given the size of the organisation and its limited budget this assessment need not be overly complex or lengthy.
- b. **Internet use.** The organisation must establish guidelines for Internet usage.
- c. **Policies.** The organisation should establish policies regarding use of information systems and how security will be implemented.
- d. **Position descriptions.** The organisation would benefit greatly from written position descriptions that make it clear who is responsible for various security functions.
- e. **Anti-virus countermeasures.** The organisation should further exploit the capabilities of anti-viral software, in particular automated updates of software patches.
- f. **Management awareness.** The correlation between threats and incidents should be made known to management in order to provide the business case for implementing more robust management methods.

#### 4.4 Case B – Commonwealth Government agency

Case B is a medium sized Commonwealth Government agency employing around 2500 staff. They are located in all states of Australia in varying sized branch offices, with the major concentration of staff being located in a single capital city. The organisation's prime responsibility was the provision of information architecture and infrastructure to support a larger government department.

The use of information is very important to Case B and as a result they use IT in a variety of ways in order to enable their core business to take place. Two senior IT professionals were chosen by the organisation to take part in the interviews.

#### 4.4.1 Risks

##### Reliance on IT

Interview and observational data were used to gain an understanding of the reliance on IT within Case B. At the time of the organisational visits it was clear to the researcher that Case B could best be described as being highly reliant on IT. All employees had a computer on their desks and they used them consistently in the conduct of their routine tasks.

*'We are totally reliant on IT. This has progressed in the last 10-15 years from very little or no reliance on IT, and lagging behind most of industry to actually leading industry in our use of IT, especially in regards to reliance' (B:1.21-4).*

The organisation used the Ethernet protocol for LAN connectivity and IP for WAN connectivity. Client/Server technology dominated, however, there were some instances of thin client implementation. Specialist application servers were maintained for specialist applications and for e-enabled services such as Intranet and Internet systems.

There were limited specialised network management tools or applications as the organisation tended to adopt 'vanilla' Microsoft software platforms. This was somewhat of an issue for the technical team within the organisation as they had recently changed network operating systems from Novell 5.0 to Windows NT Server.

The researcher's impression was that the technical support team were appropriately trained and experienced to provide a high level of technical support to the organisation.

The organisation's reliance on IT was increasing, highlighting that the organisation was, at one stage not very reliant on IT. However, this had changed over time.

*'In the past, say four years ago it was mainly just administration, a bit of e-mail here and there. Not many users. Now it is becoming a fully operational network, an integrated network, a network that people rely on. They are heavily reliant' (B:2.21-4).*

Intranet and Internet based activities are a key business requirement within the organisation, with a high reliance on Internet based technology (web browsers) and documents that reside on the Intranet or the Internet.

*'We use a whole of enterprise Intranet, connected by a corporate WAN' (B:2.37).*

*'There are Intranet users for local branch information and for corporate wide issues such as policies and procedures, globally around the organisation' (B:1.27-8).*

Whilst not specifically mentioned by the interview respondents it could be expected that the organisations reliance on interdependent systems would create broader information assurance issues. Data integrity becomes significantly more complex when remote updates of databases become an organisational imperative.

The IT within Case B is used for a wide variety of functions.

*'Pay, leave, logistics functions all happen on our networks. Asset management, personnel management, they are centrally located in data centres, so it happens over the wire' (B:2.50-2).*

*'Things like finance, pay is all done through IT based programs. They are many and quite varied' (B:1.36-7).*

Internet access and general connectivity to the outside world is also considered important to the organisation.

*'There is obviously Internet access, which is needed because we are so diverse in the things we do. The Internet is surfed like it would be in any large organisation and because of the business that we do. So the organisation is also reliant on our connectivity to the Internet' (B:1.30-3).*

One of the best indicators of how reliant an organisation is on its IT is to look at what happens when the IT doesn't function.

*'IT enhances the way we do business; if we don't have it we don't work. It is just as bad as if the power goes off, you can't do anything. We also do things like VoIP (Voice over IP), so if the networks go down we lose our phones also, so we are totally stuffed, So you can't call people when you have a problem either' (B:2.54-8).*

The other interviewee had a slightly different slant on the issue.

*'When IT doesn't work, well you can't say that the organisation stops, but a lot of administration stops' (B:1.43-4).*

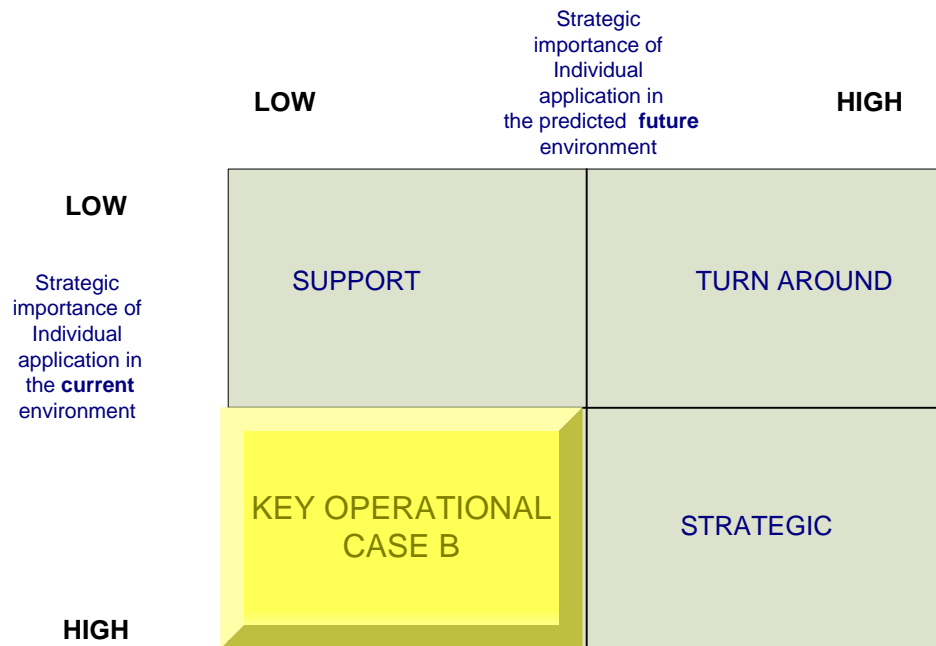
This last statement indicates that there may be room for improvement in the organisation's Business Continuity Plan (BCP).

The survey responses from the organisation strongly supported what the interviewees reported verbally; the organisation used IT as a business enabler.

Figure 4-3 below depicts the application of the McFarlan and McKenny Strategic Grid (McFarlan et al 1983) to the organisation's IT. In this case the organisation has been assessed as being in the **key operational** quadrant because IT was seen as an enabler to the business and was employed in a wide variety of applications – current IT is important to the firm but future developments in IT are unlikely to the competitive advantage.



**Figure 4-3 Case B Strategic Grid**



Source: Analysis of interview and secondary data

**Threats**

Perhaps the strongest theme discovered in the analysis of the interview data from this case was the wide variety of threats that the organisation faced.

*‘Hackers, organised groups of hackers, internal disgruntled systems users, and foreign governments are all potential threats to our systems’ (B:1.84-5).*

Contrary to findings reported in the literature, the organisation did not list ex-employees as a potential threat. A review of secondary data provided a possible explanation. It uncovered a number of procedures that involved deactivation of user accounts and verbal de-briefs from security officials regarding non-disclosure of sensitive information.

Viruses were seen as a problem for the organisation although the respondents were quick to point out that they had taken a number of steps to reduce the virus threat.

*‘The biggest threat that we have at the moment is viruses coming through the firewall, people’s e-mail mainly’ (B:2.79-80).*

*‘Viruses are probably as big a threat as they were. We do get viruses that give port 80 a hammering. That has the potential to give us a hard time. Anything that will attack an IIS server is particularly critical for us at the moment’ (B:1.93-6).*

The organisation believed that they faced a hacking threat not only because of who they were and what they did but also because of their relationship with other organisations.

*'People trying to hack in. It could be individuals it could be very hard to tell. The only time you know is if you catch what they are doing. So its definitely a threat because we have relationships with other companies, governments and organisations. It may be that those are not popular and people may attack us because of that relationship' (B:2.96-102).*

The IT within the Case operated in an encapsulated or segregated manner. For example, the organisation's more sensitive information often resided in separate computing domains. This design strategy was a clear attempt to reduce the threat to the more sensitive information; however, there were still threats that could impact upon that sensitive information.

*'We have people transferring data from one segregated network to another. From a highly sensitive system to a network designed for public information. So we have to look at issues like information sanitisation. This is to prevent the systems users stuffing up and degrading the security of the network' (B:2.80-5).*

The respondents differed in their views as to what was the most significant threat that the organisation faced.

*'The internal threat is the most significant. We have a vast organisation, although access is now tighter than in the past' (B:1.104-5).*

*'Viruses are the most significant threat. They do the most damage and are the most damming. They are the most prolific, because we are on NT. That's one of the reasons why we went to Lotus Notes rather than Outlook and Exchange' (B:2.127-9).*

Analysis of the survey responses would seem to indicate a linkage between the internal threat and the virus threat, i.e. the actions of the users increase the risk of viruses.

Both interviewees indicated that their on the job experience was how they learnt about the threats their organisation faced.

*'Experience based on my previous roles in this organisation and in others. We talk quite frequently to the security people (hands on practioners), we spend time with the staff and look at the issues that they are facing. I read a lot of the information put out about the risks' (B:2.139-43).*

This last statement highlights that the organisation had not put a lot of emphasis on hiring staff with credentials in this area. The researcher believed that this was due to

the changing focus of the organisation and the need to keep staff employed. Staff were shifted from areas of lower demand to new areas often with little training or experience in those new areas.

### **Incidents**

The organisation in Case B had suffered from a number of differing information security incidents ranging from virus attacks to instances of internal systems user access abuse.

*'We had a user who thought he had administrator capabilities when in actual fact he had access to a number of Lotus Notes ID files for the e-mail. He had access to every e-mail in the company right from the CEO to the lowest level. It included information that was commercial-in-confidence. There was enough information to know the business of 2500 people' (B:1.104-15).*

This incident was an example of poor internal security that was exploited by a system user for their own purposes.

Earlier viruses were identified as a significant threat to the organisation so it was not surprising that the organisation had encountered virus related incidents.

*'The modified Nimda virus was one issue. All of the IIS servers were turned off, we had to disable port 80. It shut everything down, we basically had to shut down the entire Intranet, and we couldn't get through to the Internet. All of which cut down access to a lot of work productivity tools' (B:2.193-6).*

The organisation also suffered from spamming or e-mail misuse incidents.

*'Another big one that is causing us a lot of grief at the moment is people spamming. Chain e-mails, pyramid letters, "you've got to send this on to 10 people otherwise you will suffer bad luck – your dog will die' (B:2.209–12).*

An interesting variation of the spamming incidents was an e-mail that prayed upon virus fears.

*'The classic is the virus alert (e-mail) where people are told to send the alert (e-mail) to everyone in their address book and if you have 2500 people in your organisation and all of them send it to all of the other people there is going to be a lot of e-mail traffic and things will stop pretty quickly' (B:2.215-8).*

The organisation had also been the victim of a number of incidents where external contractors who had been granted temporary access to the company's systems had abused that privilege.

*'Contractors are forever trying to get inside knowledge of the company's future needs and directions. So there is potential for information to be leaked to other organisations and the media' (B:1.192-8).*

The Case B organisation had recent experience with theft and loss of its computing equipment in the months leading up to the interviews.

*'Theft of laptops is a big issue. We normally contact the Police. A dedicated asset manager has been appointed to check on this and laptop hard drives are now encrypted. We have a lot of stuff stolen or misplaced' (B:2.234-6)*

Whilst hackers were mentioned as a potential threat there did not appear to be a great deal of hacker activity against the organisation.

*'There is nothing specific from the hackers that I can recall recently' (B:2.232).*

The survey responses indicated only 'routine' port scanning and no hacker incidents. The two interview respondents differed in their view of which type of incident was the most significant or the most prevalent.

*'The viruses are the most prevalent. The Nimda viruses' (B:2.247).*

*'The most significant is employee access abuse, the most prevalent is systems users having inappropriate access to information' (B:214-6).*

Reviews of the survey responses indicated that viruses were certainly the most prevalent in terms of the number of incidents encountered. Both interviewees indicated that the organisation had suffered monetary losses as a result of information security incidents and tended to believe that the losses were hard to quantify.

*'No not really (couldn't estimate a value of losses), it would be pretty huge. Mainly in lost time, a five minute outage has to be multiplied out by the amount of users that are impacted' (B:2.254-5).*

Whilst the organisation appeared to have comprehensive policies and procedures the number and nature of the incidents indicates that many of these policies are not being followed and there are control issues.

### **The business as a target**

The interview responses and the survey responses indicated that the organisation was a target for individuals and groups.

*'There is a foreign government threat because of who we are and what we do and who we share information with. There is a real*

*espionage threat and an information warfare threat. We could and would be a threat in that area' (B:1.147-51).*

*'(We are targeted) because of the nature of what we do. Especially from foreign nationals, issue motivated groups also. Because we have relationships with some bigger international organisations some may see us as an easier target to get information about those bigger organisations. If they couldn't get it from them they would try us. We are seen as a softer target, because of our association with our business partners we could be seen as a backdoor into their networks or information' (B:2.150-5).*

Whilst the organisation had detailed a number of threats and re-counted a number of security incidents they did not correlate the incidents with the fact they believed they were a target. They believed that foreign governments were a potential security threat, however, they did not know how many (if any) of their incidents could potentially be linked to the foreign government threat.

#### **4.4.2 Management**

##### **Countermeasures**

The organisation employed a variety of countermeasures to protect their IT and information from information security incidents. These countermeasures include policy and procedures as well as technology based solutions. Of these, the policies and procedure aspect of the countermeasures were seen as being the vital underpinning factor to the organisation's security posture.

*'We have organisational wide information systems security practices and procedures. They are about 12 – 18 months old. They are signed off by me as the system manager and then the regional manager for each site' (B:2.282-4).*

*'There is a generic set of procedures that will go to all levels with an overview from the top and go down to the lowest level, so that any local branch procedures can be dovetailed into the procedures and can be monitored and controlled from the highest level' (B:1.254-7).*

The organisation's use of security technology focused on the use of firewalls and anti-viral software.

*'Firewalls are central (to our security posture)' (B:2.296).*

*'The organisation uses firewalls' (B:1.273).*

The secondary data presented by the organisation showed extensive use of anti-viral products throughout the organisation. Daily updates of anti-viral patches were conducted through the system log-on process. This provided an effective manner of controlling and managing the process. The organisation had identified that this was

an important function that could easily be missed by an individual so they invested in an automated solution.

Controlling system access was also an important factor for the organisation. Whilst system access was defined and regulated by system policies and procedures, the interviewees strongly emphasised that management of system access was a key countermeasure in itself.

*'Everyone who wants access to our systems must read our policies so they are aware of the security implications of their actions and what is required of them' (B:2.288-93).*

The survey and secondary data collected illustrated that the organisation had developed and implemented Disaster Recovery Plans (DRP) and Business Continuity Planning (BCP), however, the interviewees indicated that more work was required in this area.

*'We have a DRP but in the past they haven't been very successful. We are re-writing it to improve the survivability' (B:2.303-4).*

*'Disaster recovery plans, capacity and continuity plans exist. Most of the independent area used to do their own thing, only when pain was felt did they do any planning' (B:1.268-70).*

The organisation did have a reasonable degree of correlation between their assessed threats and the countermeasures they employed, however, there seemed to be a lack of formal risk assessment at the start of the security process which detracted from the overall integration of the security picture. The organisation appeared to be doing the right thing in many aspects of their security landscape, however, there appeared to be a lack of organisational acknowledgement on the real significance of information security to the organisation.

### **Level of security expenditure**

There was a 100% variation in the amount of money claimed to be spent by the organisation on Information Security.

*'There is the cost of staff, which I think is four, cost of the firewalls, software and the production of the procedures. The organisation does keep its steps quite, we would spend about \$1 million per year' (B:1.280-3).*

This differs from the other response.

*'In the last year we have spent about \$500K on a security system. The normal budget is about \$2 million per year, which includes funds for firewalls. Standards, audits, staff and the like' (B:2.320-1).*

The reason for the difference in response was not made clear to the researcher. It was probably due to differences in what was considered to be included under

‘information security’. It did, however, potentially point to the fact that the organisation and also potentially the respondents did not understand information security as well as they perhaps should. It could also illustrate that higher IT management may not have an intimate day to day knowledge of information security issues.

#### 4.4.3 Differentiators

A number of potential differentiators were uncovered during the study of the Case B organisation that may have an impact on the organisation’s security posture. These differentiators are listed and described in the table below:

**Table 4-5 Differentiators Case B**

Differentiator Number	Differentiator	Comments
1	Dispersed nature of the business	Case B had a number of different branch offices that were in different states requiring the use of inter-connected networks. This adds additional complications to security solutions.
2	Size and structure	The size of the company impacted the amount of IT used, the amount of IT staff and amount of money spent on IT and IT security. As a bigger organisation they have been seen as a high pay-off security target. The organisation’s hierarchical structure made it easier to pass on instructions on policies and procedures
3	Value of organisational information.	Information was a key resource and at times the information needed to be kept away from public viewing. This information could be specifically targeted. Thus the organisation was more likely to face dedicated attacks rather than attacks of opportunity.
4	Reliance on the Internet	The company was heavily reliant on the Internet, which dictated that they needed to have an available connection to the outside world rather than having a closed and more secure network: the security versus functionality trade off.
5	Reliance on IT	The organisation was heavily reliant on IT and as such needed to take extra measures to ensure the continued operation of their systems.
6	Relationships with other organisations or companies.	The organisation faced additional threats because they dealt with other organisations that were likely targets for security related attacks. The Case B organisation had to strengthen its security posture because of this.
7	Lack of information security	The organisation did not appear to

	vision	make information security a priority issue for the organisation. There was no mention for example that security was included as part of the corporate planning function.
8	Lack of contingency planning	If the systems are organisational administration is stopped.

*Source: Developed for this research*

#### **4.4.4 Security Framework**

Using the framework defined and developed in chapter 2, this study's assessment of the information security position for Case B is shown in the diagram below. The table illustrates that because of the organisation's reliance on IT they are more likely to be impacted negatively from the loss of their systems. The left hand side of the table summarises the risks to the organisation. The right hand side of the table highlights the organisation's efforts to balance or mitigate those risks with the appropriate countermeasures and management practices. The summary and recommendations that follow the table offer suggestions on how the organisation's security posture can be improved.



**Table 4-6 Information security framework Case B**

Research Issue 1 Reliance on IT		Risk				Management				
		Research Issue 2		Research Issue 3		Research Issue 4		Research Issue 5		
		Threats	Incidents	Australian Business as Targets		Countermeasures		Level of Security Expenditure		
Office Automation.	-	Formal risk assessment.	+ System privilege abuse.	-	The organisation believed that they were a significant potential target due to the nature of the work that they do.	-	Well defined and enforced system security policy.	+	Significant security budget with some linkage to threats.	+
Payroll processing.	-	Hackers.	- Significant virus incidents.	-	International and national organisations could have Case B as a target.	-	Procedures and work instructions on the use of IT.	+		
Corporate wide intranet.	-	Organised groups of hackers.	- Chain e-mails (SPAM).	-	Issues motivated groups could also have the organisation as a target.	-	Anti-viral software with automated updates of virus definition files.	+		
Document management.	-	Foreign governments.	- Contractors abusing access privileges.	-			High-end hardware based firewall products that meet national certification standards.	+		
Integration of telephone systems.	-	Viruses.	- Laptop thefts (numerous).	-			System access controls.	+		
Logistics tracking.	-	System users (internal threat).	- 'Routine' port scanning.	-			Capacity planning.	+		
Self assessed as very high reliance on IT	-						Disaster Recovery plans.	+		

(+) Factor has a positive impact on the organisation's security posture

(-) Factor has a negative impact on the organisation's security posture

Source: Analysis of secondary and interview data

#### 4.4.5 Summary and recommendations

The organisation presented a picture of a reasonable robust security environment. The organisation had developed a series of comprehensive security policies and had implemented these policies with a number of supporting technologies. There was, however, a lack of formal risk assessment in regards to the threats and how these threats could be best managed. A lack of integration with overall corporate planning indicated that the organisation did not place a great deal of emphasis on information security.

The following recommendations are based on a comparison of the analysis of the current state of security in Case B with best practice as uncovered by the literature review (see chapter 2). If implemented the recommendations should significantly improve the organisation's security position:

- a. **Risk assessment.** Implement a formal risk assessment regime to clearly identify the risks and threats that the organisation faces.
- b. **Corporate planning.** Integrate information security planning with the corporate planning process in order to improve the visibility of information security issues.
- c. **Contingency planning.** Review and revise the DRP and BCP to enable work to go on in the event of system failures.
- d. **Expertise.** The organisation should consider hiring security experts in order to coordinate the information security process more effectively.

#### 4.5 Case C – Large Commonwealth agency

Case C is a large Commonwealth Government agency with approximately 60 000 staff. They are located in every state of Australia and also in a variety of overseas locations. As with the previous case the use of information in Case C was deemed to be extremely important. IT and communications technology are important in the conduct of day-to-day business within the organisation. Two senior IT professionals took part in the interviews. One represented the general management structure of IT, whilst the other was responsible for the management of the organisation's large Information Security Division.

The description of the organisation has been reduced to avoid making it obvious just which Commonwealth agency is involved.

##### 4.5.1 Risks

###### Reliance on IT

Interview, observational, survey, and secondary data analysis were reviewed in order to gain an understanding of Case C's reliance on IT. Case C could be best characterised as highly reliant on IT.

*'We are totally reliant on IT for administrative support and highly reliant for operational activities. The use of the Internet for e-*

*Commerce is driving the rest of the organisation to follow suit' (C:1.20-2).*

*'The organisation is totally reliant these days on technology. In particular the e-mail component as well as for the storage component and the distribution of information either through e-mails or the Intranet that the organisation uses' (C:2.20-2).*

Web based technologies offered important functionality to the business and this Intranet capability also offered Internet access.

*'The Intranet is a key component of the work place. People are publishing things on it in order to make things happen in their work place. Very little is published these days in hard copy' (C:2.32-4).*

*'Most of our work is done on our Intranet and that has external Internet connectivity (C:1.24).*

Whilst there was little doubt that the information and its supporting infrastructure was important to the organisation there was no mention of contingency planning. IT is clearly a business-enabling tool with the IT underpinning many work functions.

*'The infrastructure supports applications that manage personnel within the organisation so that people can be paid, take leave, and have their work competencies managed. Financial management and management information systems are also important. There are a lot of applications that are embedded into our infrastructure' (C:2.38-41).*

There are 60 000 IT users within the organisation which speaks volumes in itself for the vastness of the IT in the organisation. In general, it is reasonable to assume that the larger the infrastructure the more complicated the security environment becomes, particularly in regards to the cohabitation of various independent applications with multiple access control mechanisms. The organisation faced the very real problem of users having to remember multiple passwords to gain access to diverse systems.

The potential non-availability of systems can have serious consequences for the normal workflow of the organisation.

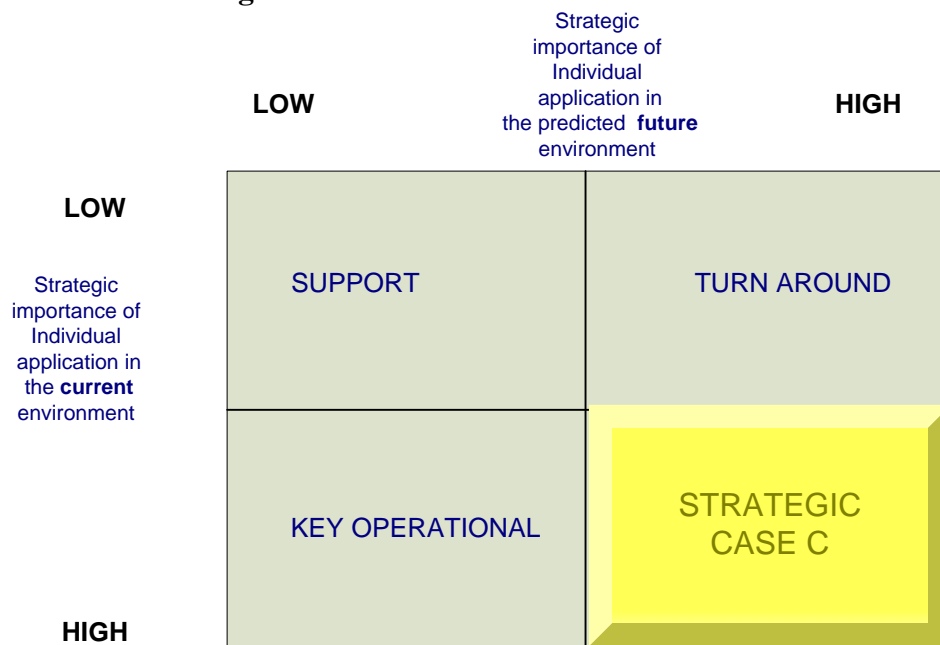
*'When things don't work we get situations where people actually go home. Which is an interesting situation. When we have a major failure people will pack up and go home even in the middle of the day' (C:2.43-5).*

The survey responses supported the statements made by the interview participants in relation to the organisation's reliance on IT. Furthermore, an analysis of other documentary evidence, such as systems security manuals highlighted not only the importance of the systems; (e.g. 'critical technology and infrastructure'), but also the importance of the information that was processed on those systems. This highlighted the interdependence of information and IT.

Ensuring that staff understood their security responsibilities and what they could and could not do on systems was far more complicated than simply producing a manual and requiring staff to read the manual. Compliance and comprehension were very real issues for this organisation.

Figure 4-4 below depicts the application of the McFarlan and McKenny Strategic Grid (McFarlan et al 1983) to the organisation’s IT. Due to the existing and future developments of IT being critical to the organisation’s continued successful operation IT was seen as being *strategically* important to the organisation.

**Figure 4-4 Case C Strategic Grid**



Source: Analysis of interview and secondary data

**Threats**

The organisation at Case C identified a number of key threats that their organisation faced. Of particular note, however was the manner in which the organisation expressed the interdependency of the threats upon each other. There was a strong belief within the organisation that the vast majority of their threats could be attributed to the actions of systems users.

*‘The highest threat is due to complacency, i.e. users not following security guidelines that have been implemented. Breaching Information Systems Security Practices and Procedures, connecting unauthorised machines to the network that have been compromised or are infected with a virus’ (C:1.62-4).*

The other interviewee related the system user threat to the information processed on the systems.

*'In this environment the threats are people getting access to information that they have no need to access for the conduct of their job. They could gather that information internally and then use it for an external purpose' (C:2.68-70).*

Viruses were listed as a problem for the organisation, however, they too were related to the actions of individual staff members.

*'Know viruses are not a problem if security procedures are followed – all problems experienced by the organisation are a result of someone not following the rules; an administrator fails to do a patch' (C:1.62-5).*

*'The organisation detects 3-4000 virus attacks each week through e-mail alone' (C:2.77-8).*

The Case C interviewees explained that there was a good reason why they considered the internal threat (system users) to be greater than the external threat. They proposed that because of their highly robust security systems it was highly unlikely that an external attack would be successful.

*'Security controls limit the potential impact of external agencies. The main type of attack they could attempt would be a Distributed Denial of Service (DDOS) attack which would simply result in the organisation disconnecting from the Internet' (C:1.69-71).*

*'I think that we have a very secure network. I think that the more secure the network the more unlikely that outsiders will get in and therefore the insider threat is seen as a bigger issue' (C:2.103-5).*

The organisation was able to make good use of the international dateline to protect the organisation from viruses.

*'An unknown virus that propagates rapidly during working hours could be a risk but it is extremely unlikely due to the time difference between Australia and the United States' (C:1.67-9).*

This statement expresses the organisation's belief that generally speaking viruses tended to be released in North America first, which typically gave this Australian organisation an early indicator of potential trouble looming on the horizon.

The hacker threat was played down by the organisation.

*'There is a hacker threat to the organisation. I don't know of any attacks that have come to fruition. I don't have any figures for hacker attacks but I'm sure that they do occur' (C:2.81-3).*

The interview respondents indicated that they were made aware of the information security threat from a variety sources.

*'Experience, study, research, conferences and advice from experts in the field are all used to keep me up to date' (C:1.81-2).*

*'Through study and through management reports that are generated each month that list the threats and changes to the environment' (C:2.116-7).*

## **Incidents**

Due to the size and profile of the organisation it was not surprising to learn that the organisation had experienced the full gamut of security related incidents.

*'Hacking discovered within the organisation tends to be people "playing" and not understanding the ramifications i.e. launching a ping of death against the firewall – discovered in time and security measures implemented so that can no longer occur' (C:1.116-8).*

In this case the organisation further restricted staff's use of their desktops. Staff could not save executable files on their PC. Additionally, Internet downloads were further restricted to stop all staff from being able to download files. These incidents prompted changes to policy and management measures.

The organisation suffered from a huge number of detected viruses.

*'We detect and destroy about 3-4000 viruses per week delivered mainly through e-mail' (C:2.168).*

*'Some viruses are connected to some unauthorised connections to the network. Launching executable e-mail attachments from someone you don't know, and even sending some hoax virus warnings' (C:1.119-20).*

There had been a number of cases of employee access abuses recorded by the organisation. A number of the more significant incidents had been perpetrated by trusted system administrators.

*'We had a situation where a network administrator accessed information that he shouldn't have by abusing his administrator's privileges. That was detected in an employment interview. After asking two questions we knew the person had had access to the questions as well as looking for key points in the answers and that was verified through the remainder of the interview. We ended up putting a dummy document on the system to catch him out and get around it' (C:2.162-7).*

This incident implies that there is a potential lack of auditing and supervision of staff with high degrees of access to resources with the IT environment. There appeared to be a lack of policy and perhaps acknowledgement that this type of event was

possible. The interviewer for example could have kept this information in a less obvious place to avoid temptation or installed auditing and tracking procedures to track the culprit.

*'Unauthorised access has included housing of movies including porn on a server which can only be accessed by a system administrator or one of their friends. They have also allowed access to systems by contractors who have not been granted permission to use these systems' (C:1.121-3).*

In this incident the system administrators were abusing their access to system resources to store data that was prohibited in accordance with system policies. The system administrators in question further abused their authority by granting permission to the contraband data to their personal friends.

These two incidents highlight that system administrators are in positions of extreme trust and in some cases they abuse that trust. Organisations such as the Case C organisation are faced with the dilemma that it could be impractical to deny administrators access to data that they may have no right to view. The more practical solution may be to increase the rigour of the personnel selection process to reduce the risk of organisations hiring less than trust worthy staff. This practice could then be monitoring and audited.

Theft of computing assets, in particular laptops, was also encountered by the organisation.

*'We have instances of people stealing laptops with information on them. It does happen in this organisation. A small amount per year' (C:2.170-1).*

*'Laptops disappear all the time. When machines were upgraded the RAM was stolen and replaced with less capable RAM' (C:1.125-6).*

At the time of the interview the organisation had yet to devise a strategy or policy that could be subsequently implemented as a countermeasure to adequately deal with the theft of hardware and software assets.

The organisation considered that the highest risk or most significant type of incidents involved system users.

*'Employee access to information is the highest, abuse of privileges, people using information that is available – leaking of information' (C:2.179-80).*

*'Data destruction can be significant, but controls should reduce the damage any one individual can do – highest risk is leak incidents – the negative press causes damage to the organisation and causes a lot more in the subsequent "damage control". Access abuse is the most prevalent, i.e. non-work related activity or activity which if discovered*

*could damage the reputation of the individual/organisation, i.e. pornography and the like' (C:1.132-7).*

Viruses were reported as the most prevalent form of information security incident experienced by the organisation.

*'Viruses are certainly the most prevalent (type of incident)' (C:2.182).*

Neither respondent could accurately determine the extent of losses suffered as a direct result of Information Security incidents.

*'Loss is mainly in unproductive time which no effort has been made to capture' (C:1.143).*

*'Couldn't really say; what is embarrassment worth for example?' (C:2.188-9).*

### **The business as a target**

The nature and the profile of the organisation when combined with the recorded number of incidents encountered pointed to the organisation being a target. The organisation clearly believed it was a target and was able to provide secondary data as evidence to support this assertion.

*'There is a lot of attention because of our profile, so I would say that we could be both the subject of a deliberate attack as well a target of opportunity. It is more than just the fact that we are there so let's have a go at them' (C:2.124-6).*

*'Yes (we are targeted) our evidence would suggest we gain some interest but it would not appear to be any higher than other large organisations connected to the Internet. Anything connected should expect to be probed or spammed to some degree' (C:1.88-90).*

A review of the source data from the organisation observations made by the researcher support the assertion by the organisation that they are a likely target for a variety of groups and threats. The organisation was unable to quantify this belief by pointing to particular incidents of note, in particular they could not produce evidence of foreign government attacks on their computing systems in anything other than anecdotal form. This may, however, reflect a limitation of gathering data in this area with this kind of organisation; national security considerations were an issue, which meant that at times the whole story might not have been revealed.

## **4.5.2 Management**

### **Countermeasures**



As might be expected of an organisation this size, Case C employed a sophisticated array of countermeasures to protect its IT from information security risks. Due to the size of the organisation and the value given to information within the organisation, it employed its own CERT to improve its security posture. The organisation also concentrated on foundational countermeasures such as valid and enforceable policies and procedures.

*'There are procedures and practices manuals or policies that people have to sign off that they have read, Information Systems Security Practices and Procedures (ISSPP), they read and sign. It tells them what they are allowed to do on a computing system' (C:2.217-9).*

As mentioned earlier the organisation had taken the unusual step of creating their own CERT.

*'There are people who monitor the network for hacker attacks and monitor for viruses. This is a CERT, it has been operating for about three months, it also does intruder detection and investigations' (C:2.221-3).*

The investigation and reporting function for information security incidents was advanced.

*'Security incidents are recordable and some are mandatory reporting under the ISIDRAS (Information Security Incident Detection, Reporting and Analysis Scheme) guidelines. Investigations are conducted for serious activities in order to identify the source and implement prevention strategies' (C:1.170-3).*

The organisation employed a number of technologies in the defence of their computing systems.

*'Firewalls exist, primitive IDS with more advanced corporate solutions as well as a range of commercial off the shelf products being procured' (C:1.176-7).*

*'We run fairly sophisticated anti-viral programs. Most things are centrally located for firewall management. We run IDS' (C:2.229-231).*

The survey responses from the organisation highlighted that the organisation used national and international standards for information security in order to benchmark their countermeasures and overall security posture. AS/NZ 77/99 and the international version of that standard ISO 17799 were both mentioned as key inputs into the formulation of security plans and responses for the organisation.

### **Level of security expenditure**

It was evident from the size of the organisation and scope of the security technologies and general countermeasures employed for the organisation that its

security budget was large. The organisation estimated that the total security budget was in the vicinity of \$8 million per year. This figure did not include any special projects or security costs absorbed as part of the network infrastructure.

*'Approximately \$2.7 million over the next three years has been allocated to the CERT alone' (C:1.186).*

A review of the secondary data provided showed an extremely detailed approach to information security and confirmed the annual security spend was \$8 million.

### 4.5.3 Differentiators

A number of potential differentiators were uncovered during the study of the Case C organisation that may have an impact of the organisation's security posture. These differentiators are listed and described in the table below:

**Table 4-7 Differentiators Case C**

Differentiator Number	Differentiator	Comments
1	Profile	Case C is a high profile commonwealth government agency that meant that it was more likely attract the attention of other of would be attackers.
2	Size	The organisation was extremely large which meant that it also had a good deal of influence within government and industry circles. The organisation was expected to be a leader in the use of technology and information security applications.
3	Importance of data/information	Information was a key resource and at times the information needed to be kept away from public viewing. This information could be specifically targeted. This would mean that the organisation was more likely to face dedicated attacks rather than attacks of opportunity.
4	Access to technology	The organisation had access to leading edge technology; in fact they had access to their own R&D facilities which could be employed to developed customised technology solutions including those in the arena of information security.
5	International footprint	The organisation had offices and business interest in many countries. This exposed the organisation to additional threats such as international espionage and other nation/state threats.
6	Relationships with other organisations or companies	The organisation faced additional threats because they dealt with other organisations that were likely targets for security related attacks. The Case

		C organisation had to strengthen its security posture because of this.
7	Study participants	Due to the size and nature of the organisation the respondents were very senior managers and therefore their responses to the interview questions tended to be more on the strategic side rather than the technical side.

*Source: Analysis of secondary and interview data*

#### **4.5.4 Security Framework**

Using the framework defined and developed in chapter 2, this study’s assessment of the information security position for Case B is shown in the diagram below. The analysis and application of the information framework for this organisation shows key areas of organisational risk – driven by the organisations high reliance on IT as well as the size and profile of the organisation. The risks are, however, well managed as is shown in the management section of the table – clear countermeasures are in place and dedicated security budgets have been established.

**Table 4-8 Information Security Framework Case C**

Risk					Management						
Research Issue 1 Reliance on IT	Research Issue 2			Research Issue 3 Australian Business as Targets	Research Issue 4 Countermeasures	Research Issue 5 Level of Security Expenditure					
	Threats		Incidents								
Information seen as a key resource or asset.	-	Complacency.	-	System privilege abuse.	-	The organisation believed that they were at risk of deliberate targeted attacks.	-	Well-defined and enforced system security policy.	+	Significant security budget with linkages to business justifications and outcomes.	+
Payroll, intranet. Document management key to organisational operation.	-	Hackers.	-	Significant virus incidents. Several thousand per month.	-	International and national organisations could have Case C as a target.	-	Procedures and work instructions on the use of IT, including mandatory reporting of incidents,	+	Budget separated into functional security areas including policy, hardware countermeasures, security personnel, CERT function.	+
Integrated logistics systems.	-	Organised groups of hackers.	-	Chain e-mails (SPAM).	-	Issues motivated groups could also have the organisation as a target.	-	Anti-viral software with automated updates of virus definition files.	+		
Connection to some business partners.	-	Foreign governments.	-	Contractors abusing access privileges.	-		-	High-end hardware based firewall products that meet national certification standards.	+		
Self assessed as very high reliance on IT	-	Viruses.	-	Computing hardware thefts.	-		-	System access controls.	+		
	-	System users (internal threat).	-	Hacking.	-		-	Internal CERT capability.	+		
	-			Data destruction.				Disaster Recovery plans.	+		

*(+) Factor has a positive impact on the organisation's security posture*

*(-) Factor has a negative impact on the organisation's security posture*

*Source: Analysis of secondary and interview data*

#### 4.5.5 Summary and recommendations

The organisation had a highly professional approach to the management of information security issues. The dedicated risk management process undertaken by the organisation provided clear guidance for how and what security countermeasures should be employed. The organisation was sufficiently large, in terms of budget and staff, to have a CERT of their own. This move in itself demonstrated that the organisation had a significant investment in protecting its valuable information and that there was a need for such a facility.

The organisation's belief that the insider threat was the most significant was particularly interesting. Whilst this belief is not uncommon in organisations this particular organisation had a slightly different explanation as to why this was the case with their organisation. Essentially the organisation believes that with the array of countermeasures that they have deployed it is highly unlikely for external originated security incidents to occur. Therefore, the majority of their security incidents were believed to be capable of being tracked back to an inside source.

The organisation's capability in conducting detailed investigations into security incidents confirmed this assertion.

The following recommendations are based on a comparison of the analysis of the current state of security in Case C with best practice as uncovered by the literature review (see chapter 2). If implemented the recommendations should significantly improve the organisation's security position:

- a. **Education program.** The organisation had comprehensive policies and procedures; however, more needs to be done to ensure that staff understand their obligations rather than simply handing them a large manual to read.
- b. **Contingency planning.** Review and revise the DRP and BCP to enable work to go on in the event of system failures.
- c. **Retention.** The organisation should consider staffing policies that improves their staff retention. Currently highly skilled and qualified staff are difficult to keep due to comparatively low wages in comparison to private organisations. The good staff tend to be poached by higher paying organisations.

#### 4.6 Case D – Resort/Hospitality Company

Case D is a medium sized publicly listed company that operates an island resort facility. They are located primarily on the resort island operating base; however they also have a small office in a capital city that handles much of the organisation's administrative functions. Two line managers who performed management and 'hands on' technical functions were chosen to take part in the research interviews. Interestingly, there was no dedicated IT manager. The various technical staff reported directly to the organisation's administration manager.

#### 4.6.1 Risks

##### Reliance on IT

Interview and observational data were used to gain an understanding of the reliance on IT within the Case D organisation. Case D described itself as highly reliant on its technology; however, it appeared that whilst failure of the technology would disrupt the business, manual systems could operate within the organisation for a reasonable amount of time without unduly impacting upon the business bottom line.

*'The organisation is highly reliant on IT and the availability of IT. Whilst most of the processes in and around the organisation could continue if the systems were to fail, they would be severely crippled' (D:1.20-2).*

*'Very reliant. All guest information is entered into the Fidelio hotel management system by the reservations office in Sydney. This information is not only used to allocate rooms to guests prior to arrival, it is also used for financial forecasting, staff rostering, allocating room numbers and times for the house keepers to service the rooms, tracking room charges from all outlets across the island, updating the PABX, routing messages, managing conference groups, first level accounts, and generating a variety of marketing statistics' (D:2.20-6).*

Approximately half of the organisation's staff regularly used computers as part of their normal work routine. The other staff, typically, cleaners, ground staff and general hospitality staff have little or no contact with computers. There was evidence of interconnection of systems with external networks to allow for bookings through third party networks belonging to holiday agencies.

*'Although the company does have a web presence and it is possible to book a stay via the web, it does not currently engage in Business to Business (B2B) electronic transactions' (D:2.30-1).*

*'External services which are dependent on our systems internally at this time are only web and e-mail facilities. We do have a web presence, but this is handled by a third party offsite' (D:1.24-6).*

When the computing facilities are not working much of the company's work continues 'as normal', for instance rooms are still cleaned, restaurants still operate. There are a pre-defined set of actions that take place when IT fails.

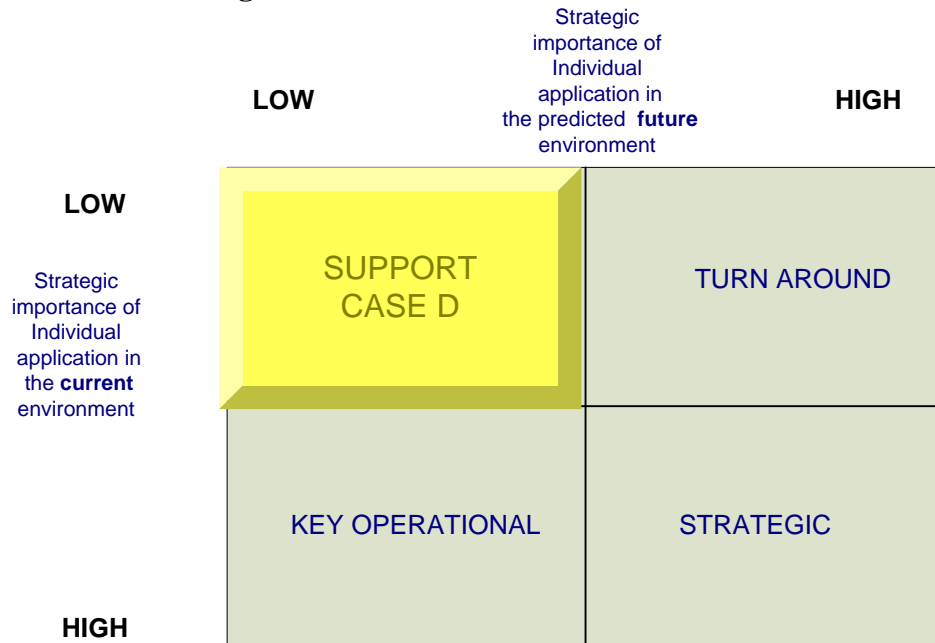
*'When the network stops working or the servers go down the reception staff fall back on a set of pre-defined contingency reports. These detail guest accounts are current, room status, and are printed off every half an hour' (D:2.33-5).*

These procedures demonstrated an informal contingency planning and business continuity arrangement. Printed reports could be used in this instance to coordinate work throughout the resort. In other cases staff were instructed to keep manual records of transactions in places like bars and restaurants in the event of an IT

failure. When systems were brought back on line batch processing could update organisational data.

Figure 4-5 below depicts the application of the McFarlan and McKenny Strategic Grid (McFarlan et al 1983) to the organisation’s IT. Whilst the interviewees deemed that the organisation was highly reliant on IT, technology was fundamentally a limited business enabler – with many functions capable of being operated without IT. The organisation was assigned the **support** quadrant as IT has little relevance to the firms existing or future success.

**Figure 4-5 Case D Strategic Grid**



Source: Analysis of interview and secondary data

**Threats**

The age of the technology employed by the organisation was considered by the respondents to be contributing factor to the kinds of threats encountered.

*‘Due to the age of technology used by Fidelio, all users have total control over the applications data folder on the server and could easily completely cripple the island’s most critical business systems.’ (D:2.57-9).*

The staff were considered a threat to the organisations IT, mainly as a result of technology vulnerability identified above but also for their general use patterns.

*‘Due to the high turnover of staff, something that has suffered is the management of user accounts. The existence of generic and password free accounts allows anyone with knowledge of this to possibly access sensitive information. Also where you have one account being used for several staff members, tracing malicious use and planning*



*responsibility for its misuse is very difficult to say the least, taking into account the style of business. A restructure of processes would be required for this to be effective' (D:1.52-8).*

The high staff turn over was as a result of seasonal or holiday workers forming a large component of the organisation's work force. The high turn over typically meant that there was little time to conduct appropriate security training and threat awareness. Additionally, there was little 'ownership' of security issues with transient staff as they typically would not be around to deal with the consequences.

Viruses were also considered a threat to the organisation.

*'Viruses – the obvious and most widespread threat to any organisation with an IT infrastructure, including ours. The origin of the viruses is usually e-mails and our external links coming in attachments' (D:1.48-50).*

The organisation seemed to overlook the reasonably obvious threat of viruses being introduced through recordable media. The transient staff had a high proportion of University students who frequently used the organisation's PCs for university related work, often introducing personal floppy discs into the environment.

Both respondents indicated that the system users were the biggest threat to the organisations security.

*'I feel that users pose the most significant risk to the integrity of these systems. Realistically valid users tend to be the most significant risk imposed against any IT system. They are the instigators and also the carriers for hacking, electronic fraud and virus infection, just to name a few' (D:1.66-9).*

*'Although the security of the Fidelio server is a problem, all users are told that being caught even browsing the network share is grounds for instant dismissal. Given the senior managements attitude to staff, they have been quite lucky, largely due to the users' lack of knowledge of this vulnerability' (D:2.71-5).*

These statements highlight a number of broader issues for the organisation. Firstly, access control is obviously an issue in relation to system account access as well as physical security problems. Secondly, the response indicates that management is not overly popular with the staff and this may increase the likelihood of disgruntled staff attempting to create problems with the system.

### **Incidents**

The organisation had suffered from three types of Information Security incidents. Viruses, thefts, and access abuse.

*'The only issues that I have come across in my time with the organisation is that of virus infections. While the infections were not serious, they outlined the need for constant monitoring of virus*

*pattern signature updates, and also the status of virus protection systems themselves. One major issue that was highlighted was the Interscan Viruswall system, which scanned all incoming and outgoing e-mail. The problem was the shortest interval for triggering a virus pattern update from the products central server on the Internet, was that of a day. Some viruses can propagate in a matter of hours, perhaps sometimes minutes it is important to upgrade the software which allowed for per hour updates' (D:1. 116-24).*

*'Approximately \$15 000 worth of equipment was stolen from the Sydney office over three months. When the IT member of staff for the Sydney office was let go, the thefts stopped and had not re-occurred. In another incident a member of the island staff was found to have caused server faults out of hours to generate call outs and therefore receive time off in lieu. The manger at the time was unable to understand the evidence, consequently that staff member is still here' (D:2.123-8).*

The organisation believed that the virus incidents were the most prevalent kind of security incident that they encountered.

*'Viruses are definitely the most frequent form of incident' (D:2.130-1).*

The organisation was unable to estimate the losses attributed to security incidents.

#### **The business as a target**

The Case D organisation did not believe that it was a specific target for Information Security incidents.

*'No (we are not a specific target). The island's competitors do not have the expertise to defeat the firewall. The island has been running for 20 years so we don't even get attention from the environmentalists anymore' (D:2.93-6).*

*'I don't feel the organisation is targeted specifically from external threats, but it does tend to get caught up in the 'general run of the mill' probing which comes via our external data connections. I attribute this to the organisation's minimal Internet presence, and non-complicated data network structure which to external perceptions is unappealing' (D:1.81-4).*

#### **4.6.2 Management**

##### **Countermeasures**

By their own admission the organisation employed limited security countermeasures.

*'Current countermeasures that exist in our organisation would be limited to that of perimeter security for the systems and network. This*

*comprises of virus protection systems and firewall devices. Internally, the built-in security of the operating system is relied upon to deter internal threats' (D:1.163-6).*

*'We are protected from external hackers by a firewall managed by our ISP. Our data is protected by nightly complete backups, with a weekly set sent to the Sydney office for permanent archiving. We are able to restore Fidelio to any day in the past six weeks' (D:2. 171-4).*

The survey responses supported the evidence presented during the interviews, with anti-viral methodologies, firewalls and operating system controls all playing a vital part of protecting the organisation's information assets.

**Level of security expenditure**

The organisation indicated via the interview data and survey data that it spent approximately \$50-70K per annum. These funds were primarily spent on firewalls and anti-viral products.

**4.6.3 Differentiators**

A number of potential differentiators were uncovered during the study of the Case D organisation that may have an impact of the organisation's security posture. These differentiators are listed and described in the table below:

**Table 4-9 Differentiators Case D**

Differentiator Number	Differentiator	Comments
1	Reliance on one central application.	The Case D organisation relied almost exclusively on one main application for the conduct of its electronic business. The application, 'Fidello' allowed the organisation to book guests into rooms, charge accounts, as well as more mundane tasks such as arranging for room cleaning. The organisation could not function for prolonged periods without the application.
2	Senior Management Attitude towards staff	The staff believed that there was a general attitude that staff were not well cared for by management. This led to a higher degree of disgruntled staff who could potentially be motivated to conduct malicious acts upon the organisation's computer systems should they have the pre-requisite technical knowledge to launch a successful attack.
3	Lack of policies and procedures.	There were very few formal policies and procedures in place within the organisation that related to IT. This led to a disjointed and at times

		uncoordinated approach to the delivery of IT and therefore of the appropriate security measures. There were no formal IT security plans.
4	No IT management structure.	The IT staff within the organisation were essentially all equal peers. This resulted in a lack of direction and failure for key individuals to accept responsibility for general IT management functions including the management of information security related issues.
5	Some components can function without IT	There were some functions in the resort that could function without IT, albeit in a less coordinated fashion. The physical work of cleaning and cooking for example could continue despite computer outage.

*Source: Analysis of secondary and interview data*

#### **4.6.4 Security Framework**

Using the framework defined and developed in chapter 2, this study's assessment of the information security position for Case D is shown in the diagram below.

The summarised findings show a lack of balance between the risks and the management sides of the information security equation. The negatives highlighted on the risk side of the framework are not adequately mitigated on the management side of the equation – which indicates a poor security posture. The summary and recommendations section provides some suggested improvements that this organisation could make to improve their current security posture.

**Table 4-10 Information Security Framework Case D**

Research Issue 1 Reliance on IT		Research Issue 2			Research Issue 3 Australian Business as Targets	Research Issue 4 Countermeasures	Research Issue 5 Level of Security Expenditure				
		Threats		Incidents							
Use IT for booking of guests.	-	Close integration of key applications.	-	System privilege abuse.	-	Not a specific target. Only seen as a target of opportunity.	-	Anti-viral software.	+	Unable to identify security budget.	-
Organisation of some work activities.	-	Staff, very high turn over.	-	Several viruses	-			Some firewall products.	+		
Billing, customer accounts.	-	Management attitude towards staff could increase instances of 'disgruntled insider'.	-	Hacking.	-						
Much work can be done without IT, for example cooking, cleaning, grounds upkeep.	+	Viruses.	-	15K of hardware theft.	-						
Self assessed as high reliance on IT	-										

(+) Factor has a positive impact on the organisation's security posture

(-) Factor has a negative impact on the organisation's security posture

Source: Analysis of secondary and interview data

#### 4.6.5 Summary and recommendations

The organisation's overall security posture was poor. The lack of policies, procedures, and a clear IT management structure resulted in no clear responsibilities for information security related tasks. The transient nature of a large proportion of the workforce combined with a reportedly strict general management regime created an environment where serious security incidents could and did occur.

The insider threat within this organisation was significant. Resentment towards management from staff coupled with lax or non-existent security measures presented motive and opportunity to would be internal hackers. The organisation assessed itself as highly reliant on its IT, however, it did have the capability to continue to operate for short to medium terms in the event of system failures.

The following recommendations are based on a comparison of the analysis of the current state of security in Case D with best practice as uncovered by the literature review (see chapter 2). If implemented the recommendations should significantly improve the organisation's security position:

- a. **Risk assessment.** The organisation should implement a formal risk assessment process to identify risks and threats.
- b. **IT management.** An IT Manager position should be created and this position should be assigned responsibility for information security.
- c. **Policies and procedures.** Comprehensive system security policies and procedures should be developed and then implemented, wherever possible through the use of technology.
- d. **Access controls.** System access controls should be defined to ensure that system users can perform only authorised functions on computing systems.
- e. **Education and awareness.** Firstly, management should be made aware of the current security posture and all identifiable risks. Wider training should be conducted for all system users to ensure they are aware of their responsibilities to help protect systems.

#### 4.7 Case E – Software Company

The organisation studied, as Case E is an Internet based software development company. The organisation had five staff each of whom fulfilled a specialist role within the organisation. The organisation is privately owned by a number of the staff members. The company had a close affiliation with information security issues as they produced a number of computer security related products. Due to the small size of the Case E organisation only one IT management professional was available to take part in the research interview. The company was located in a capital city with all staff and IT assets being located in one small office.

### 4.7.1 Risks

#### Reliance on IT

The nature of the Case E organisation pointed to a natural reliance on IT. A software development company will obviously use IT to create, develop and distribute their software products. The Case E organisation considered themselves to be completely reliant on IT.

*'We are utterly dependent on computers. With about two machines per employee, in addition to computers in mobile phones and Personal Digital Assistants (PDAs) they support every aspect of our business' (E:1.20-2).*

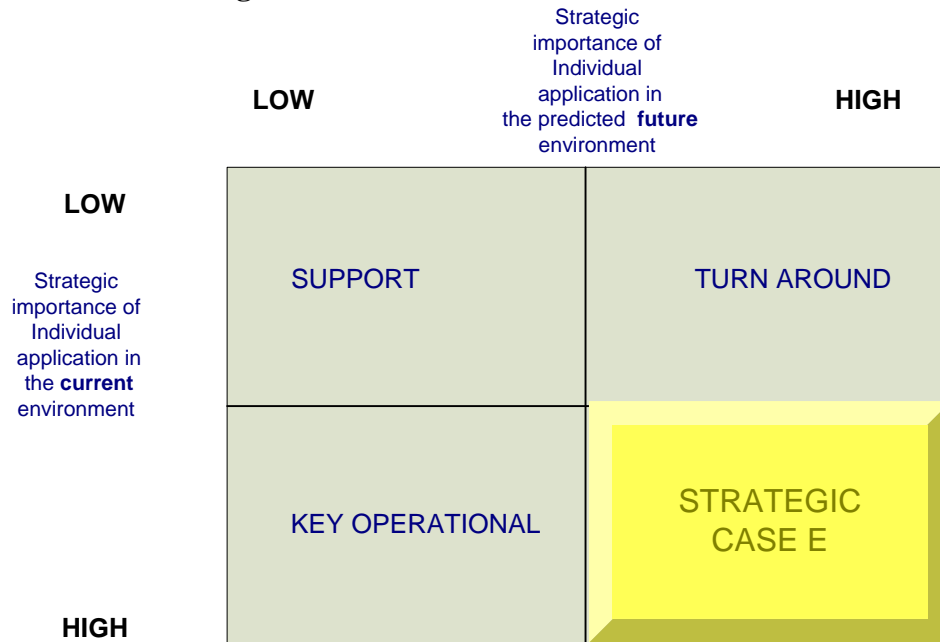
The organisation believed that they could not operate their business should the technology fail. Additionally, if the unavailability of the IT was related to security incident then this would impact upon the company's reputation as security software provider.

*'Without computers we wouldn't have a market for our security technology' (E:1.24).*

The company's systems were connected to the Internet and documentary evidence in the form of LAN and WAN diagrams demonstrated the organisation's reliance on Internet based technologies with the Internet providing access to the company's market, its customers, and open source information. Internally an Intranet was used to store and publish shared information between staff members. Observational data collected by the researcher whilst at the company's premises indicated that despite the fact that all staff were seated close enough to talk comfortably with all other staff they used e-mail even for the simplest and most informal messages between themselves.

Figure 4-6 below depicts the application of the McFarlan and McKenny Strategic Grid (McFarlan et al 1983) to the organisation's IT. This organisation was heavily reliant on the use of IT and its core products relied upon vulnerabilities in computing systems in order to create a market. Existing and future developments of IT are critical to the organisation's success – therefore IT is of *strategic* importance to the organisation.

**Figure 4-6 Case E Strategic Grid**



Source: Analysis of interview and secondary data

**Threats**

The organisation considered itself as being subjected to a wide variety of threats.

*‘The main threats come from individual hackers, organised groups of hackers, issue motivated groups, foreign governments, systems users, competitors, viruses and poor quality code’ (E:1.45-53).*

The comprehensive listing provided by the organisation indicated that they had put considerable thought into the potential threats faced by the organisation. This in itself was not surprising given the organisations place as a software provider in the information security marketplace.

The company considered viruses to be the most significant threat faced by the organisation based on the premise that the viruses were the most frequent and the hardest to detect.

*‘E-mail viruses – because they are so hard to detect, especially the newest ones, and they come from any vector – inside, external, and trusted partners’ (E:1.59-60).*

The organisation discovered or learnt about the threats that their organisation faced through a combination of evidence, study, and research.

*‘We use a variety of methods, market research is important. We look at things like the KPMG and Ernst and Young research, although a lot of that tends to support their consultancy business’ (E:1.66-73).*



## **Incidents**

The organisation had experienced a variety of information security incidents, however they did not wish to elaborate on specific incidents and indicated that their incidents were the 'run of the mill' type of incidents that any organisation connected to the Internet would expect to face.

*'We have had a variety of incidents including viruses, port scans, script kiddie tools, and the loss of a laptop' (E:1.104-105).*

There appeared to be no alarm or undue weight placed on these incidents. Secondary data (documents) and observation data recorded whilst viewing server and firewall logs pointed to a large number of port scans. When the respondent discussed these issues (outside the interview context), he expressed the belief that much of the industry warnings revolved around these relatively 'minor' kinds of incidents. When asked to identify which type of incident was the most frequent the respondent indicated that they all occurred frequently.

*'All of them. All occur easily, and almost every day' (E:1.110).*

The organisation could not estimate the financial impact of any of the security incidents that they encountered.

*'No, not really (estimate financial losses) – some time in virus eradication and the loss of the laptop. All of the others have yet to cause damage/loss' (E:1.116-7).*

## **The business as a target**

The business did not consider itself a specific target although it was evident by examining secondary data that the organisation had considered the possibility of it being a target.

*'Not especially more than anyone else is a target. We maintain a low profile with competitors and have now removed the financially sensitive information available in our Internet connected site' (E:1.79-80).*

## **4.7.2 Management**

### **Countermeasures**

The Case E organisation used a variety of countermeasures to protect their systems from incidents.

*'We have a central firewall, security policies and procedures which are enabled through technology wherever possible such as system file permissions or turning on server logs. Working in the security industry is a help in this regard as our staff are aware of the risks. We of course employ the normal range of anti-viral countermeasures and*

*perhaps most importantly assure that the patches are kept current’  
(E:1.140-4).*

**Level of security expenditure**

The organisation had a very limited security budget, however, it did employ a variety of freely available tools to perform the security function.

*‘We would spend between \$250 and \$1000 in a 12 month period, we use a lot of open source tools’ (E:1.147-9).*

**4.7.3 Differentiators**

A number of potential differentiators were identified as part of the study of the Case E organisation. These differentiators include:

**Table 4-11 Differentiators Case E**

Differentiator Number	Differentiator	Comments
1	Size	The organisation had five staff who all worked within a small office. This enabled a high degree of trust and the sharing of knowledge on a variety of issues including security. Policies could be quickly developed, implemented and monitored.
2	Reliance on IT	As a software development organisation each staff member had two computers. The extremely high reliance on IT increased the potential impact of a security incident.
3	Use of open source products	As a small business the organisation did not have large amounts of capital to invest in security. The organisation turned to a variety of Open Source, free tools to minimise its security threat. The organisation was able to customise these tools using their own skills to further enhance their security posture.
4	Use of the Internet	The Internet was a valuable research tool for the organisation and a method of testing their product. This constant reliance and connection to the Internet was seen as an unavoidable exposure by the organisation.
5	IT Security a key part of the business	The organisation developed and sold software tools that provided security countermeasures. As a security product provider the organisation had a better understanding than most of the security threats that they faced. The staff had a high level of technical security expertise that ensured tools

		and systems were appropriately implemented and configured.
--	--	--

*Source: Analysis of secondary and interview data*

#### **4.7.4 Security Framework**

Using the framework defined and developed in chapter 2, this study's assessment of the information security position for Case E is shown in the diagram below.

The security posture presented in the framework appears to be relatively well balanced. Whilst there are a number of risks that the organisation faces, it has employed a number of countermeasures in order to better mitigate those risks. The framework indicates a relatively low budget for security related items and assesses this as a negative. In context however, this organisation is relatively small and as such does not have liquid assets to dedicate to numerous security countermeasure – therefore they must be selective. This action in itself indicates a level of maturity in their risk management approach.

**Table 4-12 Information Security Framework Case E**

Research Issue 1 Reliance on IT	Research Issue 2				Research Issue 3 Australian Business as Targets	Research Issue 4 Countermeasures	Research Issue 5 Level of Security Expenditure				
	Threats		Incidents								
Business centred on the use of IT. Used to develop company product (software).	-	Individual hackers.	-	Did not want to elaborate too much on detail.	-	Didn't consider itself as a specific target.	+	Security policies and procedures that are enabled through technology.	+	Low budget (several thousand dollars).	-
Business not capable of working if IT not available.	-	Organised groups of hackers.	-	A number of virus incidents.	-	In a niche industry with a security product. Could be a target of competitors.	-	Firewalls.	+	Mitigated risk and costs by using open source products.	+
Used IT based communication in preference to face to face communication	-	Poor quality code.	-	Laptop theft.	-			Anti-viral software with automated updates of virus definition files.	+		
		Issue motivated groups.	-	Attacks from automated scripting tools.	-			Patch management procedures.	+		
		Viruses	-	Port scans.							
		Competitors.									

(+) Factor has a positive impact on the organisation's security posture

(-) Factor has a negative impact on the organisation's security posture

Source: Analysis of secondary and interview data

#### 4.7.5 Summary and recommendations

The organisation's overall security posture was good. It had a systematic approach to identifying risks and then implementing appropriate countermeasures. The organisation's reliance on the Internet for research and for testing its product introduced a number of threats to the organisation. This additional risk is somewhat counteracted by the fact the organisation is involved in the security industry, and as such was generally more aware of the security issues than the average company.

The number and type of virus incidents that they detected, mainly through their e-mail system supported the organisation's assessment that viruses were the most significant threat they faced. The organisation placed on emphasis on anti-viral defence and the backbone of this strategy included a comprehensive patch management program.

The following recommendations are based on a comparison of the analysis of the current state of security in Case E with best practice as uncovered by the literature review (see chapter 2). If implemented the recommendations should significantly improve the organisation's security position:

- a. **Contingency planning.** Due to the organisation's extreme reliance on its systems routine, system backup and recovery should be enhanced. The creation of DRP and BCP should be given a priority to reduce the impact of system failures.
- b. **Network segregation.** The organisation develops its products on systems that are connected to the Internet (albeit through firewalls). This approach should be reviewed with the aim of creating a physical air gap between their development system and the system connected to external networks.

### 4.8 Case F – Small Commonwealth Government Agency

Case F is a small Commonwealth Government department with approximately 500 staff. They are located within a single capital city where they service their clients, mainly other government departments and large business through their online presence. IT and the publication of government policy form the core businesses of this department. Due to the small size of the organisation and the fact its IT is largely outsourced meant there was only one individual within the organisation who could speak authoritatively about information security issues.

#### 4.8.1 Risks

##### Reliance on IT

The organisation at Case F described itself as highly reliant on IT. As one of the newer government departments much of the technology that it employed was new. As part of its core business was in the provision of advice and policy on the use of IT

it deemed important to ‘practice what it preached’ especially in the area of e-commerce adoption and the use of secure web technologies.

*‘Users have a degree of dependency on the network. The primary role of this department is to outreach to the Australian public and business for the development of IT for the development of PKI (Public Key Infrastructure) and Business to Business (B2B). There is a strong reliance on the Internet and Intranet availability to deliver these types of services’ (F:1.22-5).*

The organisation was part of a group of government departments whose IT is outsourced. It was evident that the organisation was less than happy with the outsource arrangement. Perceived poor performance from the outsourcer coupled with the organisation’s high reliance added to the level of user dissatisfaction.

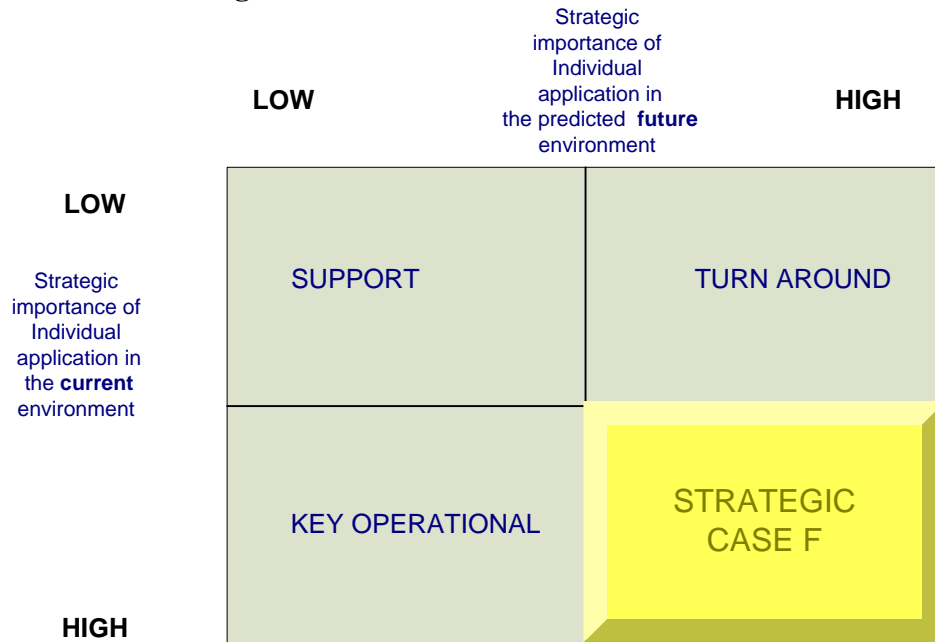
*‘IT is outsourced in a government environment. The network often runs slow and is subject to constant failure, i.e. loss of external or internal link’ (F:1.20-1).*

The relationship with the department and its service provider in this instance could be considered in itself a risk, especially given what would appear to be limited requirements to report why external links were not available, e.g., did they fail for technical reasons or for security reasons.

Analysis of the survey data indicated that disruptions to service were relatively frequent (at least twice per month). This frequency of system outages meant that the organisation’s staff were well versed at finding alternative activities when the IT didn’t function.

Figure 4-7 below depicts the application of the McFarlan and McKenny Strategic Grid (McFarlan et al 1983) to the organisation’s IT. The organisation is highly reliant on technology and is involved in drafting a number of policies and practices on the use of e-technology. It is important for the profile of the organisation that are seen to be innovative in the use of technology. The existing and future developments of IT are critical to the success of the organisation.

**Figure 4-7 Case F Strategic Grid**



Source: Analysis of interview and secondary data

**Threats**

The organisation focused quite strongly on a number of key threats. Viruses were the first and perhaps the paramount threat the organisation considered it faced.

*‘The department runs a strong anti-virus regime to combat what is obviously a well known and everyday threat’ (F:1.45-7).*

The organisation believed that there was a significant external threat.

*‘Undetected external entry into the network where many government initiatives are planned and implemented would be a significant threat’ (F:1.56-7).*

Secondary data indicates that there was generally little external access to organisation’s networks. There was access (protected) to other networks through the Internet and theoretical or logical connections to the organisation’s IT outsource partners through their common IT service providers and vendors. The maturity of this relationship required the interchange of ‘cleared’ information to ‘cleared’ partners.

*‘All outsourcing partners are cleared to the level required to operate the system. There is no external connectivity to the network. Though executive officers have remote access to the network from home’ (F:1.47-50).*

The organisation also considered itself subject to a significant internal threat. Due to the organisation’s function in the development of IT policies and standards for the Commonwealth Government, there is considerable interest in the policies and

standards under development. This interest also applies to those organisations that provide the IT service to the case organisation and therefore would have free access to information on the organisation's network.

*'The contracted service provider has an intimate interest in the policies of this Department – a significant insider risk' (F:1.58-9).*

The interview respondent indicated that they were aware of the risks faced by their organisation from experience in managing computer based networks and from the completion of recent studies in security management.

*'Throughout my career I have managed and implemented several large computer based networks. I have nationally recognised qualifications in computer management and have recently completed a Diploma of Security Risk management' (F:1.69-72).*

### **Incidents**

The organisation had encountered only one form of information security related incidents: viruses.

*'The Department uses Norton's anti-virus and other protection software. The occasional virus causes problems. Whilst it is the policy that all external disks are to be checked prior to their use in desktop PC this would appear to be the main source of this type of attack' (F:1.106-110).*

Survey data collected from the organisation supported the interview data regarding the number and type of incidents that were encountered. It appeared that the visibility of the organisation's security related incidents was greatly reduced as a result of its outsourcing arrangement.

### **The business as a target**

There was a general lack of evidence pointing to the organisation being a specific target for information security incidents; the low number of incidents and the lack of anecdotal evidence suggested a somewhat benign threat environment. The organisation did, however, believe that contrary to evidence they were a prime target.

*'I firmly believe that our IT infrastructure is targeted. However the IT outsourcing contract seems to lack the requirement for the IT outsourcer to detect and report these problems when they occur' (F:1.80-2).*

Due to the experience and knowledge of the interview respondent, coupled with the information provided as part of the analysis of the threats, including the profile and business of the organisation it is reasonable to conclude that the organisation could be a targeted organisation.



## 4.8.2 Management

### Countermeasures

The organisation’s outsourcing arrangement made it difficult to determine the exact nature of the countermeasures employed. It was surprising that there appeared to be little contract coverage to ensure that the appropriate countermeasures (whatever they were determined to be) were being taken.

*‘There is no risk management analysis of the threats to the IT of this department. There is little executive support for this type of analysis’  
(F:1.150-2)*

A review of the secondary data, mainly in the form the outsourcer’s change management documentation indicated that there were ‘extensive security mechanisms’ in place including firewalls, anti-viral protection, and system policy and procedures. In fact the change management procedures aim was to ‘maintain the integrity and security’ of the organisation’s computing systems.

### Level of security expenditure

The nature of the outsourcing contract obscured the total security expenditure that the organisation made.

## 4.8.3 Differentiators

A number of potential differentiators were identified as part of the study of the Case F organisation. These differentiators are detailed in the table below:

**Table 4-13 Differentiators Case F**

Differentiator Number	Differentiator	Comments
1	Outsourcing arrangement	The organisation received its IT support through a multi-agency outsourcing arrangement. This arrangement had been described as sub-optimal with very few if any security KPI integrated into the outsourcing agreement. Reporting on incidents was problematic.
2	Commonwealth Government Department	The organisation was a reasonably high profile department that could draw the attention of a range of would be attackers attempting to have their political message heard.
3	Responsible for IT policies	One of the key functions of the Department was to produce Commonwealth IT policy. This included policies on e-commerce and security related issues. This could be seen as both a positive and negative in terms of the organisation’s security posture. Positive → potentially a

		better understanding of what the issues are. Negative→could be a higher profile target due to this role.
4	Use of the Internet	The Internet was a valuable research tool for the organisation and a method of testing their product. This constant reliance and connection to the Internet was seen as an unavoidable exposure by the organisation.
5	Relatively new organisation	The organisation was essentially a greenfield site that enabled policies and infrastructure to be set to the appropriate standard from the outset. There were fewer change management issues that needed to be considered when implementing security issues.

*Source: Analysis of secondary and interview data*

#### **4.8.4 Security Framework**

Using the framework defined and developed in chapter 2, this study’s assessment of the information security position for Case F is shown in the diagram below.

The table presents a relatively balanced framework, indicating that the organisation is managing its risk profile – or factoring in risks when determining appropriate countermeasures. Of interest is the potential positive or negative of having an outsourced arrangement for security services.

**Table 4-14 Information Security Framework Case F**

Research Issue 1 Reliance on IT		Research Issue 2			Research Issue 3 Australian Business as Targets		Research Issue 4 Countermeasures		Research Issue 5 Level of Security Expenditure	
		Threats		Incidents						
Office automation	-	Virus	-	Viruses	-	Yes because of potential weakness in outsourcing arrangements	-	Managed by outsourcer	+/-	Not discernable due to the nature of the outsourcing arrangement
Publication of policies and procedures	-	Hackers (undetected external entry)	-			Profile of the organisation, producing policies on IT and e-commerce	-	Firewalls	+	
Automated pay and financial management	-							Anti-viral products	+	
Reliance on IT outsourcing arrangement	-							Policies and procedures	+	

(+) Factor has a positive impact on the organisation's security posture

(-) Factor has a negative impact on the organisation's security posture

Source: Analysis of secondary and interview data

#### 4.8.5 Summary and recommendations

The organisation's overall security posture was below average. They had little or no control over various aspects of their outsourcing agreement, in particular there were no specific Key Performance Indicators (KPI) that focused on security issues and reporting. The organisation's reliance on its' technology means that they are at risk of losing the use of their systems and productivity in the event of system failures. The nature of their Service Level Agreements (SLA) with their service provider meant that they were unable to differentiate between system outages that were a result of technical problems from those that could be security related. They reported frequent availability issues with the network either down or not available. It was frequently unclear to the organisation why its' systems were not available.

The organisation only reported one form of security incident – viruses. It is unclear as to whether this was the only incident that actually occurred – or rather it was the only type of incident that the organisation actually knew about.

The following recommendations are based on a comparison of the analysis of the current state of security in Case F with best practice as uncovered by the literature review (see chapter 2). If implemented the recommendations should significantly improve the organisation's security position:

- a. **Outsourcing contract.** The organisation should, at the earliest possible time renegotiate their existing support contract to include reporting on security related incidents and events. Additionally, the contract should include KPI that focus on monitoring and improving the organisation's security position.
- b. **Audit and investigation.** As the organisation is currently not fully aware of its' security exposure an independent, external audit is recommended. This audit and investigation should include a review of the policies and procedures of the service provider. Security penetration testing should also be a priority to prove the robustness of the any security countermeasures employed.
- c. **Information security ownership.** The organisation should review 'ownership' of information security within the organisation. Whilst the authority for the management of information security may be outsourced to a service provider – the organisation's leadership should retain responsibility and accountability for ensuring the system's security is maintained. This will help ensure the organisation conducts appropriate due diligence activities to ensure that the service provider is meeting the organisation's requirements.

#### 4.9 Case G – Medium Sized Utility Company

The Case G organisation is a privately owned utility company employing approximately 800 employees operating within one State. Their services are provided across that State. The organisation had a number of remotes site that were connected

to the organisation's central office via a number of telecommunications and information systems. Two IT professionals were chosen to provide information on the organisation's security issues.

#### **4.9.1 Risks**

##### **Reliance on IT**

Interview and observational data were analysed to gain an understanding of the organisation's reliance on IT.

*'Our organisation is totally reliant on IT. IT forms a central component of the way we do business, regardless of if we are talking about our administrative systems, where we have a heavy reliance on an ERP, in our case SAP' (G:2.20-2).*

IT appeared to be ubiquitous within the organisation. There were very few functions that did not have some reliance on technology, whether it be the delivery of its service or booking a conference room for a meeting.

*'Our business is very reliant on our computing assets. We have a number of diverse systems that enable our business. We have approximately 700 users in a central business HQ and a couple of hundred users in another State and throughout this State. As a minimum they would all interact with our corporate network, and many would interact with systems that controls the flow of our commodity' (G:1.20-4).*

The organisation divided its computing facilities into its corporate network and a separate network for controlling and managing its commodity. For security purposes this created two major computing domains and a third domain existed to allow controlled access to customers and national controllers for the commodity in question.

*'Our customers have access to our systems as well as national market information. We have an external web site, which is mainly used for communication of issues to the general public' (G:2.29-31).*

This evidence highlights the importance of access to the organisation's computing systems from external computing networks. Therefore, not only is Case G reliant on its IT but external organisations are also reliant on those networks.

*'We are heavy users of an ERP, SAP. Most of our applications have some hook into SAP and all of our staff use SAP for their day to day work, even if it is only submitting their time sheets' (G:1.29-31).*

The highly interdependent nature of the applications with a central ERP heightened the organisation's reliance on IT, every staff member had to interact in some fashion with IT. That interaction could range from simple time entry sheets to controlling the flow of the organisation's commodity.

The organisation could put on an estimate on the worth of their reliance on technology by knowing how much money the organisation would lose if their networks were not functioning.

*‘If the IT doesn’t work then the organisation can lose \$1000 per second in lost revenue’ (G:2.33).*

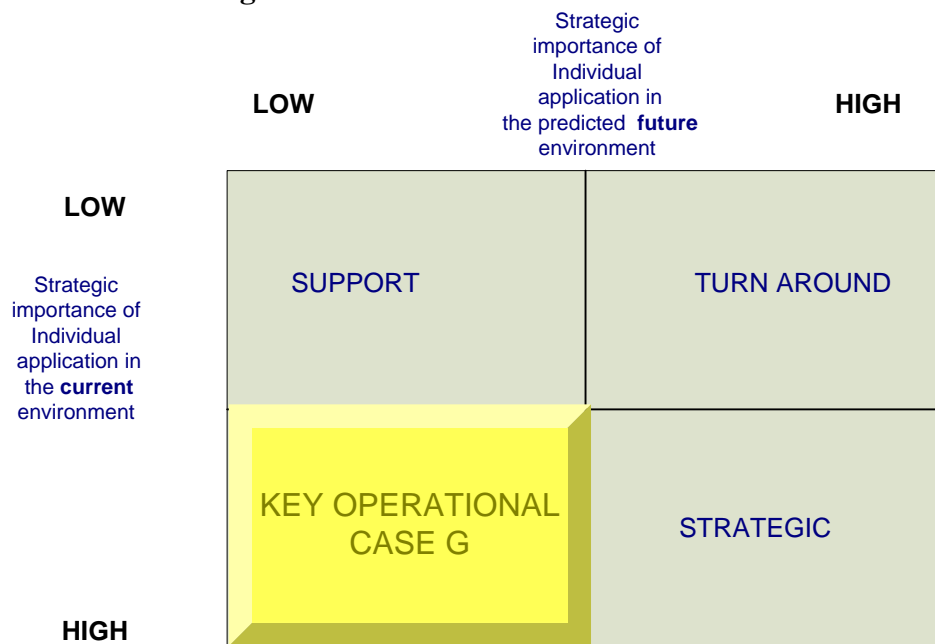
*‘Overall, I would say we are very reliant on our systems. When things don’t work people’s productivity goes down. Even the phone systems rely on computing so you may not even be able to use the phone’ (G:1.36-8).*

The organisation’s heavy use of IT and the potential consequences in terms of losses that could result if the organisation’s IT didn’t function properly pointed to a high reliance on IT.

A review of the survey responses provided by the organisation confirmed the views provided in the interviews; the organisation was highly reliant on IT with the vast majority of the organisation’s staff interacting in some way with IT.

Figure 4-8 below depicts the application of the McFarlan and McKenny Strategic Grid (McFarlan et al 1983) to the organisation’s IT. The amount of revenue that can potentially be put at risk is an indicator of the organisation’s reliance on technology – networks and systems monitoring their control systems are critical. IT is important to the organisation but future developments are unlikely to improve the competitive advantage, therefore IT is seen as playing a key operational role in the organisation.

**Figure 4-8 Case G Strategic Grid**



Source: Analysis of interview and secondary data

## Threats

Both respondents believed that viruses were the biggest information security threat that the organisation faced.

*'The biggest threat to our organisation would be viruses' (G:1.61).*

*'Viruses are potentially our greatest threat' (G:2.54).*

The respondents recognised that there were potentially other threats that the organisation faced.

*'Although as part of the national information infrastructure we can expect probes or investigations from hackers' (G:2.54-5).*

*'We receive the usual amount of port scans and spam e-mail, but there is no evidence of hacker attacks. Because of the nature of being in the utility business it doesn't mean there isn't any potential for hackers, foreign governments, or even terrorists it just hasn't materialised' (G:1.61-5).*

These responses point to an understanding that there is a potential for a wide variety of threats to the information security of the organisation. However, as the respondents have pointed out, there is little evidence that these other threats have actually occurred. This would seem to indicate that this organisation's risk analysis has identified the gamut of potential threats and which of these present the greatest risk to the integrity of their systems.

*'Again, I would have to say viruses (are the most significant threat), just because of the amount that we detect, block and clean' (G:1.71-2).*

*'Viruses are probably the most frequent, and we encounter them on a daily basis. A hacker could be more significant if they come in and start turning things off' (G:2.68-9).*

These statements acknowledge the existence of other threats; however point to the most frequent threat being synonymous with the most significant threat faced by the organisation.

Observational data recorded whilst on the organisation's premises supported the answers given by both respondents, potentially indicating that a degree of effort had been placed into the consideration of security issues, that there was a reasonable level of knowledge, and that perhaps more importantly there was a high degree of staff commitment to information security issues.

This opinion was reinforced when the respondents were asked to identify how they knew about the threats that their organisation faced.

*'Experience, we keep logs on these issues. We have also had a number of threat assessments conducted on our company which points to these areas. Most of the IT management team have a good working knowledge of security issues' (G:2.80-3).*

*'From a variety of sources, discussions and benchmarking with other organisations with similar profiles. One thing I think is relatively obvious is that there is a fair amount of hype and scare mongering out there about threats. Whilst security and the threats/risks are serious, the business case is hard to justify when there is little evidence. You read about it, but not many people that I have contact with that have suffered from hackers for example. Plenty moan about viruses on the other hand' (G:1.82-91).*

Responses such as these demonstrate that this organisation and in particular the reluctant staff members put a great deal of thought into security issues. There was also a degree of cynicism detected in the later response.

### **Incidents**

There was a direct correlation between the perceived security threats faced by the organisation and the type of incidents encountered by the organisation. This in itself was not surprising given the responses to the threat section of the interviews.

*'As I have indicated previously we get about two hundred plus viruses per month that are detected. Very few are able to get through our series of protection mechanisms' (G:1.129-130).*

*'We have about one hundred viruses a month. They come in all shapes and sizes, mainly through the Internet and through mail attachments, many of them non-work related' (G:2.115-6).*

The difference in the number of estimated viruses per month can probably be attributed to the fact that one of the respondents was directly responsible for information security, whilst the other was responsible for IT in general.

*'We have had a high amount of laptop thefts, somewhere in the order of 14 in the last 12 months, mainly from a couple of break ins at the corporate head office but also because of the employees leaving them in cars. We really don't know about the loss of associated data that could have been retrieved from those systems' (G:1.132-5).*

The theft of computing assets could have potentially had a very serious impact on the organisation and its core business. Not only could they be embarrassed by the loss of sensitive company information but it is possible for laptops to turn on and off their systems or impact on the distribution of their commodity. This point was not lost on the organisation.



*'You only have to look as far as Queen vs Bowden to see the impact of stolen and misused computing equipment and what it can do to a utility' (G:1.104-5).*

*'We have had a number of instances of laptop theft, where we have had break ins with machines stolen from the back seats of cars and also from our head office facilities' (G:2.118-9).*

Potential access abuse to computing facilities is another area where potential incidents have been recorded. The nature of these incidents within the organisation has made some of the incidents hard to detect or verify.

*'We have had a few suspicions regarding access abuse, people using mail delegations incorrectly for example' (G:1.137-8).*

*'There have been occasions where there have been accusations of employee access abuse, however, we have not been able to prove any of this' (G:2.121-2).*

The organisation indicated that there were at least two incidents that could be classified as the most serious, namely theft and viruses.

*'In our case, they could be different. I would say viruses are the most prevalent, and if not caught could easily be the most significant. A stolen laptop could be significant if it has damaging information or it allows people to gain access through your system. This is particularly the case if there are cached passwords on your systems' (G:2.130-3).*

*'Viruses. They have so many potential access points, through e-mail, web mail, and disks. We have most incidents from viruses' (G:1.146-7).*

The respondents found it difficult to estimate the amount of money or resources they had lost as a result of information security incidents. There were, however some areas where they could provide some information as well as some general opinions about the measurement of such losses.

*'Hard to say. We have lost about 100K in hardware alone. We spend about 10K per month looking for viruses' (G:2.139-140).*

*'We have lost about \$80 000 in stolen laptops alone. I am very sceptical about the figures I read regarding losses as a result of viruses. Whilst it is quite easy to estimate the amount of time to re-build a server and how much that resource costs. It is quite a different matter to estimate to estimate lost organisational time/productivity. If a machine is down for 15 minutes because of virus infection what's to say that staff were not in a meeting, doing paper work or choosing to take a coffee break while the repair work was being done. If you could measure things like that with any level of certainty surely you would have an easy time justifying things like infrastructure upgrades*

*because you would be able to estimate the cost of slow networks' (G:1.153-161).*

### **The business as a target**

The organisation did not believe that it was specifically targeted because of who they were or what they did.

*'Not specifically (are we targeted) at the moment, but given justification I believe that we would be good targets. If you could get through you could cause a great deal of havoc' (G:2.90-1).*

*'Not at the moment. I guess like many organisations we are targets of opportunity. One reason we may not see hackers is they give when they get bounced from our firewall. We get some suspicious hits from universities' (G:1.98-9).*

## **4.9.2 Management**

### **Countermeasures**

The organisation had a comprehensive approach to applying a variety of security countermeasures including technology based measures and policy implementations.

*'We have a fulltime security manager, an IT security committee with executive membership' (G:1.188-9).*

This statement emphasises the organisation's approach to promoting security issues outside of the IT area. Non IT executives were actively involved in a security committee that subsequently ratified and helped enforce security policies.

Much of the organisation's technical security services were provided by a managed security service provider. In this case the organisation's security manager effectively controlled the service providing company in order to manage systems in line with organisational policies.

*'We arrange a managed services security provider that has all of the Internet traffic flow through their trust centre. They run anti-viral services/anti spamming services as well as host based IDS on their systems, we run network based IDS on our systems with several probes in different parts of the network' (G:1.193-6).*

*'We outsource some of our security in a co-source arrangement. We have web and content filtering and we go through a trusted managed services provider' (G:2.180-3).*

Policies and standards were an important component in the organisation's defence strategy.

*'We are aiming at ISO 17799 in the near future. We have extensive security policies and procedures and disaster recovery plans' (G:1.202-3).*

*'We are aiming to meet standards such as IS18 AS/NZS 7789. We are looking at the ITIL framework for the implementation of best practices in security delivery' (G:2.175-6).*

The organisation used a suite of hardware based security devices, with an array of advanced applications to allow integration with their standard IT infrastructure.

*'We have a number of firewalls, in a layered approach with fail over of services, vendor separation also' (G:2.178-9).*

*'We have dual layers of firewalls, two different brands' (G:1.190).*

The organisation put emphasis on the selection of different firewall vendors, using different firewall technologies. This approach was seen as advantageous by the organisation as it ensured that any vulnerability in one technology or product would not automatically compromise all of their systems.

#### **Level of security expenditure**

The organisation was able to show documentary evidence of its level of expenditure on information security.

*'We have spent \$1.5m in the last 12 months' (G:2.187).*

*'Our annual security budget is about \$1.2 million. We have just spent over \$1 million introducing new infrastructure policies and security hardware' (G:1.212-3).*

#### **4.9.3 Differentiators**

The study of the Case G organisation revealed a number of potential differentiators. These differentiators include:

**Table 4-15 Differentiators Case G**

<b>Differentiator Number</b>	<b>Differentiator</b>	<b>Comments</b>
1	Nature of the organisation	As a major utility the organisation forms part of the national critical infrastructure. Disruption to its services could have a serious impact on an entire State.
2	Managed services	The organisation had a number of services including some information security services provided by external service providers. This had a potentially positive impact on the organisation's security posture in that

		subject matter experts could be employed to run critical infrastructure and systems. On the other hand there is potential for some loss of control of some services due to the 'hands off' nature of these arrangements.
3	Segregation of networks	The organisation partitioned its various networks through the use of a series of firewalls. This improved the organisations posture as potential problems could not traverse the breadth of the organisation's systems without passing through a number of security checkpoints.
4	Multiple layers of firewalls	The organisation operated multiple layers of firewalls. This provided a more robust arrangement as any would be attacker would have to defeat a series of firewalls. The firewalls were configured in such a fashion that if one firewall failed another could handle its function.
5	International standards	The organisation benchmarked its security services against international standards such as ISO 17799.
6	Government owned corporation	The organisation was a government owned corporation, which meant that it was required to adopt and comply with certain government initiatives and policies regarding information security.
7	Audited by other government agencies	As a quasi government organisation the security posture of the organisation was quite frequently audited by government accounting and auditing agencies to monitor compliance and security issues.
8	Reliance on IT/Internet	The organisation had a number of interdependent IT systems that required access to Internet for data retrieval purposes. This reliance increased the complexity of providing security services to the organisation.

*Source: Analysis of secondary and interview data*

#### **4.9.4 Security Framework**

Using the framework defined and developed in chapter 2, this study's assessment of the information security position for Case G is shown in the diagram below.

The framework indicates that risks the organisation faces are adequately addressed. A number of strong management countermeasures have been implemented and the organisation is aware of the potential cost of system outages and attempts to mitigate the risks.

**Table 4-16 Information Security Framework Case G**

Research Issue 1 Reliance on IT		Research Issue 2			Research Issue 3 Australian Business as Targets	Research Issue 4 Countermeasures		Research Issue 5 Level of Security Expenditure			
		Threats		Incidents							
High reliance on integrated applications and networks.	-	Viruses	-	Viruses	-	Not a specific target but would make a good, i.e. A high pay off for effort.	-	Fulltime security manager.	+	Detailed security budget with linkage to threats and incidents.	+
Office automation.	-	Hackers (Port Scans)	-	Laptops thefts.	-	Target of opportunity	-	Managed security service provider who are security experts.	+	Spend \$1.2 to 1.5M annually.	+
Payroll and finance.	-	Insiders	-	Access abuse	-			Policies and standards.	+		
Data sources from the Internet and external networks.	-							Auditing	+		
ERP	-							Layered firewalls	+		
								Anti-viral protection	+		
								Disaster recovery	+		

(+) Factor has a positive impact on the organisation's security posture

(-) Factor has a negative impact on the organisation's security posture

Source: Analysis of secondary and interview data

#### 4.9.5 Summary and recommendations

The organisation's overall security posture was good. Whilst the organisation faced a variety of threats, they were able to identify and order information security risks and had implemented a comprehensive suite of countermeasures. They had a clearly identifiable security program with its own budget. Their actions, process, procedures and countermeasures were subject to both internal and external audit. The following recommendations are based on a comparison of the analysis of the current state of security in Case G with best practice as uncovered by the literature review (see chapter 2). If implemented the recommendations should significantly improve the organisation's security position:

- a. **Hardware theft.** The organisation should investigate improving hardware security – especially for laptop and desktop computers. Physical security mechanisms that could be considered include the use of security locks and the installation of video cameras in high risk areas.
- b. **Benchmarking.** Whilst the current security arrangements are robust its important for the organisation to continue a process of monitoring trends and the measures employed at other organisations. By benchmarking their security against trusted peers within the utilities industry the organisation can help ensure that it remains in a strong position. The additional benefit is that IT staff will be able keep the business informed by making direct comparisons with other like organisations.

#### 4.10 Case H – Small Sized Local Council

The Case H organisation is a local council with approximately 750 employees. They have a central office and a number of small site offices. One qualified IT professional was able to provide information for the research. The organisation could be best described as stereotypical of a small government agency in that it had a range of work activities that needed to be supported by a variety of information systems. This work ranged from manual labour such as road works and garbage removal to office administration and rates billing processes. The virtual interview and online survey techniques were used to obtain data from this organisation.

##### 4.10.1 Risks

###### Reliance on IT

Data from the virtual interviews and secondary data analysis were analysed to gain an understanding of the Case H's reliance on IT. Case H described itself as heavily dependent on IT.

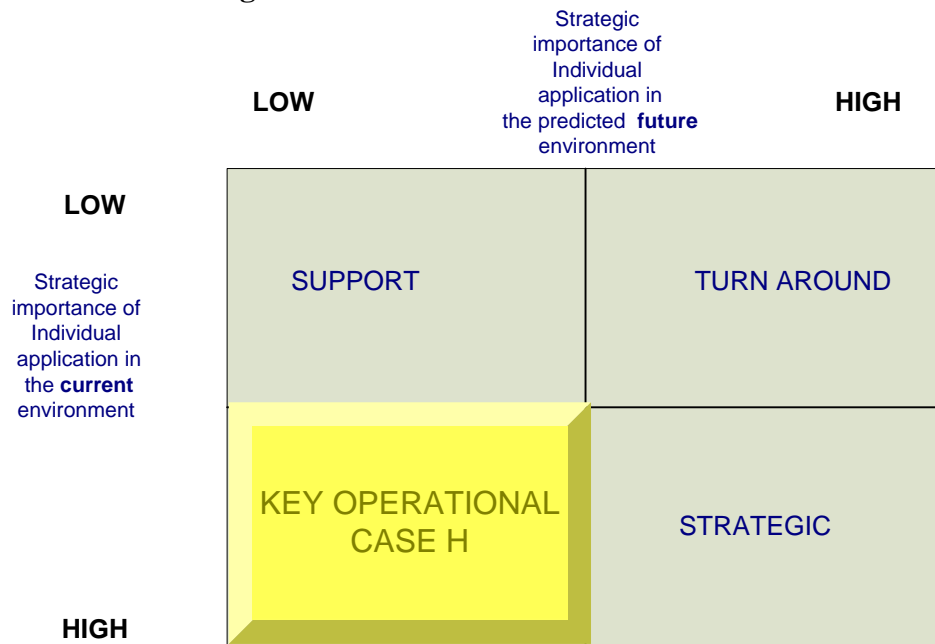
*'Our organisation has approximately 750 PCs distributed in 20 offices with the majority of staff (450) in our central office. We use 14 servers and link our remote sites using private networks. We are heavily dependent on IT and have been so for the past 20 years,*

*Major applications include business processing, office administration (MS office suite), e-mail, Intranet based applications and a few Internet based applications’ (H:1.20-4).*

This statement provides a comprehensive list of the users of IT within the organisation. The organisation’s reliance on IT can be further extrapolated by matching the number of staff to the number of computers. The one to one match of staff to computers could be considered somewhat surprising given that there are sections of the council that are manually labour intensive rather than office based.

Figure 4-9 below depicts the application of the McFarlan and McKenny Strategic Grid (McFarlan et al 1983) to the organisation’s IT. The integrated nature of the technology used in the organisation – and the reliance on distributed networks accessing central databases and file stores from central servers meant that many of the organisation’s services could not be effective without access to IT. IT was assessed as being *key operational* to the case, current IT is important but future developments in IT are unlikely to improve competitive advantage.

**Figure 4-9 Case H Strategic Grid**



Source: Analysis of interview and secondary data

**Threats**

The organisation identified viruses and the Internet as the main information security threats that it faced.

*‘In general we would be regarded as a low risk target. Not too many people are targeting the local council. However threats and attacks do take place’ (H:1.45-6).*

*‘Internet – we find our site is constantly probed for possible security flaws, generally with the intention of using these to conduct attacks on*

*other systems. Nimda is an example here. Viruses are a constant threat with approximately 20 infected e-mails arriving at our site per day' (H:1.46-50).*

The nature of the organisation brought about a unique form of risk. As an operator of public libraries the council also offers free public access to the Internet. This service could be used to expose the organisation to threats and also for would be hackers to launch attacks on other networks.

*'We provide public access to library users for catalogues and Internet use. This is a prime area for security threats and we have had people attempt to load password cracking software on the computers' (H:1.52-4).*

This threat potentially exposed the organisation on a number of fronts. Firstly it provides would be attackers an excellent platform for their activities; an outside job could then look like an inside job. Secondly there are potential legal liability issues that the organisation could face if their public access facilities were used to launch an attack on another organisation.

When asked to identify which threat was considered to the most significant the organisation nominated viruses.

*'The only one that appears to have been successful in the past has been one virus incident' (H:1.63-4).*

The organisation assessed its' threats through a number of sources.

*'Experience, research, and study. We monitor our systems to see what is happening. We talk to other organisations and software suppliers' (H:1.71-9).*

## **Incidents**

The organisation identified a number of incidents that had been encountered within the previous 12 months. Viruses, hacking, and hardware theft were specifically listed as reportable incidents.

*'The love letter virus. This occurred when virus signatures arrived too late due to a distribution server error. This incident took a day to clean up wasting significant resources. We have had the hacking attempts from the libraries as already mentioned. We have also lost around six PCs in the last 12 months from theft (break and enter)' (H:1.110-4).*

Viruses were identified as the most prevalent form of information security incident experienced by the organisation.

*'Most prevalent is virus attack occurring daily and if it succeeds then it can be disastrous. As more systems are exposed to the Internet,*



*attention will need to be placed on ensuring they are not compromised' (H:1.120-2).*

The organisation could not accurately estimate the cost of any losses.

*'Difficult. A virus incident such as love letter. Five IT staff for one day to tidy up. Loss of productivity from 400 staff (No e-mail, missed appointments etc) while the system is cleaned. We'd be talking about tens of thousands of dollars probably' (H:1.128-130).*

### **The business as a target**

The organisation could identify random firewall probes but did not believe that it was a specific target.

*'Not specifically, most sites are probed with port scans, viruses etc, however we had no hacker attacks. The closest thing we had was a security consultant using our site for some testing' (H:1.86-7).*

## **4.10.2 Management**

### **Countermeasures**

The organisation employed a modest arrangement of security countermeasures ranging from technical to policy-based countermeasures.

*'Security is considered in everything we do. Databases have appropriate security employed. Policies exist to ensure data integrity and cover disaster recovery. Investigations lead by the internal auditor drawing on IT resources as needed. Anti-virus software is deployed to all computers. It runs on the mail server doing real-time monitoring. Single Internet facing firewalls are used currently but this is being revised to provide a single perimeter and one internal firewall' (H:1.157-161).*

The policy and strategy based countermeasures are the corner stone of the organisation's response to the determined threat. The organisation had formulated a disaster recovery plan in the event of a serious compromise. There was however no evidence that the disaster recovery plan had recently been tested to determine its effectiveness.

The organisation emphasised the role of the external auditor who in effect 'kept the organisation honest' by reviewing security issues and recommending further technical investigations if required. This was theme was strongly emphasised in the organisation's response to the survey instrument.

### **Level of security expenditure**

The organisation did not provide evidence about the size of their information security budget. They were, however, capable of providing an estimate of the budget.

*'We spend in the vicinity of \$30 000 in a 12 month period' (H:1.171).*

#### 4.10.3 Differentiators

A number of potential differentiators were identified as part of the review of the organisation's information security posture.

**Table 4-17 Differentiators Case H**

Differentiator Number	Differentiator	Comments
1	Local government	The organisation was a local government and as such it provided a number of information services that could be exploited. The library service could be used to launch an attack on either the organisation's networks (e.g. viruses) or to launch hacking attacks on other organisations.
2	Use of external auditors	The organisation used external auditors as a key countermeasure and tool to ensure that organisational security policies were enforced. This was a positive way of ensuring that systems were appropriately maintained.
3	Disaster recovery	Although the organisation was relatively small it had developed a comprehensive disaster recovery plan that could be implemented in the event of a significant incident.
4	Small budget	The organisation stated that it had a small security budget and as such had to be creative in the manner in which it provided security. This included making some services unavailable, as funds were not available to provide the systems to adequately secure them.
5	Many remote sites	The organisation operated a number of remote work sites and depots. This potentially created a number of physical security problems. Computing hardware could be stolen from site offices for example.

*Source: Analysis of secondary and interview data*

#### 4.10.4 Security Framework

Using the framework defined and developed in chapter 2, this study's assessment of the information security position for Case H is shown in the diagram below.

Given the relatively small size of the organisation's IT department it was able to deploy a range of countermeasure to mitigate the information security risks to achieve a relatively balanced framework.

**Table 4-18 Information Security Framework Case H**

Research Issue 1 Reliance on IT	Research Issue 2		Research Issue 3 Australian Business as Targets	Research Issue 4 Countermeasures	Research Issue 5 Level of Security Expenditure
	Threats	Incidents			
Self assessed as heavily dependent on IT. -	Viruses -	Multiple virus incidents. -	Not a specific target, mainly seen as a target of opportunity. +	Database access security. +	Estimated at 30K per annum, which meant that the organisation had potentially deny some services.
Office automation. -	Internet – Site constantly probed for weakness and security flaws -	Hacking attacks, including use of internal resources to conduct attack. -		Policies and standards. +	
Some e-commerce and billing functions. -	Internal and potential outsider from within, e.g., library users on Internet. -	Laptop theft. -		Disaster recovery plans. +	
Customer or community information accessible through Internet. -				External auditing of information assets and policies. +	
Important document management – approvals, plans, regulations. -				Anti-virus, with real time monitoring on e-mail. +	
				Firewall. +	

(+) Factor has a positive impact on the organisation's security posture

(-) Factor has a negative impact on the organisation's security posture

Source: Analysis of secondary and interview data

#### 4.10.5 Summary and recommendations

The organisation's overall security posture was good. The organisation faced a variety of threats including some unique threats based on the Internet service that they offered to the general public. The organisation not only had to ensure that their own networks were secured from security threats but also had to ensure that their networks were not used by the general public to launch attacks on other organisations. The following recommendations are based on a comparison of the analysis of the current state of security in Case H with best practice as uncovered by the literature review (see chapter 2). If implemented the recommendations should significantly improve the organisation's security position:

- a. **Intrusion detection and prevention.** The organisation should investigate the implementation of intrusion detection and prevention systems. There was no evidence of a system that could monitor any security penetration that breached the organisation's firewalls.
- b. **System segregation.** The public access Internet facilities pose a number of threats to the organisation. Currently there is some connectivity between the organisation's networks and the systems offered to the general public for Internet access. It is recommended that the public Internet access be provided on standalone computing systems – not connected to organisation's normal computing networks. This will significantly reduce the risk of potential incidents being launched from these facilities.

#### 4.11 Case I – Small sized State Government Department

The Case I organisation was a small State government department with approximately 900 staff. IT operated a number of regional and international offices that provided a presence for the organisation to conduct its core business. The small nature of the organisation meant that in a number of instances it shared resources and components of IT infrastructure with other organisations. Two senior IT professionals took part in the interviews.

##### 4.11.1 Risks

###### Reliance on IT

The Case I organisation's core business involved the distribution and dissemination of information and services across regional and international boundaries. It was therefore not surprising that the organisation deemed itself to be highly reliant on IT.

*'The Department is a distributed environment. We have 18 regional offices located around the state and 10 international offices. There are approximately 500 – 600 staff employed within the central business district itself. The network is large and it is shared with*

*another state government department. They have approximately 800 people and have a similar number of regional offices although they have no international offices' (I:1.20-6).*

*'(We have) a high reliance on IT, both internally for office automation, and externally to the department itself. Internal IT is shared and maintained by another department' (I:2.20-5).*

The degree of reliance on IT by the organisation can be seen in its statement about how the organisation would function if the supporting IT was to fail.

*'The whole organisation is structured around the IT infrastructure and if the infrastructure doesn't work then nothing gets done. I could use a recent example when we had a fire in the south of Brisbane that cut the electricity. The building went down and we had to wait for the generators because when it came up it blew a circuit and what happened was that systems in one of our buildings were down for half a day and what it meant was that no one could do any work and basically we gave them the option to go home or do filing. If the system doesn't work then the organisation doesn't work because it can't access its files and records and the records management system is paper based but it is indexed electronically. So no access to the computer screen and there are no manual processes' (I:1.49-60).*

Further evidence of the organisation's reliance on IT can be seen in the organisation's dependence on ERP and e-commerce based applications.

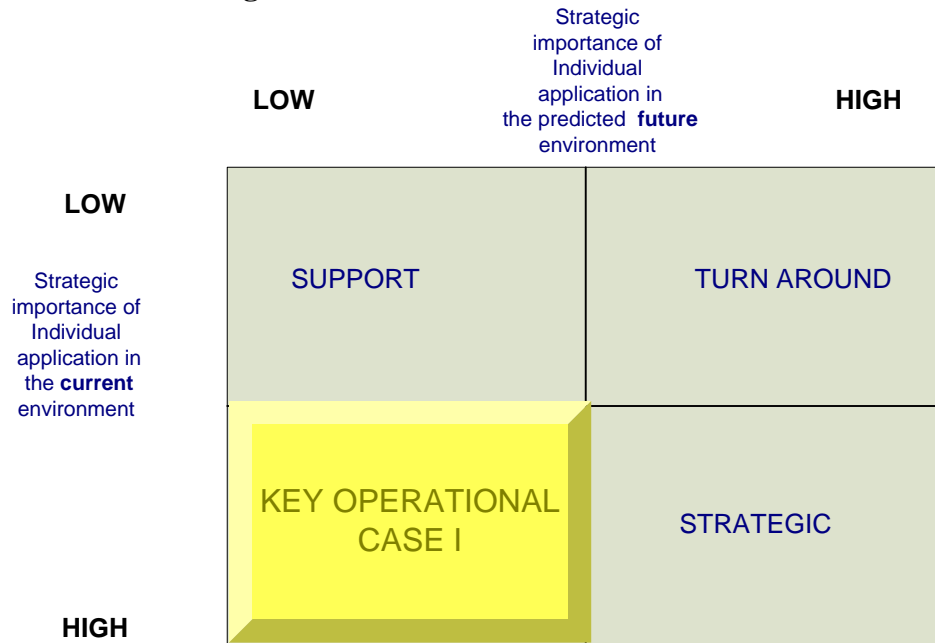
*'The organisation runs three major ERP packages. They being SAP for financials, HR which is Aurion we a business package called Organisation Online, it comprises three components. There is a CRM component, which is Applix, which is all the workflow and history of all of the department's clients. There is a component called Smart Licence that allows for business licenses to be obtained online. The third component is called virtual campus that is actually an online learning facility' (I:1.34-45).*

*'E-commerce is more like e-Government, with a focus on providing information and advice to the department's clients – mainly the State's business community' (I:2.27-9).*

The survey results provided by the organisation further confirmed its dependence on IT and the resulting interdependent nature of applications and infrastructure. The organisation provided an extensive amount of information to support the interview data.

Figure 4-10 below depicts the application of the McFarlan and McKenny Strategic Grid (McFarlan et al 1983) to the organisation's IT. The organisation's stated reliance on the current IT infrastructure coupled with the fact that future developments were unlikely to improve competitive advantage led to an the conclusion that IT was *key operational*.

**Figure 4-10 Case I Strategic Grid**



Source: Analysis of interview and secondary data

**Threats**

The organisation was able to identify a number of threats that could potentially impact on the normal operation of their IT.

*‘Threats originate mainly from internal leaks of confidential information – commercial-in-confidence or cabinet-in-confidence’ (I:2.55-7).*

A more comprehensive listing and analysis of the potential threats was provided by the other respondent.

*‘We have four threats:*

- 1. The internal threat of the dissatisfied user.*
- 2. External threat from someone who will try and write a virus and try and infect the system.*
- 3. The natural disaster threat, that’s beyond our control.*
- 4. Because we operate internationally people who live there are also a potential threat.*

*These threats determine how we structure to operate the IT environment’ (I:95-102).*

The respondents differed in their analysis regarding which particular threat was the most significant that the organisation faced.

*‘Anything that makes the newspaper or is raised in parliament: leaked documents or deleted websites’ (I:2.73-4).*

*'The one that is giving us the most trouble is viruses. I would put the risks in order of viruses first, natural disaster second, internal and international equal third. They are low risk' (I:1.114-6).*

The organisation was aware of the security threats through a comprehensive risk analysis process. The requirement for business continuity planning directs this analysis within the organisation.

*'As part of the organisation's tasks we are actually responsible to do the business continuity plan, and as part of the business continuity plan we do a risk assessment. With regard to network vulnerabilities. Internally we do our reviews. We believe that the only way we will know what is really going on is to go and ask ourselves. With regard to viruses and hacking we engage third parties' (I:1.126-35).*

The other respondent from the organisation put his knowledge of the organisation's threats down to more simple mechanisms.

*'Experience' (I:2.85).*

### **Incidents**

The organisation described a variety of security incidents that it had encountered over the previous 12 months. Viruses received the most coverage when the organisation discussed the threats that it faced. It was therefore not surprising to see that theme continue when the interview topic turned to incidents.

*'Nimda virus – got through to five or so PCs before it was stopped. Code Red defaced one web site' (I:2.122-3).*

*'Code red virus. The department's website is hosted externally by [a provider]. What happened was that our web development people actually managed that server and even though they had received the warnings to update the service packs on that server for code red but they hadn't done it so when code red was released it affected that server by dropping it off the air. The other one was the Nimda virus, with that one it actually got inside our system. As soon as that happened we cut all external links out to the rest of the world and eradicated the virus and rebuilt the system and then re-opened up the systems' (I:1.193-8).*

Theft of computing assets was also a problem for the organization.

*'Theft is an issue, mainly from an external point of view. We have had instances of people breaking into buildings and stealing laptops, in the last six months we have lost two, in the last 12 months there was something like 78 reported incidents of thefts of laptops in the city CBD' (I:1.203-6).*

The respondents differed in their assessment of what they believed to be the most prevalent or significant incidents that had occurred to the organization.

*'Viruses are the most prevalent. We do updates frequently. Because we have problems getting people to log on and off, we had to write a script to get machines to log out, automatically. Automatic updates are occurring' (I:1.217-9).*

*'Information leaked – public embarrassment' (I:2.138).*

The organization found it difficult to estimate the monetary loss that resulted from security incidents from the security incidents.

*'Don't put a monetary value on it. We have lost probably two weeks over the last financial year' (I:1.225-6).*

*'Laptops - \$3000 each. Leak of information no dollar value, but conversely has the most impact on the organisation' (I:2.141-2).*

### **The business as a target**

The organisation believed that they were not a specific target for any particular group. Rather the organisation felt it was either part of the global target base or a target of convenience.

*'No evidence of that (being targeted). We run our own packages to actually check for that. Historically, it's mainly university students trying out what they have learnt. Looking at firewall logs every University in Australia is represented there. There is a lot of SPAM activity that comes up against the firewall, but there has been no evidence of any specific attacks, other than – let's visit and see what we can do and once they realise that it's a firewall on the front they tend to go away' (I:1.155-60).*

*'Not so much targeted from external attacks (e.g. mass virus, web site defacement) these seem to just be a part of a mass attack. Internal attacks from staff (disclosure of information) may be targeted due to information held' (I:2.92-6).*

## **4.11.2 Management**

### **Countermeasures**

The organisation employed a comprehensive range of countermeasures to combat the identified threat. At the core of the organisation's security posture was the State Government's mandated security policy, Information Standard 18.

*'The Queensland Government has a significant information security standard, called Information Standard 18, it is available on the web*



*it's a generic document that each department has to apply. In some cases it is specific, and other places it is generic' (I:1.253-5).*

*'Whole of government mandatory security policy based upon AS/NZ 7799' (I:2.174).*

The organisation also indicated a significant number of other technical and policy based countermeasures.

*'We use the following:*

- *Passwords.*
- *User accounts.*
- *Specific approvals for remote access.*
- *Policies.*
- *Firewalls, DMZ, Covered circuits (VPN).*
- *Closed networks, that they are compartmentalised.*
- *Physical security.*
- *Backup and offsite storage.*
- *Specific security areas that are discrete and not accessible.*
- *Anti-viral software.*
- *Clearances for contractors, security clauses put into staff contracts.*
- *Firewall logs.*
- *Third party auditors to review the system and checks.*
- *Staff training.*
- *Security advisors.*
- *Configuration control.*
- *Risk management used to determine how we do.*
- *Disaster Recovery Plan (Separate Facility)*
- *We have a database of security incidents.*
- *We have a security professional and he can do investigations.*
- *We run security applications.*
- *Physical systems are located in all our buildings, buildings have closed circuit TV (CCTV)' (I:2.257-82).*

The completeness and the conciseness of this response indicated that this organisation had put a significant amount of time into information security.

### **Level of Security Expenditure**

The organisation was able to produce accurate information regarding the level of security expenditure. This information was supported by documentary evidence.

*'It's on going investment. Security is a cost of doing business these days. We have a facilities management contract, which covers all services and expenditure. We would spend about 50k – 100k per annum for software, probably all up over 200k per year' (I:1.287 – 91).*

### 4.11.3 Differentiators

A number of potential differentiators were identified as potential influencing factors in determining the organisation's security posture.

**Table 4-19 Differentiators Case I**

Differentiator Number	Differentiator	Comments
1	Mandated security policy from State Government.	As a State government department this organisation was required to adhere to the State's information standards. These standards were derived from national and international information security standards. These policies directly influenced the manner in which information security was managed within the organisation.
2	Organisation has international offices.	The organisation operated a number of small international offices. This direct exposure to foreign intelligence gathering organisations increased the risk the organisation faces.
3	Facilities management agreement with other agency	The organisation essentially sub-contracted its infrastructure support to another government department. This arrangement meant that some security issues and the day-to-day management of incidents were at arms length to the organisation.
4	Focus on physical security	The organisation had a high integration with physical security and information security. Access control to systems hardware and infrastructure was tightly controlled including the use of CCTV to ensure that unauthorised use of systems was minimised.
5	Importance of information to the organisation	Information was seen as a key asset to the organisation and as such the organisation adopted a proactive approach to managing information assets.
6	High level of security knowledge	The respondents for the organisation presented very polished and knowledgeable responses to the interview questions. Source data for the questions were readily available.

*Source: Analysis of secondary and interview data*

#### **4.11.4 Security Framework**

Using the framework defined and developed in chapter 2, this study's assessment of the information security position for Case I is shown in the diagram below.

The framework indicates that the organisation had a good understanding of the risks and more importantly could link the risks to appropriate countermeasures to mitigate the risks.

**Table 4-20 Information Security Framework Case I**

Research Issue 1 Reliance on IT		Research Issue 2		Research Issue 3 Australian Business as Targets		Research Issue 4 Countermeasures		Research Issue 5 Level of Security Expenditure			
		Threats	Incidents								
Self assessed as highly reliant.	-	Internal threat (System users)	-	Several virus problems.	-	No evidence of direct targeting.	+	Linkage between threats and incidents.	+	Security expenditure in vicinity of 200K.	+
Shared information resources with other organisations.	-	Viruses.	-	Theft of computing assets.	-	Perhaps from university students refining their skills.	-	Emphasis on physical security including video surveillance.	+	Some costs hidden by facilities management agreement.	-
When the IT doesn't work the staff go home	-	Natural disaster (physical threat).	-	Information leakage.	-			Implementation of standards and policies that are then audited.	+		
ERP and e-commerce focus for information tools.	-	Foreign entity threat.	-					Risk management	+		
ERP.	-							Security professionals employed.	+		

(+) Factor has a positive impact on the organisation's security posture

(-) Factor has a negative impact on the organisation's security posture

Source: Analysis of secondary and interview data

#### 4.11.5 Summary and recommendations

The organisation's overall security posture was very good. The organisation had conducted comprehensive risk assessment exercises and had implemented appropriate countermeasures to mitigate the identified risks. Their facilities management contract did complicate their security environment to some degree, however, the organisation implemented proactive steps to ensure its service provider met or exceeded its' expectations. The following recommendations are based on a comparison of the analysis of the current state of security in Case I with best practice as uncovered by the literature review (see chapter 2). If implemented the recommendations should significantly improve the organisation's security position:

- a. **Benchmarking.** Whilst the current security arrangements are very good the organisation should implement a process of monitoring trends and the measures employed at other organisations. By benchmarking their security against trusted peers within the utilities industry the organisation can help ensure that it remains in a strong position. The additional benefit is that IT staff will be able keep the business informed by making direct comparisons with other like organisations.
- b. **Audit and investigation.** As the organisation is involved in a facilities management arrangement an independent, external audit is recommended. This audit and investigation should include a review of the policies and procedures of the service provider. Security penetration testing should also be a priority to prove the robustness of the any security countermeasures employed. Once established the audit program should be undertaken regularly.

#### 4.12 Case J – Large State Government Department

The Case J organisation is a large sized State Government agency employing around 7500 staff. They have offices throughout the State of varying size that access central information systems. The department operates a number of interdependent relationships with other State government departments in either a service provider or client role.

In instances where the department operates as a service provider, it provides access to the organisation's databases, primarily providing another department with end customer details. These relationships highlight the importance of information and information systems to the organisation.

Two senior IT professionals were chosen by the organisation to take part in the interviews.

#### 4.12.1 Risks

##### Reliance on IT

The Case J organisation's core business involved recording qualifications and certifications for a large proportion of the state's population: The organisation shares its clients information with a number of other organisations by providing controlled access to the organisation's databases. The Department describes itself as heavily reliant on IT.

*'The Department's Information Services Branch provides IT Services to the Department and one other major government department. Both departments have a heavy reliance on IT for service delivery to our customers and for internal business processes' (J:1.20-2).*

*'We are highly reliant on IT. The main sources of reliance are key enterprise applications, communications, information sharing across a widely distributed organisation and desktop productivity (probably in that order of importance). Without our key enterprise application, we should probably be out of business in days' (J:2.20-23).*

The Department's information systems support essential applications, third party organisations and large numbers of customers.

*'The enterprise network has approximately 6500 users across 150 sites geographically dispersed throughout the State. There are many B2B exchanges and these are continuing to increase. E-Commerce activities are not extensive at this stage however this is now becoming a focus via emerging electronic service delivery and will continue to evolve. The department has an extensive Intranet with many different systems. Novell – File/Print, Lotus –Mail/Workgroup databases, Lotus Domino – Websites, Tn3270 – Mainframe access, SAP for financials and many Oracle databases' (J:1.30-5).*

*'There are a number of e-commerce systems in place and a number projects underway, E-commerce will become increasingly important. Although there is minimal transaction/order processing currently, we are developing an online payment service to accept projects and future applications. This environment is reasonably complex and includes web front ends, Borland Application Server middleware (Java Beans), and back end applications such as TRAILS which runs on a mainframe' (J:29-35).*

The organisation's reliance on IT is further highlighted by the interviewees' responses to the question regarding what happens when the IT doesn't work.

*‘What happens when the IT doesn’t work? – This is a broad question. If we take one example – our customer service centres most critical application is used for interaction with the general public – in the event of loss of this system the users utilise a local offline processing system (access database) on a file server which batches transactions up when connectivity is restored. In the event of total IT loss at the customer support centre there is a certain amount of transactions that can be still be performed via paper based transactioning’ (J:2.37-43).*

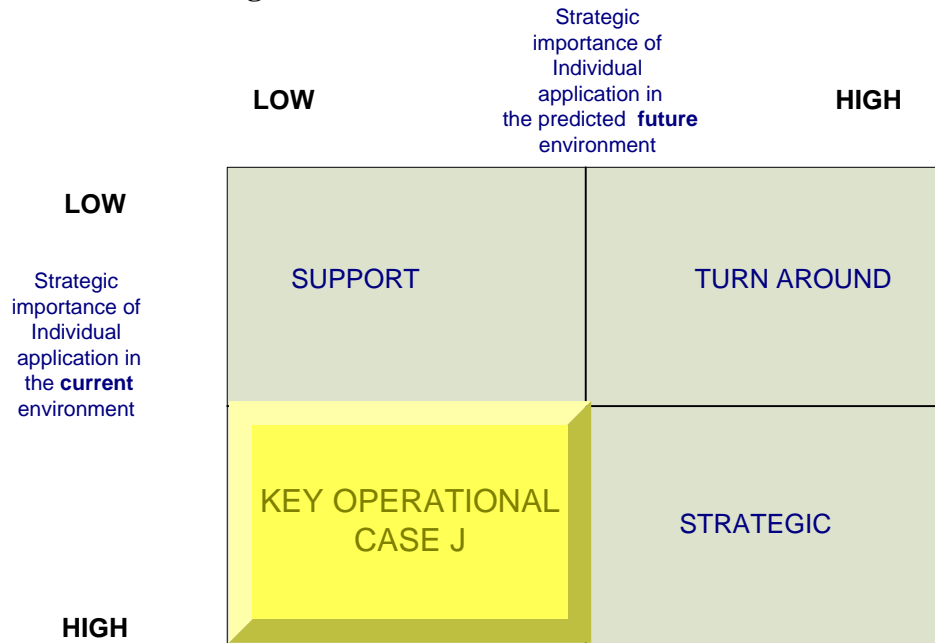
*‘In case of problems with IT, we have a number of levels of support ranging from helpdesk from level 1 support through to technical experts in the relevant operational areas for more detailed assistance. The prime focus of these support arrangements is to restore normal services as quickly as possible. This is important due to the heavy reliance on automated systems’ (J:2.41-4).*

A review of the organisation’s system documentation provided a comprehensive list of the applications maintained. The organisation had a large Internet site, which provides information to the public.

The survey data provided by the interview respondents supported the data provided during the interviews and the secondary data provided by the respondents. In particular the survey data highlighted the interdependent nature of applications and the interconnection of infrastructure between other government agencies. This data confirmed the organisation’s heavy reliance on IT and the reliance of other organisations on the department’s computing assets.

Figure 4-11 below depicts the application of the McFarlan and McKenny Strategic Grid (McFarlan et al 1983) to the organisation’s IT. The organisation is highly reliant on its central databases, the support IT infrastructure and the connectivity between other departments. IT was assessed as being **key operational** to the organisation as current IT is important to the organisation but future developments are unlikely to improve the competitive advantage.

**Figure 4-11 Case J Strategic Grid**



Source: Analysis of interview and secondary data

**Threats**

The organisation presented documentary evidence of a series of risk assessments that had been conducted in order to determine what threats the organisation faced, A review of the documentation revealed that there was an emphasis on establishing evidence of threats as well as perceived threats; there was an attempt to link the threats to incidents.

*‘Generally, I don’t think that we are the specific target of organised external hackers or groups. I see the main risk coming from users, introducing Trojans through e-mail, instant messaging, unauthorised modems – mostly education issues and of course the ever present threat of viruses and worms. However, there is still a risk from external hackers taking advantage of any vulnerabilities that may exist in our infrastructure’ (J:2.66-70).*

*‘Hackers, viruses and system users are all possible sources of threats to our organisations. I would not consider foreign governments a threat or competitors as we don’t really have any competitors as a state government department’ (J:1.68-71).*

Both respondents agreed that virus related threats were the most significant threats faced by the organisation. The threat of Trojans combined with access gained through system privileges of internal system users.

*‘I would consider viruses and system users to be the greatest risk. We have extensive virus monitoring in place but because viruses are constantly evolving you can potentially be affected before a patch is deployed. Viruses can be carried inside our flows (e.g. HTTP port 80)*



*that are otherwise allowed making them all the more dangerous....system users are only a risk because of the trusted nature of these individuals, and they are generally empowered to access information' (J:1.76-81).*

*'I think the most immediate danger is if an internal user opens up a security hole (via a Trojan of some kind) through our firewall and other defences. Some of these Trojans can be hard to stop and they basically nullify your perimeter defences. Also, education of users can be difficult and time consuming' (J:2.80-3).*

The organisation had calculated the threats that it faced through a number of sources including risk assessments, experience of practitioners and personal research.

*'We have experienced all of these security issues that I've discussed to some extent. Also by monitoring notification services such as CERT and BugTraq, it is possible to see trends' (J:2.93-6).*

*'(I have learnt about these threats from) experience, research, seminars' (J:1.91).*

## **Incidents**

The respondents described several recent security incidents that had had some form of impact upon the operation of IT within the business. As the organisation indicated that viruses were its most significant threat it was not surprising that most of the incidents reported by the organisation were viruses.

*'Many viruses affect systems like Microsoft Outlook/Exchange which we do not use, so I suppose we have been protected somewhat by the lack of using these systems, We did get a couple of instances of Nimda, however these were quickly isolated' (J:2.128-130).*

*'I've only been in this position for about three months, however I believe that we have recently had problems with viruses/worms and inappropriate downloads by users. I'm not aware of any recent hacking/unauthorised access incidents. I do know that a recent virus/worm outbreak, Nimda I think caused a lot of problems and took a significant amount to clean up' (J:2.127-132).*

The respondents indicated that no particular threat was particularly prevalent however they believed that the incidents of viruses were the most significant.

*'I think the virus/worm scenario is most significant as users are the hardest part of the equation to control. These, also seem to be the most common day-to-day' (J:2.138-9).*

*'I do not consider any of these to be prevalent – although you don't know what you don't know! I would consider currently viruses to be*

*our biggest risk, however as the department increases its e-business activities with the external public then hacking attempts will become an area requiring even more vigilance' (J:1.139-42).*

The business was unable to estimate the value of any losses that could be attributed to security related incidents.

#### **The business as a target**

The organisation believed that there was some potential for it to be targeted.

*'I suppose we run the risk of particular issues/political decisions making us a potential target for dissatisfied communities however I doubt that generally speaking the department is a high priority target amongst the hacker community as I feel there are more interesting targets out there....Needless to say this information is not for open consumption – hackers may see this as a challenge' (J:1.98-102).*

*'At this point of time, I don't believe we are being targeted' (J:2.103).*

#### **4.12.2 Management**

##### **Countermeasures**

The organisation as a State Government Department was required to adhere to the state's information security standards.

*'We have a project underway to implement Qld Government Information Standard 18 – based on ISO 17799. This implementation a formal information security management framework and associated policies, standards and procedures. We do have policies and procedures currently in place covering major security issues (Passwords, Internet use, viruses, etc) although these will be overhauled as part of the project' (J:2.172-8).*

*'We have a range of policies in place. The Department has a project in place pursuing compliance with IS18' (J:1.104-5).*

The organisation had recently created an enterprise security manager role in order to better coordinate security matters.

*'We now have a specific security position (me) to ensure security is appropriately addressed' (J:1.180-1).*

*'We have an enterprise security manager and security expertise in functional areas, networks and servers and such' (J:1.180-1).*

The organisation employed a range of policy, procedures, and technical countermeasures.

*'We subscribe to AusCERT. We have firewalls, virus/e-mail scanning, two factor authentication for remote access, we will be shortly implementing IDS. We have a range of policies in place, for example, user responsibilities, Internet access, remote access' (J:1.175-9).*

*'We have a standard technical controls in place such as virus scanning, firewalls, monitoring, although I plan to review this architecture to ensure that it is appropriate. I monitor CERT and BugTraq for new vulnerabilities. I plan to have an external organisation perform a security review each year to ensure we maintain a robust security environment' (J:2.183-9).*

### **Level of security expenditure**

Due to the limited time that the respondents had spent in the organisation they were unable to estimate the organisations level of security expenditure.

*'I haven't been here long enough to be able to give an accurate answer. Plus it is hard to come up with a figure – what do you include?' (J:2.194-5).*

### 4.12.3 Differentiators

A number of potential differentiators were identified during the review of the organisation's security posture:

**Table 4-21 Differentiators Case J**

Differentiator Number	Differentiator	Comments
1	Large customer base	The organisation has an extremely large customer base, in excess of 3 million people. This creates strains on infrastructure, data storage, transmission and integrity. The security of the data becomes more complex with the more transactions and interactions required with the customer base.
2	Interdependent relationships with other departments	The organisation needs to make its data available for both read and write access to other government departments over multiple sites. This creates an information integrity and assurance challenge for the organisation.
3	Service provider relationship	In some instances the organisation operates as a service provider to other organisations. This creates at times unique security restraints and conflicts on the organisation.
4	Mandated security policy from the state government	As a State Government Department the organisation was required to implement certain government standards in relation to information and security.
5	Size	The organisation is large with a large amount of staff interacting frequently with organisational information systems. This makes issues such as access control and system access more difficult.
6	Public profile	The organisation has a significant public profile with data that is both sensitive and of interest to a wide variety of parties.

*Source: Analysis of secondary and interview data*

### 4.12.4 Security Framework

Using the framework defined and developed in chapter 2, this study's assessment of the information security position for Case J is shown in the diagram below. The framework illustrates a relatively balanced risk versus threat posture. The

organisation has identified key threats to the organisation and has instigated a number of countermeasures in an attempt to mitigate the risk.

**Table 4-22 Information Security Framework Case J**

Research Issue 1 Reliance on IT	Research Issue 2				Research Issue 3 Australian Business as Targets	Research Issue 4 Countermeasures	Research Issue 5 Level of Security Expenditure				
	Threats		Incidents								
Self assessed as highly reliant on IT.	-	Main risk is from users (introducing Trojans through e-mail, instant messaging)	-	Small incidents of viruses.	-	Not seen as a major threat although the organisation could be seen as a high payoff target.	+	Selection of Lotus Notes for e-mail rather than Exchange.	+	Data from the organisation was not available.	+
Large distributed customer database that is essential for business.	-	Viruses and worms.	-	Some user access abuse.				Implementation of standards.	+		
Interdependent information with other organisations	-	Hackers.	-					Corporate policies and procedures.	+		
ERP	-							Creation of an enterprise security manager.	+		
Emerging electronic delivery.	-							Firewalls.	+		
								AusCERT	+		

(+) Factor has a positive impact on the organisation's security posture

(-) Factor has a negative impact on the organisation's security posture

Source: Analysis of secondary and interview data

#### 4.12.5 Summary and recommendations

The organisation's overall security posture was very good. The organisation had conducted comprehensive risk assessment exercises and had implemented appropriate countermeasures to mitigate the identified risks. The interdependent relationships with other organisations did complicate their security environment to some degree – especially in regards to the sharing of sensitive data, however, the organisation implemented proactive steps to ensure the systems remained secure. The following recommendations are based on a comparison of the analysis of the current state of security in Case J with best practice as uncovered by the literature review (see chapter 2). If implemented the recommendations should significantly improve the organisation's security position:

- a. **Benchmarking.** Whilst the current security arrangements are very good the organisation should implement a process of monitoring trends and the measures employed at other organisations. By benchmarking their security against trusted peers within the utilities industry the organisation can help ensure that it remains in a strong position. The additional benefit is that IT staff will be able keep the business informed by making direct comparisons with other like organisations.
  
- c. **Audit and investigation.** As the organisation is involved in a facilities management arrangement an independent, external audit is recommended. This audit and investigation should include a review of the policies and procedures of the service provider. Security penetration testing should also be a priority to prove the robustness of the any security countermeasures employed. Once established the audit program should be undertaken regularly.

Having completed the analysis of each of the ten cases the next section presents the findings of the cross-case analysis from which conclusions are drawn for each of the three research questions.

#### 4.13 Cross – case analysis

This section documents the results of the cross-case analysis for this research. A summary of each of the disciplines, as defined in the literature review are presented. The conclusions about risks and management are drawn from the themes that emerged from the within case analysis and therefore quotations to support these findings have not been repeated.

##### 4.13.1 Risks – Reliance on IT

This section discusses the conclusions regarding the research issues that address the risk component of the research problem. A broad cross-section of risks were identified for each of the ten organisations that participated in this research.

The major risks that emerged from the ten organisations in relation to their reliance on IT are summarised in table 4-23. Most of the risks re-occurred in two or more cases, therefore demonstrating literal replication logic (Yin 1994) (See chapter 3 section 3.2.2).

In summary, in eight of the ten organisations there were a group of core functions that relied upon IT. This indicated that the organisations themselves were at the very least reliant on IT, as the interruption of these functions would adversely impact the conduct of business operations.

Eight of the ten organisations were able to demonstrate the linkage between their reliance on IT and the impact of the loss of IT on services. It was apparent that not only did the organisation's specific use of IT help determine the business impacts of the loss of IT, it also determined the amount of exposure to security risks that the organisation faced.



**Table 4-23 Indicators of Risk – Reliance on IT**

Indicator	Cases									
	A	B	C	D	E	F	G	H	I	J
Office automation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Financials	✓				✓	✓	✓		✓	✓
Low reliance	✓									
Payroll processing		✓	✓			✓	✓		✓	✓
Intranet		✓	✓		✓	✓	✓		✓	✓
Document management		✓	✓			✓		✓	✓	✓
Integration of telephone systems		✓								
Logistics tracking		✓	✓							
Internet		✓		✓	✓	✓	✓	✓	✓	✓
Very high reliance on IT		✓	✓		✓	✓				
Information a key resource			✓							✓
Connection to business partners			✓							✓
Customer ordering				✓						
Workflow				✓						
Billing and customer accounts				✓				✓		
High reliance on IT				✓			✓	✓	✓	✓
Used to develop company product					✓					
Business not capable of working without IT					✓				✓	
Used in preference to face to face comms					✓					
Reliance on IT outsourcing arrangement						✓				
ERP							✓		✓	✓
Direct community access to systems								✓		

✓ Shows the cases from which the indicator for risk emerged – as assessed by the organisation.

*Source: analysis of within-case analysis (all cases)*

**4.13.2 Risks - Threats**

This next section presents the perceived threats that each of the ten cases believed they faced. The threats that emerged are summarised in table 4-24. Approximately half of the themes emerged in more than one case demonstrating literal replication. Of the threats where literal replication was not demonstrated it could be expected that the threats may have been present in the other organisations but were either not identified or were perhaps considered not important enough to mention. For example, a threat that was identified only by the Case I organisation that would clearly be applicable to most of the other cases is that of natural disaster. An earthquake, fire or flood could cause a serious disruption to the provision of reliable IT services. This could occur indirectly, such in the case of widespread power blackouts. These types

of circumstances are typically considered as part of Business Continuity Planning (BCP) rather than information security per se.

**Table 4-24 Risks – Threats**

Threat	Cases									
	A	B	C	D	E	F	G	H	I	J
Viruses	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hackers	✓	✓	✓		✓	✓	✓	✓		✓
Port scans	✓						✓	✓		
System users	✓	✓	✓	✓			✓	✓	✓	✓
Organised group of hackers		✓	✓		✓					
Foreign governments		✓	✓						✓	
Complacency			✓							
Close integration of key applications				✓						
Staff turn over				✓						
Poor quality code					✓					
Issue motivated groups					✓					
Competitors					✓					
Outsider from within (Library access)								✓		
Natural disaster (earthquake, flood, fires)									✓	

✓ Shows the cases from which the theme for risk emerged

Source: analysis of within-case analysis (all cases)

In summary three threats were identified by eight of the ten participating organisations. Hackers, viruses and system users were seen as the major threats faced by each organisation. As discussed earlier in the within-case analysis, organisations used a variety of methods, including formal risk assessments to identify the threats that were relevant to their businesses.

**4.13.3 Risks – Incidents**

This section presents data discovered regarding the actual information security incidents experienced by the ten case participants. The incidents that emerged are summarised in table 4-25. Only three of the incidents did not appear in more than one case, therefore demonstrating a high degree of literal replication among the other incidents.

**Table 4-25 Risk – Incidents**

Incident	Cases									
	A	B	C	D	E	F	G	H	I	J
Port scans	✓	✓			✓					
Viruses	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
System privilege abuse - users	✓	✓	✓	✓			✓			✓
Chain e-mails/SPAM		✓	✓							

Contractors abusing system privileges		✓	✓							
Hardware theft (e.g.Laptops)		✓	✓	✓	✓		✓	✓	✓	
Hacking			✓	✓				✓		
Data destruction			✓							
Attacks from automated scripting tools					✓					
Information leakage									✓	

✓ Shows the cases from which the theme for risk emerged

Source: analysis of within-case analysis (all cases)

In summary, there were three types of incidents that were relevant across most organisations, namely; viruses (all organisations) , hardware theft (seven of ten) , and system access abuse by system users (six of ten). These results explain why most of the case organisations listed viruses as the key threat to the security of their systems; they actually experienced virus attacks more often any other security incident. Relatively few organisations reported incidents of hacker attacks despite several of the cases listing hackers as a credible threat to their business. At least two different conclusions can be drawn from this point. Firstly, the threat is not as significant as suggested by much of the literature (see chapter 2); or the countermeasures that each organisation puts in place effectively reduces the number of incidents.

#### 4.13.4 Risks - Australian business as targets

This section summarises the responses of the case organisations regarding the likelihood of them being specifically targeted by would be attackers. The results for each of the ten cases is summarised in table 4-26.

**Table 4-26 Risk – The business as a target**

Security Risk	Cases									
	A	B	C	D	E	F	G	H	I	J
Believed they are a target	✓	✓	✓			✓				
Believed they were not a target				✓	✓		✓	✓	✓	✓

✓ Shows the cases from which the theme for risk.

Source: analysis of within-case analysis (all cases)

As shown, two more organisations believed that they were not at risk (six), as specific targets than those (four) who believed they were subjected to dedicated targeting from attackers. It is important to emphasise that these results are based on the organisations perceptions or views, and in fact an organisation could be targeted and not know it. For example, a number of the cases believed that at most they would be considered targets of opportunity. If they were to not consistently employ countermeasures to reduce the general risk then security incidents could occur. This point of view is not always supportable based on the researcher’s analysis of the cases. An organisation could be a specific target for any number of reasons.

#### **4.13.5 Management – Countermeasures**

This next section presents the countermeasures discovered in relation to the countermeasures that were employed by each of the case organisations. The results for each of the ten cases are summarised in table 4-27

The organisations responses regarding the countermeasures that they employed displayed a high degree of literal replication. Only five of the twenty countermeasures mentioned were adopted by a single case. The table and the responses illustrate that all organisations rely on anti-viral software and seven of the ten organisations employ security policies and firewalls to protect their systems.

However, there were only a five of ten instances of organisations specifically matched the countermeasures that they employed with the perceived threats and incidents. This essentially demonstrates the lack of effective risk management and risk analysis that is undertaken to define the threat and then systematically counter that threat through the thoughtful application of policies and technology.

**Table 4-27 Management - countermeasures**

Security Countermeasure	Cases									
	A	B	C	D	E	F	G	H	I	J
Freeware security tools	✓									
Anti-viral software	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Software firewalls	✓			✓				✓		
Security policies	·	✓	✓		✓	✓	✓		✓	✓
Procedures and work instructions for the use of IT		✓	✓			✓	✓			✓
Automated patch management of virus definitions		✓	✓		✓					
Hardware firewalls		✓	✓		✓	✓	✓	✓	✓	✓
System access controls		✓	✓		✓	✓	✓	✓	✓	✓
Capacity planning		✓								
Disaster recovery plans		✓	✓				✓	✓	✓	✓
Reporting of incidents		✓	✓							
Internal CERT capability			✓							
Software patch management					✓					
Security service provider						✓	✓			
Full-time security manager		✓	✓				✓			✓
Security auditing							✓	✓	✓	
Linkage between threat and incidents identified		✓	✓						✓	
Physical security		✓	✓						✓	
Lotus Notes instead of Microsoft Exchange										✓
AusCERT subscription										✓

✓ Shows the cases from which the theme for management  
*Source: analysis of within-case analysis (all cases)*

#### 4.13.6 Management – Level of security budget

This section summarises the responses briefly presents the responses regarding security budgets. The responses are summarised in table 4-28. In four of the ten organisations either no information or limited information was available from the cases regarding their security budget. Due to limited information about budgets it was deemed to be more informative to report on those organisations where a dedicated and separate security budget was in existence, rather than reporting on the actual amount of each budget as this information was either unknown, too sensitive, or was highly variable for any number of reasons.

**Table 4-28 Level of Security Budget – Security Budget**

Element of Management	Security Budget	Cases									
		A	B	C	D	E	F	G	H	I	J
Does the case have a	Identifiable security budget		✓	✓		✓		✓	✓	✓	

separate security budget?	No identifiable security budget	✓			✓		✓				✓
---------------------------	---------------------------------	---	--	--	---	--	---	--	--	--	---

✓ Shows the cases from which the theme for management emerged.  
 Source: analysis of within-case analysis (all cases)

In summary, four of the ten organisations did not have a recognisable security budget. Rather, they could however estimate a percentage of the overall IT budget that was spent on security or make an estimate based on their understanding of recent capital acquisitions.

When comparing the qualitative and quantitative results in this area it was observed that all organisations (and all interviewees) provided a figure in response to the survey question (quantitative) regarding a figure for the organisation’s information security budget. In the interviews the responses were far more general in nature. If the survey data were viewed in isolation from the interview data it would have been possible to assume that the organisations did have separate security budgets and that the interviewees had an intimate knowledge of the actual figures. The interview provided the opportunity to fully explore the nature of the information security budgeting process in each of the organisations. This allowed for a higher degree of confidence that the results listed in Table 4-28 are an accurate reflection of the state of budgeting in the organisations.

**4.13.7 Differentiators**

Differentiators have been previously defined as those themes, ideas or issues that may help to explain why each case organisation approaches information security in the way it does. In addressing the specific research issues, it was planned to see if differentiators would also explain if and why Australian businesses’ security positions may be different to their international counterparts. Unlike the other elements previously compared in the cross-case analysis the researcher derived the differentiators after an analysis of all responses. The derived differentiators for each of the cases are summarised in table 4-29.

As might be expected with a list of differentiators table 4-29 does not illustrate a high degree of literal replication between cases. Size, relationships with other organisations, and the value the business placed on information were each present as differentiators in three or more of the cases. The table demonstrates that whilst concern about information security issues is common across all organisations, each organisation is faced with a unique environment, which impacts on how it addresses its concerns.

**Table 4-29 Differentiators**

Differentiator	Cases									
	A	B	C	D	E	F	G	H	I	J
Nature of the business	✓						✓			
Size	✓	✓	✓		✓					✓
Role of security professional	✓									
Use of the Internet	✓					✓				



#### **4.14 Summary**

This chapter reported the results of the data that were collected from the ten case organisations that participated in this research. Qualitative analysis techniques were applied to the in-depth interview transcripts to understand the risk management issues firstly, for each case, and secondly across all ten cases demonstrating literal replication. It was found that the top three issues of hardware theft, viruses, and system user access abuse were common across most organisations, and that the organisations had a variety of responses in terms of countermeasures to potentially defend against those threats and incidents. Additionally it was discovered that organisations did not have a rigorous approach to defining and managing separate information security budgets.

In the next and final chapter, conclusions are drawn by comparing the findings presented in this chapter with the evidence from the literature that was presented in chapter 2.



## CHAPTER 5 - CONCLUSIONS AND IMPLICATIONS

The purpose of this research was to investigate information security issues in Australian businesses. Chapter 1 outlined this research problem, highlighting the need to compare international information security issues with those found in Australia. This research was justified in terms of its importance to business and the lack of previous research regarding information security within the Australian business context.

Chapter 2 reviewed the information security literature relating to the disciplines of risk management and information security and discussed a range of concepts and issues within information security. The literature was then reviewed in relation to information security threats, incidents, and countermeasures. From that literature, a model was developed depicting the relationship between security risks and management of those risks, including identified business-specific differentiators. The theoretical support for this model highlighted the expected types and effects of risks and risk management countermeasures.

Chapter 3 outlined and justified the use of a multiple case study approach to collect data to address the research problem. The multiple case study design applied to this research was described, along with details of how the data were prepared for analysis and then analysed.

The analysis of the data collected from the interviews with sixteen IT security professionals in ten organisations was presented in chapter 4. The results of the within-case analysis were presented for each case, followed by the results of the cross-case analysis.

In this final chapter, firstly conclusions are drawn regarding the five research issues (RI):

- RI 1. How reliant are Australian organisations on their IT?
- RI 2. How is the threat to organisations' computers, data, and networks manifesting itself in Australian industry?
- RI 3. Is the information security threat greater in Australia? If so, why?
- RI 4. How are Australian organisations protecting their computers, data, and networks from information security risks?
- RI 5. What level of resource expenditure are Australian organisations committing to protect their systems and data?

Secondly, implications of this research for theory and practice are discussed along with suggestions for future research. Conclusions will be derived through a comparison of case findings with the applicable literature (in chapter 2, section 2.3) and the data (in chapter 4 section 4.13). Finally, the limitations of this research are discussed.

### 5.1 Conclusions about IT reliance

This section presents conclusions about the first research issue: *How reliant are Australian organisations on their IT?*

In particular the research issue is divided into two sub issues:

RI 1.1. How dependent are Australian organisations on their IT in terms of computing systems and the data that resides on those systems?

RI 1.2. What is the likely impact of the loss of use of an organisation's IT capability?

The following conclusions are drawn from a comparison of the evidence in the IT security literature (reviewed in chapter 2) with the results of the cross-case analysis (presented in section 4.13).

This study uncovered additional information regarding organisational reliance on IT. As indicated in chapter 2 (literature review) and the previous chapter much of the existing data on information security is contained in quantitative research reports in magazine and newspaper articles as well as vendor sponsored material. Some of it tends to be superficial and potentially biased in nature – especially with regards to the last mentioned source. The qualitative approach of this research study enabled a more in-depth review of the level of reliance on IT within the case organisations, uncovering a greater level of detail in regards to what organisations actually used their technology for and how dependent they are on it. For example, this study found that even small organisations are now using computer systems to manage their financial data. According to much of the existing literature the management of this data has relied on manual book keeping methods.

The existing literature describes IT reliance at the macro-level, for example, in terms of 'Internet and Intranet' usage or in terms of general 'computer use'. The in-depth approach used by this study provided a better understanding of the overall reliance on IT by organisations and of how the loss of IT through an information security incident could impact the business. In the previous chapter each organisation's overall use of IT was assigned to a quadrant according to its fit within the McFarlan and McKenny strategic grid. In keeping with expectations this research found that the greater the importance of its current and future information systems to the organisation the greater the potential loss the organisation would face as a result of a serious information security incident. Even though this finding in itself may seem obvious, it highlights the need for organisations to conduct a fundamental analysis of the risk they face based on the importance of their information technology.

Table 5-1 provides a summary of the responses given by the organisations when they asked what they used their IT for and how critical their IT was to the conduct of their core business. This then allowed an assessment to be made regarding the extent to which each business was reliant IT (see case summaries in chapter 4) and to determine if the organisations understood the relationship between use, reliance, and impact as depicted in Figure 2-7, section 2.3.5 of chapter 2.

**Table 5-1 Indicators of IT reliance: this study’s findings versus the literature**

Indicators of IT Reliance	Cases – This study’s findings										Main emphasis in Literature
	A	B	C	D	E	F	G	H	I	J	
Billing and customer accounts				✓				✓			
Business not capable of working without IT					✓				✓		
Connection to business partners			✓							✓	
Customer ordering (e-Commerce)				✓							✓
Direct community access to systems								✓			
Document management		✓	✓			✓		✓	✓	✓	
ERP							✓		✓	✓	
Financials	✓				✓	✓	✓		✓	✓	
Information a key resource (Info Mgt Systems)			✓							✓	
Integration of telephone systems		✓									
Internet		✓		✓	✓	✓	✓	✓	✓	✓	✓
Intranet		✓	✓		✓	✓	✓		✓	✓	✓
Logistics tracking		✓	✓								
Office automation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Payroll processing		✓	✓			✓	✓		✓	✓	
Implementation of an IT outsourcing arrangement						✓					
Used in preference to face to face comms					✓						
Used to develop company product					✓						
Workflow				✓							

*Source: analysis of interview data, observation data and literature*

As shown in the table, the most prolific indicators of IT reliance in the literature and this research were: office automation, Internet use, and Intranet use. In comparison with this study’s findings the literature identified only a limited number of indicators. This emphasises the contribution of this research to the detailed understanding of organisational reliance on IT.

The research discovered indicators of IT reliance that were not present in the literature. As shown in Table 5-1, the following indicators of IT reliance surfaced in two or more of the organisations that participated in this research, suggesting that these factors may also be present in organisations generally:

- Office automation (10 out of 10 organisations)
- Financials (6 out of 10 organisations)
- Payroll processing (6 out of 10 organisations)
- Document management (6 out of 10 organisations)
- ERP (3 out of 10 organisations)
- Logistics tracking (2 out of 10 organisations)
- Information a key resource (2 out of 10 organisations)
- Connection to business partners (2 out of 10 organisations)

- Billing and customer accounts (2 out of 10 organisations)
- Business not capable of working without IT (2 out of 10 organisations)

All ten organisations used their IT for office automation and most also used their systems to access the Internet. Three of the five medium-to-large organisations that took part in the research (500 + employees) had an ERP deployed that offered an integrated management system that included financials, payroll, and customer billing. Four of the six smaller organisations (less than 200 employees) used applications that were specifically designed for small business accounting and financial management – a best of breed approach. Based on the evidence provided, it is concluded that nine of the ten organisations that participated in the study are reliant on their IT. Only one organisation said it could continue to operate at a reasonable level of effectiveness without access to its information systems.

The following indicators of IT reliance were reported once in this research. It is therefore planned to undertake further research in the future covering a larger number of organisations be undertaken to determine if these indicators have an impact on the overall reliance on systems, the assessed risk, and proposed response to those risks:

- Integration of telephone systems
- Customer ordering
- Workflow
- Used to develop company product
- Used in preference to face-to-face communication
- Implementation of an IT outsourcing arrangement
- Direct community access to systems

These factors tended to be either specific to an organisation (such as providing direct access to organisational systems in the case of one organisation operating a community library), or involved emerging technology that had been implemented only by organisations that could be considered to be early adopters of technology (such as the integration of telephony and data systems).

The summary and recommendation component of the within-case analysis presented in chapter four specified how reliant each organisation was on its technology. Having determined that the majority of organisations in this study (nine out of ten) were highly reliant on their IT systems it was then important to assess the impact of the loss of those systems. (This was achieved via analysis of the data gathered as part of this research).

The literature indicated in very general terms that the impact of loss of systems would be related to the organisation's overall reliance on IT. This study provides additional evidence to support that rule of thumb. With the exception of one organisation, each case participant emphasised how their organisation's core business would be negatively impacted by the loss of its IT systems or data. The realisation of this point had led six of the organisations in the study to invest in disaster recovery and other business continuity initiatives.

In summary, this study on information security adds to the body of knowledge relating to organisational reliance on IT and the potential impact on organisations should they lose access to those systems. In addition, it expands on our ability to identify the extent of IT reliance by reference to frameworks such as the McFarlan and McKenny strategic grid. The adoption of qualitative data collection techniques enabled significantly more data to be collected on what organisations were using their IT for. Further, it confirmed the link identified in chapter two, (section 2.3.5, Figure 2.7) between organisational use of IT, reliance on those systems, and the impact suffered if the systems were not available. Based on that additional information, this study's findings indicate that information security has not been adequately addressed in the literature and that the need for information security is still evolving and can be recognised by a growing number of emerging factors.

Conclusions relating to information security threats are discussed next.

## 5.2 Conclusions about threats

This section presents conclusions about the second research question: *How does the threat to organisations' computers, data, and networks manifest itself in Australian industry?*

This research issue was divided into three sub issues (RI):

RI 2.1. What potential threats to computers, data, and networks are Australian organisations likely to face? (*Potential security threats*)

RI 2.2. What threat(s) do Australian organisations perceive to be the most likely and prevalent/significant? (*Perceived security threats*)

RI 2.3. What is the level of actual information security incidents in Australian organisations? (*Actual security incidents*)

### 5.2.1 Potential security threats

The following conclusions are drawn from a comparison of the evidence in the literature regarding the different types of information security threats (presented in chapter 2) with the results of the cross-case analysis (presented in section 4.13).

The similarities and differences between the evidence in the literature and the findings of this research in relation to information are highlighted in table 5-2 below.

**Table 5-2 Types of information security threats: this study's findings versus the literature**

Threat	Cases										Literature
	A	B	C	D	E	F	G	H	I	J	
Close integration of key applications				✓							
Competitors					✓						✓
Complacency			✓								
Foreign governments		✓	✓						✓		✓
Hackers	✓	✓	✓		✓	✓	✓	✓		✓	✓
Issue motivated groups					✓						✓
Natural disaster (earthquake, flood, fires)									✓		
Organised group of hackers		✓	✓		✓						✓
Outsider from within (Library access)								✓			
Poor quality code					✓						
Port scans	✓						✓	✓			
Staff turn over				✓							
System users	✓	✓	✓	✓			✓	✓	✓	✓	✓
Viruses	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

*Source: analysis of interview data, observation data and literature*

Organisations were asked to identify what the complete list of information security threats were. These included a number of information security threats that were not discussed in the literature (thus adding to previous research on information security). The following threats surfaced in more than one case, suggesting that they may be common to organisations generally.

- Port scans
- Foreign governments
- Hackers
- Organised groups of hackers
- System users
- Viruses

The literature's inconsistent use of terms used to describe information security issues and in particular threats increases the difficulty of the classification of threats. For example, the literature also refers to port scans as hacking attempts or as the use of automated scripting and analysis tools. It could be argued that rather than a type of threat in itself, these two could be classified as methods of hacking.

The following threats were reported only once in this research and therefore additional research will be needed to assess their importance:

- Complacency
- Staff-turn over
- Poor quality code

- Outsider within
- Natural disaster

The literature suggests that organisations face a wide variety of potential threats and that these threats are serious in nature. In particular the literature defines viruses, hacking and internal threats to be the major threats faced by organisations. The internal versus external categorisation should be seen to be a macro classification in that both threats can be made up of a variety of other threats such as viruses, hacking and the like

Eight of the organisations that participated in this study reported that viruses, hackers, and internal system users are the main threats to their systems, (all ten indicated viruses as a potential threat). While this study confirmed the literature’s view of the ‘core’ potential threats to security as viruses, hackers, and insiders, it also identified nine additional potential threats (see table 5-2).

**5.2.2 Perceived security threats**

In order to investigate research issue 2.2 the organisations were asked to name the threats that they perceived that they were likely to face and the ones that they deemed to be the most significant (i.e. the ones that can potentially cause the most harm to an organisation’s information systems).

A comparison between the perceived threats from this study’s findings and the literature is presented in Table 5-3 below. Participant selected the threats deemed to be the most likely were from the list of potential threats. They recognised that whilst there may be a very wide selection of potential threats, their business were likely to be subjected only to a limited sub set of those threats. Therefore, for risk management purposes they would dedicate their limited resources to defending against those threats that were most likely to be encountered and that would cause the most significant damage.

**Table 5-3 Types of security threats: this study’s findings versus the literature**

Security Risk	Cases										Literature
	A	B	C	D	E	F	G	H	I	J	
Viruses	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hackers	✓	✓	✓		✓	✓	✓	✓		✓	✓
System Users	✓	✓	✓	✓			✓	✓	✓	✓	✓

*Source: analysis of interview data, observation data and literature*

A review of the literature (see chapter 2, section 2.3.1) identified the most significant threats in the following order:

- Hackers
- System users
- Viruses

They are the threats that are reported as being perceived as being of greatest concern to organisations.

While this study uncovered the same perceived significant threats it revealed a difference in the order of importance of these key threats. It found that the most significant perceived threats in order of importance are:

- Viruses
- System users
- Hackers

Due to identified perceived significance of each of these threats specific findings and comments regarding each of these three threats follow.

**(i) Viruses**

In this research, viruses were determined to be the major threat to Australian computing systems. There is an increasing level of concern regarding the growing number and the potential impact that viruses can have on an organisation's information security posture. The findings of this research support the literature's position that viruses are commonplace and that they are increasing in number, and the potential detrimental impact that they can have on computer systems is also increasing. However, this study's evidence placed viruses ahead of all other threats in terms of perceived prevalence and significance.

**(ii) System users**

This research provided additional insight into the threat posed by internal system users: that is, employees of an organisation as being a significant threat. Findings uncovered that there was a perception that system users frequently created security incidents due to a lack of diligence in following system processes and procedures. However, most organisations indicated that an increased awareness of policies and countermeasures had reduced their concern about the internal threat.

The literature on the other hand tended to focus on deliberate, malicious acts of hacking or hacking-like activities perpetrated by internal system users. It emphasised the significance of the threat faced from system users and highlighted how internal system users could potentially use their authorised access to the system to create other forms of threats, (e.g. as an internal person launching a hacker attack).

This research confirmed that organisations believed system users were a threat. This research differed from the literature in that it revealed that the perceptions are that system users are more likely to be a threat as a result of ignorance or failure to adhere to system policies rather than any deliberate or malicious act.



**(iii) Hackers and Hacking**

The literature provided numerous examples (see section 2.3.13) of serious hacker attacks on a variety of organisations’ computer systems. That quantitative data gathered in industry-based surveys summarised in chapter 2. The findings of this study’s qualitative research supports these reports,, (i.e. organisations are concerned about the hacker threat). Eight out of the ten organisations perceived that hackers were a threat to their business and as such considered it appropriate to consider the hacking threat when formulating their security plans.

However as discussed in section 5.2.3, despite this strongly held perception, there appear to be few serious hacker related incidents..

**5.2.3 Actual security incidents**

This section deals with research issue 2.3, the level of information security incidents actually encountered by Australian organisations.

The following conclusions are drawn from a comparison of the evidence in the literature regarding information security threats (presented in chapter 2, section 2.3.1) with the results of the cross-case analysis (presented in section 4.13).

Table 5-4 below summarises the type of incidents actually experienced by the organisations that participated in this research as well as an indication as to whether the type of incident was mentioned in the literature (i.e. the literature which provided quantitative evidence of organisations reporting actual security incidents).

**Table 5-4 Information security incidents: this study’s findings versus the literature**

Incident	Cases										Literature	
	A	B	C	D	E	F	G	H	I	J		
Attacks from automated scripting tools					✓							✓
Chain e-mails/SPAM		✓	✓									
Contractors abusing system privileges		✓	✓									
Data destruction			✓									✓
Hacking (excluding port scans)			✓	✓				✓				✓
Hardware theft (e.g.Laptops)		✓	✓	✓	✓		✓	✓	✓			✓
Information leakage									✓			
Port scans	✓	✓			✓							
System privilege abuse by users	✓	✓	✓	✓			✓			✓		✓
Viruses	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

*Source: analysis of interview data, observation data and literature*

For the purposes of this research it was important to separate potential and perceived threats from those actually experienced by Australian organisations. With most of the

literature being comprised of newspaper reports and vendor sponsored articles, distinction between the types of threats and their relationship to the actual incidents experienced by organisations is often not clear.

The table above indicates that viruses are the most prevalent form of security incident. This confirms that the perceived threat matches the incidents experienced by the organisation. Section 2.3.11 highlighted that there was a large difference in the literature in the percentage of organisations encountering virus incidents (from 49% up to 90%). The different results could be due to varying methodologies used in the conduct of the research. For example, this qualitative approach allowed for a definition to be presented and discussed as well as allowing it to be assessed. This study found that all participants had encountered virus incidents.

Table 5-4 also shows that seven of the participating organisations had incidents of IT hardware theft. It is interesting to note that no organisation mentioned this when listing the threats. This could perhaps indicate a lack of analysis regarding the potential consequences (risks) associated with security threats. For example, the theft of a laptop computer could give access to an organisation's systems or to confidential data stored on it. The evidence available in the literature suggests that the theft of IT equipment is a serious issue (Brinery, 1998; Thompson, 1998; Rapalus, 2000). The literature, does however, lack detailed analysis of the issue. It does not separate theft of easily-removed assets with thefts that could be the part of a larger security incident (e.g. the theft of a laptop computer that is later used to remotely access the organisation's computer systems).

The other significant difference between the threat and the actual incidents is that despite the perception of high frequency, relatively few organisations actually experienced a hacker related incident. Eight of the organisations rated the hacker threat as high but didn't have any evidence that this type of incident had occurred in their organisations. When this point was made during interviews with the participants it became clear that the organisations' perceptions are not based on their own experiences, but are based on reported incidents from other organisations, from the press, and vendor marketing.

There is a higher level of incidents reported in the literature than was uncovered in this study, i.e. the actual level of incidents experienced by the participating organisations. The literature reported an increase in the number of reported hacker incidents in recent years (from single digits per year to several thousand). What is not clear in the literature is if this is due to a rise in hacker incidents, or from better/more consistent reporting, or even from an increase in the number of people asking questions regarding hacking.

As has been noted, there was no correlation between the perceived hacker threat and the actual rate of hacker related incidents within the organisations. One interpretation of this finding is that the literature itself is influencing the perceptions of organisations. They read reports about the severity of the hacker problem and assume it is an issue for their business too. This is a key insight of this research.

The findings of this study suggest that organisations should take a more specific approach in determining what threats are relevant to their business. For example, by

reviewing information security threats based on the likelihood of a threat actually occurring and by assessing the impact of that incident on the organisation (i.e. risk assessment). This approach in itself will allow organisations to better understand the risk versus countermeasure equation, and therefore enable them to make more informed decisions regarding their investments in information security; allowing them to migrate from 'I think' to 'I know' based decision making.

Conclusions about Australian businesses as information security targets are discussed next.

### **5.3 Conclusions about Australian businesses as targets**

This section presents conclusions about the third research issue: *Are Australian organisations being targeted? If so why?*

In particular this research issue was divided into two sub issues:

RI 3.1. In comparison with the international experience, is there any difference in the extent to which Australian organisations are being targeted for information security related attacks?

RI 3.2. If so, what are the identifiable differentiators?

The conclusions are drawn from a comparison of the evidence in the literature regarding the potential of Australian businesses as targets (presented in Chapter 2) with the results of the cross-case analysis (presented in section 4.13)

#### **5.3.1 Information security incidents: Australia vs. overseas**

This research has attempted to add to the body of knowledge in this area by specifically identifying potential reasons (or differentiators) as to why Australian organisations may be targeted. In comparison with the majority of studies contained in the literature is that study, being qualitative in nature, allowed more comprehensive answers to be given in response to the interview question.

The literature suggests that Australian businesses are the specific targets of information security attacks. As Australian businesses adopt new technology and rely upon IT to underpin their business the literature implies that the chances of Australian organisations being targeted increase (Rapalus, 2000). As mentioned in chapter 1 (section 1.3) the body of knowledge on information security contains a number of comparative quantitative surveys that compare organisations who are targeted in various parts of the world. There is empirical evidence that indicates that as organisations have implemented Internet and e-Commerce based technologies the rate of security incidents has increased (Kearvekk-White, 1996; Lichtenstein, 1998; Rapalus, 2000; Power, 2000a).

Table 5-5, below illustrates that in both the literature and this study there were instances where organisations felt that they were specific targets. However, there were also organisations in both that believed they were not specific targets.

**Table 5-5 Target status: this study's findings versus the literature**

Target Status	Cases										Literature
	A	B	C	D	E	F	G	H	I	J	
Believed they are a target	✓	✓	✓			✓					✓
Believed they were not a target				✓	✓		✓	✓	✓	✓	✓

*Source: analysis of interview data, observation data and literature*

In order to understand the Australian information security environment, and to properly address this research issue it was necessary to identify why organisations either feel they are targeted or not. The four organisations that believed they were specifically targeted gave the following as reasons why they felt they were targeted:

- Foreign governments are interested in their business
- The nature of the organisation's business makes them a potential target
- Because they are connected to the Internet
- High profile organisation with a potential high pay-off if the attack is successful
- Profile of the organisation
- Weaknesses in outsourcing agreement(s) – where there is unclear accountability regarding security responsibilities.

This belief resulted in a series of comprehensive countermeasures aimed at specifically defeating the aforementioned threats.

The six organisations in this study that did not believe they were specific targets of any specific threat gave these reasons for their belief:

- Competitors do not have the technical expertise to defeat firewalls
- Organisation maintains a low profile and potentially sensitive information is not on Internet-connected machines
- Not an interesting target for would-be attackers
- No evidence of being a specific or dedicated target

The organisations that fell into this latter group believed that if they were targeted it would be an opportunistic rather than a dedicated attack. This belief resulted in the application of standard countermeasures to ensure that the organisation's security posture was adequate.

This study agrees with the previous research that Australian organisations can be specific targets of information security attacks. However, this study found that the majority of organisations studied (i.e. six out of 10) believed that they were not specific targets; rather they were more likely to be subjected to random opportunistic attacks.

Previous research does not specifically indicate reasons for Australian businesses being considered as targets, other than the growing proliferation of technology into standard business operations. The literature suggests that Australian businesses are subjected to less attacks than businesses in countries such as the United States of

America or United Kingdom. However, it also suggests that Australian organisations were less likely to employ sufficient countermeasures (Thompson, 1997; Kearvell-White, 1996; Rapalus, 2000).

In summary, this study adds to the body of knowledge on information security by providing a more definitive and descriptive answer regarding the targeting of Australian businesses. The study has determined that even though Australian organisations may be specific targets of information security attacks, the majority of organisations studied (i.e. six out of 10) believed that they were not specific targets and that any attack would be random and opportunistic.

### 5.3.2 Differentiators

As stated in chapter 4, this research identified a number of potential differentiators that could explain or justify an organisation’s information security posture. It determined that an organisation typically has a unique set of differentiators that determined its security posture. Additionally, those organisations that believed that they were specifically targeted could identify key differentiators that led to that targeting. Each organisation had made the point that it was its unique set of differentiators that either made it a specific target or not.

Table 5-6 below summarises the assessed differentiators for each of the organisations.

**Table 5-6 Differentiators: this study’s findings versus the literature**

Differentiator	Cases										Literature
	A	B	C	D	E	F	G	H	I	J	
Access to new technology			✓								
Commonwealth Government department						✓					
Disaster recovery capability							✓	✓			
Dispersed nature of the business		✓									
Facilities management arrangements – how data centres are managed and secured							✓	✓	✓		
Focus on physical security – how organisations take steps to secure computing facilities with locked rooms, limited access, etc.							✓	✓	✓		
Government owned corporation							✓				
High level of security knowledge							✓	✓	✓		
International footprint			✓								
International offices							✓	✓	✓		
International standards							✓				
Interviewees			✓								
IT security a key part of the business					✓						
Lack of contingency planning		✓									
Lack of information security vision		✓									
Lack of policies and procedures				✓							

Large customer base							✓	✓	✓	✓	
Local government							✓	✓			
Managed services							✓				
Mandated state security policy							✓	✓	✓	✓	✓
Many remote sites							✓	✓			
Multiple layers of firewalls							✓				
Nature of the business	✓						✓				✓
New organisation						✓					
No IT management structure				✓							
Outsourcing arrangement						✓					
Profile			✓								
Public profile							✓	✓	✓		
Relationships with other organisations		✓	✓							✓	✓
Reliance on IT		✓			✓						✓
Reliance on one central application				✓							
Reliance on the Internet		✓					✓				✓
Responsible for Government IT policies						✓					
Role of security professional	✓										
Segregation of networks							✓				
Senior management attitude towards staff				✓							
Service provider relationship										✓	
Size	✓	✓	✓		✓					✓	✓
Small budget							✓	✓			
Some components can function without IT				✓							
Structure		✓									
Use of external auditors							✓	✓			✓
Use of open source products	✓				✓						✓
Use of the Internet	✓					✓					✓
Value of organisational information		✓	✓						✓		✓

Source: analysis of interview data, observation data and literature

The literature provided limited data on potential organisational differentiators. It focused on organisations being ‘targets of opportunity’ rather than being the focus of a dedicated attack. As stated previously, the quantitative nature of much of the research literature meant that questions such as how and why respondents answered questions in the manner that they did was not known. This study’s qualitative approach supports those earlier the findings, however; with the benefit of in-depth follow up questions, it also uncovered that some organisations could be the victims of dedicated attacks.

There appears to be some anecdotal evidence that suggests that the major security threat, viruses, tends to infect systems based on the international time zone, as this was mentioned by a number of the participants. Essentially, this results in major virus outbreaks impacting in the Northern Hemisphere first, allowing some time (albeit limited) for Australian organisations to proactively respond to the threat before it becomes an actual threat here.

The spread of the participants' business was seen as a key-determining factor in the extent to which they were exposed to threats. For example a multi-national company would have significantly more exposure to security risks in comparison to a small organisation operating only in Australia.

As much of the research recorded in the literature has been conducted in the United States or the United Kingdom, it was considered important to identify differentiators that might make Australian information security different. These differences in themselves are general in nature and should be read in compare and contrast fashion. For example, there are far more large multinational organisations operating out of the America and Europe than in Australia.

A number of differentiators were identified that could explain divergence from the international norm. These included:

- Nature of the business
- Size
- Use of the Internet
- Value of organisational information
- Relationships with other organisations
- Use of open source products
- Use of external auditors
- Mandated state security policy.

From a practitioners point of view this information is important as it should influence the security countermeasures that an Australian organisation may decide to employ.

As noted in section 4.13.7, there was not a high degree of literal replication between the 10 cases in this study. This highlights the point that each organisation has unique security issues. This realisation raises issues regarding how security consultants should approach their assignments. Thus it is important that security professionals do not simply apply a standard approach based on their previous experience in other organisations. The unique aspects of each organisation need to be identified and addressed. Conclusions about countermeasures are discussed next.

## **5.4 Conclusions about countermeasures**

This section presents conclusions about the fourth research issue: *How are organisations protecting their computing, data, and networks from security threats?*

Thus far this chapter has addressed the information security risks that the participants believe they face or that have actually experienced. This section addresses the countermeasures that the 10 case organisations have employed in order to protect their organisations against the risks.

This research found (section 4.3) that there was frequently little correlation between an organisation's perceived threat posture and the actual countermeasures that the organisation employed. One possible reason could be the low instance of organisations conducting formal threat and risk assessment tailored to their

organisation (as indicated in their responses to the questions). This of course, increases the risk of making erroneous information security investment decisions.

Only three of the research participants (i.e. B, C and I) could demonstrate a linkage between their perceived threats, the actual threats, and the countermeasures that they employed. This potentially indicates that there is insufficient risk analysis being conducted to ensure that investment decisions are being made correctly.

As shown in Table 5-7, the majority of countermeasures employed by the participating organisations were discussed in the literature. This research did, however, uncover additional details regarding how organisations deployed their countermeasures. For example, this research revealed that while all the case organisations use anti-viral countermeasures only a few used sophisticated management processes and technologies to ensure that the anti-virus definitions were up to date.

**Table 5-7 Countermeasures employed: this study’s findings versus the literature**

Security Countermeasure	Cases										Literature
	A	B	C	D	E	F	G	H	I	J	
Anti-viral software	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AusCERT subscription											✓
Automated patch management of virus definitions		✓	✓		✓						✓
Capacity planning		✓									✓
Disaster recovery plans		✓	✓				✓	✓	✓	✓	✓
Freeware security tools	✓										
Full-time security manager		✓	✓				✓			✓	✓
Hardware firewalls		✓	✓		✓	✓	✓	✓	✓	✓	✓
Internal CERT capability			✓								
Linkage between threat and incidents identified		✓	✓						✓		✓
Lotus Notes instead of Microsoft Exchange										✓	
Physical security		✓	✓						✓		✓
Procedures and work instructions for the use of IT		✓	✓			✓	✓			✓	✓
Reporting of incidents		✓	✓								✓
Security auditing							✓	✓	✓		✓
Security policies		✓	✓		✓	✓	✓		✓	✓	✓
Security service provider						✓	✓				
Software firewalls	✓			✓				✓			✓
Software patch management					✓						✓
System access controls		✓	✓		✓	✓	✓	✓	✓	✓	✓

*Source: analysis of interview data, observation data and literature*

Table 5-7 depicts the variety of countermeasures that are available to an organisation to deploy. The cases have a good representation of both hardware and infrastructure-related countermeasures, as well as the ‘softer’ countermeasures such as people and policies. The organisations that had the most comprehensive approach to information



security issues (i.e., organisations B, C, and D) demonstrated good alignment between threats, incidents, and countermeasures. In the area of countermeasures, policies and procedures were used to underpin the infrastructure-based countermeasures such as firewalls. For example, in order for firewalls to be deemed appropriately managed they need to have policies that dictated how they should be configured the types of attack they are intended to resist. The procedures should indicate how, when, and by whom are applied.

The countermeasures listed in table 5.7 that were reported only by a single organisation warrant investigation in a larger study. These are:

- AusCERT subscription
- Use of an internal CERT capability
- Freeware security tools
- Lotus Notes used instead of Microsoft Exchange
- Software patch management

The use of CERT capabilities within case organisation 'C' provided an insight into some of the differences between the literature and this research as well as the differences between the Australian and the international experience. The literature presented numerous examples of organisations using the CERT subscriptions to supplement their internal security expertise. This study, however, uncovered a general apathy towards the use of the recognised Australian CERT agency, AusCERT. Respondents believed that they offered a lower than their international equivalents. Some organisations stated that they believed because security vulnerabilities tended to follow the international dateline they would be better served by using a North American agency such as CANCEC. One organisation, the largest of the participants, had an internal CERT capability of their own.

The range of countermeasures that organisations employ is an indication of how comprehensive the security management process is within an organisation. The above table provides two indications of the extent of each participant's risk management process. Firstly, a review of the linkage between threats and countermeasures indicates which organisations have implemented a countermeasure based on a specific threat. Secondly, more countermeasures generally indicate greater complexity and comprehensiveness in the organisation's security program.

From an information systems security management point of view the output of tables 5.1, 5.2, 5.3, 5.4, 5.5, and 5.6 indicate the overall risk posture. If the risk analysis (information security parent discipline: see chapter 2, section 2.3) has been conducted appropriately, the output countermeasures should be those listed in table 5.7. The importance of aligning the various components of the information security landscape by matching the organisation's defined risks with an appropriate set of countermeasures is a key contribution of this research.

Table 5.4 illustrates that all the organisations are experiencing issues with viruses and that they are the most significant and prevalent threat. Reference to tables 5.4 and 5.7 indicates that all the organisations employed anti-viral countermeasures. However only three employed automated patch management to protect against known vulnerabilities and only one had a defined software patch management process that enabled it to stay ahead of the virus/trojan/exploit cycle. The findings

suggested that all the organisations could improve their security posture by being more proactive in updating operating systems, applications and virus definition files.

One organisation had taken into account that many of the virus exploits are designed to take advantage of vulnerabilities in Microsoft’s exchange e-mail platform. To avoid these vulnerabilities and the cost associated with the management of updates they had chosen to use Lotus Notes as their preferred e-mail server and client. A review of primary and secondary evidence suggested that they did have fewer virus related incidents that were associated with e-mail deliveries and exploits – vindicating the organisation’s selection of the alternative e-mail platform.

Conclusions about security budgets are discussed next.

### 5.5 Conclusions about security budgets

This section presents conclusions with regard to the final research issue: *What level of resource expenditure are Australian organisations committing to protect their systems and data?*

This research found that organisations were either reluctant or were unable to give the exact details of their security budgets. However table 5-8 below shows that six of the ten organisations could readily demonstrate that they had a specific information security budget. (This table and table 4-28 were developed after the review of interview transcripts, exit surveys, and secondary data analysis).

**Table 5-8 Security Budgets: this study’s findings versus the literature**

Security Budget	Cases										Literature
	A	B	C	D	E	F	G	H	I	J	
Identifiable security budget		✓	✓		✓		✓	✓	✓		✓
No identifiable security budget	✓			✓		✓				✓	✓

*Source: analysis of interview data, observation data and literature*

As all the organisations employed some form of information security countermeasure, they all had some form of budget for security products and or services. The amount of the budget often was not available as there was not a clear separation of information security funds from other IT expenditure. For example, one of the organisation’s IT infrastructure was managed through an outsourcing agreement where they simply paid one fee for all services. As part of that fee the outsourcing company was expected to deploy a range of information security countermeasures.

Information security resource research (see chapter 2, section 2.3.4) states that 45% of Australian organisations don’t have an information security budget. This study provides support for the literature to the extent that whilst all the organisations have some form of information security resource expenditure, 40% do not and budget for that type of expenditure separately from other IT expenditure (see table 5-8).

It was evident that there was difficulty in all the organisations in justifying expenditure based on Return on Investment (ROI) for security related projects. This coupled with the lack of robust threat and risk assessment meant that even business-critical information security initiatives were hard to justify (unless there was a clear understanding of the cost of the potential losses). There was no evidence in any of the case organisations of a successful methodology for identifying ROI for security initiatives. From a business management perspective no evidence was uncovered of performance management or Key Performance Indicators (KPI) that were based on achieving information security outcomes.

The absence of a detailed security budget in four of the organisations highlights a flaw in much of the popular data on information security literature which reported losses as a result of security incidents. This research indicated that it was certainly not being used to justify, at least successfully, additional investment in information security.

A final difference between the literature and the findings of this qualitative, interview based research! The literature reported on quantitative surveys highlighting the increasing trend of organisations to devote more resources to information security issues. In most cases the interview respondents were willing to discuss in general terms the nature of, or even present documentary evidence on their security budgets. However, none of the organisations provided resource expenditure data that correlated facts with that information put forward in chapter 2. Information security expenditure is therefore considered to be worthy of further research outside the context of this study.

## **5.6 Implications for theory**

Through the development and testing of a model to investigate the effects of information security within the Australian business context, this research makes the following five contributions to theory:

- It was the first comprehensive qualitative-based investigation into information security in Australia
- Its innovative use of technology and in particular the Internet, to gather data (via virtual interviews) enabled increased confidence in the findings via data triangulation
- It is the first study to investigate a broad spectrum of information security issues within the framework of Australian business
- It explored the relevance to the Australian context of existing information security theories
- It confirms the appropriateness of case studies in obtaining rich data to assist in the understanding of information security issues.

A discussion of each of these five contributions follows.

### **5.6.1 Qualitative based research**

As introduced in chapter 1, section 1.3, and subsequently addressed throughout, this research is distinctive in its use of qualitative research to gain a better understanding of the Australian information security scene. The review of the current literature (chapter 2) showed that most of the research in the field is quantitative, and as such without specific context, resulting in a general lack of understanding as to around why certain responses may have been given in survey-based studies. The qualitative research paradigm addresses the *why* and the *how* to explored, not just the *what* (Yin 1994).

While there has been considerable research in an international context, there has been no previous major qualitative study focusing on the information security issues faced by Australian businesses.

### **5.6.2 Innovative use of technology**

The use of a qualitative research methodology in this study was underpinned by an innovative use of Internet based technologies to supplement traditional interview and survey techniques. During the pilot research phase it became clear that the potentially sensitive nature of information security meant that some organisations may be reluctant to divulge certain facts. To overcome this issue a web based virtual interview was developed to follow the same structure and guidelines as those of the face-to-face in-depth interviews. In all cases it was found to be an extremely effective tool in gathering high quality data. It was found that the respondents often put forward more comprehensive, targeted responses to interview questions than those given in normal interview conditions. Whilst the reason for this is not entirely clear, it may be that the virtual interview provides a perceived degree of anonymity.

It allowed respondents to consider their answers as well as seek facts to back up their statements rather than feeling the need to give an instant response.

Data collection and accuracy was improved at the completion of the virtual interview by directing respondents to a quantitative ‘exit’ survey that was aimed at triangulating the responses given as part of the interview.

### **5.6.3 Broad approach**

As far as could be ascertained, this study is the first of its kind to take a broad approach to the investigation of information security issues faced by Australian organisations. Thus, one of its contributions is that it provides a more complete understanding of information security within Australia. This was especially so with regard to the link between information security risks and the management of those risks.

#### 5.6.4 Use of existing theories

This research made use of the existing theories in information security in order to determine where a gap in literature existed and to help create a research framework to apply to the collection and analysis of data. The literature review (chapter 2) highlighted the lack of detailed qualitative research in information security it was in addressing this gap, this research examined existing theories to create a research framework to apply to the collection and analysis of data. As recommended in section 5.7 that framework provides practitioners with a rigorous approach for managing their information security environment.

#### 5.6.5 Appropriateness of case study research

There is a growing body of research that indicates that the qualitative paradigm will assist in increasing our understanding of issues facing IS researchers and practitioners (Benbasat, Goldstein & Mead 1987; Franz & Robey 1987, Lee 1989, Cavaye 1996; Doolin 1996; Trauth 1997). The successful application of this multiple case study design to collect data to examine the information security issues in Australian business provides additional support for the appropriateness of case study research for the discipline of IS.

### 5.7 Implications for practice

The application of this study's information security framework will enable an organisation to obtain a detailed understanding of its information security environment, and then to take appropriate steps to manage that environment. This framework can also be applied as an information security awareness and improvement program. The stages of the security framework (that was developed and implemented in the collection and analysis of data for this study) are:

#### Stage 1 – Identify Information Security Risks

- a. Determine the organisation's reliance on IT.
- b. Assess what the potential information security threats are to the organisation.
- c. Determine if the organisation could be at risk (or a specified target) due to the nature of its business.
- d. Conduct an audit of information security incidents that the organisation has experienced in its recent history.
- e. Assess the likelihood of any differentiators that may create a situation where the organisation has a different information security posture to that of other Australian organisations.
- f. The output of this stage is a ***Threat and Risk Assessment***.

#### Stage 2 – Management of the Security Risks

- a. Identify what the current information security countermeasures are that are used within the organisation.
- b. Conduct a gap analysis to determine if the countermeasures employed make sense in comparison to identified risks.

- c. Conduct an assessment of the information security budget and match it to organisational countermeasures plan.
- d. The output of this stage is a *list of required countermeasures* and an *information security budget estimate*.

### Stage 3 – Action Plan

In the final stage a plan is developed for the implementation of the countermeasures to ensure the organisation can overcome the threats and risks identified in stage 1 with the countermeasures highlighted in stage 2. The on-going monitoring of the effectiveness of the plan is essential.

## 5.8 Implications for future research

Suggestions for future research to further the body of knowledge in relation to information security in Australia were provided in sections 5.1 to section 5.5. This section deals with three further recommendations for future research: a longitudinal study, a detailed comparison between information security issues in another country (for example the US or UK), and the use of experimental research techniques. These implications for future research address the limitations of this research discussed in section 1.6.

**Longitudinal study.** Information security issues and the strategies that organisations employ to manage those issues change over time. Therefore, the collection of time series data would provide a greater depth of understanding of information security issues. A longitudinal study of the implementation of the best practice information security management practices (see stages 1 to 3 above) would allow an assessment of the impact of this study's model especially with regards to organisational information security weaknesses and the practical countermeasures to address identified risks.

**Comparison of information security across different countries.** This research explored information security within the Australian business context. As this research has shown, there are a number of differences between Australian information security issues and those reported in the literature for in North America. Future research could compare the findings of this research with similar research undertaken in organisations in another country. For the comparison to be valid the research methodology used in this study would need to be adopted.

**Experimental research techniques.** At times in this research reference has been made to the perception of threats and some of the findings have been presented in anecdotal form. As such there is an opportunity for the conduct of experiments into information security focusing on the nature of information security attacks, perhaps through the establishment of computer systems that could be open for attack or where 'would-be' computer hackers are 'invited' to attempt to exploit security vulnerabilities.

## 5.9 Limitations of this study

Limitations of this research were discussed in sections 1.6. This section outlines two further limitations that should be noted in relation to the findings of this research: that the results are not generalisable; and that the data were collected over a period of two years, and analysed in the third year. 'Write up' occurred subsequently.

Results not generalisable. A weakness of case research is that the findings cannot be generalised across populations (Yin 1994; Cavaye 1996). As case studies were used in this research, no attempt has been made to statistically generalise the results across all organisations in Australia.

Duration of the study. Data were collected for this research in 2002 and 2003 with the analysis conducted in 2004. The time taken for data collection and subsequent analysis and 'write up' was unavoidable due to excessive work commitments. However, constant updates of the literature were conducted to ensure that changes in the information security environment over the course of the study were taken into account. As the field is constantly changing – the data collection time frames must be considered when making conclusions regarding the current issues facing similar Australian organisations.

## 5.10 Concluding remarks

In summary, this research provided insights into information security in the Australian business context through the investigation of organisational reliance on IT; information security threats; actual incidents; countermeasures; Australian businesses as targets; and information security budgets. A qualitative, case based research methodology was used. Prior to this research much of the data used to drive information security management decisions were based either on quantitative research or from studies conducted overseas. Through the development of a theoretical framework, a pragmatic methodology for uncovering information security issues was created. It enables an in-depth understanding of an organisation's information security posture to be gained. As a result, this research has made several significant contributions to both information security theory and practice.

The major findings with regard to this study's research issues are:

- The case-study organisations are generally highly reliant on IT for the conduct of their business and therefore would be heavily impacted if it was unavailable
- They face a variety of information security threats with viruses being the most prevalent threat. The hacking threat was not as evident as reported in the literature
- There are some differences between the Australian information security experience and that reported in the literature for international organisations in particular many of the very large business overseas operate on a much larger scale than those in Australia
- The organisations do not believe that they are specific targets for security attacks; rather they believe that are 'targets of opportunity'

- A wide range of countermeasures are employed; generally, the larger the organisation the greater the diversity and complexity of countermeasures. However, the majority do not have a clear link between risks and countermeasures
- The majority of the organisations do not have a specific security budget.

The objectives of this research have been achieved, with improved insights into the effects of the information security in Australia having been gained. Practitioners now have a framework that enables them to obtain an in-depth understanding of information security threats, incidents, countermeasures, and then to apply appropriate countermeasures.



## REFERENCES

Arquilla, J, and Ronfekdt, D., 1997, *In Athena's Camp – Preparing for conflict in the information age*, RAND, National Defense Institute, Washington.

Australian Bureau of Statistics, Communications and Information Technology, Business Use of Information Technology, 2000, accessed online at <http://www.abs.gov.au>

AusCERT, Australian High Tech Crime Centre, the Australian Federal Police, New South Wales Police, Northern Territory Police, Queensland Police, South Australia Police, Tasmania Police, Victoria Police and Western Australia Police, 2006 *Australian Computer Crime and Security Survey*, access online <http://www.auscert.org.au/crimesurvey>

Babbie, E. 1995. *The practice of social research* (7th ed.). Belmont, CA: Wadsworth.

Baker, W.H., Hylender, D.C., and Valentine, A.J. 2008, *2008 Data Breach Investigations Report*, Study Report, Verizon Business.

Bandyopadhyay, K., Mykytyn, P., and Mykytyn, K, 1999, 'A framework for integrated risk management in information technology', *Management Decision*, Vol. 37, No.5, pp 437-444.

Bejtlich, R., 2004, 'The Tao of Network Security Monitoring and Extrusion Detection', Addison-Wesley Professional.

Bequai, A., 1998, 'A guide to Cyber-Crime Investigations', *Computers and Security*, Vol.17 pp. 579-582.

Bischoff, G., 2001, 'Fear of a black hat', *Telephony*, Vol. 241, Issue 10, pp 24-33.

Bissett, A., and Shipton, G., 2000, 'Some human dimensions of computer virus creation and infection', *International Journal of Human-Computer Studies*, No.52, pp 899-913.

Briney, A. 1998, '1998 – Annual Industry Survey', *Information Security*, December 1998, accessed online, <http://www.infosecurity.com>.

Brown, P., 2001, 'Internet economy booming: report', *The Australian*, 26 July 2001, accessed online, <http://www.australianIT.com.au>.

Caelli, W., Longley, D., and Shain, M., 1989, *Information Security for Managers*, Stockton Press, New York.

\_\_\_\_\_, 1994, *Information Security Handbook*, Macmillian, Basingstoke.

\_\_\_\_\_, 2005, Gaskell, G.I and Longley, D., High Risk System Integrity Controls. *Information Risk Management & Audit (IRMA) Journal*, 15(3):5--8, 2005.

Ceraolo, J., 1998, 'The Devil you know', *Computer Security Institute Newsletter*, March, No.180.

Cavaye, A. L. M. (1996). "Case Study Research: a multi-faceted research approach for IS." *Information Systems Journal* **6**: 227 - 242.

Conrow, E.H. and Shishido, P.S., 1997, 'Implementing risk management on software intensive projects', *IEEE Software*, May/June, pp. 83-9.

Davis, D and Cosenza, R.M., 1993, *Business Research for Decision Making*, Belmont, California, Wadsworth.

Dearne, K., 2002A, "Business ignores hacking dangers", *The Australian*, 30 April 2002.

Dearne, K., 2002B, "Cyber Crime Doubles", *The Australian*, 21 May 2002.

Denning, D.E. 1999, *Information Warfare and Security*, Addison-Wesley, New Jersey.

Denning pers comms 2001

Dhillon, G., *Principles of Information Systems Security: text and cases*, John Wiley & Sons, 2007

Di Gregoria, J, and King, G., 2000, *The Current State of Play: Australia and the Information Economy*, National Office of Information Economy, accessed online <http://www.noie.gov.au/>

Dinnie, G., 1999, 'The second annual global information security survey', *Information Management and Computer Security*, Vol 7, No.3, pp. 112-120.

Dojkovski, S, Lichtenstein, Sharman and Warren, Matthew 2007, Fostering information security culture in small and medium size enterprises: an interpretive study in Australia, in *Proceedings of the 15th European Conference on Information Systems*, University of St. Gallen, St. Gallen, Switzerland, pp. 1560-1571.

Ernst and Young, 1996, 'The Ernst and Young International Information Security Survey 1995', *Information Management and Computer Security*, Vol 4, No. 4, pp 26-33.

Escamilla, T., 1998, *Network security beyond the firewall*, Wiley, Toronto.

Eschelbeck, G., 2000, Active Security – A proactive approach for computer security systems', *Journal of Network and Computer Applications*, Vol. 23, pp 109 – 130.

Fenn, D., 2001, 'Hacked!', *Inc.*, Vol 23, Issue 12, pp134 – 140.

Fisher, R.P., 1984, *Information Systems Security*, Prentice-Hall – Inc, New Jersey.

Frazer, L., and Lawley, M., 2000, *Questionnaire design and administration*, John Wiley and Sons, Brisbane.

Furnell, S.M. and Warren, M.J. 1999a, 'Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?', *Computers and Security*, Vol.18, No.1, pp. 28-34.

\_\_\_\_\_ 1999b, 'Cyber-terrorism – The political evolution of the computer hacker', *Australian Institute of Computer Ethics Conference*, July, Lilidale.

\_\_\_\_\_, Dowland, P.S., and Sanders, P.W., 1999, 'Dissecting the "Hacker Manifesto"', *Information Management and Computer Security*, Vol. 7, No.2, pp 69 – 75.

Gable, G.G. 1994, 'Integrating case and survey research methods: An example in information systems', *European Journal of Information Systems*, Vol.3, No.2, pp.112 - 26.

Gaudin, S., 2000, 'Case Study of Insider Sabotage: The Tim Lloyd/Omega Case', *Computer Security Journal*, Vol XVI, No.3, pp 1 –8.

Ghosh, S., and Schumacher, H.J., 1997, 'A fundamental framework for network security', *Journal of network and computer applications*, Vol 20, No.3, March 1997, pp.305-322.

Gillham, B., 2000, *Case Study Research Methods*, Continuum, New York.

Gouldson, T., 2001, 'Hackers and crackers bedevil business world', *Computing Canada*, Vol.27, Issue 16, pp13 – 14.

Guba, E.G. & Lincoln, Y.S. 1994, 'Competing paradigms in qualitative research', in *Handbook Qualitative Research*, eds N.K. Denzin & Y.S. Lincoln, Sage, Thousand Oaks, pp.105-17.

Halliday, S., Badenhorst, K., and von Solms, R, 1996, 'A business approach to effective information technology risk analysis and management', *Information Management and Computer Security*, Vol. 4, No.1, pp.19-33.

Hancock, B. 2000, 'From the Editor', *Computers and Security*, Vol. 19, No.1, pp. 6 – 17.

Harrison, A. 1999, 'Cost of cyber attacks rises sharply', *Computerworld*, January 1999, accessed online, <http://www.computerworld.com>.

Hassler, V., 2001, *Security fundamentals for e-commerce*. Artech House Inc, Norwood.

Healy, M. & Perry, C. 1999, Validity and reliability of qualitative research within the realism paradigm, unpublished paper.

Hedges, A. 1985, 'Group interviewing', *Applied Qualitative Research*, ed., R. Walker, Gowe, Aldershot.

Hinde, S., 1998. 'Cyber Wars and Other Threats', *Computers and Security*, Vol. 17, No.2, pp.115 – 118.

Hutchinson, W. and Warren. M., 2001a., Information Warfare and Ethics, *Australian Journal of Information Systems*, Vol 8, No 2, pp. 58-62, University of Wollongong, Australia

\_\_\_\_\_, 2001b. *Information Warfare – corporate attack and defence in a digital world*, Butterworth-Heinemann, Oxford.

Johanson, S., and Park, B., 2001, 'Australia so far escaping hacker war', *The Age*, <http://www.theage.com.au>, accessed 3 May 2001.

Kearvell-White, B., 1996, 'National UK Computer Security Survey', *Information Management and Computer Security*, Vol.4, No.3, pp 3-17.

Khadraoui, D., and Herrman, F., 2007, *Advances in Enterprise Information Technology Security – Illustrated Edition*, Premier Reference Source.

Lichtenstein, S. 1998, 'Internet Risks For Companies', *Computers and Security*, Vol. 17, No.2, pp.143 – 150.

Lowe, S., 2002, 'Computer virus victims urged to change passwords' *The Age*, 5 October 2002, <http://www.theage.com.au> , accessed online 10 Jun 09.

McClure, S., J. Scambray & G. Kurtz. 2005 *Hacking Exposed: Network Security Secrets and Solutions*. Berkeley: Osborne Press.

McFarlan, W., McKenny, J., and Pyburn, P., 1983, 'The Information Archipelago: Plotting a Course', *Harvard Business Review*, Vol.61.No.1, pp.145-156.

McNurlin, B. & Sprague, R 1998, *Information Systems Management in Practice*, 4<sup>th</sup> edn., Prentice Hall, New Jersey.

McPhail, J. 2000, 'Foundations of Research', *Research Methodologies Study Guide No 1*, Distance Education Centre, Toowoomba.

Miles, M.B. and Huberman, A.M. 1994, *Qualitative Data Analysis – An Expanded Sourcebook*, Sage, Newbury Park.

Neuman, W.L. 1994, *Social Science Research Methods Qualitative and Quantitative Approaches*, Allyn and Bacon, Boston, pp. 406-9.

NUA, 2001, 'Insiders the biggest security threat', *NUA Internet Surveys*, 21 Jun 01, <http://www.nua.ie/surveys> accessed on 15 Aug 01.

OECD discussion paper, 'Defining and measuring electronic commerce,' National Office of Information Economy, February 10, 2000.

Perry, C. 1998, 'Processes of a case study methodology for post graduate research in marketing', *European Journal of Marketing*, Vol. 32, No. 9, pp. 785-802.

\_\_\_\_\_, Riege, A. & Brown, L. 1998, 'Realism rules ok: Scientific paradigms in marketing research about networks', *Proceedings of ANZMAC 98 Conference*, University of Otago, Dunedin, December, pp. 1-12.

Power, R. 2000a, *Tangled Web – Tales of Digital Crime From the Shadows of Cyberspace*, Que, Indianapolis.

Power, R., 2000b 'Stop living in denial about DoS attacks', *Computer Security Institute Newsletter*, No. 203, February.

Rapalus, P. 2000. *Ninety percent of survey respondents detect cyber attacks, 273 organisations report \$265, 589, 940 in financial losses*, Press Release, Computer Security Institute, 22 March 2000.

\_\_\_\_\_, 2001., *Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar*, Press Release, Computer Security Institute, 12 March 2001.

Richardson, R., 2007, *2007 CSI Computer Crime and Security Survey*, Computer Security Institute, <http://www.csi.com>, accessed 4 April 2008

Schwartau, W. 1997, *Information Warfare – Cyberterrorism: Protecting Security in the Electronic Age*, 2<sup>nd</sup> Edition Thunder's Mouth Press, New York.

Seidman, I.E, 1997, *Interviewing as qualitative research: a guide for researchers in education and social science*, 2<sup>nd</sup> Edition, Teachers College Press, New York.

Stainback, S.B., & Stainback, W., 1988, *Understanding and Conducting Qualitative Research*, Kendall/Hunt, Dubuque.

Thompson, D., 1998, '1997 Computer crime and security survey', *Information Management and Computer Security*, February, Vol.6. No. 2, pp.78-101.

Thomson, J., 2009, 'Conflicker computer virus to take new turn on April Fools day', <http://www.smartcompany.com.au> , 30 March 2009, accessed online 10 June 2009.

Varadarjan, P. 1996, 'From the editor: Reflections on research and publishing', *Journal of Marketing*, Vol. 60, October, pp. 3 –6.

Ward, J. & Griffiths, P. 1998, *Strategic Planning for Information Systems*, 2<sup>nd</sup> Edition, Wiley, Chichester.

Warren, M.J., & Hutchinson, W. 2003, 'Australian Hackers and Ethics', *Australian Journal of Information Systems*, Vol.10.No.2, pp.151-156

Warren, M. 2008 Hackers and Cyber Terrorists, *Encyclopedia of Information Ethics and Security*, pp. 304-311, Information Science Reference IGI Global, USA

Warren, M. 2008 Computer Crime, *Ethics in ICT: an Australian perspective 1st ed.*, pp. 165-178, Pearson Education Australia, Australia

Westwood, C., 1997, *The future is not what it used to be: Conflict in the Information Age*, Air Power Studies Centre, Department of Defence, Canberra.

Williamson, K., Lichtenstein, S., Sullivan, J. and Schauder, D. (2006) To Choose or Not to Choose: Exploring Australians` Views about Internet Banking, *International Journal of Technology and Human Interaction*, Vol 2, No 4, pp. 17-33, Idea Group Publishing, Hershey, PA

Withers, S, 2002, 'IT reliance key to disaster recovery planning', ZDNET UK, 13 Aug 2002, <http://news.zdnet.co.uk> accessed on 10 Apr 2007.

Van Doorn, L., Computer Break-ins: A Case Study, Case Study Report, Vrije Universiteit, Amsterdam, The Netherlands.

Venter, H.S., and Eloff, J.H.P., 1998, 'Data Packet Intercepting on the Internet: How and Why? A Closer Look at Existing Data Packet-Intercepting Tools, *Computers and Security*, Vol. 17, pp 683 – 692.

Yin, R.K. 1994, *Case Study Research – Design and Methods*, Applied Social Research Methods Series, Vol.5., 2<sup>nd</sup> edn, Sage, Newbury Park.

Zikmund, W.G, 1997, *Business Research Methods*, Fifth Edition, The Dryden Press, Oklahoma.

## **APPENDIX A – INTERVIEW PROTOCOL**

Preliminary Information.

### **Introductions**

Interviewer introduces himself as Warren Darragh.

**Purpose** – I am conducting research as part of my dissertation for my Master of Information Technology degree, studied through the Faculty of Business and Commerce at the University of Southern Queensland.

**Topic** – A study into IT Security in Australia – Computer, Data, and Network security in an Australian business context.

**Confidentiality** – Confidentiality is assured. There will be no linkage between a specific organisation and the information it supplies. Only aggregate information will be used. Specific instances will be referred to in very general terms, ‘.... such as one large organisation’

**Interview recorded** – It is my intention to use a mini-disc recorder and microphone to record this interview. The mini-disc and microphone are in plain sight. The reason for recording the interview is to ensure that the notes I take are accurate. It is also my intention to provide you with a copy of my notes to ensure that the information recorded is a true and accurate reflection of the interview.

**Duration** – The expected duration of the interview is 45 minutes.

Conduct of the interview – The interview will be conducted in five parts

- a. IT in your organisation
- b. Threats to computers, data, and networks in your organisation
- c. Computer, data, and network security incidents
- d. Security Practices and Procedures
- e. Your organisation

## **Section A - Use of IT within your organisation**

The aim of this part of the interview is to understand an organisation's level of reliance on Information Technology. The underlying question that needs to be asked in relation to Information Security is what is the impact or result of the loss of use of IT resources.

Research Issue: 1 (Reliance on IT within an organisation).

Tell me the story/about your organisation's reliance on IT?

Possible probe questions/or points (ie what about, tell me about)

- Reliance/level of.
- Business and enhancement.
- E-commerce.
- B2B.
- Intranet.
- Training.
- Customers/orders processed online?
- What happens when it doesn't work?

## **Section B - Threats to computers, data, and networks**

This section relates to RI 2 and 3. This section aims at identifying the type and nature of Information Security threats and how prevalent or serious they are. This section attempts to discover if organisations perceive that they are targeted for specific reasons, i.e. due to the type of organisation.

Please tell me about the threats that your organisation's systems. Where do they originate from?

Possible probe questions.

- Individual hackers.
- Organised groups of hackers.
- Issue motivated groups.
- Foreign governments.
- System users.
- Suppliers.
- Competitors.

Of these which would you describe as the most significant risk?

How do you know about these threats?

- Experience
- Study



- Research.

Do you believe that your organisation is targeted? Why?

### **Section C - Computer, data, and network security incidents**

This section relates to RI 2 and 3.

Section C, which deals with specific incidents may provide evidence that the organisation has been targeted. The comparison component of this research issue can only be answered by review previous research.

Can you relate to me any experiences that your organisations may have had of computer, data, or network security incidents?

Possible probe questions.

- Viruses.
- Employee Access abuse.
- Theft or destruction of resources.
- Leak incidents.
- Data destruction.
- Access abuses.
- Unauthorised access.
- Hacking.

Please describe/detail which type of incident you believe is the most prevalent/significant? Why?

Could you estimate the monetary value of any losses you have had as a result of any breaches

### **Section D - Security Practices and Procedures**

This section relates to RI 4 and aims at discovering the systems, methods and techniques used by the organisation to protect themselves from information security incidents.

Can you tell me how your organisation protects itself from the threat?

Possible probe questions.

- Database of security incidents.
- Conduct of investigations.
- CERT.
- Firewalls.
- Risk Management.
- IT Policy and procedures.
- Training.
- Disaster recovery plans.

How much money would you estimate your organisation would spend on IT security?

This question attempts to answer RI 5.

### **Section E - Your Organisation**

This section gathers demographic information.

What is your position title? \_\_\_\_\_

What is the category of your organisation? \_\_\_\_\_

What is the mission of your organisation? \_\_\_\_\_

What is the role of IT within your organisation? \_\_\_\_\_

How long have you been with your organisation?

### **Conclusion of interview**

Thank interviewee for allowing the interview.

Assure of confidentiality.

Remind if intention to send a record of the interview to ensure that the record is accurate.

Ask if they want a copy of the aggregate results of the study.

## **APPENDIX B – SURVEY INSTRUMENT**

(Intentionally blank)

*Information Security*



An Australian survey

This survey, which is sponsored by the University of Southern Queensland, will produce findings about Information Security in Australia, which should benefit you, and author organisations who rely on Information Technology.

**Please complete the following questions. If you wish to comment on any questions or qualify your answers, please use the space provided on the back cover.**

Section A: Information Technology in your Org

Faculty of Business and Commerce  
University of Southern Queensland  
TOOWOOMBA QLD 4350

<p><b>A1.</b> My organisation's networks are connected to the Internet <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	<p><b>A4.</b> Does your organisation have written procedures governing the use of IT resources (Such as software manuals, rules for use etc)? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p>
<p><b>A2.</b> What is your organisation's annual IT&amp;T budget? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Less than \$10 000</p> <p><input type="checkbox"/> \$10 000 to \$50 000</p> <p><input type="checkbox"/> \$50 000 to \$250 000</p> <p><input type="checkbox"/> \$250 000 to \$1 000 000</p> <p><input type="checkbox"/> More than \$1 000 000</p>	<p><b>A5.</b> My organisation's computing networks are connected to other companies' networks? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p> <p><b>A6.</b> My organisation conducts business online? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p>
<p><b>A3.</b> How many computers and computer network devices are connected to your organisation's networks? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Less than 50</p> <p><input type="checkbox"/> 50 to 200</p> <p><input type="checkbox"/> 200 to 500</p> <p><input type="checkbox"/> 500 to 1000</p> <p><input type="checkbox"/> 1000 to 5000</p> <p><input type="checkbox"/> More than 5000</p>	<p><b>A7.</b> My organisation has a web page? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p> <p><b>A8.</b> Do most users receive training on the use of IT resources including how to access data and use software packages? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p>

The following statements describe possible objectives or uses of IT within an organisation. For each statement please indicate the extent to which it applies to your organisation.

For each of the following statements, please tick the box which best describes your opinion. *(Please rate your agreement or disagreement by ticking the appropriate box using the following scale)*

<b>1 = Strongly Agree</b> <b>2 = Agree</b> <b>3 = Neutral</b> <b>4 = Disagree</b> <b>5 = Strongly disagree</b> <b>NA = Not applicable</b>						
	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>NA</b>
<b>A9.</b> IT Improves the operational effectiveness of my organisation.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>A10.</b> IT Improves managerial effectiveness in my organisation.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>A11.</b> IT networks improve information sharing in my organisation.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>A12.</b> IT is an essential component of business operations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>A13.</b> If the IT doesn't work the organisation does not work.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>A14.</b> My organisation has little or no reliance on IT.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>A15.</b> My organisation has a clearly defined IT management structure.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>A16.</b> Would you like to make any other comments about the use of IT within your organisation? <i>(Please use the space provided below)</i>						
<b>Please proceed to Section B Threats</b>						

<b>Section B: Threats to Information Security</b>						
<p>This section relates to the threats that you perceive exist to computers, networks, and the data that reside on those systems. The threat, in relation to this study refers to who or what originates a computer or network security incident rather than the method employed (ie denial of service attack or data theft).</p> <p>For each of the following statements, please tick the box which best describes your opinion.  <i>(Please rate your agreement or disagreement by ticking the appropriate box using the following scale)</i></p>						
<p><b>1 = Strongly Agree</b>  <b>2 = Agree</b>  <b>3 = Neutral</b>  <b>4 = Disagree</b>  <b>5 = Strongly disagree</b>  <b>NA = Not applicable</b></p>						
	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>NA</b>
<b>B1.</b> Individual hackers are a threat to my organisation's computers, data, and networks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>B2.</b> Organised groups of hackers are a threat to my organisation's computers, data, and networks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>B3.</b> Issue motivated groups are a threat to my organisation's computers, data, and networks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>B4.</b> Foreign governments are a threat to my organisation's computers, data, and networks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>B5.</b> My organisation's competitors are a threat to my organisation's computers, data, and networks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>B6.</b> Foreign business competitors are a threat to my organisation's computers, data, and networks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>B7.</b> My organisation's IT users are a threat to my organisation's computers, data, and networks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>B8.</b> There is no threat to my organisation and its' computing networks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>B9.</b> Overall, I would classify the threats to my organisation's IT as significant.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>B10.</b> My knowledge on the threats faced by my organisation is based on research.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>B11.</b> My knowledge on the threats faced by my organisation is based on my experience.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>B12.</b> My knowledge on the threats faced by my organisation is based on study and training on the topic.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

<p><b>B13.</b> Which of the following threats do you perceive as potential threats (or likely threats) to your organisations IT resources? <i>(More than one box may be ticked)</i></p>			
Individual Hackers	<input type="checkbox"/>	Computer Viruses	<input type="checkbox"/>
Organised groups of hackers	<input type="checkbox"/>	Lack of security policy and procedures	<input type="checkbox"/>
Issue motivated groups	<input type="checkbox"/>	Lack of adherence to security procedures	<input type="checkbox"/>
Competitors	<input type="checkbox"/>	Lack of knowledge on security issues	<input type="checkbox"/>
Foreign competitors	<input type="checkbox"/>	Apathy	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	Partners or suppliers with connectivity and access to your systems	<input type="checkbox"/>
Disgruntled employees	<input type="checkbox"/>	Customers with connectivity and access to your systems	<input type="checkbox"/>
System users in General	<input type="checkbox"/>	Lack of resources committed to security	<input type="checkbox"/>
<p><b>B14.</b> Would you like to make any other comments about the threats to the IT resources of your organisation? <i>(Please use the space provided below)</i></p>          			
<p><b>Please proceed to Section C: Information Security incidents.</b></p>			



<b>Section C: Information Security Incidents</b>	
<b>The following questions relate to computer security incidents that have occurred at your organisation.</b>	
<p><b>C1.</b> Has your organisation experienced any unauthorised use of its IT resources within the last 12 months? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No        -----&gt; <i>Please go to Section D</i></p>	<p><b>C6.</b> How many of your recorded incidents originated from within the organisation? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> 1-5            <input type="checkbox"/> 6 - 10        <input type="checkbox"/> 11 - 20</p> <p><input type="checkbox"/> 21 - 50        <input type="checkbox"/> 51 - 100</p> <p><input type="checkbox"/> More than 100 <i>(please specify)</i></p>
<p><b>C2.</b> How many separate incidents have occurred? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> 1-5            <input type="checkbox"/> 6 - 10        <input type="checkbox"/> 11 - 20</p> <p><input type="checkbox"/> 21 - 50        <input type="checkbox"/> 51 - 100</p> <p><input type="checkbox"/> More than 100 <i>(please specify)</i></p>	<p><b>C7.</b> Please estimate the monetary value of losses that have resulted from breaches to your organisation's Information Security <i>(Include the costs of loss of resources, hardware, time, resources required to fix the problem)</i></p> <p><input type="checkbox"/> No losses    <input type="checkbox"/> Less than \$10 000</p> <p><input type="checkbox"/> \$10 000 to \$50 000</p> <p><input type="checkbox"/> \$50 001 to \$100 000</p> <p><input type="checkbox"/> \$100 001 to \$500 000</p> <p><input type="checkbox"/> More than \$500 000</p> <p><input type="checkbox"/> Don't know   <input type="checkbox"/> Intangible</p>
<p><b>C3.</b> How many of these incidents originated from outside the organisation? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> 1-5            <input type="checkbox"/> 6 - 10        <input type="checkbox"/> 11 - 20</p> <p><input type="checkbox"/> 21 - 50        <input type="checkbox"/> 51 - 100</p> <p><input type="checkbox"/> More than 100 <i>(please specify)</i></p>	<p><b>C8.</b> Was your organisation's Internet connection a source of security attacks? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p>
<p><b>C4.</b> Was your organisation's remote dial-in service a source of security attacks? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p>	<p><b>C9.</b> The number of security incidents in my organisation over the last 12 months has: <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Increased            <input type="checkbox"/> Decreased</p> <p><input type="checkbox"/> Stayed the same    <input type="checkbox"/> Don't know</p>
<p><b>C10.</b> Which of the following incidents has your organisation experienced in the last 12 months? <i>(More than one box may be ticked)</i></p>	

- Viruses
- Information Leaks  
*(Information being released to unauthorised parties)*
- Theft of IT resources. *(i.e. laptop theft)*
- Destruction of IT resources  
*(ie hard drives destroyed, CD-ROMS, computers etc)*
- Theft or destruction of data *(theft or deletion of organisational data)*
- Unauthorised access by employees
- Industrial espionage  
*(Security incidents, including those types that are listed in this question that you believe can be traced to competitors)*
- Unauthorised use by contractors/suppliers/customers
- System Penetration from outside *(Including breaking into company IT networks, system probes, defacing web sites, running programs, altering or modifying system settings)*
- Denial of Service  
*(Attack that stops or prevents system users from accessing resources)*
- Financial fraud  
*(The use of your organisation's computer systems for personal financial benefit)*
- Employee abuse of Internet  
*(Accessing inappropriate web sites, general surfing instead of work)*
- Other *(Please specify)*

**C11.** Using the scale below please indicate your opinion as to where your security breaches have originated?

- 1 = Very Likely**
- 2 = Likely**
- 3 = Neutral**
- 4 = Unlikely**
- 5 = Very Unlikely**
- NA = Not applicable**

	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>NA</b>
Individual Hackers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Organised groups of hackers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Issue motivated groups	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Competitors	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign competitors	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Suppliers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Disgruntled employees	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System users in General	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

On the scale indicated below, please indicate the frequency of attacks relating to the listed access points?

- 1 = Least Frequent
- 2 = Not Frequent
- 3 = Frequent
- 4 = Most Frequent
- NA = Not applicable

	1	2	3	4	NA
Internal systems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Internet Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Remote dial-in access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify, i.e. direct business to business link)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**C12.** Were the Information Security incidents reported to an organisation outside of your company? (Please tick one box)

- Yes Go to question C13       Don't Know
- No Go to question C14

**C13.** Who did you report the incident(s) to? (More than one box may be ticked)

- Police       Customers       Suppliers       AusCERT
- Partners       Other (Please specify)

(If you reported all incidents please proceed to Section D, otherwise proceed to question C14.)

**C14.** Please indicate below your reasons for not reporting incidents?

**C15.** Would you like to add any other comments about Information Security incidents? (Please use the space provided below)

**Section D: Security Practices and Procedures**

The following section relates to those IT security practices and procedures that your organisation has established in anticipation of likely threats or as a result of past incidents.

**D1.** A database of security incidents is maintained by my organisation? (Please tick one box)

- Yes       Don't Know
- No

**D6.** My organisation has an IT security policy. (Please tick one box)

- Yes       Don't Know
- No

<p><b>D2.</b> Security investigations are conducted by my organisation and action is taken to remedy problems? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p>	<p><b>D7.</b> Training is conducted in my organisation on Information Security issues. <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p>
<p><b>D3.</b> My organisation is a subscriber to the Australian Computer Emergency Response Teams (AUSCERT) and they are an important part of my organisation's IT security strategy? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No <i>(Please specify if there are any reasons why you choose not use AUSCERT's services)</i></p>	<p><b>D8.</b> My organisation has a disaster recovery plan. <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p> <p><b>D9.</b> My organisation has a business continuity plan. <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p>
<p><b>D4.</b> Encryption is used to protect data in my organisation? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p>	<p><b>D10.</b> Consultants or external agencies are used to provide advice on Information Security related issues. <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p>
<p><b>D5.</b> My organisation uses firewalls to protect its networks? <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p>	<p><b>D11.</b> My organisation has an individual or group of people who are solely responsible for Information Security. <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p>
<p><b>D12.</b> Senior non-IT management are informed of Information Security incidents. <i>(Please tick one box)</i></p> <p><input type="checkbox"/> Yes            <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p>	

For each of the following statements, please tick the box which best describes your opinion. *(Please rate your agreement or disagreement by ticking the appropriate box using the following scale)*

- 1 = Strongly Agree**  
**2 = Agree**  
**3 = Neutral**  
**4 = Disagree**  
**5 = Strongly disagree**

NA = Not applicable

	1	2	3	4	5	NA
<b>D13.</b> My organisation takes Information Security seriously.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>D14.</b> There are probably security incidents on my organisation's computers, data, and networks that are not reported.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>D15.</b> There are probably security incidents on my organisation's computers, data, and networks that are not detected.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>D16.</b> The measures employed by my organisation to ensure computer and network security are effective.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>D17.</b> The number of computer and network related security incidents are increasing.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**D18.** Please indicate in the boxes below the approximate amount of money your organisation commits to Information Security? *(Please tick one box)*

- Less than \$10 000     
  \$10 000 to \$50 000     
  \$50 000 to \$100 000  
 \$100 000 to \$500 000     
  Greater than \$500 000 *(Please Specify)* \_\_\_\_\_

**D19.** Would you like to make any other comments on Information Security Practices and Procedures in your organisation? *(Please use the space provided below)*

### SECTION E: Demographics

These questions relate to the organisation that you work for. These questions are asked in order to make more valid inferences in relation to the findings of this research. The term 'organisation' in this survey refers to your organisation, which is the Australian-based division or business unit that you see yourself as belonging to.

<p><b>E1.</b> Please indicate the primary function performed by your organisation. <i>(Please tick the nearest equivalent box)</i></p>	<p><b>E2.</b> What is your position title in the organisation?</p> <p>_____</p>
<ul style="list-style-type: none"> <li><input type="checkbox"/> Manufacturing</li> <li><input type="checkbox"/> Wholesale and retail trade</li> <li><input type="checkbox"/> Financial Services</li> <li><input type="checkbox"/> Mining</li> <li><input type="checkbox"/> Transport and Storage</li> <li><input type="checkbox"/> Construction</li> <li><input type="checkbox"/> Business Services</li> <li><input type="checkbox"/> Communications and Media</li> <li><input type="checkbox"/> IT &amp; T</li> <li><input type="checkbox"/> Agriculture/Forestry</li> <li><input type="checkbox"/> Government (Federal)</li> <li><input type="checkbox"/> Government (State)</li> <li><input type="checkbox"/> Government (Local)</li> <li><input type="checkbox"/> Other (Please specify)</li> </ul> <p>_____</p>	<p><b>E3.</b> What is the level of your position in the organisation? <i>(Please tick the nearest equivalent)</i></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> CEO</li> <li><input type="checkbox"/> Senior Management</li> <li><input type="checkbox"/> Middle Management</li> <li><input type="checkbox"/> Supervisory Level</li> <li><input type="checkbox"/> Other <i>(Please specify)</i></li> </ul> <p>_____</p> <p><b>E4.</b> Would you classify your position as an IT&amp;T role or a management role? <i>(Please tick appropriate box)</i></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT &amp; T</li> <li><input type="checkbox"/> Management</li> </ul> <p><b>E5.</b> How long have you been with your organisation? <i>(Please tick the nearest box)</i></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Less than 1 year</li> <li><input type="checkbox"/> 1 to 5 years</li> <li><input type="checkbox"/> 6 to 10 years</li> <li><input type="checkbox"/> More than 10 years</li> </ul>
<p><b>A2.</b> Approximately how many staff in total does your organisation employ? <i>(Please tick one box)</i></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Less than 25 full-time staff or equivalent</li> <li><input type="checkbox"/> 25 to 49 full-time staff</li> </ul>	

**E6.** Approximately how many staff in total does your organisation employ? *(Please tick one box)*

- Less than 25 full-time staff or equivalent
- 25 to 49 full-time staff
- 50 to 99 full-time staff
- 100 to 499 full-time staff
- 500 to 2000 full-time staff
- More than 2000 full-time staff

Are there any other comments you would like to make in relation to computer and network security?

If you would like a copy of the research results please write your details in the box below (Confidentiality is assured). Or you can e-mail at [wdarragh@bigpond.com](mailto:wdarragh@bigpond.com) stating that you would like a copy of the research results.

That concludes the survey on computer and network. Thank you for taking the time to complete the questionnaire, you are making a significant contribution to knowledge in the area. Please use the reply paid envelope enclosed to return your response.

## **APPENDIX C - VIRTUAL INTERVIEW**

(See next page)



## Virtual Interview Protocol

### Introduction

Thank you for support research at the University of Southern Queensland. A virtual interview was designed in order to encourage the maximum amount of interview participation as possible. The primary method of data collection for this study is case based in-depth interviews. Where possible these interviews are conducted face-to-face. Given the potential sensitive nature of the topic and a number of fundamental limitations (such as travel and time), this technique has been designed to increase the participants. The more participants the more accurate the data is.

**Confidentiality** - Confidentiality is assured. There will be no linkage between a specific organisation and the information it supplies. Only aggregate information will be used. Specific instances will be referred to in very general terms, '.... such as one large organisation'

**Interview recorded** - The face-to-face interviews are recorded. The virtual interview keeps a transcript of what you type and sends it to the researchers via e-mail when you hit the submit button. The transcript will then be coded and analysed using a number of software techniques that have been specifically designed for this kind of research.

**Duration** - Depending on how fast you type and how much you have to tell us, the expected duration of the virtual interview is 45 minutes.

### Conduct

Conduct of the interview - The interview will be conducted in five parts

- a. IT in your organisation
- b. Threats to computers, data, and networks in your organisation
- c. Computer, data, and network security incidents
- d. Security Practices and Procedures

e. Your organisation

The sections have been designed to ensure that the defined research issues for the study are answered.

**General Instructions**

In each area you will be presented with a general question followed by a series of dot points which are given as possible probe points/issues or questions. Please consider how these issues relate to your organisation in context with the stated question. There is no need to feel limited by the probe questions. They are designed merely to give guidance on the question. Please add any additional points or issues that you feel fit the question(s). Each question has a scrolling textbox in which you can type your response. You will need to use your mouse to select each of the text areas, however you can use the [ENTER] key to create new lines within the text. You may wish to quickly view the scope of the questions asked in each component of the Virtual Interview so that you can better target your responses to each area.

**The virtual interview begins.....**

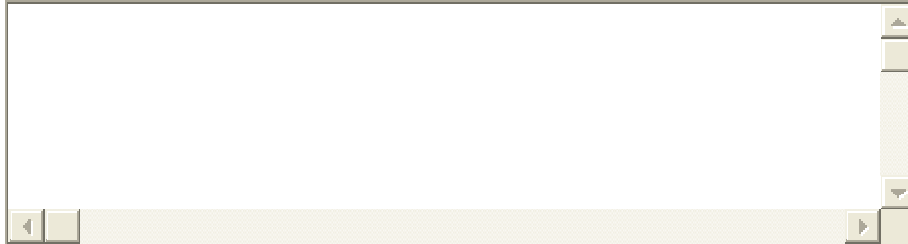
**Use of IT within your organisation**

In the box below please tell the story of your organisations organisation's reliance on IT. ie How reliant is your organisation on IT?

Possible probe questions/or points (ie what about, tell me about etc)

- Reliance/level of.
- What is the scale of IT use in terms of the number of users and the number of computer etc?
- Business and enhancement.
- E-commerce.
- B2B.
- Intranet.
- Customers/orders processed online?

- What happens when the IT doesn't work?
- Do you have a web site?

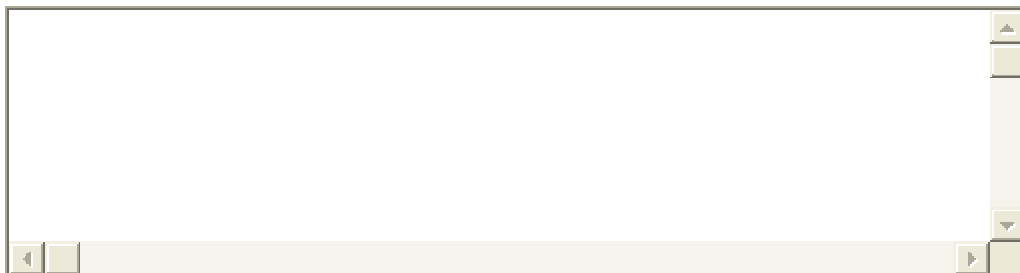


### Threats to computers, data, and networks

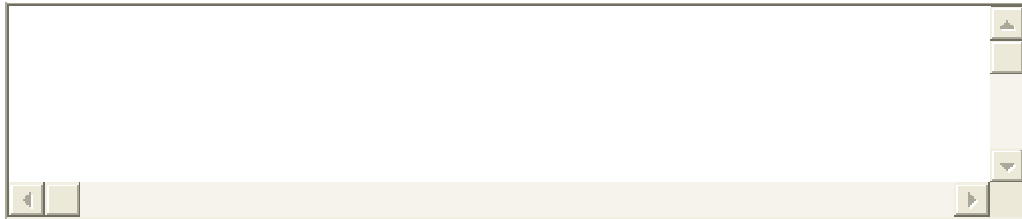
**Please describe the threats to your organisation's systems. Where do they originate from?**

Possible probe questions.

- Individual hackers.
- Organised groups of hackers.
- Issue motivated groups.
- Foreign governments.
- System users.
- Suppliers.
- Competitors.
- Viruses
- Poor quality code?

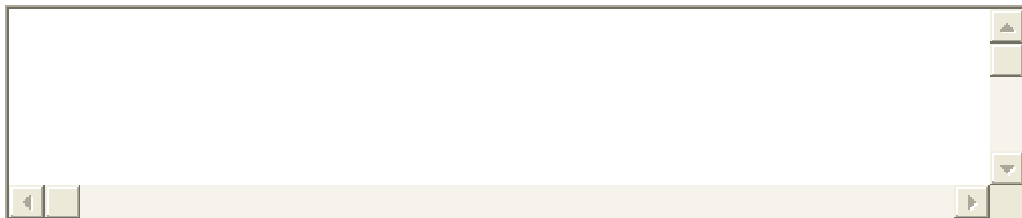


**Of these which would you describe as the most significant risk?  
Why?**

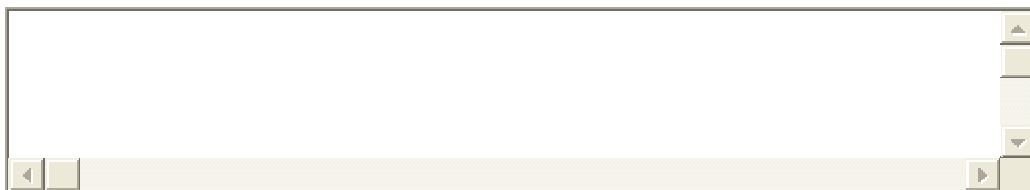
A large, empty rectangular text input box with a light beige background. It features a vertical scrollbar on the right side and a horizontal scrollbar at the bottom, both with small square buttons for navigation.

**How do you know about these threats?**

- Experience?
- Study?
- Research?
- Other?

A large, empty rectangular text input box with a light beige background. It features a vertical scrollbar on the right side and a horizontal scrollbar at the bottom, both with small square buttons for navigation.

**Do you believe that your organisation is targeted? Why?**

A large, empty rectangular text input box with a light beige background. It features a vertical scrollbar on the right side and a horizontal scrollbar at the bottom, both with small square buttons for navigation.

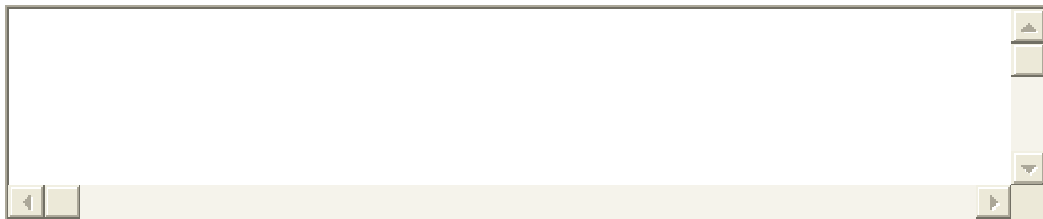
### **Computer, data, and network security incidents**

This section deals with actual Information Security incidents as they may have occurred within your organisation.

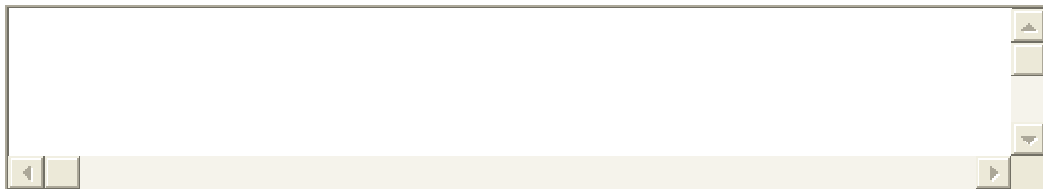
**Can you relate to us any experiences that your organisations may have had of computer, data, or network security incidents?**

Possible probe questions.

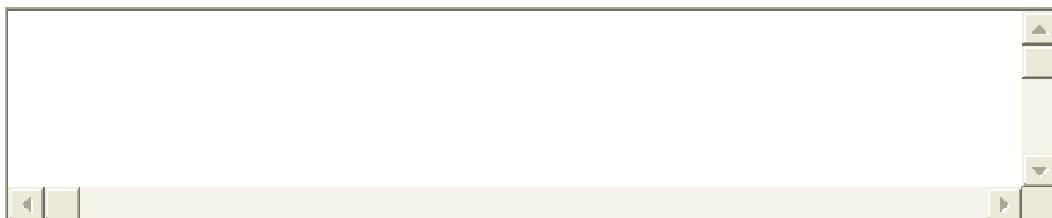
- Viruses.
- Employee Access abuse.
- Theft or destruction of resources (including PC/Laptops).
- Leak incidents.
- Data destruction.
- Access abuses.
- Unauthorised access.
- Hacking.
- Other.

An empty rectangular text input box with a light beige background and a thin grey border. It features standard scrollbars on the right and bottom edges.

**Please describe/detail which type of incident you believe is the most prevalent/significant? Why?**

An empty rectangular text input box with a light beige background and a thin grey border. It features standard scrollbars on the right and bottom edges.

**Could you estimate the monetary value of any losses you have had as a result of any breaches?**

An empty rectangular text input box with a light beige background and a thin grey border. It features standard scrollbars on the right and bottom edges.

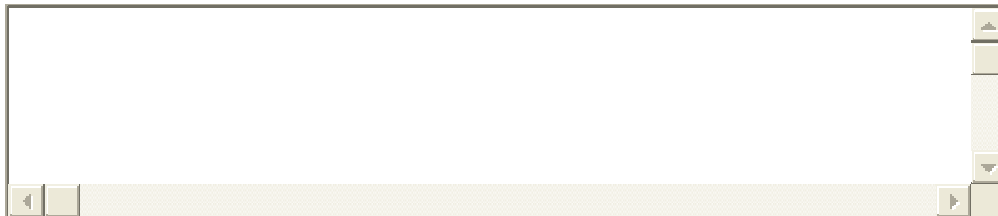
## Security Practices and Procedures

This section deals with the general countermeasures that your organisation uses in order to protect itself from the threat of information security related threats.

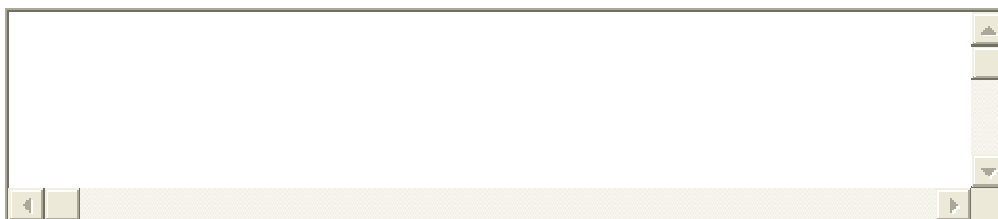
**Can you describe how your organisation protects itself from the threat? What countermeasures do you employ?**

Possible probe questions.

- Database of security incidents.
- Conduct of investigations.
- Security staff (how many)?
- CERT.
- Firewalls.
- IDS
- IT Policy and procedures.
- Training.
- Disaster recovery plans.
- AS/NZS 7799
- Other standards.
- Other counter measures.

A rectangular text input box with a light beige background and a thin black border. It features a vertical scrollbar on the right side and a horizontal scrollbar at the bottom, both with standard arrow and track icons.

**How much money would you estimate your organisation would spend on IT security in a 12 month period?**

A rectangular text input box with a light beige background and a thin black border. It features a vertical scrollbar on the right side and a horizontal scrollbar at the bottom, both with standard arrow and track icons.

## Your Organisation

The final part of the virtual interview is designed to gather information about your organisation. This information is used merely to allow accurate comparisons and benchmarks of similar sized organisations operating within similar industries.

**What is your position title?**

**What is the industry sector of your organisation?**

**Are you a government or a private organisation?**

**How many staff (approx) are there in your organisation?**

**What is the mission of your organisation?**

**What is the role of IT within your organisation (ie support, etc)?**

**How long have you been with your organisation?**

Please include your e-mail address so we can send you a transcript of the interview (to ensure that it is accurate) and also to address any issues that may require clarification.

### **Conclusion of interview**

Thank you for answering the questions and supporting research at the University of Southern Queensland.

Again, I assure you that the information gathered by this research is to be used only for research purposes, and will in no way be linked to you personally or your organisation.

Would you like to make any comments about this research topic or mention anything else that you have yet to state? If so please use the box below.



## **APPENDIX D – LETTER TO PARTICIPANTS**

**«Title» «FirstName» «LastName»  
«JobTitle»  
«Company»  
«City» «State» «PostalCode»**

**Dear «Title» «LastName»**

### **Information Security in Australia**

A good understanding of computer and network security is essential to ensure that Information Technology and Telecommunications systems and devices are used in an effective and efficient manner. Recent media coverage has highlighted that some companies are vulnerable to computer network attacks, viruses, and in extreme cases to industrial espionage. Much of the current knowledge on computer and network security and security related incidents originates from international sources. There has been little informative data gathered in Australia. In order to redress the current information vacuum in this area and to enable Australian IT managers to make more informed decisions in regards computer and network security issues the University of Southern Queensland is conducting research in this area.

Your organisation has been specifically chosen because the nature of your business makes information and information technology important to you. The information gathered in this research will enable organisations like yours to make better-informed decisions regarding information security. Importantly, it will provide clearer information to enable you decide what resources should be committed to combating information security problems such as hackers, computer viruses, and industrial espionage.

We would be most grateful if you could participate by taking part in two short interviews. We require access to two IT managers or IT security staff within your organisation. Each interview is expected to last approximately sixty minutes. The results will be analysed and form the basis of a dissertation on information security.

Information gathered in the interviews will be kept strictly confidential. The results will be published in aggregate form only and we can assure you that there will be no means by which your organisation or employees could be identified. Our aim is to accurately articulate the current state of play in regards to information security problems and issues that Australian business faces. All participants will be making a significant contribution to the current knowledge in the field.

I would like to thank you in advance for your participation in the study. Should you have any questions, please feel free to contact Warren Darragh on 07 3332 7833 or Dr Andy Koronios on 07 46311266. If you are willing to take part of the research we

would greatly appreciate it if you could contact us so arrangements can be made for the conduct of the interviews. Further information for participants can be found on the Internet at the following address:

<http://www.connect.usq.edu.au/students/q9520838/security.htm>

Yours sincerely

Warren Darragh  
Student  
Department of Information Systems  
Faculty of Business and Commerce  
07 3332 7833

[wdarragh@bigpond.com](mailto:wdarragh@bigpond.com)

Dr Andy Koronios  
Associate Professor  
Department of Information Systems  
Faculty of Business and Commerce  
07 46311266

[koronios@usq.edu.au](mailto:koronios@usq.edu.au)

## **APPENDIX E – EXAMPLE INTERVIEW TRANSCRIPT**

(See following page)

1 Section One

2

3 Use of IT within your organisation

4

5 In the box below please tell the story of your organisations organisation's reliance on  
6 IT. ie How reliant is your organisation on IT? Possible probe questions/or points (ie  
7 what about, tell me about etc)

8

9 Reliance/level of.

10 What is the scale of IT use in terms of the number of users and the number of  
11 computer etc?

12 Business and enhancement.

13 E-commerce.

14 B2B.

15 Intranet.

16 Customers/orders processed online?

17 What happens when the IT doesn't work?Do you have a web site?

18

19

20 Department of State Development has 900 employees, it is a distributed  
21 environment. We have 18 regional offices that are located around Queensland. We  
22 have 10 international offices. There are approximately 500 - 600 staff employeed  
23 within the central business district itself.

24 The network is large and it is shared with the Department of Premiers and Cabinet,  
25 they have approx 800 people as well. They have similar types of regional offices here  
26 in Qld they have no international offices.

27 It is largely a NT4 Client/Server Network. We have a central firewall system located  
28 in Brisbane and then each of the international offices has its own firewall. The  
29 network comprises of a WAN regionally that is linked by ATM/frame relay that is  
30 provided by Telstra. The overseas networks are linked back to Australia using VPN  
31 over the internet.

32

33 The state development assets base is approximately \$6M is capital.

34

35 The organisation runs three major ERP packages. They being SAP for financials, HR  
36 which Aurion we have a business package, called DSD online, it comprises three  
37 components. There is a CRM component, which is applix, which is all the work flow  
38 and history of all of the departments clients. Its a new project, it has been rolled out  
39 to about 200 people as a stage 1 client. Subject to the success of that it will rollout to  
40 the remainder of the department. At the moment it is looking very good. There is also  
41 a component called smart license, gives the ability for businesses to register online it  
42 is a brockorage for a number of other government departments. It allows people to do  
43 all the things they need, get permits etc to start up a business.

44

45 There is a third part which is called the virtual campus which is actually an online  
46 learning facility and thats there so that business can register to do training such as,  
47 'how to write a business plan', and that comprises DSDonline, which is provides  
48 services throughout QLd.

49

50 The whole organisation is structured around the IT infrastructure if the infrastructure

51 doesn't work then nothing gets done. I could use a recent example when we had a fire  
52 in the south of Brisbane that cut the electricity the building went down and we had to  
53 wait for the generators to come up, there was a problem with the generators because  
54 when it came up it blew a circuit and what happened was that systems in one of our  
55 buildings was done for half a day and what it meant was that no one could do any  
56 work and basically we gave the option to go home or do filing.

57

58 If the systems doesn't work then the organisation doesn't work because it can't access  
59 its files and records and the records management system is a paper based system but  
60 it is indexed electronically. So no access to the computer screen and there are no  
61 manual processes there to be used.

62

63 State Development has an induction course. As part of the induction course they get  
64 given an account. Now that account is only good for a five day period at the of that 5  
65 day period they have to go attend what we call a quick start course and that introduces  
66 them to basic applications in the department, its the office suite and it also talks  
67 about internet and computer security issues. If they don't complete that course in the  
68 first five days then their account permissions are revoked until they attend that  
69 course. The course is an internal course.

70

71 With regards the enterprise packages, those courses are conducted by the particular  
72 areas and are conducted on an as required basis. Classes on DSDonline, as a new  
73 product are being run at 20 students per time. People don't get the icon on their  
74 screens until they have done the course. They have to be trained to use it. We use the  
75 profiles and groups features of the operating systems to deny people access until they  
76 have been trained.

77

78

79

80 Section Two

81

82 Threats to computers, data, and networks

83

84 Please describe the threats to your organisation's systems. Where do they originate  
85 from? Possible probe questions.

86 Individual hackers.

87 Organised groups of hackers.

88 Issue motivated groups.

89 Foreign governments.

90 System users.

91 Suppliers.

92 Competitors.

93 Viruses

94 Poor quality code?

95

96

97 We have four threats.

98 1. The internal threat of the dissatisfied user.

99 2. External threat from someone who will try and write a virus and try and infect  
100 the system.

101 3. The natural disaster threat, that's beyond our control.  
102 4. Because we operate in overseas countries is the people who live in those countries.  
103  
104 These threats determine how we structure to operate the IT environment.  
105  
106 We have only had one instance of a hacker. That was the code red - virus, where this  
107 was released and actually appeared on one of our internal systems. Because we are  
108 an international organisation it doesn't look good for people to be greeted that this  
109 site has been hacked by the chinese. We actually tend to look at that a little more  
110 seriously then perhaps a normal user.  
111  
112  
113  
114 Of these which would you describe as the most significant risk? Why?  
115  
116 The one that is giving us the most trouble is viruses.  
117 I would put the risks in order of Viruses first, natural disaster second, internal and  
118 international equal third. They are the low risk.  
119  
120  
121 How do you know about these threats?  
122 Experience?  
123 Study?  
124 Research?  
125 Other?  
126  
127  
128 As part of the organisations' task we are actually responsible to do the business  
129 continuity plan, and as part of the business continuity plan we do a risk assessment,  
130 with regard to network vulnerabilities. We also do it with regard to specific  
131 applications so we go to the business units and say give us your priorities for  
132 restoration should the system go down, you know how critical is this business  
133 application to your system, we then equate the ERP, e-mail, explorer, those kinds of  
134 things, it interesting that each of the business systems, as we go around to the  
135 business units that the risk is not so much someone placing something into the e-mail  
136 system its the person who used to have access to the payroll system for example, the  
137 person who has access to the financial system.  
138  
139 Internally we do our own reviews. We believe that the only way we will know what  
140 is really going on is to go and ask the questions ourselves. With regard to viruses and  
141 hacking we actually engage third parties. We check on maintenance and virus  
142 reports so we can go through and determine what viruses are coming, what have been  
143 identified. We also conduct discussions with the Queensland University of  
144 Technology and talk to Prof Caelli and his team and Mark Lui, we have discussed  
145 the opportunities with organisations such as AUSCERT, however, we haven't really  
146 seen the value in what they can provide.  
147  
148 We don't really see any benefit in AUSCERT as their services are available through a  
149 maintenance agreement with a number of the software and virus packages that we  
150 have anyway.

151 We haven't joined AUSCERT. Its not worth our while.

152

153

154 Do you believe that your organisation is targeted? Why?

155

156

157

158 No evidence of that. We run our own packages to actually check for that.

159 Historically, its mainly university students trying out the theories that they have

160 learnt. Looking at the firewall logs that every university in Australia is represented

161 on there. There is a lot spam activity that comes up against the firewall, but there has

162 been no evidence of any specific attacks, other than lets visit and see what we can do

163 and once they realise that its a firewall on the front of it they tend to go away.

164

165

166 Section Three

167

168 Computer, data, and network security incidents

169

170 This section deals with actual Information Security incidents as they may have

171 occurred within your organisation.

172

173 Can you relate to us any experiences that your organisations may have had of

174 computer, data, or network security incidents?

175 Possible probe questions.

176

176 Viruses.

177

177 Employee Access abuse.

178

178 Theft or destruction of resources (including PC/Laptops).

179

179 Leak incidents.

180

180 Data destruction.

181

181 Access abuses.

182

182 Unauthorised access.

183

183 Hacking.

184

184 Other.

185

186

187 Code red Virus. The departments web site is hosted externally by web central. What

188 happened was that our web development people actually managed that server and

189 even though they had received the warnings to update the service packs on that

190 server for code red is that they hadnt done it and so when code red was released it

191 affected that server by dropping it off the air. We had to close it down and re-build it.

192 The reason that occurred whilst there was an awareness of the protective measures

193 they had not followed through within the time frame that they were required to do it.

194

194 So basically, we have instigated a new set of checks and balances to check on that.

195

196 The other one was the Nimda virus, with that one it actually got inside our system.

197

197 As soon as that happened we cut all external links out to the world and eradicated

198

198 the virus and rebuilt the systems and the re-opened up the systems. That one was

199

199 particularly interesting as not only did we have to do it in the central computing

200

200 system but we also had to do it in each of the nine offices and then internationally

201 and clean those ones as well.  
202  
203 Qld audit are on top of access issues. The biggest issues are people attempting to go  
204 to unauthorised web sites. There is an internal audit program that is right on top of  
205 that.  
206  
207 Theft is an issues, mainly from an external point of view. We have had instances of  
208 people breaking into buildings and stealing laptops, in the last 6 months we have lost  
209 two, in last 12 months there was something like 78 reported incidents of thefts of  
210 laptops in the cbd of brisbane.  
211  
212 PC vault stops people from accessing information if machine is stolen.  
213  
214 Electronic mail stuff has slipped out of the media and appeared in the bottom line.  
215  
216  
217  
218 Please describe/detail which type of incident you believe is the most  
219 prevalent/significant? Why?  
220  
221 Viruses are the most prevelant. We do updates frequently. Because we have  
222 problems getting people to log on and off, we had to write a script to get machines to  
223 log out automatically. Automatic updates are occuring.  
224  
225  
226 Could you estimate the monetary value of any losses you have had as a result of any  
227 breaches?  
228  
229 Don't put a monetary value on it. We have lost probably 2 weeks over the last  
230 financial year.  
231  
232  
233 Section Four  
234  
235  
236 Security Practices and Procedures  
237  
238 This section deals with the general countermeasures that your organisation uses in  
239 order to protect itself from the threat of information security related threats.  
240 Can you describe how your organisation protects itself from the threat? What  
241 countermeasures do you employ?  
242 Possible probe questions.  
243 Database of security incidents.  
244 Conduct of investigations.  
245 Security staff (how many)?  
246 CERT.  
247 Firewalls.  
248 IDS  
249 IT Policy and procedures.  
250 Training.



251 Disaster recovery plans.  
252 AS/NZS 7799  
253 Other standards.  
254 Other counter measures.  
255  
256  
257 Queensland Government has a significant information security standard. Called  
258 information standard 18, it available on the web, its a generic document that each  
259 department has to apply, in some cases it is specific, and other places it is generic.  
260  
261 We use the following:  
262 Passwords  
263 User Accounts  
264 Specific approvals for remote access  
265 Policies  
266 Firewalls, DMZ, Covered circuits (VPN)  
267 Closed networks, that compartmentalised.  
268 Physical security  
269 Backup and storage off-site  
270 specific security areas that are discrete and not accessible.  
271 Compartmentalised information,  
272 Virus software.  
273 Clearances for contractors, staff put into clauses on contracts.  
274 Firewalls logs.  
275 Third party auditors to review the system and checks.  
276 Staff training  
277 Security advisers  
278 Configuration control  
279 Risk management used to determine how we do.  
280 Disaster Recovery Plan. (Separate Facility)  
281 We have a database of security incidents  
282 We have a security professional, and he can do investigations  
283 We run security applications.  
284 Physical systems are located in all of our buildings, buildings have CCTV  
285 Only IDS on firewalls and logs and inspected by FM team  
286 USed AS/NZ 7799.  
287  
288 How much money would you estimate your organisation would spend on IT security  
289 in a 12 month period?  
290  
291 Facilities management contract includes all.  
292 50-100K for software.  
293 About 200 000 per year.  
294 Its an ongoing investment.  
295 Security is a cost of doing business these days.  
296  
297  
298  
299 Section Five  
300

301 Your Organisation  
302  
303 What is your position title?  
304  
305 Director IM  
306  
307  
308 What is the industry sector of your organisation?  
309  
310 Lage Government  
311  
312 Are you a government or a private organisation?  
313  
314 Government  
315  
316 How many staff (approx) are there in your organisation?  
317  
318 600  
319  
320  
321  
322 What is the mission of your organisation?  
323  
324 Grow qld globally to create to more jobs and a better environment for qld  
325  
326  
327 What is the role of IT within your organisation (ie support, etc)?  
328  
329 Business enabler  
330  
331 How long have you been with your organisation?  
332  
333 4 years  
334  
335  
336 E-Mail address  
337  
338  
339  
340  
341 Comments  
342  
343  
344 FILEEND  
345  
  
346  
  
347

## **APPENDIX F – THANK YOU E-MAIL TO PARTICIPANTS**

Thank you for your participation in our research.

Below is the transcript for your interview. Please indicate if it is a correct record of your comments and responses.

If you have not already done so, could you please have another relevant member of your organisation take part in the virtual interview.

Thank you again for your participation in this valuable research opportunity.

regards

Warren Darragh

<begin transcript>