



Trusted Information
Sharing Network
for Critical Infrastructure Protection
.....

LEADING PRACTICES AND GUIDELINES FOR ENTERPRISE SECURITY GOVERNANCE

June 2006
(Revision 1, August 2007)



Trusted Information
Sharing Network
for Critical Infrastructure Protection

ISBN 0 642 75361 X

© Commonwealth of Australia 2006

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968* no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to:

Commonwealth Copyright Administration
Attorney-General's Department
Robert Garran Offices
National Circuit
BARTON ACT 2600

Or visit www.ag.gov.au/cca



Contents

1	EXECUTIVE SUMMARY	1
1.1	BACKGROUND	1
1.2	WHAT ARE THE DRIVERS, RISKS AND THREATS TO SECURITY FOR CRITICAL INFRASTRUCTURE INDUSTRIES?	2
1.3	WHAT IS SECURITY GOVERNANCE?	3
1.4	HOW IS SECURITY GOVERNANCE RELATED TO SECURITY MANAGEMENT?	3
1.5	WHY IS SECURITY GOVERNANCE IMPORTANT?	4
1.6	HOW CAN WE ACHIEVE STRONG SECURITY GOVERNANCE?	5
1.7	CONCLUSION	6
2	DISCLAIMER	8
3	PROJECT OVERVIEW	10
3.1	BACKGROUND	10
3.2	APPROACH	10
3.2.1	RESEARCH	10
3.2.2	CONSULTATIONS	11
3.3	DELIVERABLES	12
3.3.1	BOARD OF DIRECTORS AND CEO GUIDANCE	12
3.3.2	CIO, CISO AND PRACTITIONER GUIDANCE	12
4	DETAILED GUIDANCE	13
4.1	SETTING THE STAGE	13
4.1.1	WHERE ARE WE TODAY?	13
4.2	DRIVERS, RISKS AND THREATS	13
4.2.1	DEFINITION OF CRITICAL INFRASTRUCTURE	13
4.2.2	RISK ASSESSMENT AND MANAGEMENT	14
4.2.3	EVOLUTION OF A “RISKIER” ENVIRONMENT	14
4.2.4	THE CHANGING LANDSCAPE OF THREATS	18
4.3	CASE STUDIES	20
4.3.1	UTILITIES	20
4.3.2	FINANCE	23
4.3.3	COMMUNICATIONS	24
4.3.4	EMERGENCY SERVICES	24
4.3.5	REGULATORY	25
4.3.6	OTHER	25
4.4	WHAT IS SECURITY GOVERNANCE?	26
4.4.1	DEFINING ATTRIBUTES	26
4.4.2	WORKING DEFINITION	27
4.4.3	RELATIONSHIP TO CORPORATE GOVERNANCE	27
4.4.4	RELATIONSHIP TO IT GOVERNANCE	28
4.4.5	HOW DOES IT ALL FIT TOGETHER?	28



Trusted Information
Sharing Network
for Critical Infrastructure Protection

4.5	HOW IS SECURITY GOVERNANCE RELATED TO SECURITY MANAGEMENT?	29
4.5.1	SECURITY MANAGEMENT	29
4.5.2	ENTERPRISE SECURITY ARCHITECTURE MODEL	29
4.6	WHY IS SECURITY GOVERNANCE IMPORTANT?	30
4.6.1	STAKEHOLDER EXPECTATIONS	30
4.6.2	RISK	31
4.7	HOW CAN WE ACHIEVE STRONG SECURITY GOVERNANCE?	31
4.7.1	CORE PRINCIPLES	32
4.7.2	ROLES AND RESPONSIBILITIES	33
4.7.3	ACTIVITIES	34
4.8	SUPPORTING STANDARDS AND RELEVANT LEGISLATION	36
4.8.1	STANDARDS	36
4.8.2	RELEVANT LEGISLATION	39
5	CONCLUSION	41
A	APPENDIX A—REFERENCES	43
B	APPENDIX B—CONSULTATION QUESTIONNAIRE	47

1. EXECUTIVE SUMMARY

1.1 Background

Corporate governance is top of mind in boardrooms across Australia. It is now widely understood that effective corporate governance is required to protect the interest of an organisation's stakeholders, which in turn protects Australia's economic and social interests.

Information Technology (IT) governance is a relatively new topic that is gaining more attention as public and private organisations realise that the dependence on technology has resulted in a need to also have strong IT governance in order to support corporate governance requirements.

Security governance is a very new topic that still has not made its introduction into many boardroom agendas. However, there is an increasing realisation domestically and abroad that an organisation cannot effectively achieve its corporate and IT governance objectives without a strong and effective security governance framework.

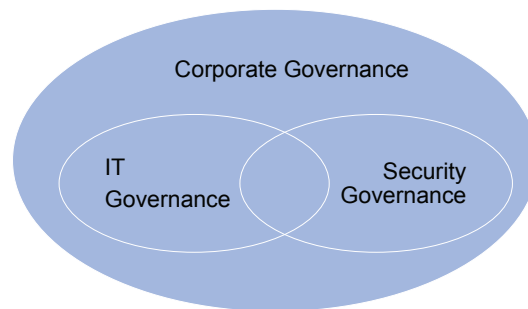


Figure 1: Corporate, IT and security governance relationships

The figure above illustrates the relationships between the three governance areas, highlighting the need to have all three in place and aligned to ultimately achieve stakeholders' needs.

The Department of Communications, Information Technology and the Arts (DCITA) on behalf of the Information Technology Security Expert Advisory Group (ITSEAG) engaged KPMG to assess and develop a report on leading practice for the governance of IT and information security matters for the corporate governance needs of owners and operators of critical infrastructure.

This report contains the summary of research, consultations and thought leadership to provide owners and operators of critical infrastructure with guidance on the following:

- What are the drivers, risks and threats to security for critical infrastructure industries?
- What is security governance?
- How is security governance related to security management?
- Why is security governance important?
- How can we achieve strong security governance?

1.2 What are the drivers, risks and threats to security for critical infrastructure industries?

The risk landscape for Australia’s critical infrastructure industries has changed in recent times, leading to three primary observations on what may have contributed to these changes:

Observation #1: There is a growing gap between the rate of technology adoption and the rate of controls adoption.

The perceived benefits of leveraging technology for improved time-to-market, business efficiency and operational excellence have driven organisations—public and private—to adopt technology at an ever-increasing rate: the *What If Factor*. However, the controls natively available within the technology along with the diligence in using those controls (or implementing other controls) is not maintaining pace with this adoption rate. The result is an increasing gap between the two, creating a greater opportunity for risk. Figure 2 illustrates this trend:

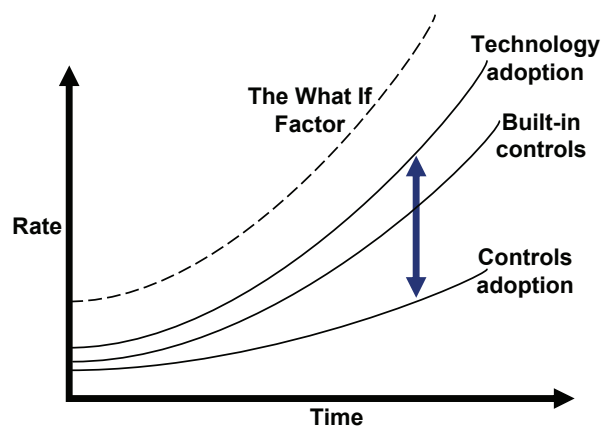


Figure 2: IT adoption vs. controls adoption

The second observation relates to the interconnectedness and consolidation—or convergence—of disparate technologies, which has increased the potential for risks in one technology to affect other technologies, and thereby impacting the business:

Observation #2: Convergence of technologies has led to a convergence of risk, greatly increasing the potential impact to the business.

While these other changes have taken place, the level of dependence placed on IT has led to the third and final critical observation regarding the changing risk landscape:

Observation # 3: The increased dependence on technology has greatly increased the potential impacts in the event of failure.

This dependence is not limited to a tangible set of IT systems and processes, which support the business functions they control. It extends to all aspects of how technology is implemented, controlled and leveraged to provide services to all stakeholders.

These three observations summarise the major changes that have taken place which have created a general environment of higher inherent risk. It is therefore now important to understand the nature of threats that exist which can impact an organisation's ability to meet stakeholder requirements.

The following list, which is not intended to be considered all-inclusive, represents categories that have been identified as the greatest threat to critical infrastructure industries:

- **Human error**—can be considered inevitable but the number of incidents related to human error can be prevented and reduced considerably with effective governance. This category also includes people's failure to act, and their lack of accountability.
- **System failure**—system, infrastructure and application failures can have a high impact, especially in critical infrastructure industries where ageing legacy systems are predominately found. Lack of security measures in place for early detection generally contributes to the extent of the impact.
- **Malicious software**—viruses, worms and spyware, are increasingly being linked to organised criminal activity whether it be for financial gain, political tactics or general pandemonium. Legacy systems, historically treated as self-sufficient systems, can no longer be placed in the corner and left alone; they are just as susceptible to attack as any other network based system.

1.3 What is security governance?

While there are many characteristics to security governance, an all-inclusive definition is difficult to contextualise. Leading practice dictates that security governance defines the core security principles, the accountabilities and actions of an organisation, to ensure that its objectives are achieved.

Through research and consultation, a list of essential attributes of security governance was developed which consequently led to the following definition:

Establish and uphold a culture of security to provide assurance that the business objectives and stakeholder requirements for the protection of information are continually met.

1.4 How is security governance related to security management?

Security governance and security management, although related, are not the same. In simple terms, security governance is used to ensure that all security management functions are designed, implemented and operating effectively.

Security governance sets the tone at the top (CEO, CIO) for implementing a culture of accountability in order for effective security management to take place. Where as security management establishes policy, principles and processes for the management of information security and is the primary focus of security operations executives.

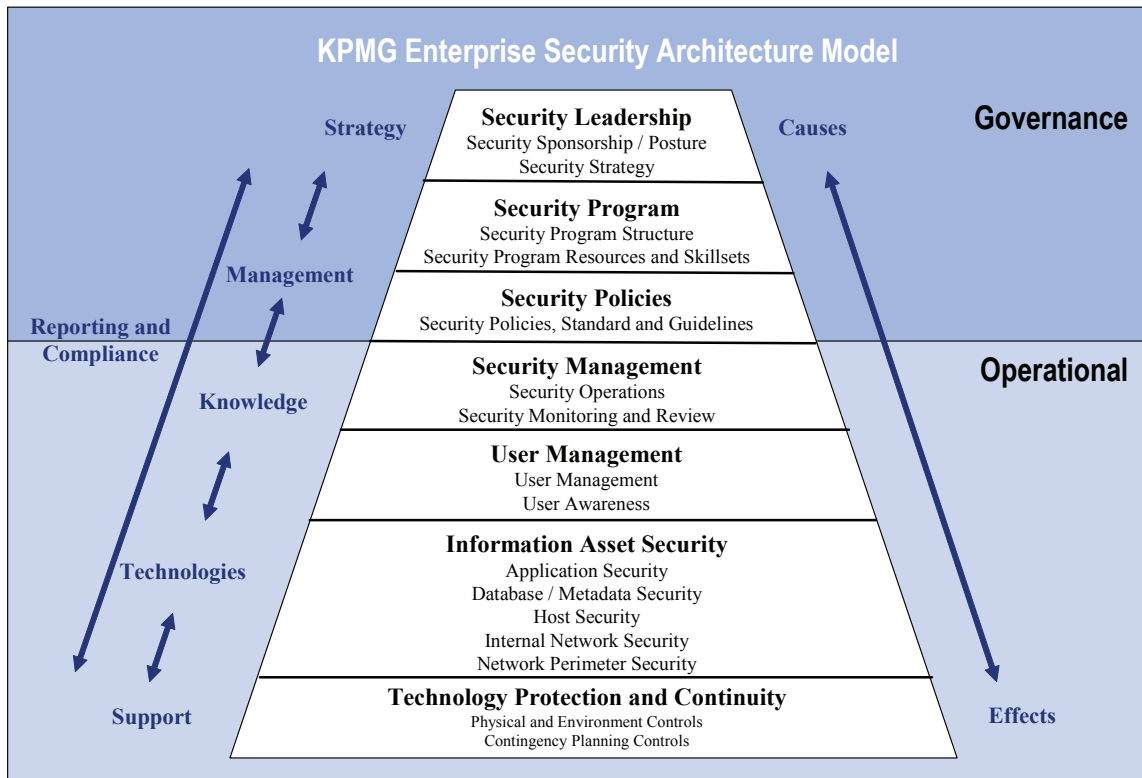


Figure 3: KPMG Enterprise Security Architecture Model

Figure 3 demonstrates the relationship between security governance and management (operations). It provides a top-down view of security governance and operations, indicating each of the key focus areas for capability. All layers of the model above are interdependent on one another, thus organisations should ensure that the responsibilities and capabilities of individuals within the organisation adequately cover each layer and that the linkages between each layer are clearly understood.

This model has been developed by considering leading international practices (such as ISO17799 / ISO27001), as well as practical examples of how leading companies organise their information security functions. Experience tells that this model aligns well with how leading organisations manage information security.

A key component of this model, as indicated by the arrows on the left side of the figure, is a reporting and compliance capability that provides monitoring at all levels of the organisation and transparency to the Board regarding the effectiveness of security functions and capabilities. These overarching reporting and compliance functions are critical in supporting the implementation of any security governance framework.

1.5 Why is security governance important?

The Australian economy and society are dependent on a core set of critical infrastructures that are interdependent on each other in order to function. A strong increase in technology adoption, technology convergence and the growing use of standard technologies has made it essential that all critical infrastructure industries focus on securing their information and assets.

The quantifiable impacts of security incidents in Australia have more than doubled in the last year alone. The total average annual loss has increased by 63 per cent per organisation compared to 2005¹. The failure to meet society’s expectations is a common reason for organisations exposure to unacceptable intangible impacts. The bearing on trust, reputation, economic and social confidence is often said to be an order of magnitude larger than the tangible effects.

With the risks and threats to IT security dynamically changing, owners and operators of critical infrastructure require strong security governance to ensure effective ongoing management of risk.

1.6 How can we achieve strong security governance?

Based on the research completed, the following components, as illustrated in the diagram below, have been identified as fundamental to effective security governance:

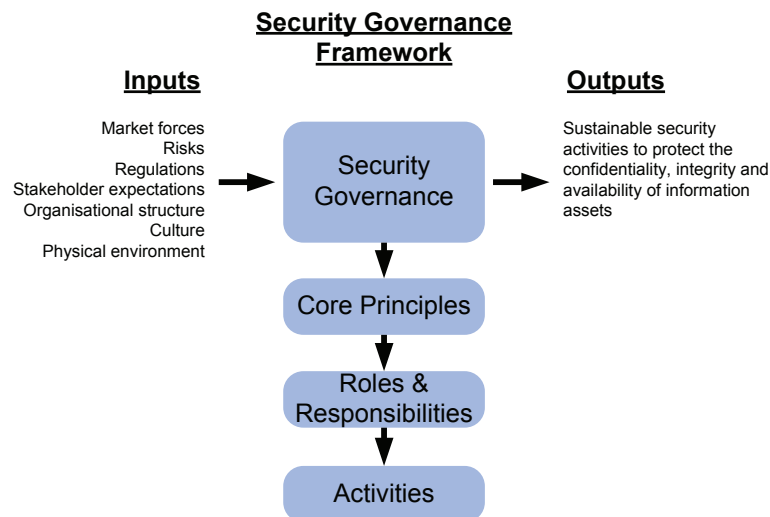


Figure 4: Leading practice security governance framework

- **Core principles:** Core security principles serve as the primary driver for all security governance functions and activities. They are:

Core principles	
Accountability	Transparency
Awareness	Measurement and Reporting
Compliance	Scope
Effectiveness	Response
Ethics	Risk Management
Inclusion	

¹ AusCERT, 2006, 2006 Computer Crime and Security Survey, Brisbane.

Roles & responsibilities: An organisation must define roles and responsibilities in security governance. This assignment of accountabilities is to ensure security governance activities take place and achieve the spirit of the core principles.

Activities: Activities are the underlying processes that are owned and operated by accountable individuals to implement and maintain security governance capabilities. It can also be stated that security, as an activity itself must be integrated into an organisation’s core functions and processes.

These three key components of security governance should be implemented using a top-down approach to ensure that the highest value is achieved and that all layers of risk are covered. Identification of stakeholder expectations and the determination of the level of dependence on supply chains should be considered prior to the introduction of governance controls throughout the organisation, IT and business process. This is illustrated in the Figure 5:

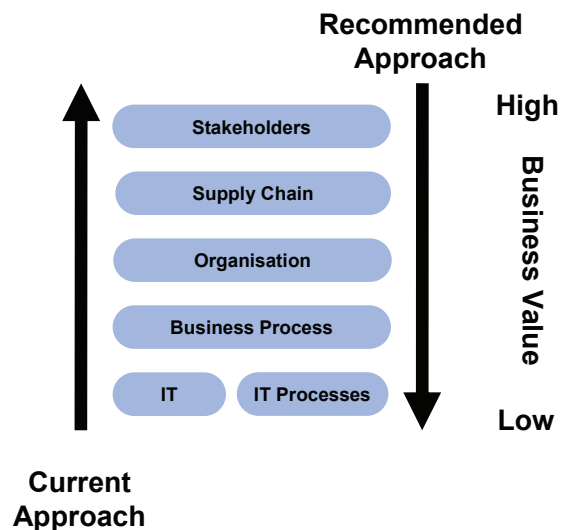


Figure 5: Approach to implementing security governance

1.7 Conclusion

The risk landscape to critical infrastructure owners and operators is rapidly changing. Although Australia has been relatively fortunate as compared with other countries concerning security failures, Australia cannot afford to employ an “it won’t happen to us” attitude. It is not a question of “if”, but “when”.

It is estimated that 90 per cent of Australia’s critical infrastructure is owned and operated within the private sector². Whilst the government has a role in raising the awareness of the need to implement security governance, effective measures must occur at the corporate level.

The public sector is subject to higher regulatory mandates and as such rely security frameworks offered by Australian Standards (e.g. Protective Security Manual and ACSI 33).

² Rothery, M. (Critical Infrastructure Protection Branch, Attorney-General’s Department), 2005, ‘Critical infrastructure protection and the role of emergency services’, *The Australian Journal of Emergency Management*, vol. 20, no 2, pp. 45–50



Privately owned and operated critical infrastructure may also be affected by such mandates that apply to their industry—in particular—where service delivery may have been outsourced.

Board and executive commitment to security governance will not ensure its success but a board's lack of commitment will guarantee its failure.

Security governance should be seen as a business success objective. It is all about what level of risk an organisation and its stakeholders are willing to allow. Every executive needs to understand that it should be addressed with the same logic that is applied to make financial, acquisition and other 'non-security' related business decisions.

To protect Australia's social and economic interests, all organisations—public and private—must take action now to ensure that they are meeting their stakeholders' expectations for IT security and governance, corporate and regulatory compliance and social responsibility.

2. DISCLAIMER

KPMG's analysis is based on economic, market, regulatory, technical and other conditions prevailing at the date of this report. Such conditions in this industry can change significantly over a relatively short period of time.

KPMG has not audited, nor should it be construed to have audited, any of the information provided to us by DCITA or any other party. All such information has been received and accepted in good faith by KPMG as being factually correct. Consequently, we specifically exclude any representation or warranty whether expressed or implied, as to the accuracy, reliability or completeness of such information contained in this report.

KPMG does not warrant that its enquiries have identified or verified the matters which an audit or due diligence investigation might disclose.

This report has been prepared solely for the use of the Management of DCITA and members of the Trusted Information Sharing Network. Distribution beyond this aforementioned stakeholder group is prohibited without KPMG's prior written consent. In no circumstances should a third party rely upon any opinions, reports, advice or other information provided by KPMG for any purpose. KPMG expressly disclaims any liability to any third party in this respect.

KPMG expressly disclaims to the fullest extent permitted by law, all liability for any loss, damage, cost or expense of any kind whatsoever as a result of any inaccuracy, misinterpretation or omission in this report.

To the extent permitted by law, this document is provided without any liability or warranty. Accordingly, it is to be used only for the purposes specified and the reliability of any assessment or evaluation arising from it are matters for the independent judgement of users. The document is intended as a general guide only and users should seek professional advice as to their specific risks and needs.

Note:

This paper has been prepared by the IT Security Expert Advisory Group (ITSEAG). For more information on the work of the ITSEAG, please contact the Secretariat in the Department of Communications, Information Technology and the Arts on (02) 6271 1595.*

The ITSEAG is part of the Trusted Information Sharing Network for critical infrastructure protection (TISN) which enables the owners and operators of critical infrastructure to share information on important issues. It is made up of a number of sector-specific Infrastructure Assurance Advisory Groups (IAAG), several Expert Advisory Groups (EAG), and the Critical Infrastructure Advisory Council (CIAC—which is the peak body of the TISN and overs the IAAGs and the EAGs). One of the expert advisory groups within the TOSN framework is the ITSEAG which provides advice to the CIAC and the sector-based IAAGs on IT issues as they relate to critical infrastructure protection. The ITSEAG is made up of academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security field.



The ITSEAG and TISN have published papers on:

- Leading Practices and Guidelines for Enterprise Security Governance including CEO and CIO guidelines
- Managing IT Security When Outsourcing to an IT Service Provider, Guide for Owners and Operators of Critical Infrastructure – Summary Report for CEOs and Boards of Directors
- Managing IT Security When Outsourcing to an IT Service Provider Guide, for Owners and Operators of Critical Infrastructure – Full Report
- Secure Your Information: Secure Your Business – Advice for CEOs and Boards of Directors
- Secure Your Information: Information Security Principles for Enterprise Architecture – Advice for CIOs and CSOs
- Secure Your Information: Information Security Principles for Enterprise Architecture – Full Report
- GPS—An Overview for CEOs
- National Strategy for Critical Infrastructure Protection
- SCADA—Advice for CEOs
- Security of Voice Over Internet Protocol—Advice for CEOs
- Security of Voice Over Internet Protocol—Advice for CIOs
- Trusted Information Sharing Network for Critical Infrastructure Protection (brochure)
- Wireless Security—Overview for CEOs
- Wireless Security—Overview for CIOs

More information on the TISN and its work is available at www.tisn.gov.au

3 PROJECT OVERVIEW

3.1 Background

DCITA on behalf of the Information Technology Security Expert Advisory Group (ITSEAG) engaged KPMG to assess and develop a report on leading practice for the governance of IT and information security matters for the corporate governance needs of owners and operators of critical infrastructure.



Figure 6: Project approach

3.2 Approach

As outlined in the original proposal, KPMG adopted the following approach to completing this engagement:

Assess international and national leading practices and standards for information infrastructure, security and governance through extensive research; and

Conduct a number of focus group sessions with key industry contacts, provided by DCITA, in addition to a selection of KPMG clients which are sourced from the various critical infrastructure sectors.

As *Figure 6: Project approach* above illustrates, KPMG considered a wide variety of security risks, threats and trends along with business requirements and leading practices to develop a consolidated view of the security governance landscape. The nature of the research and consultation activities are detailed below.

3.2.1 Research

KPMG conducted research via a number of methods, as follows:

- Assessed relevant examples from global practice and collected internal / external research;

- Contacted KPMG professionals worldwide (Americas, EMEA and Asia Pacific) with experience delivering security and governance services to critical infrastructure organisations;
- Performed external research of international standards and leading research firms;
- Examined material that is offered in the public domain, i.e. the Internet, the press and specific technology publications;
- Researched leading practice models with supporting guidance for information infrastructure and security governance for critical infrastructure owners and operators;
- Researched KPMG's proprietary KWorld knowledge management global intranet for information and security governance examples; and
- Examined documents and surveys provided by clients and contacts during the consensus building stage. Some of these documents are still in confidence and as such, not specifically referenced in this report.

A listing of resources used for this report is included in the appendix of this report.

3.2.2 Consultations

Focus group sessions and interviews were conducted within DCITA, TISN and the ITSEAG to gain the Australian industry perspective on the existing security governance, risks and mitigation practices. KPMG met with all contacts provided by DCITA:

Professor Bill Caelli, Dave Campbell, Bill Davey, Kim Duffy, James Galloway, Tim Hartman, Allan LeBusque, Chris Marsden, Geoff Rhodes, Greg Stone, and Steve Stroud.

In addition to the consultations conducted with ITSEAG members, KPMG also conducted industry sessions to provide a means of collating valuable practical industry experience and observations as they relate to the regulatory environment, stakeholder expectations, risk management and leading and accepted practices. KPMG met with a number of clients within critical infrastructure industries, including Country Energy (Energy), Telstra (Communications), ABC (Broadcasting), HealthTECHNOLOGY (Health), and Westpac (Banking & Finance).

A number of companies were unable to meet with KPMG as a result of either disclosure concerns from senior management or limited availability due to the time constraints of the engagement.

A list of questions used for facilitating discussions with industry representatives is included in appendix 0 of this report.

3.3 Deliverables

In addition to this detailed report, the outcome of this project included the development of a guidance paper for Board of Directors and Chief Executive Officers, and guidelines for CIOs and other practitioners.

3.3.1 Board of Directors and CEO Guidance

The CEO guidance is a form of a ‘user guide’ targeted at Board Members, CEOs and senior executives, that summarises industry sound practice, provides practical tips, includes case studies and suggested steps for achieving improvements in the governance of enterprise level information, IT security and related engineering systems.

The Board of Directors and CEO Guidance has been provided as a separate document to this report.

3.3.2 CIO, CISO and Practitioner Guidance

The detailed information paper is for use and reference by CIOs, CISOs and the respective security management practitioners. It includes the material contained in the CEO guidance, highlighting the importance of an appropriate governance framework for the management of corporate information networks and IT security systems to ensure the continuity of the delivery of core services.

The CIO, CISO and Practitioner Guidance has been provided as a separate document to this report.

4 Detailed guidance

4.1 Setting the stage

Over the last several years, the topic of security has moved from backroom discussions to mainstream coverage in the media. Awareness is rapidly growing of security risks and the potential impacts to individuals and the economy.

Increasing dependence on IT and the interdependencies between organisations is escalating the level of focus required to place on addressing security risks across the enterprise.

Within critical infrastructure industries, this equates to understanding the variety and nature of threats that exist which can affect the organisation's ability to conduct its business and protect the interests of the wider community.

This report provides guidance and reference material for owners and operators of critical infrastructure to support the implementation of strong security governance practices in order to protect the interests of the Australian community and maintain its position of economic strength in the global community.

4.1.1 Where are we today?

Based upon consultations with key stakeholders in the critical infrastructure community, the following positions summarise security governance in today's environment—in Australia:

- In the absence of local benchmarking, there is a general feeling that the current level of security governance activity (and implementation) in Australia is inadequate. This is supported through a recent Australia National Audit Office (ANAO) report into Internet security in six Australian government agencies which found that the audited agencies did not have security documentation that complied with ICT standards, had limited business continuity planning and inadequate email filtering in place;³
- Although new standards have been introduced for IT governance (e.g. AS8015 in January 2005), organisations have not yet fully embraced or adopted the recommended practices;

There is a false sense of security arising from the lack of major incidents in Australia; and

Critical infrastructure industries are not forced by regulation or legal directives to ensure that effective security governance frameworks and practices are in place.

The result is that while the awareness of the risks has increased, there is still a lot of work to be done.

4.2 Drivers, risks and threats

4.2.1 Definition of critical infrastructure

As taken from the Trusted Information Sharing Network (TISN) website⁴, critical infrastructure is defined as the following:

³ Crawford, M., 15 June 2006, *Nairn disappointed with ANAO report: launches workgroup*, www.computerworld.com.au

⁴ www.tisn.gov.au

“The Australian Government defines critical infrastructure as those physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation or affect Australia's ability to conduct national defence and ensure national security.”

The threats to Australia’s critical infrastructure are constantly evolving and changing. This dynamic environment requires diligence on the part of all owners and operators of critical infrastructure to not only look after their own commercial interests, but at the interdependencies that exist between organisations.

If one considers the relationships between critical infrastructure organisations as links in a chain, it is easy to understand that the strength of the chain is only as strong as the weakest link. This means that everyone is responsible for ensuring that his or her organisation is not the weakest link.

4.2.2 Risk assessment and management

Traditional risk assessment practices focus on assessing the value of an asset, the threats to the asset, the likelihood that a particular threat will occur and the vulnerability that exists to the asset (the ease of which a threat can compromise the asset). This is illustrated by the following equation:

$$\text{Risk} = \text{Value} * \text{Threat} * \text{Vulnerability} * \text{Likelihood}$$

In an ideal world, these variables would be controlled and thereby managing risks to very specific levels. However, real world experience has shown that direct control is really only over the **Vulnerability** to a particular asset. Therefore, the art of risk management comes through the pragmatic application of controls to reduce vulnerability to that asset.

Through the implementation of robust risk management frameworks and practices, critical infrastructure industries can make sound commercial decisions on what controls to put into action through a stronger understanding of the value of its assets and the environment they operate under. Risk management frameworks for example, those based upon AS/NZS4360, can provide a constant view of an organisation’s risk profile.

For the purposes of this report, through research and consultations, a consolidated view of generic risks to critical infrastructure has been developed, leaving detailed risk assessment (and subsequent risk management) of specific organisational assets up to the reader.

4.2.3 Evolution of a “riskier” environment

Before listing specific risks and threats to critical infrastructure, it is important to understand the nature of changes that have occurred in recent times and the changes that are continuing to contribute to the development of a “riskier” environment within Australia and around the world. These changes have a direct impact on all organisations – public and private – within the critical infrastructure industry.

4.2.3.1 Rate of IT adoption

Society is continuing to embrace technology at an unprecedented rate. This can be seen through the amount of technology used daily, even for simple tasks. For example, some toothbrushes contain integrated technology which automatically indicates to the user when two minutes have elapsed (the recommended length of time to brush), or when the head should be replaced for optimal brushing results. While this example might seem out of place in the context of critical infrastructure protection, it illustrates that technology is everywhere and society's dependence on the technology is increasing at a very rapid rate. Imagine how many people might never change the head of their toothbrush if the technology fails to indicate that replacement is needed.

In the business community, this adoption rate is evident through the rapid introduction of relatively new technologies such as Voice over Internet Protocol (VoIP), wireless networks, radio frequency identification (RFID), global positioning system (GPS) devices and more. In this regard, the purchase and use of a high-tech toothbrush and relying on it to tell the user when to replace the head is no different from the integration of an RFID chip on a food package to automatically broadcast its contents and location to eliminate the need for visual inspection and verification. In both cases, an element of human judgment is removed and it is assumed that the technology will perform according to its intended purpose without human intervention.

4.2.3.2 The What If Factor of IT adoption

One of the primary drivers of this adoption rate is the perceived opportunity from the use of technology – the What If Factor. As more technology is integrated into existing practices, the desire to do more continues to drive the What If Factor even higher. The result is a race between the actual benefits achieved through the technology implementation and the perceived benefits of implementing even more technology.

The What If Factor does not create a riskier environment by itself. Risk is still dependent on the variables in the risk equation listed earlier, many of which cannot be controlled. However, the What If Factor does broaden the scope of technology and the level of dependence placed on it.

4.2.3.3 Rate of controls adoption

As described earlier, the art of risk management comes through the pragmatic application of controls to reduce vulnerability to assets. The ability to implement controls is therefore somewhat dependent upon the availability of controls within the technology. There are many cases where these needs have not been met, for example, some legacy systems which do not require passwords to gain access to information. Prior to the introduction of networked environments, simply providing adequate physical controls around the system may have been sufficient to protect the information stored on the legacy system. Today, anyone with a basic understanding of IT and security would agree that a networked system must have password protection as a control.

This demonstrates a dependency, in part, on technology vendors providing a certain level of available controls which can be used to reduce the vulnerabilities (and thereby the risks) to assets.

The onus is not completely on the vendors to provide controls. It is also on the owners and operators of critical infrastructure to adopt those controls (and implement other controls) to manage risks to acceptable levels for the organisation and the interests of the wider community.

What is evident through the research and consultations, however, is that the rate of controls adoption is not maintaining pace with the rate of IT adoption. This is the first of the critical observations regarding the changing risk landscape:

Observation #1: There is a growing gap between the rate of technology adoption and the rate of controls adoption.

This gap creates the opportunity for increased risk, independent of the type of technology involved.

The combined effect of IT adoption rate, the What If Factor and the controls adoption rate is illustrated in *Figure 7 - IT adoption vs. controls adoption*, below:

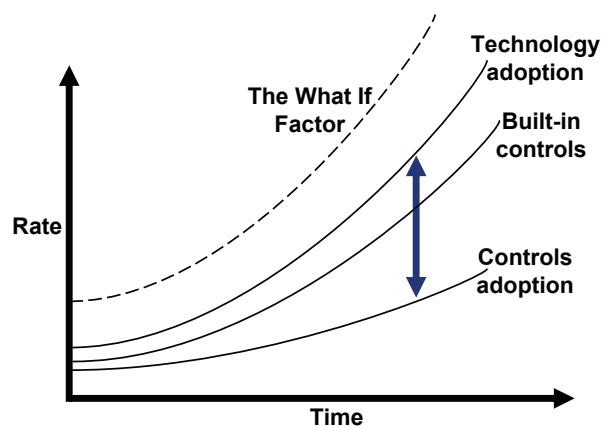


Figure 7 - IT adoption vs. controls adoption

The arrow on the graph highlights the increasing gap and resulting increased opportunity for risk as described.

4.2.3.4 The effects of convergence

Another factor in creating a riskier environment is convergence. Convergence can be described simply as the coming together of previously independent technologies to provide increased convenience and value to the user. For example, mobile telephones, personal digital assistants (PDAs), digital cameras and portable music players were all once contained in separate devices. Now, virtually every mobile phone is also a PDA, digital camera and portable music player (and vice versa!).

In the business community, convergence manifests itself through the blurring lines between previously independent infrastructures and environments.

Different business functions or processes used to be supported through specialised applications and systems which did not integrate (or even communicate with each other). For example, in a number of critical infrastructure industries, specialised proprietary technology was in place to support the provision of services to the end user. This might have been electricity, water, phone services, food packaging or a television news broadcast. Historically,

the systems that controlled the provision of these services were not logically connected to any other environments and the primary controls for their protection were physical.

Over time, business requirements have driven the need to communicate with, control and monitor these specialised systems so that efficiency, operations and quality could be better controlled.

Cost has also been a major factor in driving convergence as maintaining proprietary systems is often far more expensive than implementing and operating similar functions on newer, consolidated technologies.

The result has been an increase in the interconnectedness between systems that perform different functions throughout the business as well as a consolidation of technologies to reduce the total cost of ownership and provide more functionality within a single system. This interconnectedness and consolidation – or convergence – of disparate technologies has increased the potential for risks in one technology to affect other technologies. This can translate directly into enterprise-wide impacts from a single technology risk. This is the second critical observations regarding the changing risk landscape:

Observation #2: Convergence of technologies has led to a convergence of risk, greatly increasing the potential impact to the business.

4.2.3.5 Dependence and interdependence

As alluded to earlier, the dependence on technology has increased as more technology becomes integrated with (or automates) business processes.

Considering this increase in dependence along with the other factors as described—the rate of IT adoption vs. controls, the What If Factor and convergence—has led to the third and final critical observation regarding the changing risk landscape:

Observation #3: The increased dependence on technology has greatly increased the potential impacts in the event of failure.

This dependence is not limited to a tangible set of IT systems and processes which support the business functions, it extends to all aspects of how technology is implemented, controlled and leveraged to provide services to its stakeholders and should where relevant include the principles of defence in depth for the security framework across the enterprise.

Critical infrastructure industries are not only dependent on the systems they control, but the systems used or provided by their business partners, customers, service providers, vendors, outsourcers and any other stakeholder in their business.

The impacts to the business (and ultimately on the integrity of Australia's critical infrastructure) due to the level of dependence and interdependence on technology is simply demonstrated by the following figure, *Figure 8 – Dependence on IT vs. business impact*:

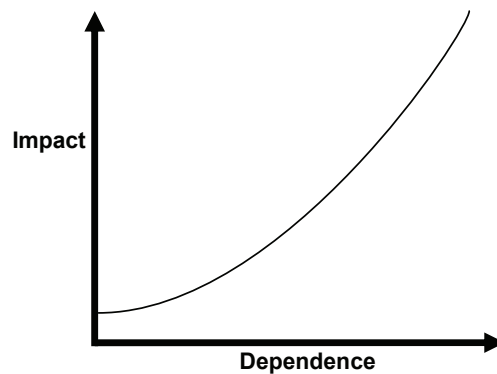


Figure 8 – Dependence on IT vs. business impact

After covering some of the major factors contributing to a riskier environment for critical infrastructure owners and operators, it is important to look at the changing landscape of threats.

4.2.4 The changing landscape of threats

There was a time when nearly everyone would have agreed that the likelihood of a commercial aeroplane being deliberately flown into a building in a central business district was extremely low. Regardless of what level the likelihood assigned to a particular scenario occurring, it can and may occur.

Perspectives on considering the possibilities have therefore changed which has raised the awareness of the issues and created a stronger platform for action to better manage security risks.

The following list covers the greatest areas of threats to critical infrastructure owners and operators, stemming from the research and consultations. It is not intended to be an all-inclusive list as there are likely many more types of threats.

4.2.4.1 Human error

Mistakes are a fact of life. Consultations have identified numerous examples of human error that may have been prevented through stronger security governance and control. These included changes to infrastructure which rendered a business function inoperable, physical cutting of the sole communication link to a critical process control system, inadvertent disclosure of highly sensitive information and more.

One could argue that human error is unavoidable. To a certain extent this is true. However, it is relatively easy to see that the number of incidents related to human error and misjudgement could be reduced.

Research, consultations and professional experience have demonstrated that human error is by far the largest contributor to security incidents (occurrence of risk). Given the changing risk landscape, the cost of not addressing the human factor is no longer acceptable.

The human error threat also includes the failure to act. Many discussions around key threats to critical infrastructure concluded that particular risks were avoidable if human action had been

taken or clearly defined processes (including exception processing) were in place to guide and control activities and response.

4.2.4.2 System failure

Another fact of life is that systems do not last forever (although several organisations may argue this point based on the age of some legacy systems!).

Applications fail. Databases fail. Servers fail. Networks fail. Any type of component or system failure can have far reaching impacts to the business simply based on the changes in risk due to lack of controls, convergence and dependence as described earlier.

System (and component) failure was another large contributor to outages and security related incidents that were uncovered during consultations. A common theme to these failures was the lack of notification (or identification) when it first occurred. In many cases, a single failure did not have an immediately noticeable impact. For example, one interviewee described an incident that occurred when the power to the data centre had been lost. At first, the uninterruptible power supply (UPS) to the data centre did its job and maintained function of the environment. However, after several hours the batteries died and all power to the data centre was lost. No one noticed the power outage until UPS failure because the alarms were either not functioning or not enabled.

4.2.4.3 Malicious software

Viruses, Trojans, spam, spyware, adware, worms and other forms of malicious code continue to represent a large threat to critical infrastructure owners and operators. Although many organisations described comprehensive approaches to virus management (e.g. use of multiple vendors, strong relationships with their vendors, standard operating environments), there were an equal number of organisations who described ongoing challenges in reducing the threat of viruses.

In particular, organisations that have some form of process control (utilities, water, food chain, telecommunications and broadcasting) tended to be more affected by the malicious code threat due to the inability to install and maintain prevention software on hosts within the process control environment. This was often because of conflicts between the operational software and the prevention software or the utilisation impact of scanning software on systems that required real-time performance.

Current forms of malicious software are also being increasingly used by organised crime and other attackers to conduct fraud or create other significant impacts on organisations (e.g. extortion) and individuals.

While earlier forms of malicious software were ad-hoc in nature, concentrating simply on the disruption of systems, organisations are now observing a large increase in the penetration of targeted software such as spyware and key-loggers which are being used in a more focused way. An example of this focused approach is the emergence of *spear-phishing*—where attackers are targeting specific individuals through the use of aggregated information gathered from compromising multiple systems (or capturing physical information) and attempting to lure the target into inadvertently installing malicious software through specially-crafted emails and websites.

It is estimated that nearly 70 per cent of all malicious software detected in the first quarter of 2006 was cybercrime related, with the threat from non-targeted software such as email worms becoming less significant⁵. Furthermore, this trend signifies the malicious software developers growing intent to remain hidden and avoid detection for as long as possible.

4.3 Case studies

The risk of attacks both malicious and non-malicious are more than a possibility as demonstrated in the case studies which have been summarised in this section of the report.

Although the number (volume) of successful attacks have decreased in recent times, their impacts can be catastrophic from both a financial and reputational perspective. Table 1 has been drawn from the conclusions of the *2006 Australian Computer Crime and Security Survey*⁶ and demonstrates this trend.

Total annual loss (\$)				
	2003	2004	2005	2006
Total	11 800 783	15 921 064	16 856 900	48 471 208
Average	93 657	116 212	153 245	241 150

Table 1: Total annual cyber crime losses

This table clearly shows that the financial impact of security incidents has nearly trebled in just the last year alone—a nearly 300 per cent increase!

Given the changes to the risk landscape as mentioned earlier and the continually changing threat environment, this trend is expected to continue. Without a strong focus being placed on enterprise security governance in both public and private organisations, it is just a matter of time before most Australian organisations become a part of the statistics.

Detailed below are a number of case studies in a variety of domestic and international critical infrastructure industries where the incidents and impacts are real, emphasising the point that action must be taken or fall victim to the trend.

4.3.1 Utilities

4.3.1.1 Hunter Watertech (Maroochy Water Services)

In April 2000, a disgruntled ex-employee of Hunter Watertech compromised the security of Maroochy Shire Council's sewerage management system and released over a million litres of raw effluent into local parks and rivers. During the previous two months, the offender made 45 unsuccessful attempts to access the sewerage management system.

⁵ Panda Software International 2006, *Quarterly Report PandaLabs (January – March 2006)*, Author, Glendale.

⁶ AusCERT 2006, *Computer Crime and Security Survey*, Brisbane.

Whilst the offender used specialised control software and had extensive “insider” knowledge of the system (gained while employed at Hunter Watertech), one of the key failures observed was that the facility did not detect or react to the threat as it was occurring.

A lesson that can be learned from this case is that a lack of security governance can not only cause major disruptions to an organisation, but also directly impact any interrelated entity—in this case, the health and safety of the Maroochy community and environment was affected.

The direct cost of the spill was \$13 000 in clean up and \$176 000 in system security changes. It also resulted in an extensive and costly in-house investigation, extensive media activity over five months, and a loss of Maroochy Water Service’s reputation.

4.3.1.2 Davis-Besse

On 25 January 2003, the Davis-Besse nuclear power plant became infected by the Microsoft SQL Server 2000 worm. The infection propagated causing increased data traffic on the network, making the Plant’s Safety Parameter Display System (SPDS) and process computer inoperable for several hours.

Although the attack, by means of the worm, can be seen as a malicious attack to the nuclear plant, the two primary causes for the infection were fundamental examples of non-malicious threats and failures in security governance.

- 1 The primary cause identified by FirstEnergy (licensee at Davis-Besse) was an unprotected T1 connection to the corporate network that was established by a contractor whose company’s network allowed use of UDP (User Datagram Protocol) for data transfer (from which the worm infects).
- 2 The second cause of the attack was the lack of awareness of a security patch released by Microsoft approximately six months prior. The implementation of this patch could have prevented the outbreak.

Fortunately the systems under attack were isolated and therefore neither system affected the plant’s safe operation.

4.3.1.3 Salt River Project

On 14 August 2003, the worst blackout in the United State’s history occurred. A report which was published by the U.S.-Canada Power System Outage Task Force⁷ identified the caused of the blackout, which traversed two areas of known threats, as human error and system failures.

The human factor which can be better assessed as the consequence of insufficient security governance incorporated outdated procedures and shortcomings at a regional grid monitoring centre. Monitoring of the power grid—the Midwest Independent System Operator (MISO) operators, were using outdated information and did not have the means to identify significant transmission problems developing in the system.

The North American Electric Reliability Council (NERC) also conducted an independent investigation of the blackout⁸. They concluded that the lack of operating policies and

⁷ U.S.-Canada Power System Outage Task Force, 2003, *Interim Report: Causes of the August 14th Blackout in the United States and Canada*, United States and Canada

⁸ North American Electric Reliability Council, 2004, *August 14, 2003 Blackout: NERC Actions to Prevent and Mitigate the Impacts of Future Cascading Blackouts*, Princeton, New Jersey.

planning standards, inadequate monitoring and not assuring compliance with NERC standards and guidance were major contributing factors for the blackout.

System failure of FirstEnergy's SCADA alarm and logging software was another inherent contributor to the blackout. However, if standardisation of system protection technologies were applied it would have optimised their ability to slow down or stop the uncontrolled cascading failure of the power system.

This particular incident had a US\$6 billion impact in economic and other losses. The incident provoked new calls for upgrading the technology, improving communication protocols and procedures and enabling the government to enforce reliability standards.

4.3.1.4 California Independent System Operator (CAL-ISO)

During March 2001, CAL-ISO—a non-profit corporation that controls the distribution of 75 per cent of the California's power—was hacked into by way of a security flaw in the agency's Solaris based systems which were connected directly to the Internet. The breach was not discovered until a month after the initial compromise.

The attacker took control of two servers that were unprotected by the organisation's firewalls.

As part of the Energy Management System (EMS) upgrade project, developers placed an FTP server outside CAL-ISO's firewalls in order to download code urgently. After the files were transferred, the FTP server was forgotten and left enabled outside the firewalls.

The hackers gained root access and introduced BOTs, which were used to hijack other computers and broadcast mail virus attacks.

The BOTs went undetected until MCI (a communications outsourcer) noticed the high level of traffic and discovered the attack during their investigation.

Similar to previous case studies, the malicious attack was consequently brought about by operational and procedural failures in security governance. There is obvious evidence in a breakdown of procedures, the policy was not obeyed and the change management processes were not followed.

Fortunately the amateur hackers did not get near the power grid; the impact was purely that of a public relations nature. The hackers did not appear to know what they had compromised. The outcome could have been different if they had launched a focussed attack on the SCADA servers.

Due to increase in awareness and organisations such as FERC/NERC⁹—the energy industry is becoming ever more regulated. Certain organisations will have to become compliant by next year. If the industries affected do not want to be heavily regulated, they will have to take more proactive steps to security governance.

⁹ www.ferc.gov

4.3.2 Finance

4.3.2.1 Westpac

In May 2004, Westpac, a leading Australian financial organisation, was hit by the unrelenting Sasser worm forcing the bank to use manual procedures, and more detrimental, to close the doors of some of its branches for a day and a half.

The worm spread from infected computers to other vulnerable computers without user intervention, by creating a remote connection and downloading itself onto the new host. The virus attacked computers through a flaw in Microsoft's Windows operating systems, which caused systems in the bank's operational environment to be rendered inoperable.

The impact was not largely criticised as the financial impact was to Westpac itself as opposed to its customers. However, customer and shareholder expectations of the level of service and security from such an institution, and the flow on effects of public perception to the Westpac brand are factors which can be quite difficult to measure but can not be ignored.

4.3.2.2 Australian Prudential Regulation Authority (APRA)

In 2004 / 2005, APRA—a prudential regulator of the Australian financial services industry—recognised the growing threat of identity theft and online fraud which had the potential to affect all financial institutions with Internet connected systems. In order to combat this risk, APRA requested that the external auditors of the major retail banking organisations in Australia perform an Internet banking security assessment as part of the year's annual tripartite review¹⁰.

These assessments covered a number of key areas including:

- customer access control management;
- infrastructure management;
- application security;
- incident response management; and
- reporting and governance.

This targeted review highlighted APRA's focus on security and served to assist the finance industry in recognising the importance of sound security management and the implementation of a security governance framework.

4.3.2.3 CardSystems

In 2005, CardSystems Solution, Inc.—a global third party processor of payment data—was impacted by a security vulnerability that allowed an intruder to infiltrate the network and gain access to cardholder data compromising more than 40 million credit cards.

The intrusion illustrated a breakdown in security governance and compliance to procedures and processes. Even though CardSystems passed the Payment Card Industry (PCI) data security standard certification in 2004, there was a lack of ongoing monitoring and management inevitably leading to the breach.

¹⁰ www.apra.gov.au

This breach intensified the already increasing pressures being put on service providers such as MasterCard and Visa to demonstrate stronger diligence with data-protection requirements and standards. The requirements include:

- technology mandates—such as data-protection, end-user access control and activity monitoring and system logging; and
- procedural mandates—including the implementation of formal security policies and vulnerability management programs.

The impact of the attack, both financial and reputational, forced the acquisition of CardSystems by Pay by Touch as both Visa and American Express terminated their contracts with the organisation.

4.3.3 Communications

4.3.3.1 T-Mobile

T-Mobile, a global communications provider, has recently been the centre of much scrutiny after a hacker was able to access information on 400 U.S. customers including a U.S. secret service agent and Paris Hilton.

The malicious attacker was able to penetrate the organisation through a design flaw in a website feature to reset T-Mobile account passwords.

It has been reported that the website was full of security faults. Jack Koziol, a senior instructor at InfoSec Institute has been reported as stating “the problems facing T-Mobile's website are common to companies that move quickly to open their corporate networks to the Internet through web-based applications”.¹¹

The incident could have been avoided and the impacts to the company and its customers could have been minimised if T-Mobile simply had strong security governance practices implemented as part of their system development lifecycle (SDLC) practices.

4.3.4 Emergency Services

4.3.4.1 Victoria Police

In May 2006, officers in the Victorian Police were disciplined for the misuse of the Law Enforcement Assistance Program (LEAP) database.

LEAP, a database which stores information of all crimes brought to the notice of police, as well as family incidents and missing persons including details on locations, vehicles and persons involved, was used by as many as 35 officers who inappropriately accessed information of people including friends, family and in at least one case, an Australian celebrity.

In-house auditing systems which check appropriate use of such systems and data discovered the breaches. Other LEAP database breaches have also brought the Victorian Police under scrutiny, including sending the wrong criminal record to a potential employer. These events led the state government last year to promise a AU\$50 million replacement of the database.

¹¹ Roberts, P., March 2005, *Paris Hilton: Victim of T-Mobile's Web Flaws?*, published on www.pcworld.com

In a critical infrastructure industry where trust and security are paramount, the reputational damage to the Victorian Police and the state government could be catastrophic.

"The public is losing confidence in the police minister and this government to properly handle these records," Opposition justice spokesman Andrew McIntosh said, due to "its failure to secure the troubled database."¹²

4.3.5 Regulatory

4.3.5.1 Senate Bill 1386 (California)

In 2004, the state of California introduced Senate Bill 1386 (SB1386). Under this bill all businesses and government entities must notify customers whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorised person.

In this bill a security breach is defined broadly as the "unauthorised acquisition of computerised data that compromises the security, confidentiality or integrity of personal information maintained by the person or business."¹³

Mitigating factors that led to its introduction are suggested to include the surge in high profile security breaches and increases in the compromise of personal information. A Federal Trade Commission survey estimated the financial impact of such identity theft cost consumer victims in 2003 approximately US\$5 billion, and businesses, including financial institutions, almost US\$50 billion¹⁴.

4.3.5.2 Sarbanes-Oxley Act of 2002

In July 2002, the Sarbanes-Oxley Act (SOX) came into force in the United States (US), introducing major changes to the regulation of corporate governance and financial reporting practices. The Act mandates stronger internal controls (including system controls) and institutes personal liability for executives of companies that are publicly traded in the United States. In short, its aim is to improve the accountability of managers to shareholders.

This legislation is a great example of reactive regulatory actions following a series of high profile scandals and governance failures at Enron, WorldCom and other companies.

The legislation has received much media and public attention, a major motivation for compliance and has triggered a ripple effect globally.

4.3.6 Other

4.3.6.1 ChoicePoint

It was discovered in 2005 that ChoicePoint—a data aggregation firm in the United States which collects and sells information on nearly every adult American and also deals with government organisations such as the Justice Department and the Drug Enforcement Agency (DEA)—sold personal information including social security numbers, to illegitimate

¹² Australian Associated Press, May 2006, 'Vic: Police sorry for another criminal file bungle', The Australian

¹³ DeLoach R, Pastor, N, n.d., *Bad News, Good News: Identity Theft and Data Security* viewed 15 May 2006, www.namb.org/Images/namb/GovernmentAffairs/WFW%202006-01%20_Identity%20Theft%20Data%20Security_.pdf

¹⁴ Synovate 2003, *Federal Trade Commission—Identity Theft Survey Report*, Author, McLean

enterprises. Consequently, 160 000 identity theft cases have been reported, while more than 500 000 people have potentially been exposed.

ChoicePoint stated that “a small number of very well-organised criminals posed as legitimate companies to gain access to personal information about customers.”¹⁵

In response to the incident, the company did not act out of ethical obligation to notify customers of the breach. It took them four months to notify anyone, and that was only in response to California’s consumer protection laws and then other states’ law enforcement demands.

Legislation can only be one component of security governance. Organisations have social obligations to the protection of its stakeholders and the public in general. In this instance the acceptable level of due diligence expected was not demonstrated via the validation and profiling of these “small” businesses.

Consequences of the breach included:

- 160 000 customer records were compromised;
- The U.S. Federal Trade Commission imposed a US\$10 million civil penalty against ChoicePoint;
- ChoicePoint has been asked to set up US\$5 million trust fund for individuals who might have become victims of identity theft; and
- ChoicePoint will have to submit a comprehensive security audit every two years for the next twenty years.

4.4 What is security governance?

4.4.1 Defining attributes

Security governance can take many forms, depending on the organisation and the external forces at play. Research and consultations indicated that there is no universally accepted definition of security governance. However, there are several attributes that were common throughout each of the definitions encountered. These attributes are provided in *Table 2: Security governance definition attributes*.

One thing that becomes immediately apparent is the connection between security governance definition attributes and the business.

¹⁵ Rosencrance, L., July 2005, *ChoicePoint says data theft cost it US\$6 million*, www.computerworld.com.au/index.php?id=1374868418

Security governance attributes	
Accountability	Ongoing
Aligned to business	Sustainable
Authority	Process
Cost of doing business	Policy
Culture	Protection
Good business sense	Risk, regulations and laws
Non-negotiable	Meet stakeholder needs

Table 1: Security governance definition attributes

4.4.2 Working definition

Taking these attributes into account and evaluating the variety of definitions that have been published, the following can be considered to be a sound way of defining security governance for any critical infrastructure organisation:

Establish and uphold a culture of security to provide assurance that the business objectives and stakeholder requirements for the protection of information are continually met.

If organisations—public and private—base their security governance models on this working definition, then all of the key attributes as described will be incorporated, aligning to global leading practices.

4.4.3 Relationship to corporate governance

The Australian Stock Exchange (ASX) Corporate Governance Council provides the following definition for corporate governance:

“Corporate governance is the system by which companies are directed and managed. It influences how the objectives of the company are set and achieved, how risk is monitored and assessed and how performance is optimised.

*Good corporate governance structures encourage companies to create value (through entrepreneurship, innovation, development and exploration) and provide accountability and control systems commensurate with the risks involved.”*¹⁶

Security governance is merely an extension of the definition of corporate governance to include specific aspects of information protection and assurance.

¹⁶ The ASX Corporate Governance Council, March 2003, *Principles of Good Corporate Governance and Best Practice Recommendations* (2003), www.asx.com.au/about/pdf/ASXRecommendations.pdf

4.4.4 Relationship to IT governance

The IT Governance Institute defines IT governance as the following:

*“IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation’s IT sustains and extends the organisation’s strategies and objectives.”*¹⁷

Again, it is evident that security governance is closely linked and related to IT governance and contains a number of the same attributes as defined earlier.

4.4.5 How does it all fit together?

The summary of the relationships between corporate, security and IT governance is shown in *Figure 9: Corporate, IT and security governance relationships*.

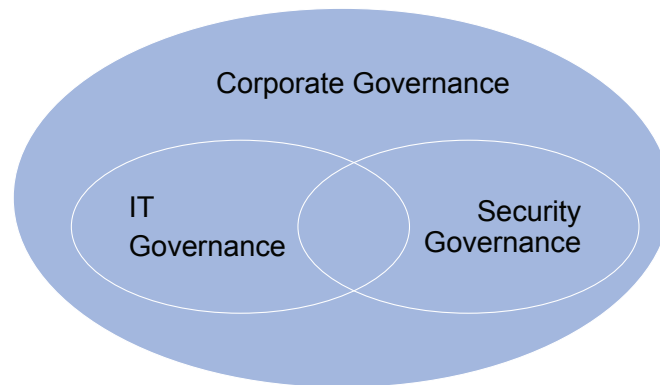


Figure 9: Corporate, IT and security governance relationships

This Figure illustrates how corporate governance serves as the overall framework for driving all governance activities within the organisation. IT governance provides outcomes specifically focused on aligning IT with the business while security governance provides outcomes specifically focused on aligning security with the business.

Although IT governance and security governance contain a number of similar attributes, their different focus results in an overlap of activities (one is not entirely contained within the other). This is a very important distinction that must be made to ensure that the organisation’s security governance framework (and subsequent structures, accountabilities and processes) is not solely driven from an IT point of view.

Leading practices dictate that security is not a technology issue and must be addressed from a top-down, holistic perspective across the enterprise. The relationships between different governance areas as shown in Figure 9 help to reinforce this point.

¹⁷ www.itgi.org

4.5 How is security governance related to security management?

Security governance and security management, although related, are not the same. In simple terms, security governance is used to ensure that all security management functions are designed, implemented and operating effectively.

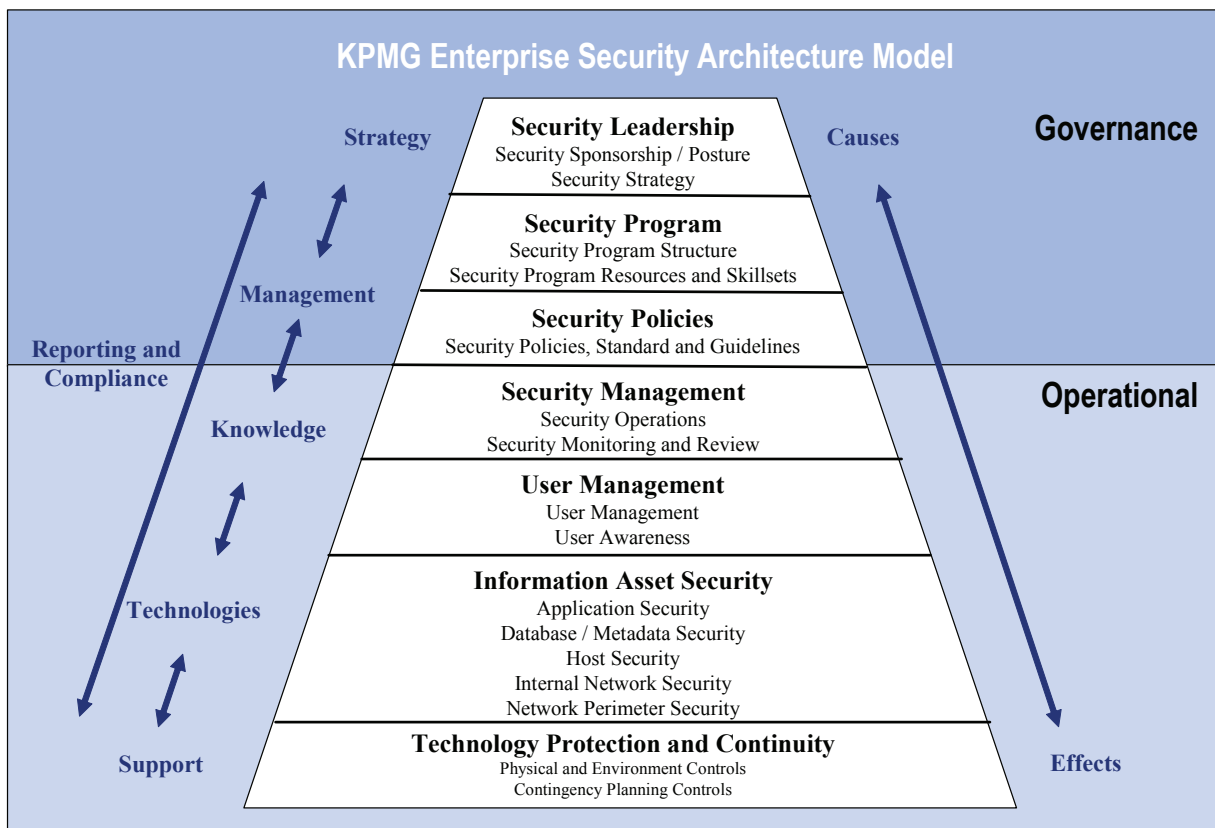
Security governance sets the tone at the top for implementing a culture of accountability in order for effective security management to take place.

4.5.1 Security management

An Information Security Management System (ISMS) establishes policy, principles and processes for the management of information security throughout the organisation, according to a risk-based model.

It is a methodical and cyclical approach to managing the protection of information to support the achievement of organisational goals. International standards such as ISO27001—described later on in the report—provide guidelines for how to design and implement an ISMS to support effective security management.

4.5.2 Enterprise security architecture model



This model demonstrates the relationship between security governance and security management (operations).

KPMG’s Enterprise Security Architecture Model provides a top-down view of security governance and operations, indicating each of the key focus areas for capability. All layers of the model above are interdependent on one another, thus organisations should ensure that the responsibilities and capabilities of individuals within the organisation adequately cover each layer, and that the linkages between each layer are clearly understood.

This model has been developed by considering leading practices (such as ISO17799 / ISO27001), as well as practical examples of how leading companies organise their information security functions.

A key component of this model, as indicated by the arrows on the left side of the figure, is a reporting and compliance capability that provides monitoring at all levels of the organisation and transparency to the Board regarding the effectiveness of security functions and capabilities. These overarching reporting and compliance functions are critical in supporting the implementation of any security governance framework.

4.6 Why is security governance important?

4.6.1 Stakeholder expectations

In today’s world, stakeholder expectations for the protection of information are already high and are continuing to increase. Failures are no longer considered acceptable and the impacts of failure can be far-reaching and devastating.

Through the research and consultations, one of the primary themes regarding stakeholder expectations dealt with reputation and trust. This was consistent across virtually every industry within critical infrastructure.

The general belief is that the real impact to the critical infrastructure industry is not necessarily the cost of an outage or compromise, but the ability of the organisation to demonstrate that it was operating with the stakeholders’ interests at heart and responded effectively to maintain trust.

Corporate scandals related to Enron, MCI and Tyco are perfect examples of unacceptable failures in an organisation’s ability to operate with the stakeholders’ interests at heart, undermining the confidence in capital markets. The result was the passing of legislation—the US Sarbanes-Oxley Act of 2002—that forced the issue of ensuring companies were doing what many people felt they should have been doing all along.

This leads us to the first key reason why security governance is important:

Stakeholders of owners and operators of critical infrastructure expect strong security governance to already be in place. Failure to meet this expectation can result in unacceptable impacts to the business or the community.

4.6.2 Risk

The risks to society, economy and ultimately the industry’s ability to meet stakeholder expectations are ever increasing. Dependencies on technology, the rate of convergence, the increasing gap between technology adoption and the controls adoption has created a riskier environment where the opportunities for threats are greater than ever before.

These changes in the risk landscape for owners and operators of critical infrastructure have resulted in a higher level of diligence required to ensure that risks are managed to acceptable levels for the organisation, across the enterprise.

Leading practices demonstrate that security governance and management activities should be driven from a risk management point of view. This has led to the second key reason why security governance is important:

Owners and operators of critical infrastructure require strong security governance to ensure effective ongoing management of risk.

4.7 How can we achieve strong security governance?

There is no single leading practice model defined for security governance. Each organisation’s security risk profile will differ and each organisation’s business objectives and practices will differ (even within the same industry!). Therefore, it is important to recognise that any model must be adapted and tailored to the individual organisational needs.

Based upon the research and consultations, Figure 10 represents a leading practice framework, which illustrates the key components for security governance via a top-down approach.

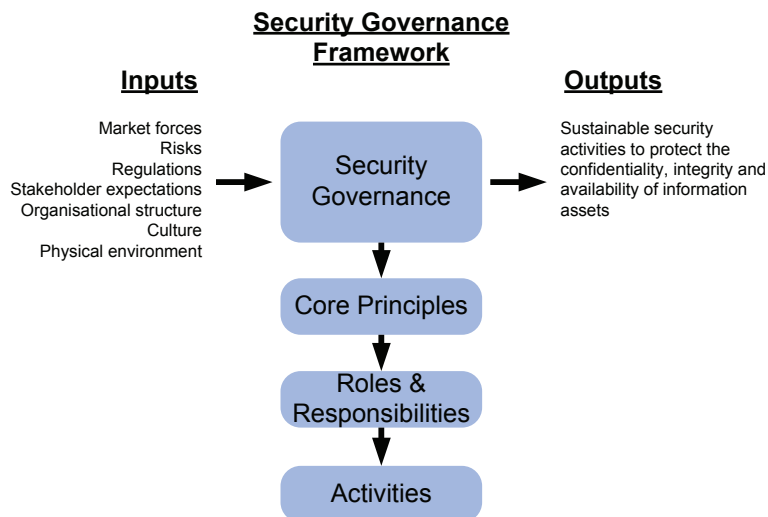


Figure 10: Leading practice security governance framework

This framework is composed of three components:

- 1 **Core principles:** serve as the primary driver for all security governance functions and activities;
- 2 **Roles & responsibilities:** define the assignment of accountabilities to ensure security governance activities take place and achieve the spirit of the core principles; and
- 3 **Activities:** the underlying processes that are owned and operated by accountable individuals to implement and maintain security governance capabilities.

4.7.1 Core principles

Underpinning any security governance framework (as illustrated in Figure 11—Leading practice security governance framework), is a set of core principles. In this way, the decision-making structures and subsequent processes can differ, but remain focused on the common goal as derived from the definition of security governance provided earlier in this document.

The following set of core principles represents leading practice and establishes the foundation for strong security governance. These principles are not intended to be prescriptive and are provided as a reference guide to build enhanced capabilities, manage security risk, provide an appropriate level of transparency, optimise performance and maximise accountability.

	Principle	Description
1	Accountability	Accountability is defined at all levels of the organisation—from the board of directors to operational staff. Authority for security governance decision-making is clearly defined and oversight functions are well understood throughout the organisation.
2	Awareness	Every stakeholder in the security governance framework is aware of and understands their role and responsibility in upholding the framework and the consequences (both internal and external) of not performing the required functions.
3	Compliance	The organisation’s activities are continually in compliance with legal and regulatory requirements, business requirements and stakeholder requirements. Compliance activities are defined and performed at all levels of the organisation.
4	Effectiveness	The security governance model is sustainable across the enterprise, where security functions are clearly aligned with corporate objectives, critical success factors, and the mitigation of enterprise security risks.
5	Ethics	The organisation has a culture of ethics where every stakeholder understands their role in maintaining an ethical organisational culture.

	Principle	Description
6	Inclusion	The security governance framework includes both internal and external stakeholders to the organisation (board of directors, business partners, customers, supply chain partners, vendors, regulators, auditors, management and employees). For example an appropriate level of stakeholder involvement exists for the development and review of principles, policies, procedures, processes and controls.
7	Transparency	Information reporting on security governance activities and outcomes is completely transparent throughout all levels of the organisation with ultimate transparency at the board level.
8	Measurement and Reporting	Continuous monitoring is in place to ensure value and adequacy (or lack thereof) of enterprise security and the extent to which enterprise security actions are aligned with enterprise objectives. Metrics are defined and regularly reported throughout all levels of the organisation.
9	Scope	Security is defined and addressed at a holistic level, including corporate culture, people, training, processes, communications and technology. The organisation's security strategy is directly aligned to the corporate strategy and is implemented through an integrated set of principles, policies, procedures, processes and controls.
10	Response	The organisation has a planned, tested and dynamic capability for responding to enterprise security threats. Response capabilities include a key focus on the maintenance of trust and public confidence.
11	Risk Management	Decisions regarding security governance are based upon the determination of risk to information assets and sound commercial and social responsibility judgment. Costs of compromise (such as loss, damage, disclosure, denied/interrupted access, costs to reconstitute) are quantified to the extent possible as part of ongoing risk management functions. Controls are selected to effectively mitigate risk and their performance is regularly measured and reviewed. Plans for risk mitigation are developed and executed following each assessment.

Table 2 - Core principles for effective security governance

4.7.2 Roles and responsibilities

Security governance framework models should take a view of people, process and technology factors to achieve the following objectives:

- propose an oversight and management function hierarchy;
- establish security governance as a core function alongside other key corporate governance functions, such as financial and operational risk management; and
- provide a reference guide for those implementing security governance within a corporate governance environment.

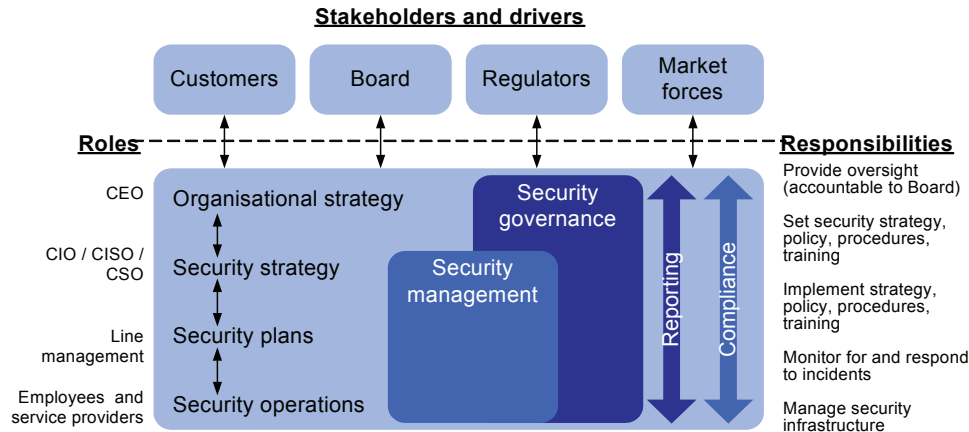


Figure 11: Security governance framework

Figure 11 outlines the responsibilities for key executives and employees to achieve the level of accountability necessary for effective security governance at an enterprise level.

This figure illustrates an example of a leading practice model that incorporates the external and internal interactions required to operate an organisational security function. Key to any organisation (in both public and private sectors) is the security governance activities that foster and maintain a sustainable and controlled security function that meets the organisational objectives and strategy.

Supporting this interaction model are various security critical success factors, organisational capabilities, core principles (as described above) and approaches that seek to facilitate an organisation in meeting their security goals.

An organisational hierarchy, supporting security accountability, should be developed depending on the size and individual nature of stakeholders and drivers of the organisation.

4.7.3 Activities

The Corporate Governance Task Force of the National Cyber Security Partnership (NCSP) developed an Information Security Governance (ISG) Framework¹⁸ and subsequent recommendations that can be leveraged in the definition of a leading practice security governance framework.

The activities described by the ISG framework not only include compliance with legislative and regulatory requirements, they also focus on the realisation of business benefits such as improved internal processes and controls and the potential to reduce audit and insurance costs.

¹⁸ Corporate Governance Task Force 2004, *Information Security Governance A Call to Action*, Washington D.C.

The combination of the ISG Framework activities and other effective security governance encountered through research and consultations, defines a comprehensive set of activities to support the implementation of the roles and responsibilities as defined. These recommended activities for owners and operators of critical infrastructure are:

- conduct an annual security evaluation, review the evaluation results with staff, and report on performance to the board of directors;
- conduct periodic risk assessments of information and IT assets as part of a risk management program;
- implement and maintain policies and procedures based on risk assessments to secure its information and assets based on industry sound practice. ISO17799 describes one such standard which can be used to do this. This standard covers 11 core domains:
 - information security policy;
 - organising information security;
 - asset management;
 - human resources security;
 - physical and environmental security;
 - communications and operations management;
 - access control;
 - information systems acquisition, development and maintenance;
 - information security incident management;
 - business continuity management; and
 - compliance.
- establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability;
- develop plans and initiate actions to provide adequate security for networks, facilities, systems and information;
- treat security as an integral part of the system lifecycle;
- provide security awareness training and education to all personnel;
- conduct periodic testing and evaluation of the effectiveness of security policies and procedures;
- create and execute remediation action plans to address any security deficiencies;
- develop, implement and regularly test incident response procedures;
- establish plans, procedures and tests to provide continuity of operations; and
- use security best practices guidance to measure security performance, such as ISO17799/ISO27001.

4.8 Supporting standards and relevant legislation

There are a variety of local and international laws and standards that govern how companies must address information security. In order to effectively implement a security governance framework it is important to understand what legislation and standards apply today and in the future.

4.8.1 Standards

When defining a security governance framework, benefits can be realised by applying elements from a wide variety of local and international standards. In Australia, businesses subject to regulation in the private sector may choose the Standards Australia based framework (e.g. AS/NZS 4360, AS/NZS 8015, etc).

In some cases regulatory bodies have mandated, or are in the process of mandating publicly operated critical infrastructure sectors with specific standards (e.g. Protective Security Manual and ACSI 33). While these security standards apply at a state and territory level, they may also cascade to the local government sector such as in the instance of water and sewerage utilities.

Table 4 lists the range of standards applicable for the implementation of security governance for the protection of critical infrastructure within Australia:

Standards	Summary
Publisher	
<p>ISO17799 / ISO27001 / AS/NZS17799— Code of Practice for Information Security Management</p> <p>Standards Australia, International Organization for Standardization</p>	<p>Is a globally accepted code of practice for information security management. It is a controls based standard for organisations to manage their information security according to 11 domains:</p> <ul style="list-style-type: none"> - Information security policy - Organising information security - Asset management - Human resources security - Physical and environmental security - Communications and operations management - Access control - Information systems acquisition, development and maintenance - Information security incident management - Business continuity management - Compliance



Standards	Summary
Publisher	
<p>COBIT—Control Objectives for IT ISACA</p>	<p>It provides a flexible framework for organisations to meet business objectives and quality, financial and security requirements. It defines seven information criteria:</p> <ul style="list-style-type: none"> - Effectiveness - Efficiency - Confidentiality - Integrity - Availability - Compliance - Reliability of information
<p>AS/NZS 4360:1999—Risk Management Standards Australia / SAI Global</p>	<p>Is a risk management standard. It defines a general framework consisting of five major stages:</p> <p>Stage 1: Establishing the Context</p> <p>Stage 2: Identifying the Risks</p> <p>Stage 3: Analysing the Risks</p> <p>Stage 4: Assessing & Prioritising Risks</p> <p>Stage 5: Determining Appropriate Controls</p>
<p>AS8015—Corporate Governance of ICT Standards Australia</p>	<p>Is an Australian standard for corporate governance of information and communication technology (ICT). It provides six guiding governance principles and a model by which organisations can ensure that IT is aligned with their business objectives. The principles are:</p> <ul style="list-style-type: none"> - Establish clearly understood responsibilities for ICT - Plan ICT to best support the organisation - Acquire ICT validly - Ensure ICT performs well, whenever required - Ensure ICT conforms with formal rules - Ensure ICT use respects human factors
<p>Australian Government Protective Security Manual (PSM) Protective Security Coordination Centre (PSCC)</p>	<p>It is the principal means for publishing Australian Government protective security policies, principles, standards and procedures to be followed by all Australian Government agencies for the protection of official resources. The PSM is the Australian Government's top-level framework for physical, information and personnel security.</p>



Standards	Summary
Publisher	
<p>ACSI 33— Australian Government Information and Communications Technology Security Manual</p> <p>Defence Signals Directorate (DSD)</p>	<p>Is an Australian standard to provide policies and guidance to Australian Government agencies on how to protect their ICT systems?</p>
<p>FERC/NERC Urgent Action Standard 1200— Cyber Security</p> <p>The Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Council (NERC)</p>	<p>Is a standard that is designed to safeguard the industry and its customers against these risks through vulnerability assessments, threat response strategies, emergency management planning, employee background checks, physical and communications fortifications, and other measures a prescriptive approach that can help compliant companies:</p> <ul style="list-style-type: none"> - Demonstrate a serious security commitment to customers, partners and regulatory agencies - Prioritise spending - Enable integration and scalability - Reduce operational risk - Establish a focused framework for compliance audits - Improve overall corporate stability

Table 3: Globally recognised standards

4.8.2 Relevant legislation

Organisations, in both public and private sectors, are potentially liable for the acts of their employees. For example, if an employee propagates a virus attack via an email the organisation may be liable for damages if it is found that there was failure to take reasonable care resulting in the damage incurring.

The Corporations Act 2001 imposes a number of legal responsibilities upon company directors, secretaries and “officers” which are broadly defined to cover COOs, CTOs, CIOs and Information Systems Managers. These requirements suggest, as a director or officer, an obligation to uphold due care and diligence.

The Privacy Act 1988 imposes obligations on certain companies on the way they collect, retain, use and disclose personal information. Companies must take reasonable steps to protect the personal information they hold from misuse and loss from unauthorised access, modification or disclosure. This will require that most companies implement appropriate physical and information security systems to ensure that information held is protected.

If an organisation or individual fails to take “reasonable care” causing damages to another person or company, the negligent company may be liable to pay to the other party. However, if reasonable security governance measures are in place, including awareness and accountability, negligence may be avoided.

Table 5: Impact of Recent Information Security Legislation derived from Information Security Governance: Toward a Framework for Action—Business Software Alliance¹⁹, details examples of local and international legislation that owners and operators of critical infrastructure should become familiar with and leverage in the context of establishing their security governance frameworks and capabilities.

Recent Legislation	Who is affected?	What do the security provisions cover?	What are the penalties?
Privacy Act 1988 / Privacy Amendment (Private Sector) Act 2000	Australian health care providers, Commonwealth government agencies and large Australian private companies	Security of customer records including health and financial information	CIP, CIF, RoA
State Privacy Legislation: Information Privacy Act 2000 (Vic) Invasion of Privacy Act 1971 (QLD) Health Records (Privacy and Access) Act 1997 (ACT) Privacy and Personal Information Protection Act	Australia health care providers and the Australian public Sector	Security of personal data and the enforcement of the privacy principles	CIP, CIF, RoA

¹⁹ Business Software Alliance 2003, Information Security Governance: Toward a Framework for Action, Washington D.C.



Recent Legislation	Who is affected?	What do the security provisions cover?	What are the penalties?
1998 (NSW)			
Telecommunications Act 1997	Australian Communication and Media Authority (ACMA), carriers and carriage service providers	Security of telecommunications networks	CrP, CIP, RoA
Statutory Corporations (Liability of Directors) Act 1996	All Australian directors of corporations	Exercising reasonable care and diligence	CIF, RoA
Corporations Act 2001	Australian private Sector	Exercising reasonable care and diligence	CIF, RoA
Sarbanes-Oxley Act of 2002	All public companies subject to US security laws	Internal controls and financial disclosures	CrP, CIP
Gramm-Leach- Bliley Act of 1999	US Financial institutions	Security of customer records	CrP, CIP
Health Insurance Privacy and Accountability Act (HIPAA)	US Health plans, health care clearinghouses, and health care providers	Personal health information in electronic form	CIF, CrP
SB1386 California Database Security Breach Information Act	US California agencies, persons, and all businesses that conduct business in the State of California	Reporting of breaches of unencrypted personal information	CIF, RoA
Federal Information Security Management Act (FISMA)	US Federal agencies	US Federal information, IS, and security programs	Loss of IT funding

Table 4: Impact of Recent Information Security Legislation

Penalty Keys

CrP - Criminal penalties

CIP - Civil penalties

CIF - Civil fines

RoA - Right of action

5 CONCLUSION

The risk landscape to critical infrastructure owners and operators is rapidly changing. They depend more on technology than ever before and the impacts of failure extend beyond traditional thinking.

The incidence of deliberate attacks on critical infrastructure is also increasing, driven by a wide range of motivators: financial gain, curiosity, vandalism, opportunism, ideological differences and more.

The quantifiable impacts of security incidents in Australia have more than doubled in the last year alone. The intangible impacts to trust, reputation and economic and social confidence are often said to be an order of magnitude larger than the tangible impacts and may never be truly understood. In fact, the capability to measure the downstream impacts of an incident (impacts external to the organisation directly affected) are not in place.

Although Australia has been relatively fortunate as compared with other countries with regards to security failures, it cannot afford to employ an “it won’t happen to us” attitude. It is not a question of “if”, but “when”.

We must learn from the lessons of others, and leverage leading practices from within Australia and around the world to implement the strongest relevant security governance frameworks and practices to support the safe achievement of business objectives.

Australia’s economic chain is only as strong as its weakest link, which makes critical infrastructure, both in public and private sectors, responsible for ensuring that they are contributors to the solution, not the problem.

It is estimated that 90 per cent of Australia’s critical infrastructure is owned and operated within the private sector²⁰. Whilst the government has a role in raising the awareness of the need to implement security governance, effective measures must occur at the corporate level.

In some cases regulatory bodies have mandated, or are in the process of mandating, publicly operated critical infrastructure sectors with specific standards (e.g. Protective Security Manual and or ACSI 33). While these security standards apply at a state and territory level, they may also cascade to the local government sector such as in the instance of water and sewerage utilities. Privately owned and operated critical infrastructure may also be affected by such mandates that apply to their industry in particular where service delivery may have been outsourced.

Board and executive commitment to security governance will not ensure its success but a board’s lack of commitment will guarantee its failure.

Security governance should be seen as a business success objective. It is all about what level of risk an organisation and its stakeholders are willing to accept. Every executive needs to understand that it should be addressed with the same logic that is applied to make financial, acquisition and other ‘non-security’ related business decisions.

²⁰ Rothery, M. (Critical Infrastructure Protection Branch, Attorney-General’s Department), 2005, ‘Critical infrastructure protection and the role of emergency services’, *The Australian Journal of Emergency Management*, vol. 20, no 2, pp. 45-50

To achieve what is required, organisations need to consider the information presented in this report, apply it to their environment and ensure the three main components of an effective security governance framework are in place:

- principles;
- roles & responsibilities; and
- activities.

This should be implemented using a top-down approach as illustrated in the following figure to ensure all layers of risk are covered.

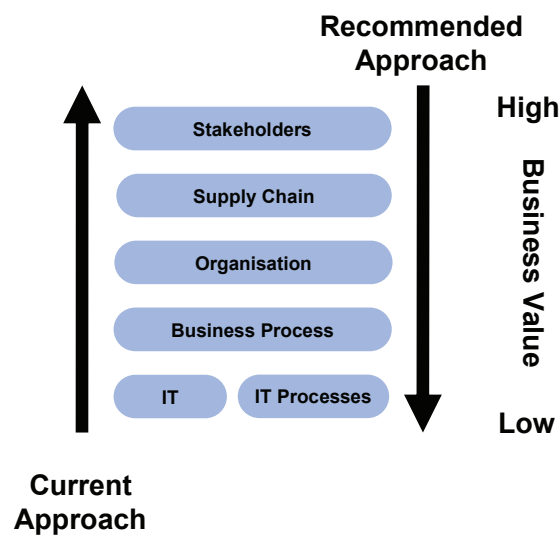


Figure 12: Approach to implementing security governance

In particular, organisations need to know:

- Their stakeholders' expectations for organisation resilience;
- Their dependence on the supply chain and the up-stream and down-stream impacts (interdependencies) in the event of an incident;
- The awareness of employees and capability at all levels of the organisation;
- The ongoing effectiveness of controls at the business process layer; and
- The resilience of IT and IT processes to support business processes.

All of these questions can be answered through the implementation of an effective security governance framework as described in this report.

To protect Australia's social and economic interests, all organisations—public and private—must take action now to ensure that they are protecting their own interests as well as meeting their stakeholders' expectations for corporate and social responsibility. Society's future depends on it.



Further information is available at the TISN website (www.tisn.gov.au), including:

Reports

- Denial of Service and Distributed Denial of Service, Managing DoS Attacks
- Leading Practices and Guidelines for Enterprise Security Governance
- Critical Infrastructure Protection: Whose Responsibility is it?
- National Guidelines on Protecting Critical Infrastructure from Terrorism

Information for CEOs

- IT Security and Governance for Board of Directors and CEOs
- GPS—An Overview for CEOs
- SCADA—Advice for CEOs
- Security of Voice Over Internet Protocol (VoIP)—Advice for CEOs
- Wireless Security—Overview for CEOs

Information for CIOs

- Denial of Service /Distributed Denial of Service: Advice for CIOs
- CIO and CISO Practitioner Guidance: IT Security Governance
- Security of Voice Over Internet Protocol (VoIP)—Advice for CIOs
- Wireless Security—Overview for CIOs

Appendix A—References

- Standards Australia 2004, *Risk Management AS/NZS 4360:2004*, Third Edition, Sydney
- International Organisation for Standardization 2005, *Information Technology—Security Techniques—Code of Practice for Information Security Management ISO/IEC 17799:2005*, 2nd Edition, Geneva
- IT Governance Institute 2000, *COBIT Audit Guidelines*, 3rd Edition, Rolling Meadows
- Rothery, M. (Critical Infrastructure Protection Branch, Attorney-General’s Department), 2005, ‘Critical infrastructure protection and the role of emergency services’, *The Australian Journal of Emergency Management*, vol. 20, no 2, pp. 45-50
- Australian Stock Exchange (ASX) Corporate Governance Council 2003, *Principles of Good Corporate Governance and Best Practice Recommendations*, Sydney
- IT Governance Institute 2003, *Board Briefing on IT Governance*, 2nd Edition, Retrieved January 18, 2006
www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Board_Briefing_on_IT_Governance/26904_Board_Briefing_final.pdf
- Corporate Governance Task Force 2004, *Information Security Governance A Call to Action*, Washington D.C.
- Bridge Point Communications Pty Ltd, October 2001, *Information Security: Corporate and Individual Liability*, Australia
- Communications Technology Inc. 2004, *Supervisory Control and Data Acquisition (SCADA) Systems*, Technical Information Bulletin 04–1, Office of the Manager National Communications System, Arlington
- The Institute of Internal Auditors 2001, *Information Security Governance: What Directors Need to Know*, Florida
- IT Governance Institute 2001, *Information Security Governance: Guidance for Boards of Directors and Executive Management*, Rolling Meadows
- The Institute of Internal Auditors 2001, *Information Security Management and Assurance: A Call to Action for Corporate Governance*, Author, Florida
- Allen, J. 2005, *Governing for Enterprise Security*, Carnegie Mellon University, Pittsburgh
- Synovate 2003, *Federal Trade Commission—Identity Theft Survey Report*, McLean
- Australian National Audit Office 2005, *IT Security Management*, ANAO Audit Report No. 23 2005-06, Canberra
- The White House 2003, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Washington D.C.
- Business Software Alliance 2003, *Information Security Governance: Toward a Framework for Action*, Washington D.C.
- ISACA, 2006, *Why Information Security Governance is critical to wider corporate governance demands—A European perspective*, Poole, V.

United States General Accounting Office 2004, *Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems*, Washington D.C.

Stamp, J., Dillinger, J., Young, W. & DePoy, J. 2003, *Common Vulnerabilities in Critical Infrastructure Control Systems*, 2nd Edition, Sandia National Laboratories, Albuquerque

Varnado, S. 2005, *Supervisory Control and Data Acquisition Systems*, Congressional Testimony by CQ Transcriptions, Washington D.C.

Attorney General's Department, *Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection*, viewed March 2006, www.tisn.gov.au

AusCERT 2006, *Computer Crime and Security Survey*, Brisbane

Hammond A IV, Magnin C J. 2001, *The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?* Santa Clara University, Santa Clara

Leslie Senate Bill 1386, 1998, Analysis of original Bill SB1386 developed by the SCS Agency

Panda Software International 2006, *Quarterly Report PandaLabs (January–March 2006)*, Glendale

US–Canada Power System Outage Task Force, 2003, *Interim Report: Causes of the August 14th Blackout in the United States and Canada*, United States and Canada

North American Electric Reliability Council, 2004, *August 14, 2003 Blackout: NERC Actions to Prevent and Mitigate the Impacts of Future Cascading Blackouts*, Princeton, New Jersey

Cunningham M, May 2006, *8 police punished*, Herald-Sun

Roberts, P, January 2005, *U.S. Secret Service data compromised in T-Mobile hack*, published on www.pcworld.com

Roberts, P., March 2005, *Paris Hilton: Victim of T-Mobile's Web Flaws?*, published on www.pcworld.com

Crawford, M., 15 June 2006, *Nairn disappointed with ANAO report: launches workgroup*, www.computerworld.com.au

Verton D. 2001, *California Hack Points to Possible Surveillance Threat*, Computerworld, www.computerworld.com

Lemos R. 2001, *Hack raises fears of unsafe energy networks* viewed on ZDNet News, www.news.zdnet.com

FTC settles with CardSystems over data breach, 2006, viewed 24 May 2006 on www.out-law.com

Vijayan J, and Weiss T., 2005, *CardSystems breach renews focus on data security*, www.computerworld.com

Evers J, 2005, *Credit card breach exposes 40 million accounts*, CNET News.com, www.news.com

Shermach K, 2005, *ChoicePoint and Data Security*, CRM Buyer, www.crmbuyer.com



Trusted Information
Sharing Network
for Critical Infrastructure Protection

Sarbanes-Oxley Act 2002, *Sarbanes-Oxley Act Summary and Introduction* viewed on 24 May 2005 www.soxlaw.com/introduction.htm

The United States Nuclear Regulatory Commission Office of Nuclear Reactor Regulation, 2003, *NRC Information Notice 2003-14: Potential vulnerability of Plant computer network to worm infection*, Washington, DC.

The United States Nuclear Regulatory Commission Office of Nuclear Reactor Regulation, 2003, *NRC Issues Information Notice on potential of nuclear power plant network to worm infection*, Washington, DC.



Appendix B—Consultation questionnaire

Question	
Project overview / related projects	
1	Have you been involved in similar studies? If so, what was the approach and what were the outcomes?
Perception of current state / future state	
2	What is your perception regarding the current state of security governance? What is driving (influencing) the future state?
3	What models have you identified as successful models for security governance, both nationally and overseas?
Security governance in the organisation	
4	What is your role in your organisation's Security framework? Who do you report to?
5	How do you define IT security governance? Do you feel it is different than IT security management?
6	Please provide an overview of your current Corporate Security Governance framework in the organisation.
7	How does the organisation security governance framework interlink with the IT governance and corporate governance framework?
8	What is the role of security architecture in security governance?
9	Is the security architecture updated periodically to take into account new business needs and strategies as well as changing security threats?
10	When was your framework last reviewed?
SCADA / process control	
11	How are risks to SCADA / Process Control infrastructure identified, classified and managed?
12	What are the major attacks or other relevant case studies you have heard of on SCADA infrastructure?
Corporate information security	
13	Which security risks are high priority for the organisation?
14	Do you regularly re-assess your implementation for vulnerability to attack? If so, when was the last time you did this?
15	Do you regularly re-assess your policy?
16	Is there anything unique about being in CI that impacts your overall security policy?
17	Have you ever had any issues relating to enterprise security? If "YES" – what was the nature of the issues and what was the business impact? If "NO" what measures are in place to monitor the CI to detect breaches?
18	What examples / case studies have you encountered?
19	What would you consider to be the greatest risks and areas of exposure with CI in your industry? What practical advice can you give on how to manage those risks?