Trusted Information
Sharing Network
for Critical Infrastructure Protection

Secure Your Information:

Information Security Principles for Enterprise Architecture

Advice for CIOs and CSOs

June 2007

DISCLAIMER: 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 judgment of users. This document is intended as a general guide only and users should seek professional advice as to their specific risks and needs.

Introduction

Responsibility for protecting enterprise information assets is at the core of the role of the Chief Information Officer (CIO). However, balancing conflicting priorities in meeting operational needs and information protection is a challenge that cannot be achieved by just one person or even one department. Establishing core principles that lie at the heart of an enterprise strategy for information security must start at the top and filter through the entire enterprise—creating a “culture of security”.

This paper defines the Seven Basic Principles of Information Security that must underpin the enterprise’s strategy for protecting and securing its information assets.

1. Information Security is Integral to Enterprise Strategy

Information security must have the endorsement and support of executive management and the Board.

2. Information Security Impacts on the Entire Organisation

Information security involves considering people, technology and processes throughout all areas of the business.

3. Enterprise Risk Management Defines Information Security Requirements

The proposed treatment of risk must be proportional to the business impact.

4. Information Security Accountabilities Should be Defined and Acknowledged

All users and managers of information systems should be informed of the consequences of their actions.

5. Information Security Must Consider Internal and External Stakeholders

The legitimate interests of all stakeholders should be considered in information security decision-making.

6. Information Security Requires Understanding and Commitment

Awareness and understanding within the organisation supports the development of a culture of security.

7. Information Security Requires Continual Improvement

Ongoing improvement allows the organisation to sustain the state of information security at a level that is acceptable to all stakeholders.

Background

Convergent technologies are at the centre of change in the modern business enterprise. Internet Protocol (IP) based networks are transforming existing business processes. They are redefining the value of critical business information by altering where it resides, how it is shared and the business processes it controls. While convergent technologies have delivered benefits to business such as reduced operational costs and improved efficiency, they also expose the organisation to new risks, threats and vulnerabilities. Failure to adequately address information security in an environment where convergent technologies have the potential to transform business processes and functions can leave the organisation exposed to serious risks.

There are three papers in this series:

- The full report which:
  - establishes a baseline set of information security principles to support the development of enterprise strategy for information security; and
  - provides guidance on the application of the principles in the context of Enterprise Architecture and with specific consideration of Australian critical infrastructure sectors.
- The CEO paper, which summarises the full report, and is designed to provide senior executive guidance on developing an enterprise strategy for information security.
- This CIO paper which is an extended summary that considers the development of enterprise strategy for information security with the perspective of building the seven identified principles into the Enterprise Architecture.

These documents outline a foundation upon which to build a secure and robust Enterprise Architecture within critical infrastructure organisations.

Since 2005, the IT Security Expert Advisory Group (ITSEAG)[i] of the Trusted Information Sharing Network (TISN)[ii] has released a series of papers designed to help CEOs, Boards of Directors and CIOs understand the threats to the information and IT infrastructure of their organisations and provide recommendations for mitigating those threats. The papers cover many topical issues including information security governance, managing denial of service attacks, and the security implications of technologies such as global positioning systems, Voice over IP and wireless networking.

The ITSEAG's 'Leading Practices and Guidelines for IT Security Governance' report highlighted the need to manage security within this emerging environment. Specifically, threats associated with "convergence" were identified for attention[1]. A mapping between the principles presented in both reports is shown in Figure 1.

Enhanced technology and improved software and hardware engineering have enabled businesses to achieve more with less. This has raised the level of dependence on IT infrastructure to a point where many businesses would fail (or suffer severe impacts) if an extended outage of the IT infrastructure were to occur. By merging elements and

[1] ITSEAG (Trusted Information Sharing Network*), Leading Practices and Guidelines for IT Security Governance*, 2006, *http://www.dcita.gov.au/__data/assets/pdf_file/41308/IT_Security__and__Governance.pdf*

functionalities within the Enterprise Architecture, convergence exposes the organisation to new risks. Critical information that is vital for business processes may now be located in various formats, in dispersed locations and on different integrated networks.

Information Security is Integral to Enterprise Strategy	Information Security Impacts on the Entire Organisation	Enterprise Risk Management Defines Information Security Requirements	Information Security Accountabilities Should be Defined and Acknowledged	Information Security Must Consider Internal and External Stakeholders	Information Security Requires Understanding and Commitment	Information Security Requires Continual Improvement	
			■				Accountability
					■		Awareness
						■	Compliance
■	■						Effectiveness
				■			Ethics
	■			■			Inclusion
■	■	■					Transparency
		■				■	Measurement and Reporting
	■		■	■			Scope
				■			Response
		■					Risk Management

Figure 1—Mapping the Seven Enterprise Security Principles to the TISN Governance Security Principles

At the enterprise strategy level, information security must have, at its foundation, a series of high-level principles that are understood by all within the organisation. The seven principles and their practical recommendations developed in this paper map to the 11 core principles of security governance contained within the ‘Leading Practices and Guidelines for Enterprise Security Governance’.

These principles are fundamentally not new. However, given a rapidly changing technological environment, it is timely to re-frame and re-emphasise these basic principles, as they apply to Enterprise Architecture within Australian critical infrastructure sectors. CIOs must work with others, including security practitioners to maintain an effective information security regime.

Enterprise Architecture and Organisational Strategy

Technology has enabled the new “dynamic enterprise” to change the way business is conducted. In so doing, it has required organisations to become adaptable, resilient and flexible in changing environments, dictating a shift from the focus on production to information. Information management is now a core business process as critical as cash flow management. Meanwhile, the evolution of technology and new strategic approaches to business has increased the complexity for handling an organisation’s information assets.

Critical business information now exists extensively on laptops, personal digital assistants (PDAs) and portable hard drives, components which often exist outside the traditional definition of the organisation’s secure perimeter. This perimeter is now changing to include customers, suppliers, business partners, and the mobile workforce, creating a new ‘mobile perimeter’ that increases corporate risk.

In order to adapt to these complex contemporary requirements, organisations need to re-examine the way in which enterprise information assets are organised and managed. This has led to the wider adoption of strategies such as Enterprise Architecture modelling. The principal goal of Enterprise Architecture is to support business strategy by providing a high-level definition of the fundamental technology and process structure of an organisation.

While Enterprise Architecture assists CIOs to visualise current and future business and technology requirements, it also assists in the development and management of the organisation’s information assets—including their protection.

Matching Enterprise Architecture outcomes with information security requirements can be achieved by building the principles outlined in this document into the entire information infrastructure.

Convergence Driving Security Concerns

A major precipitator in the evolution of Enterprise Architecture is the concept of convergence—the merging of elements and functionalities within the Enterprise Architecture.

Recent prominent architectural changes resulting from convergence include:

- Centralisation of business functions;
- An increasing interconnectedness of organisations through shared networks;
- Deployment of service-oriented architectures (SOA);
- Simplification of applications through the use of ubiquitous web interfaces;
- Integration of voice and data networks on single infrastructures; and
- Wide deployment of multifunctional wireless hand-held and network devices.

Integration of convergent technology affords organisations with benefits including operational efficiencies, increased speed to market, improved customer service and a quicker return on investment. However, the removal of security barriers from previously strictly defined organisational structures and the blurring of the organisation’s secure perimeter present significant challenges including:

- Potential degradation in quality of service over shared infrastructure;
- Distribution of and added complexity to authentication and authorisation mechanisms;
- Increased points through which systems and organisations can be attacked;
- Increased confusion on where and to whom responsibility and accountability apply; and
- Incident detection and response in interconnected environments with many external parties.

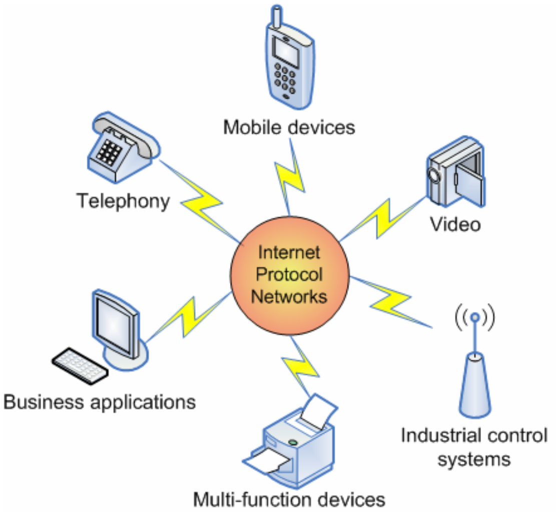

Figure 2—Convergence of Enterprise Architecture

In order to manage these security threats, risks and vulnerabilities, proactive management of information security is required. The information security governance framework must address the management of the blurring of the security perimeter and seek to develop a 'culture of security'. Of particular importance is the concept of enterprise-wide responsibility for security, which should be adopted.

The set of principles further developed in the full report is intended to provide a best practice framework that will allow organisations to implement sound and proven security techniques and strategies. The principles are outlined below. Associated recommendations are expanded further in the full 'Secure Your Information' report.

Information Security Drives Regulatory Compliance

Organisations today are being asked by more entities to comply with more regulations covering more aspects of the organisation. Many of these regulations are based around the protection of the organisation's information assets. Protecting these assets and demonstrating how that protection forms part of the Enterprise Strategy will be at the core of any compliance program.

By including the Principles of Information Security described in this document into the Enterprise Architecture, the organisation positions itself to use best practice principles and procedures to satisfy the spirit of almost any regulatory framework for information security. Using International standards frameworks (such as *ISO 27001*) as the basis for the development of an information security governance program will provide the foundation for building a robust response to regulatory requirements.

Principles of Information Security

The principles provide key requirements to be considered in order to ensure information security considerations are addressed within the organisation and in the context of Enterprise Architecture. Listed under each principle are recommendations which suggest actionable items where the principles can be applied to the organisation.

Figure 3 below demonstrates the relationship between the components that form the basis of a successful enterprise strategy. The principles are in the outer ring while the enterprise architecture components are in the inner ring.

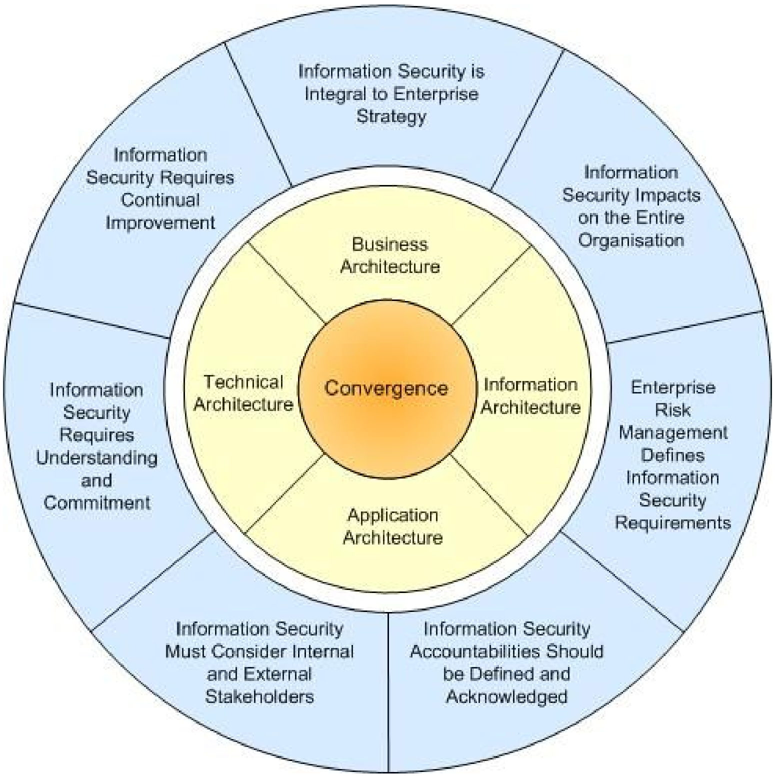
Information Security is Integral to Enterprise Strategy
Information Security Impacts on the Entire Organisation
Enterprise Risk Management Defines Information Security Requirements
Information Security Accountabilities Should be Defined and Acknowledged
Information Security Must Consider Internal and External Stakeholders
Information Security Requires Understanding and Commitment
Information Security Requires Continual Improvement
Business Architecture
Information Architecture
Application Architecture
Technical Architecture
Convergence

Figure 3—Relationship between Principles of Information Security, Enterprise Architecture and Convergence

1. Information Security Is Integral to Enterprise Strategy

Information security is a key support to the business objectives of enterprise strategy by both minimising risk and enabling trust to be maintained in new generations of services. Given this, information security must have the endorsement and support of executive management and the Board.

Recommendations

- Develop information security strategy consistent with the business goals and overall responsibilities of the organisation, with Board-level approval.
- Ensure consistency of information security planning with strategic and operational planning.
- Executive management should demonstrate support for enterprise information security at all levels of the organisation.
- Ensure information security complies with legal and regulatory requirements.

2. Information Security Impacts on the Entire Organisation

A holistic approach to implementing enterprise information security is likely to be the most cost-effective. This involves considering people, technology and processes throughout all areas of the business. To maximise return on security investment, information security must be designed into information systems and processes from the outset.

Recommendations

- Include representatives of all areas of the organisation in information security decision-making.
- Implement enterprise processes that support practical and timely solutions for information security.
- Consider physical security aspects of information protection within information security.
- Engage the human resources department to ensure people are managed as a component of information security within the organisation.
- Embed information security within the lifecycle of enterprise information systems.
- Implement security based on transparent, trusted and proven solutions.

3. Enterprise Risk Management Defines Information Security Requirements

A fundamental requirement of all business operations is the management of risk. As one component of this, organisations need to assess, protect against and report on information security risk. The proposed treatment of risk—via introduction of information security requirements—must be proportional to its business impact and prioritised accordingly.

Recommendations

- Conduct information security risk assessments in line with the enterprise risk assessment methodology.
- Prioritise the treatment of risks and ensure the treatment is proportionate to the business impact.

4. Information Security Accountabilities Should Be Defined and Acknowledged

Organisations should develop and formally enforce information security responsibilities within the enterprise. These responsibilities exist internally and also extend across organisational boundaries to outsourcers, business and service partners or customers. All users of information systems should be informed of the consequences of their actions.

Recommendations

- Advise executive management where accountabilities should be placed for the state of enterprise information security.
- Assign information security responsibilities throughout the organisation.
- Allocate responsibility for information security to match business roles.
- Define information security responsibilities for external parties in the engagement contract.

5. Information Security Must Consider Internal and External Stakeholders

As the interconnectedness of systems grows, the importance of the security of each node is increased. The legitimate interest of stakeholders—including customers, suppliers and other business partners—should be considered in information security decision-making. Owners and operators of critical infrastructure have a responsibility to meet the security expectations of the community at large.

Recommendations

- Implement information security controls to support service continuity.
- Ensure sensitive customer and community data is protected appropriately.
- Assess the security of all organisations involved in the business value chain.
- Consider employee interests in the design of security systems.

6. Information Security Requires Understanding and Commitment

An understanding of information security threats is critical to the ability of an organisation to manage risks. A raised level of awareness and understanding within the organisation supports the development of a culture of security and can reduce the frequency and impact of information security incidents. An appropriate level of awareness of security is required for all staff. A deeper understanding is required for staff with key roles in information security.

Recommendations

- Develop and maintain the information security policy to be practical and current.
- Establish employee and contractor education and awareness programs relevant to the organisation and individual roles.
- Incorporate information security into existing communications processes.
- Participate in informal and formalised information sharing networks in information security.

7. Information Security Requires Continual Improvement

As an organisation’s risk exposure is dynamic, information security review and improvement must be a part of ‘business as usual’. Ongoing improvement due to the changing business environment allows the organisation to sustain the state of information security at a level which is acceptable to internal and external stakeholders and maintains the organisation's risk at an appropriate level.

Recommendations

- Ensure information security expertise and experience are available to meet the organisation’s needs.
- Review information security controls against national and international standards.
- Implement systems and processes to identify and respond to malicious or unintended information security breaches.
- Develop a feedback process to incorporate incident details into risk assessments and control selection as part of the systems lifecycle.
- Include security as a selection criterion for assessing new technologies and applications for the organisation.

Questions for the Enterprise

An enterprise strategy for information security requires the involvement and commitment of all components of the organisation. It cannot be handled by the IT department or the CIO or even the Chief Security Officer alone. However, the CIO drives the rest of the organisation to achieve the secure management of information.

Questions to ask the CEO and Board of Directors

Does the organisation have a Board-level position statement for information security such that legal and regulatory requirements are met?

There must be a leader if people are to follow. The CEO and Board of Directors should adopt a leadership role in ensuring that information security is given appropriate profile.

Are adequate resources allocated to build an appropriate security infrastructure?

Information security will require effort and expense. This will be related to the risks and strategies that the organisation has identified. Resource allocation commensurate with the assessed organisational exposure will be required.

Is the Board committed to allocating information security responsibilities and accountabilities at every level of the enterprise without exceptions?

Responsibility for managing and enforcing the policies, procedures and strategies established by the enterprise to protect its information assets is a key requirement. This must be demonstrated by the full commitment of everyone from the top down.

Questions to ask organisational units

Do the enterprise organisational entities understand the value of their information assets?

The first step in ensuring that everyone understands the importance of information security is to understand the value of critical information which impacts on business processes, service delivery, business continuity, reputation and regulatory compliance.

Do managers engage their staff in information security?

Leadership in managing information security and reporting of suspected breaches must come from the top and business managers must ensure their staff have an appropriate understanding of the importance of information security. Staff education is a significant way to ensure an ongoing adherence to a successful information security program. Appropriate staff education must be encouraged.

Do organisational entities recognise that information security management systems can help with their regulatory compliance requirements?

Developing and implementing a well-designed information security management system will often ensure that regulatory requirements around 'IT control' are readily met.

How does the organisation treat information security in its risk assessment processes?

Risk assessment activities in the enterprise must consider all threats to a project, process or product. Information security threats and vulnerabilities should always be considered given the reliance on electronic processing of information today.

Is information security part of everyone's key performance indicators?

Recognition of the importance of information security will be easily seen if it is part of the staff measurement process. Inclusion as part of both managers' and employees' Key Performance Indicators (KPIs) will ensure that the issue of information security remains a motivator for action.

Do organisational units engage business partners, suppliers and customers in discussions about information security?

As business systems become more interconnected, the security of trading partners becomes even more important. Discussions around information security should be held at all levels of the relationship starting with business level partners.

Do organisational units strive for continual improvement in their information security strategies?

Too often, managers believe that once security technologies such as anti-virus software or firewalls are in place, security is complete. Understanding that information security is a continuous improvement process—which must be budgeted accordingly—is essential to ensuring evolving threats continue to be addressed. Information security may also be part of contractual undertakings (e.g. outsourcing arrangements) that exist both internally and externally to the organisation. Stakeholder involvement in information security should not be overlooked.

Questions to ask the Human Resources Department

Is information security considered when hiring people for sensitive positions?

As information is the key asset of any enterprise, all staff who handle it or have access to it must be of the highest level of trust. The human resources department must consider this in their hiring practices.

Is information security education part of staff induction and training processes?

All staff should receive training in the enterprise's information security practices when they join. The appropriateness of who will deliver this training needs to be determined. However, the more senior the better to address Principle 1.

Is information security included as a topic in regular staff education?

Given the rate of change of security threats and controls, refresher education in information security should be regularly attended by all employees.

Do existing HR information and educational resources contribute to keeping information security training relevant to organisational strategies?

A five-year-old information security training course or induction process will be almost useless in today's environment; it must be regularly maintained.

Does HR ensure that information security is part of everyone's job description?

Information security is part of everyone's job. This is a key message.

Questions for the CIO and CSO to ask themselves

Is information security considered at every stage of every project?

Information security must not be an afterthought. The cost of security is minimised and the value maximised by including it early and throughout the project lifecycle.

Are all IT staff fully aware of aspects of information security that may affect their activities?

Awareness of current issues is key to ensuring that the organisation's information assets remain secure. Regular security reviews will help to keep staff aware of current trends.

Is the IT department a leader and facilitator of information security strategies in the organisation?

Although information security is an organisation-wide issue, it is common for the organisation to look to the IT department to take the lead.

Does the CIO help all senior executive staff understand the importance of information security?

As the owner of information security in the enterprise, it is up to the CIO to maintain visibility of the issue with other senior executive staff and ensure their understanding and commitment is in place.

Can the CIO state that the organisation's information security strategies are built on the seven principles for information security?

Information security starts with the leadership of the information technology group. They must be first to build the seven principles outlined above into their operations.

Conclusion

The increasing complexity of enterprise information systems can be effectively addressed by a comprehensive information security governance framework. While it is the role of the CIO to protect the organisation's information assets in this complex environment, it is not something that can be done alone. Engaging the entire enterprise in the protection of the assets is a core component of an enterprise strategy for information security. Establishing a strategy with the principles presented in this document at its core will help to ensure the adequate protection of these enterprise information assets.

Detailed Versions of this Paper

This paper is one of three titled ‘Secure Your Information’, each with a slightly different focus. The three reports are:

- Secure Your Information—Advice for CIOs and CSOs [This paper];
- Secure Your Information—Advice for CEOs and Boards of Directors; and
- Secure Your Information—Full report.

These papers are also complemented by another ITSEAG paper, ‘CIO, CISO and Practitioner Guidance: IT Security and Governance’, which highlights the importance of an appropriate governance framework for the management of corporate information networks and IT security. The techniques and frameworks discussed in the Governance Practitioner Guidance paper provide a valuable mechanism for ensuring the effective adoption of the Information Security principles outlined in ‘Secure Your Information’.

The Trusted Information Sharing Network

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

- Managing IT Security When Outsourcing to an IT Service Provider—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;
- Denial of Service/ Distributed Denial of Service—Advice for CEOs
- Denial of Service/ Distributed Denial of Service—Advice for CIOs
- Denial of Service/ Distributed Denial of Service—Report
- 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
- Wireless Security—Overview for CEOs
- Wireless Security—Overview for CIOs

[i] The ITSEAG is one of three Expert Advisory Groups established within the Trusted Sharing Information Network for Critical Infrastructure Protection. The ITSEAG provides advice to the Critical Infrastructure Advisory Council (CIAC) and the sector based Information Assurance Advisory Groups on IT security issues as they relate to critical infrastructure protection. The ITSEAG membership consists of academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security fields.

[ii] TISN 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, three Expert Advisory Groups, and the Critical Infrastructure Advisory Council (CIAC—the peak body of TISN that oversees the IAAGs and EAGs). More on TISN can be sought from www.tisn.gov.au or by contacting cip@ag.gov.au.