Trusted Information Sharing Network
for Critical Infrastructure Protection

Secure Your Information: Secure Your Business

Advice for CEOs and Boards of Directors

June 2007

CEOs and Boards of Directors are ultimately responsible for protecting enterprise information (both physical and electronic) from unauthorised access or damage—whether malicious or accidental. The security of information is vital for an organisation, operationally, legally and financially.

Failure to fully understand these requirements can have serious consequences for the business, its owners and managers. These consequences may include:

- Significant financial loss;
- Prosecution and resulting damages;
- Long term reduction in revenue and profit as a direct result of damage to reputation; and
- Personal liability for directors and senior managers.

Securing your information is essential to securing your business.

The following paragraphs outline seven basic principle of information security developed by the IT Security Expert Advisory Group (ITSEAG)[1] for the Trusted Information Sharing Network (TISN)[2]. The Expert Advisory Group recommends these be adopted by all organisations, particularly those operating critical infrastructure. To assist CEOs and Boards identify if their organisation has adopted these principles, the Expert Advisory Group has developed the following questions to put to senior management.

Questions To Ask Your Chief Information Officer (CIO) and Chief Security Officer (CSO)

1. Are legal and regulatory requirements being met by the organisation's approach to information security?
2. Do we have an integrated approach to information security across the organisation that reflects the challenges of the current security environment?
3. Do you believe your Senior Managers and the Board are sufficiently engaged and that they have endorsed appropriate strategies for information security?
4. Does the organisation have arrangements in place which adequately address the security and privacy of employee, customer, supplier and other stakeholder information?

---

[1] 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.

[2] 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.

5. Are managers and users of information systems in the organisation accountable for their actions? What measures are in place to ensure they understand their accountability for the security of information?
6. What resources are being allocated to ensure everyone in the organisation is adequately informed and aware of the importance of information security? Is appropriate training available?
7. How is information security being continuously improved in the organisation to respond to this changing environment?

Regulatory Compliance through Information Security

CEOs and Boards need to be aware that information security must be an integral part of the overall design of the organisation, in other words, its enterprise architecture. Adherence to a set of information security principles when designing or reviewing the enterprise architecture will greatly enhance the effectiveness of security as the organisation changes. Fostering a 'culture of security' within the organisation will also greatly assist in ensuring that risks are addressed at the appropriate level.

This paper defines Seven Basic Principles of Information Security that must underpin the enterprise's strategy for protecting and securing its information assets—and achieving regulatory compliance:

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 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. If the information security aspects of convergence are not adequately addressed, the organisation could be exposed to serious risk.

Figure 1— Convergence of Enterprise Architecture

Critical business information now resides 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. To manage the secure evolution of this perimeter, the adoption of an enterprise wide, strategic approach to information security is critical.

Security Principles to Secure Your Information

The ITSEAG for the TISN has developed a resource entitled 'Secure Your Information' which includes:

- Seven key information security principles (blue outer ring) for developing an enterprise strategy for information security;
- Advice on how to link these seven key information security principles to your enterprise architecture (yellow inner ring);
- Recommendations for integrating information security principles throughout the organisation; and
- A self-assessment Checklist for validating an enterprise strategy for information security.

The seven principles above provide direction for the development of a strategic approach to integrating information security into the enterprise.

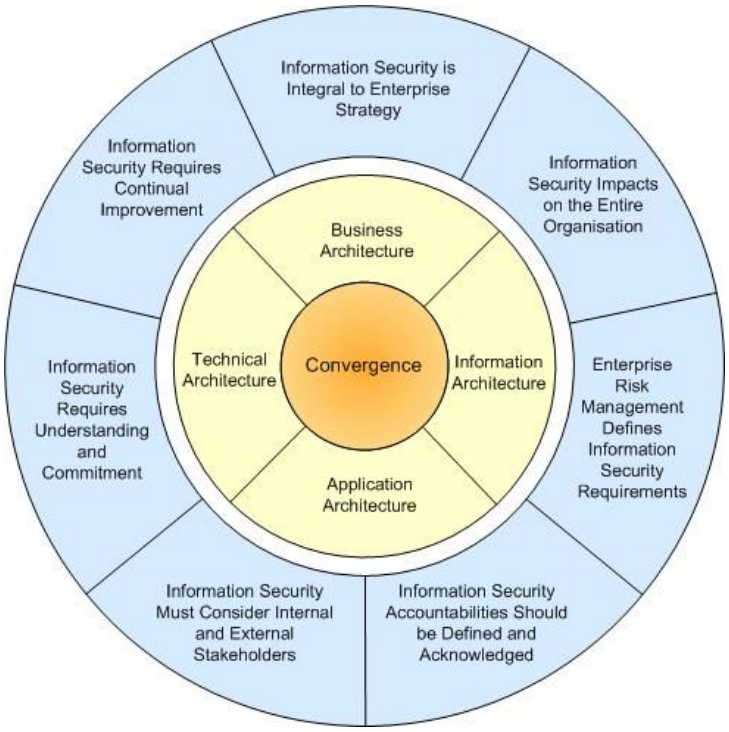

Figure 2—Relationship between Principles of Information Security, Enterprise Architecture and Convergence

Detailed Versions of this Paper

This paper is complemented by the following more detailed papers:

- Secure Your Information—Advice for CIOs and CSOs; and
- Secure Your Information—Full Report.

These papers are also complemented by another ITSEAG paper, 'IT Security and Governance for Boards of Directors and CEOs' (available at *www.tisn.gov.au*), which highlights how a successful governance structure defines key security principles, accountabilities and actions which an organisation must follow to ensure their objectives are achieved. The techniques and frameworks discussed in the Governance paper provide a valuable mechanism for ensuring the effective adoption of the information security principles outlined in 'Secure Your Information'.

Further IT Security Advice for CEOs

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

- Managing IT Security When Outsourcing to an IT Service Provider: Advice for CEOs;
- Denial of Service/ Distributed Denial of Service—Advice for CEOs;
- SCADA and Industrial Control Systems;
- Security of Voice Over Internet Protocol—Advice for CEOs; and
- Wireless Security—Overview for CEOs.