



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

**IT Security and Governance for  
Board of Directors and CEO**

**June 2006**  
(Revision 1, August 2007)



Trusted Information  
Sharing Network  
for Critical Infrastructure Protection

This paper provides guidance for CEOs, Board Members and senior executives on how to build IT security into overall security planning and corporate governance arrangements. It provides practical tips for achieving improvements in IT security and governance at the enterprise level.

Corporate computer networks are being threatened by a more sophisticated range of IT security threats and vulnerabilities. It is important to understand the implications of these threats in terms of the potential liabilities for your organisation when planning, implementing or reviewing your overall security governance.

The vulnerabilities stem from an increasing dependence on information technology and Internet-based applications and the emergence of new and converging technologies such as Wireless and Voice over the Internet Protocol (VoIP). The main areas of potential liability for your organisation as a result of ineffective security include negligence, vicarious liability for employees and Privacy and Corporations Act obligations.

***“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.”***

In this environment, your IT, communications and physical security planning should be fully integrated as part of your overall security strategy—encompassing IT, communications and physical and personal security measures. High level, top down, executive support is crucial if organisations are to attain sound IT security governance.

***This paper summarises these issues and provides a series of questions to pose to your Chief Information officer (CIO) and Chief Information Security Officer (CISO).***

The paper was developed by the Information Technology Security Expert Advisory Group (ITSEAG)<sup>1</sup>. A more detailed paper for CIOs and CISOs has also been developed<sup>2</sup>. These papers are drawn from a report undertaken by KPMG<sup>3</sup>.

---

<sup>1</sup> The ITSEAG is one of several 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 (IAAGs) 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. The ITSEAG Secretariat can be contacted on 02 6271 1595.

<sup>2</sup> TISN CIO, CSIO and Practitioner Guidance for IT Security Governance, June 2006 or TISN Leading Practices or Guidelines for IT Security Governance for CSOs and CSIOs, June 2006.

<sup>3</sup> TISN Report - Leading Practices and Guidelines for IT Enterprise Security Governance, June 2006.



Trusted Information  
Sharing Network  
for Critical Infrastructure Protection

### ***Current threats and drivers***

Losses from cybercrime increased significantly in 2005–06<sup>4</sup>. The greatest areas of threat for owners and operators of critical infrastructure are:

- **human error**—lack of accountability or a failure to act;
- **system failure**—legacy systems and inadequate security measures; and
- **malicious software**—viruses/worms/spyware and network based attacks for mischief or financial gain.

#### **CASE STUDY CardSystems (US Company)**

2005

A security vulnerability allowed an intruder to infiltrate the network and gain access to cardholder data compromising more than 40 million credit cards worldwide.

The intrusion illustrated the ineffectiveness of 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 no ongoing monitoring and management which inevitably lead to the breach.

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

### ***Why is security important?***

#### **Standards and legislation**

The Corporations Act 2001 imposes legal responsibilities upon company directors, secretaries and other “officers” to uphold due care and diligence.

The Privacy Act 1988 also imposes obligations on certain companies on the collection, retention, use and disclosure of personal information. This requires companies covered by the Act to implement appropriate physical and information security systems to ensure the 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 financially liable to the

<sup>4</sup> AusCERT 2006, Computer Crime and Security Survey, (ISBN: 1-86499-849-0)



Trusted Information  
Sharing Network  
for Critical Infrastructure Protection

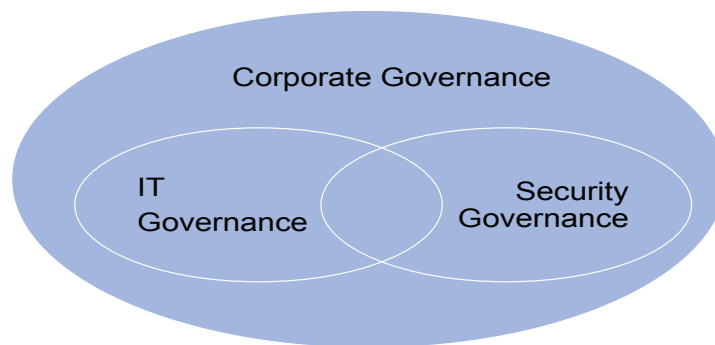
other party. However, if reasonable security governance measures are in place, including awareness and accountability, negligence may be avoided.

#### **TIP #1**

*Be aware and fully up to date on what is happening in your organisation to protect information systems*

### ***What is security governance?***

IT and security governance contain a number of overlapping attributes; enmeshing these aspects in mainstream corporate governance is a sound business decision.



*Figure 1: Corporate, IT and security governance relationships*

### ***What is a good framework?***

Good security governance framework specifically assigns responsibility for IT security governance within the overall corporate governance platform. This is best achieved by a top-down approach aligned with the following:

- 1 **Core principles**—core security principles serve as the primary driver for all security governance functions and activities.
- 2 **Roles & responsibilities**—an organisation must define roles and responsibilities for security and governance.
- 3 **Activities**—activities are the underlying processes that are owned and operated by accountable individuals to implement and maintain security governance capabilities.

#### **TIP #2**

*CEOs should have an annual overall security evaluation conducted, review the evaluation results with staff, and report on performance to relevant stakeholders (including the Board)*



### ***How should CEOs and Board Members respond?***

CEOs and Board Members have a responsibility to the organisation's stakeholders to understand and uphold the implementation of security governance across the organisation. An effective security governance framework includes well defined roles and responsibilities to ensure accountability for success.

#### **TIP #3**

*Assign responsibility for IT security governance within your overall security governance framework*

### ***What questions can you ask?***

Security is an activity in itself that should be integrated into an organisation's core functions and processes. To ensure the implementation of a sound security governance framework **Board Members and CEOs should seek answers from CIO/CISO to the following questions:**

- Is there appropriate 'top down' management for effective development and implementation of governance and IT security frameworks?
- Do our overall IT security frameworks and practices provide for an integrated and holistic approach to managing our exposure to communications, IT and physical security risks?
- Do our corporate governance practices take into account how security and IT security governance issues overlap, providing effective mechanisms for identifying, monitoring and managing cyber and other security risks?
- What procedures and strategies have been implemented to identify, monitor and manage cyber risks in the IT infrastructure which supports our business processes?
- Have our staff been adequately informed of their responsibilities under our IT and governance security policies and procedures and do we have enterprise-wide processes for review and enforcement?
- Are our business processes including supply chains, stakeholder and outsourcing, off-shoring and tele-working arrangements that are supported by our IT networks adequately protected?
- Do our IT security governance arrangements and practices align with regulatory compliance and appropriate Australian and international standards for all our business processes?
- Do we regularly review our exposure to the internet and new IT technologies to ensure that corporate and IT security governance practices have not been breached?
- How often does our organisation undertake vulnerability assessments of key business processes and supporting IT infrastructure<sup>5</sup>?

---

<sup>5</sup> Grant assistance may be available to owners and operators of critical infrastructure under the Computer Network Vulnerability Assessment (CNVA) program. Further information on the CNVA grants program is available from [www.tisn.gov.au](http://www.tisn.gov.au)



Trusted Information  
Sharing Network  
for Critical Infrastructure Protection

### **CASE STUDY: ChoicePoint—2005**

---

US company ChoicePoint exposed its customers to fraud by selling personal information to organisations with criminal intentions.

The company did not act out of sense or ethical obligation to notify customers of the breach.

There was no due diligence being performed over new customers who were being given access to sensitive information.

Consequences:

- 160,00 customer records were compromised;
- The U.S. Federal Trade Commission imposed a US\$10 million civil penalty;
- ChoicePoint has been forced to set up a US\$5 million trust fund for individuals who might have become victims of identity theft; and
- They will have to submit a comprehensive security audit every two years for the next 20 years.



Trusted Information  
Sharing Network  
for Critical Infrastructure Protection

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

### ***Reports***

- Secure Your Information: Information Security Principles for Enterprise Architecture
- Managing IT Security When Outsourcing to an IT Service Provider, Guide for Owners and Operators of Critical Infrastructure
- 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***

- Secure Your Information: Secure Your Business – Advice for CEOs and Boards of Directors
- 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
- 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***

- Secure Your Information: Information Security Principles for Enterprise Architecture – Advice for CIOs and CSOs
- 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



Trusted Information  
Sharing Network  
for Critical Infrastructure Protection

---