Trusted Information Sharing Network
for Critical Infrastructure Protection

DEFENCE IN DEPTH—OVERVIEW FOR CEOS

CEOs and Boards of Directors are ultimately responsible for protecting enterprise information from malicious and accidental damage and unauthorised access. Maintaining security requires continued vigilance as an attacker only needs to find one flaw in your security—whereas you need to protect against them all.

This responsibility arises in many cases from specific regulatory regimes including:

- corporate governance regulation—the Corporate Law Economic Reform Program (Audit Reform and Corporate Disclosure) Act 2004 (Australia) and Sarbanes-Oxley (United States).
- the Australian Privacy Act, including proposed 'Data Breach Disclosure' amendments increasing the likelihood of significant brand damage from a loss of data.
- the Payment Card Industry Data Security Standard (PCI DSS).

Also, if your organisation maintains connections to unsecure systems and networks (such as the internet), 'due care' requires that controls are established to minimise the risk of:

- significant financial loss from either direct theft of funds or information, or through the application of fines associated with regulatory non-compliance.
- significant brand damage and associated loss in consumer confidence in your company.
- directors' liability in the event of insufficient care being taken.

This overview has been developed to support a 'defence in depth' approach to critical infrastructure and organisation protection, addressing risk factors such as:

What is defence in depth?

Threats to an organisation's information resources can arise through its people, trading partners, external sources, and technological innovation. Examples of threats to the confidentiality, integrity and availability of your information include:

People	Trading partners
• Disaffected employees • Financially troubled employees • Politically motivated employees • Corporate espionage	• Partners with poor data security • Physical access to shared systems • Misunderstanding of allowed access • Competitive environment
External threats	**Technological improvements**
• Hackers • Organised crime • Politically motivated activists	• Faster networks • More storage in smaller devices • Technological convergence • Working any time, any where

No single strategy or technology (such as a firewall) will ever protect against all these threats. Defence in depth involves the application of people, process and technology controls, in a holistic risk-management approach to ensure that all threats are covered.

Defence in depth is far more than an IT concept as it delivers:

- effective risk-based decisions
- reduced overall cost and risk, along with improved information security
- enhanced operational effectiveness and efficiency
- protection of system and operational availability.

How do we implement defence in depth?

Implementing defence in depth requires co-ordinating knowledge of:

- enterprise strategy—including the organisation's overarching goals
- the internal environment—including information assets, systems and personnel
- the threat environment—both internal and external.

What do I need to ask my CIO?

A defence in depth initiative will generally be driven by the CIO and will impact on people, policies and procedures, processes and technology. The following is a suggested list of issues to discuss with your CIO in reviewing the organisation's Defence in Depth strategy.

Governance
• Does a process exist for revisiting the organisation's information and system controls based on changes to the external threat environment? • Are controls implemented in alignment with the cost of risk? • Does the organisation understand the avenues through which key systems and information could be compromised?

People
• Are roles and responsibilities for information security formally assigned? • Are staff aware of information security requirements? • Is the security of third parties with access to sensitive systems or information comprehensively assessed?
Operations
• Has an assessment of security process effectiveness been completed? • Are incident identification and response procedures established and tested? • Have partner systems been reviewed or evaluated?
Technology
• Are layered technical controls in place to ensure that no single control failure will result in an information or system compromise? • What controls are in place to detect attacks against key systems? • Does the organisation have a process for identifying new technical threats?

This information has been developed by the IT Security Expert Advisory Group which is part of the Trusted Information Sharing Network (TISN) for critical infrastructure protection. More information on TISN can be sought from www.tisn.gov.au or by contacting cip@ag.gov.au.