Defence in depth
Summary Report for CIOs and CSOs

June 2008

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. This information is not legal advice and should not be relied upon as legal advice.
Introduction

In today’s business environment, controlling access to information is critical to long-term competitive advantage. Alongside significant benefits, every new technology introduces new challenges for the protection of this information. As a result, it is vital for owners and operators of critical infrastructure to develop appropriate strategies for mapping and understanding the layers of information that need to be protected.

Responsibility for protecting the organisation’s information assets is at the core of the role of the Chief Information Officer (CIO).

This report has been developed by the IT Security Expert Advisory Group (ITSEAG) which is part of the Trusted Information Sharing Network (TISN) \(^1\) for critical infrastructure protection.

**Defence in Depth** is the systematic security management of people, processes and technologies, in a holistic risk-management approach. The concept is based on military strategy which implements defences primarily to delay rather than prevent the advance of an attacker. It is assumed that an attack will lose momentum over time, allowing for those being attacked to respond appropriately.

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

- Effective risk-based decisions.
- Enhanced operational effectiveness.
- Reduced overall cost and risk and improved information security.

Defence in Depth provides an approach to security that is integrated with the organisation’s business processes and enterprise-wide risk-management capability.

The determination of system priorities is paramount to achieving Defence in Depth. A Defence in Depth strategy requires first the in depth understanding of system criticality to business operations.

This document, along with the CEO guide and the full *Defence in Depth* report, provide guidance on how to effectively layer and integrate security controls in an organisation:

- **The full report** establishes the Defence in Depth lifecycle, providing information on key steps to implement Defence in Depth controls, and monitor and review performance.
- **The CEO paper** is an outline designed to provide senior executive guidance on the benefits of Defence in Depth.

---

\(^1\) TISN enables the owners and operators of critical infrastructure to share information on important issues. It is made up of nine 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 TISN and oversees the IAAGs and the EAGs). More information on TISN can be sought from [http://www.tisn.gov.au](http://www.tisn.gov.au) or by contacting [cip@ag.gov.au](mailto:cip@ag.gov.au). The ITSEAG is one of the expert advisory groups within the TISN framework. The ITSEAG provides advice to the CIAC and the sector-based IAAGs on IT security issues as they relate to critical infrastructure protection. It 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 Secretariat can be contacted on (02) 6271 7018.
This CIO paper is a summary which considers the requirements for effectively deploying Defence in Depth and its role in modern risk management and information security.

The Need for Defence in Depth

A Defence in Depth strategy has become increasingly important as a result of overall business and IT trends which may weaken an organisation’s control of information assets, including:

- **Break down of the perimeter** – the trend towards organisations having a hard-to-define external boundary, resulting from the creation of close relationships with customers, business partners and suppliers.
- **Mobile workforce** – employees increasingly are required to work in non-conventional environments with flexible arrangements and requiring flexible access to information and systems.
- **Decentralisation of services** – the provision of services and systems that were previously available only to a tightly controlled internal group of users, to a broader set of users via the internet and extranets.
- **Increasing value of information** – the perceived value of information in building a sustainable competitive advantage has rapidly increased.

Figure 1 outlines the principles involved in Defence in Depth methodologies.

![Figure 1: People, process, technology & governance](image)

People
- Security roles & responsibilities for internal and external persons

Process
- Standardised actions which are used to ensure security posture is sustained

Technology
- Solutions employed which enable the achievement of business objectives

Governance
- Management framework providing oversight and coordination of people, process and technology

---


The Defence in Depth Lifecycle

The report is divided into four (4) main sections, following a lifecycle model for strategic implementation (see Figure 2). The phases of the Defence in Depth lifecycle are:

- **Establishing context** – ensuring that the organisation clearly understands its enterprise strategy, internal environment, assets and systems, and threat environment.
- **Risk analysis** – ensuring that all threat vectors are considered and understood throughout the organisation (e.g., including supply chain and customer connectivity and vulnerabilities).
- **Implement Defence in Depth** – ensuring that controls are integrated with business processes and are consistent with the organisation’s enterprise risk-management process.
- **Monitor and review** – adapting to environmental changes including changes to mission/business objectives, the regulatory environment and the threat environment.

### Control Domains

A fundamental principle in Defence in Depth is the balanced and integrated approach to people, process (operations) and technology controls. An overall element of governance

---

Defence in Depth – Advice for CIOs and CSOs

Responsibility is required to manage this coordinated effort. These elements are described in detail as follows:

- **Governance** – the governance element of Defence in Depth refers to the overall management framework used to provide oversight and coordination of people, process and technology elements.

- **People** – the people component of Defence in Depth describes the definition, maintenance and enforcement of security roles and responsibilities for employees, contractors, outsourcing providers, and vendors.

- **Process** – the process component of Defence in Depth describes the definition, maintenance and enforcement of standardised actions which are used to develop and ensure security posture is sustained on a day-to-day basis.

- **Technology** – the technology component of Defence in Depth describes technology and product solutions which are employed to enable the achievement of business objectives in a sustainable manner.

**Implementing Defence in Depth**

The core principles of a Defence in Depth strategy are:

- Implement measures according to business risks.
- Use a layered approach such that the failure of a single control will not result in a full system compromise.
- Implement controls such that they serve to increase the cost of an attack.
- Implement personnel, procedural and technical controls.

Additionally, Defence in Depth requires that mechanisms be implemented to protect against attack and also to detect such attacks and provide an effective response.

In order to successfully implement Defence in Depth in an organisation, management must include these core principles within the organisation’s strategy, planning and structure. These core principles then correspond to design and implementation actions in the areas of governance, people, processes and technology.

In implementing Defence in Depth controls, specific attention is provided to key focus areas as follows:

**Governance**

- Risk management.
- Information security.
- Policy & compliance management.

**People**

- Personnel security (including user awareness).

**Process**

- User-access management.
- Identity management.
- Incident response management.
- Audit management.
Defence in Depth – Advice for CIOs and CSOs

Technology
- Communications management.
- Infrastructure management.
- Network architecture management.
- Application security.

Implemented in an integrated and balanced fashion, these control areas will ensure the core principles are effectively applied.

Layers of Control

In recent years it has become apparent that ‘perimeter security’ as a silver bullet solution is dead.

Given the emerging trends such as increased mobility and use of remote access, and increasing numbers of third parties accessing the organisation’s data and systems, the only effective mechanism for securing this information is via a layered Defence in Depth approach.

With an understanding of the organisation’s goals, the critical processes supporting these goals, and their inter-relationships, the control structure surrounding the processes can be assessed. Controls will generally include both technical and process. Figure 3 provides a graphical representation of the layers of control implemented around a business process or key piece of business information.

Using the model outlined in Figure 4, the individual protection layers – whether currently in place, or proposed for implementation – can be analysed for their combined effectiveness, and can be considered in the context of the threat environment.
# Maintaining Defence in Depth

The information security environment – both in terms of threats and controls – continues to change rapidly, requiring an ongoing assessment process to ensure the organisation maintains appropriate Defence in Depth. Issues requiring ongoing attention include:

- Security breaches.
- Weaknesses in existing controls.
- Changes in mission/business objectives.
- Changes in the security profile.

The assessment of these items can be supported through the following actions.

<table>
<thead>
<tr>
<th>Governance</th>
<th>People</th>
<th>Process</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Monitor environmental changes – including changes to regulation and public perception</td>
<td>- Allocate roles and responsibilities clearly – where possible, security responsibilities should be part of the job description</td>
<td>- Assess Defence in Depth effectiveness – using metrics where possible to allow for objective comparison</td>
<td>- Maintain awareness of new technologies and services – using a risk-based approach in the selection process</td>
</tr>
<tr>
<td>- Maintain understanding of internal environment – work habits, morale and contractual arrangements</td>
<td>- Conduct training and awareness sessions – both general and tailored to specific roles</td>
<td>- Develop incident response procedures</td>
<td>- Track technical threats – reviewing these threats in the context of the organisation’s environment and vulnerabilities</td>
</tr>
<tr>
<td>- Information sharing – with service providers, industry bodies and interest groups</td>
<td>- Ensure security of third parties – via training and audit of the outsourcers’ employees</td>
<td>- Standardise procedures to minimise uncontrolled changes – ensuring that all required stakeholders are satisfied with the change</td>
<td></td>
</tr>
<tr>
<td>- Define accountabilities – ensure ownership of information security responsibility</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Assess Defence in Depth performance – ensuring effectiveness over time</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Ensure currency of policies – maintain relevance to changing operational requirements and new technology</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Implement standards, procedures and guidelines – driving adoption through awareness, enforcement and providing users with practical examples and tools</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Questions to Ask

Does the board’s enterprise risk-management framework incorporate information security-related threats and events?

Defence in Depth requires a risk-management approach integrated with the business operations and consistent across the enterprise.

Are adequate resources allocated to appropriately deploy integrated Defence in Depth controls?

Both analysis and implementation phases of Defence in Depth will require effort and expense. This will be related to the risks and strategies that the organisation has identified. While long-term operational efficiencies may arise from an effective control structure, initially it will be necessary for resources to be allocated commensurate with the assessed organisational exposure.

Does the organisation implement security controls incorporating people, processes and technology?

Effective layering of controls requires not just technical controls but also policies, procedures, staff training and effective monitoring.

Do we understand our systems well enough to assess their exposure?

Defence in Depth requires a deep understanding of the organisation’s goals, information assets and systems, and the threats to these. This knowledge is required in order to assess and design appropriate layers of control.

Do our existing policies and processes provide for ongoing monitoring and review of performance?

Given the speed with which the business and threat environment is changing, it is crucial to ensure that the components of a Defence in Depth strategy – from risk assessments to specific controls – are subject to regular monitoring and review.

Can the CIO state that the organisation’s information security strategies are aligned with the core principles of effective Defence in Depth?

Information security starts with the leadership of the information technology group. Ensuring alignment with the Defence in Depth core principles will support investments in effective and relevant controls.

Conclusion

While new threats are arising constantly, the strategy of Defence in Depth has proved its value over hundreds of years. The use of the core principles described in this report, in conjunction with prudent risk management, will ensure an appropriate and effective information security profile is maintained.
Detailed Versions of this Paper

This paper is one of three titled *Defence in Depth*, each with a slightly different focus. The three reports are:

- Defence in Depth – Summary Report for CIOs and CSOs [This paper].
- Defence in Depth – Executive Brief for CEOs.
- Defence in Depth – Full Report.

The Trusted Information Sharing Network

Further information, reports and resources are available at the TISN website (www.tisn.gov.au). The Australian Government provides support to critical infrastructure organisations in maintaining a secure IT environment. Services and support available include:

- Computer Network Vulnerability Assessment (CNVA) Program
- Trusted Information Sharing Network (TISN)
- SCADA Community of Interest - Secretariat - scada@dbcde.gov.au