



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

Secure Your Information: Information Security Principles for Business Resilience

Summary Report for CIOs and CSOs

December 2009

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.

Executive Summary

Technologies such as cloud computing are continuing the erosion of organisational boundaries and are transforming existing business processes. At the same time, a rapid increase in the number of parties who are intent on compromising or destroying organisational information has driven a global increase in the cyber-threat level. This has served to emphasise the importance of securing an organisation's information against these threats.

Responsibility for protecting enterprise information assets is at the core of the role of the Chief Information Officer (CIO) and if the organisation has such a role, the Chief Security Officer (CSO). 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 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**
- 2. Information Security Impacts on the Entire Organisation**
- 3. Enterprise Risk Management Defines Information Security Requirements**
- 4. Information Security Accountabilities Should be Defined and Acknowledged**
- 5. Information Security Must Consider Internal and External Stakeholders**
- 6. Information Security Requires Understanding and Commitment**
- 7. Information Security Requires Continual Improvement**

Introduction

An increased cyber-threat level in 2010 and beyond means there is increased potential for disruptions to occur to the business processes of Australian organisations if their information systems are not appropriately secured. In response, the Australian Government has developed a cyber security strategy¹ which is designed to facilitate the existence of a secure and resilient electronic operating environment that supports national security and maximises the benefits of the digital economy.

This series of papers provides guidance to organisations on how to best secure and protect their information assets. 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

¹ Australian Government, *Cyber Security Strategy*, 2009, [http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/\(4CA02151F94FFB778ADAEC2E6EA8653D\)~AG+Cyber+Security+Strategy++for+website.pdf/\\$file/AG+Cyber+Security+Strategy++for+website.pdf](http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy++for+website.pdf/$file/AG+Cyber+Security+Strategy++for+website.pdf)

- 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 securing organisational information.
- This CIO paper which is an extended summary that supports the integration of the seven identified principles into the Enterprise Architecture.

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

Enterprise Architecture and Organisational Strategy

Technology has enabled the new “dynamic enterprise” to change the way business is conducted. 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.

Critical business information now exists extensively on mobile devices, virtualised systems and in cloud-based services: 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. The increased use of the Internet for services and connectivity presents risks to organisations that need to be carefully managed through the creation and implementation of appropriate policies, processes and technologies.

Information management is now a core business process as critical as cash flow management. Organisations need to carefully consider the required confidentiality, integrity & trustworthiness, and availability requirements of information they both produce and use.

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.

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

Perimeter Erosion Driving Security Architecture

The merging of elements and functionalities within Enterprise Architecture has resulted in a number of prominent architectural changes including:

- An increasing interconnectedness of organisations through shared networks;
- Deployment of service-oriented architectures (SOA);
- Simplification of applications through the use of ubiquitous web interfaces;
- The inclusion of security functionality in a broad array of IT devices through product function growth;

Secure Your Information – Advice for CIOs and CSOs

- Utilisation of shared application, storage and bandwidth resources through virtualisation, Software as a Service and “cloud computing” technologies;
- Integration of voice and data networks on single infrastructures; and
- Wide deployment of multifunctional wireless hand-held and network devices.

These changes have led to the breakdown of the organisation’s traditional security perimeter, as illustrated by the diverse array of external communications and data shown in Figure 2.

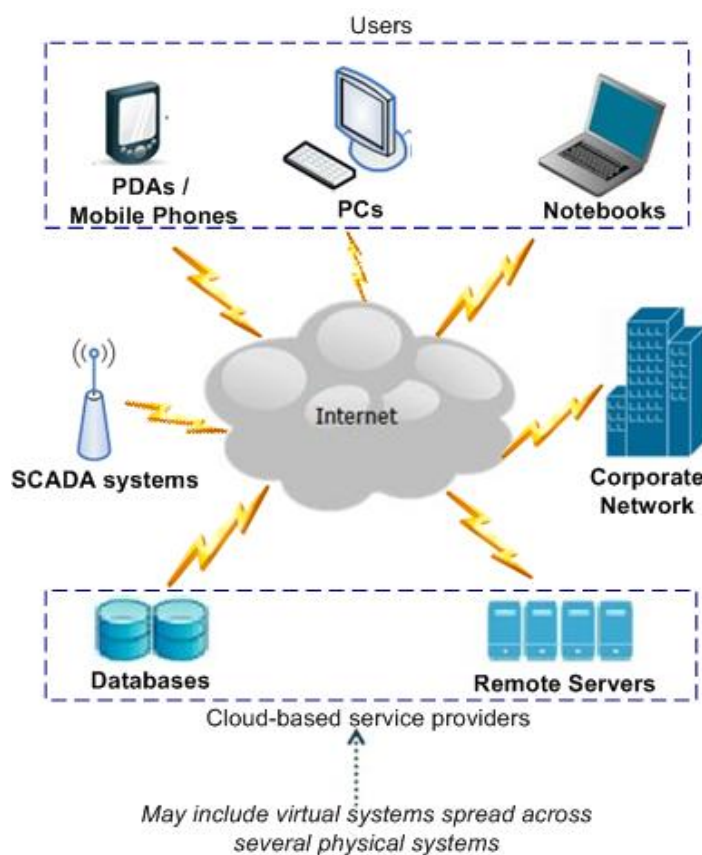


Figure 2—De-Perimeterisation of Enterprise Architecture

These architectural changes have afforded organisations 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;
- The combination of previously separate vulnerabilities and creation of new vulnerabilities through the convergence of specific technologies (e.g. computing and telephony);

- Increased confusion regarding responsibility and accountability for data protection, including legal jurisdictional ambiguities created by developments such as cloud computing;
- Incident detection and response in interconnected environments with many external parties; and
- An increased need to carefully manage situations where organisational information is held by external parties (for example, through conducting compliance audits, vetting personnel or demanding regular compliance reports).

In order to manage these security threats, risks and vulnerabilities, proactive management of information security is required. Of particular importance is the concept of enterprise-wide responsibility for security, which should be adopted as part of the ‘culture of security’ in the organisation.

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.

Regulatory Compliance an Increasing Consideration

Organisations today are being asked to comply with more regulations, covering more aspects of the organisation, than ever before. Many of these regulations are based around the protection of the organisation’s information assets, or information assets they hold on behalf of others in the course of their business. Protecting these assets and demonstrating how that protection forms part of the enterprise strategy is becoming a core component of any compliance program.

Ongoing reforms to legislation and regulation in the area of information security must be continually monitored by organisations to ensure that regulatory compliance is maintained. This may be industry-based (for example, the Australian Prudential Regulation Authority’s discussion paper on management of IT security risks²), data-type based (such as the Payment Card Industry Data Security Standard), or broad community wide legislation (such as the *Privacy Act 1988* (Cth)).

By including the Principles of Information Security described in this paper 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 further provide the foundation for building a robust response to regulatory requirements.

Principles of Information Security

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

² Australian Prudential Regulation Authority, *Management of IT Security Risk*, 2009, <http://www.apra.gov.au/Policy/IT-Security-Risk.cfm>

security governance contained within the TISN report on ‘Leading Practices and Guidelines for Enterprise Security Governance’³.

These principles are fundamentally not new, and are intended to be timeless. 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.

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.

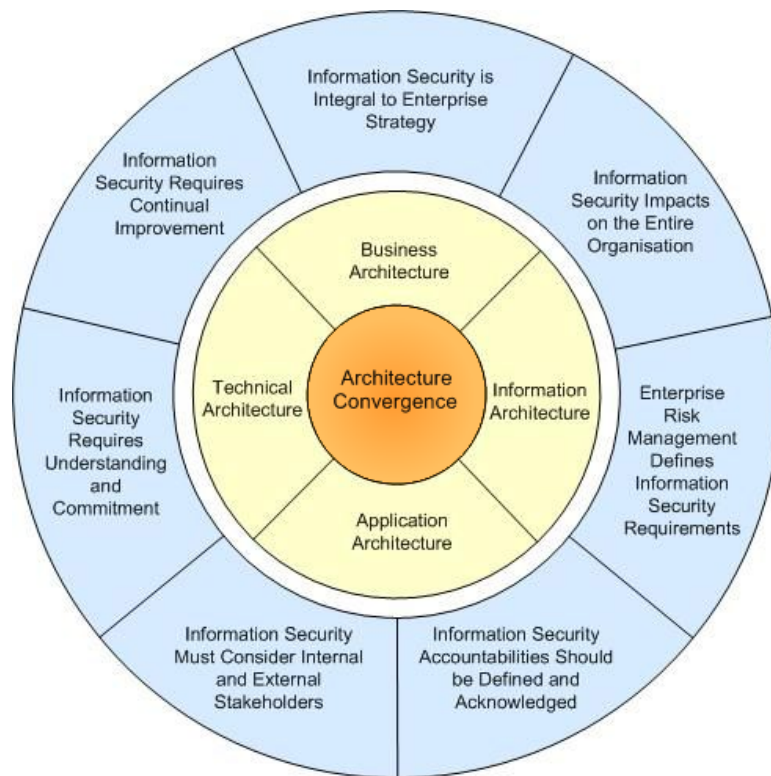


Figure 3—Relationship between Principles of Information Security, Enterprise Architecture and Convergence

³ ITSEAG (Trusted Information Sharing Network), *Leading Practices and Guidelines for IT Security Governance*, 2006,

[http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/\(427A90835BD17F8C477D6585272A27DB\)~LEADING_PRACTICES+AND+GUIDELINES+FOR+ENTERPRISE+SECURITY+GOVERNANCE.pdf/\\$file/LEADING_PRACTICES+AND+GUIDELINES+FOR+ENTERPRISE+SECURITY+GOVERNANCE.pdf](http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(427A90835BD17F8C477D6585272A27DB)~LEADING_PRACTICES+AND+GUIDELINES+FOR+ENTERPRISE+SECURITY+GOVERNANCE.pdf/$file/LEADING_PRACTICES+AND+GUIDELINES+FOR+ENTERPRISE+SECURITY+GOVERNANCE.pdf)

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 a ‘Defence in Depth’⁴ strategy using a layered approach.



Figure 4—Defence in Depth: A Layered Approach

⁴ For further information on the Defence in Depth strategy, see ITSEAG (Trusted Information Sharing Network), *Defence in Depth*, 2008, [http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/\(99292794923AE8E7CBABC6FB71541EE1\)~SIFTD-I-D+++Full+++15+Oct+2008+++1.pdf/\\$file/SIFTD-I-D+++Full+++15+Oct+2008+++1.pdf](http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(99292794923AE8E7CBABC6FB71541EE1)~SIFTD-I-D+++Full+++15+Oct+2008+++1.pdf/$file/SIFTD-I-D+++Full+++15+Oct+2008+++1.pdf)

- 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.
- Control access to organisational information by implementing a robust User-Access Management scheme⁵
- 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, including the establishment of monitoring and review processes to ensure those responsibilities are met.

⁵ For further information on User Access Management, see ITSEAG (Trusted Information Sharing Network), *User-Access Management: a Defence in Depth Control Analysis* 2008, [http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/\(99292794923AE8E7CBABC6FB71541EE1\)~SIFT-UAM-Full-Report+-+15+Oct+2008-2.pdf/\\$file/SIFT-UAM-Full-Report+-+15+Oct+2008-2.pdf](http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(99292794923AE8E7CBABC6FB71541EE1)~SIFT-UAM-Full-Report+-+15+Oct+2008-2.pdf/$file/SIFT-UAM-Full-Report+-+15+Oct+2008-2.pdf)

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 is 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.
- Monitor security advisories and alerts made available by key government organisations as well as software and hardware vendors, particularly in the area of patch management.
- Consider developments in security technology that could assist in managing information; for example, data security tagging.

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?

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.

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.

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.

Are business process changes assessed for information security impacts?

Many current business strategies such as outsourcing and off shoring, and IT initiatives such as virtualisation and software as a service, have significant information security implications and requirements. It is essential that business managers involved in reviewing such business process changes are aware of these potential impacts and involve the necessary experts to ensure risks are identified and effectively managed.

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 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.

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 both aware and trained in 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 training and 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.

Is information security effectively included in vendor selection?

With convergence bringing organisations ever closer together with their suppliers and business partners, it is critical that the security profile of these organisations is assessed and considered in vendor selection activities.

Do I provide enough information to the CEO, Board and my fellow senior executive staff to help them 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 staff and ensure their understanding and commitment is in place.

Conclusion

Developments in technology have facilitated an erosion of traditional enterprise perimeters. While this process has introduced several operational benefits, it has also added further complexity to the important task of developing an enterprise-wide strategy for securing information assets. This task has become increasingly important in the context of a growing cyber-threat level.

Focusing on the core principles of information security discussed in this paper will ensure that strategic approaches to securing information assets remain effective and viable irrespective of changes in technology and in the context of a continually evolving cyber-threat landscape.

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

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, the strategy of defence in depth, managing denial of service attacks, effectively implementing user access management, and the security implications of technologies such as global positioning systems, Voice over IP, mobile devices and wireless networking.

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:

- Trusted Information Sharing Network (TISN)
<http://www.tisn.gov.au/>
- SCADA Community of Interest
Secretariat - scada@dbcde.gov.au

CERT Australia

To enhance Australia's cyber security capability, the Australian Government announced in May 2009 that it would create CERT Australia, the new national computer emergency response team. CERT Australia will be managed by the Australian Government

CERT Australia will be a source of cyber security information for the Australian community and point of contact for Australia's international cyber security counterparts. It will also provide a trusted environment for information exchange between the Government and business on cyber security related issues.

CERT Australia will coordinate government and non-government cyber security efforts and have a coordination role in the event of a serious cyber event.

By facilitating the sharing of information between Australian Internet service providers (ISP), major corporations, anti-virus researchers and information technology security vendors, CERT Australia will provide the Australian community with relevant and timely information on cyber security issues.

CERT Australia will incorporate a number of cyber security activities currently undertaken by Australian Government agencies, including the Australian Government Computer Emergency Readiness Team (GovCERT.au). It will also complement the work undertaken by the Cyber Security Operations Centre (CSOC), recently established in the Defence Signals Directorate, and help inform the Australian Government about the national cyber threat picture.

Contact details:

Website: www.cert.gov.au

Secure Your Information – Advice for CIOs and CSOs

Email: info@cert.gov.au

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.

End of Document