



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

Achieving IT Resilience

Summary Report for CIOs and CSOs

May 2010

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

The level of dependence of organisations on IT infrastructure, both internally and externally managed, has reached a point where many businesses would suffer severe impacts to operational capacity and revenue generating capability if an extended outage of IT infrastructure was to occur as a result of a disruptive event. These impacts are also likely to extend to the community at large given the key role many organisations play in operating critical infrastructure.

Resilience addresses this by improving the robustness of both IT systems and organisational processes more generally. Resilience can be divided into three distinct areas:

1. **Preparation:** employing a strategic approach to resilience so as to prevent or reduce the impact of disruptive events on IT infrastructure.
2. **Endurance:** including the prompt detection of such events.
3. **Response & recovery:** with the aim of effectively handling disruptive events and returning to normal operations as soon as possible.

This paper describes a number of actions that organisations can take in order to achieve IT resilience based on these key areas. These actions have been formulated to assist owners and operators of critical infrastructure (such as those parts of the Infrastructure Assurance Advisory Groups formed by the Trusted Information Sharing Network) in developing a common approach to achieving resilience for the benefit of the Australian community.

INTRODUCTION TO RESILIENCE

There is a wide range of potentially disruptive events that have the ability to detrimentally affect the operation of IT infrastructure. This includes a broad range of possible threats, from malicious attacks on critical systems instigated by skilled hackers, deliberate or inadvertent acts by employees that compromise system operations, through to equipment failures and natural disasters such as fires or floods.

As a result, there is an increasing necessity for organisations to implement measures to increase the resilience of IT systems in order to improve their ability to effectively adapt to sudden changes in the operating environment. This will support continuity of business operations and minimise the potential detrimental impacts of system outages to the community as a whole.

The Australian Government has acknowledged this need in its 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.

While the concept of ‘resilience’ can be defined in a number of ways, this paper uses a definition involving three distinct elements, identified in Figure 1 below.

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)

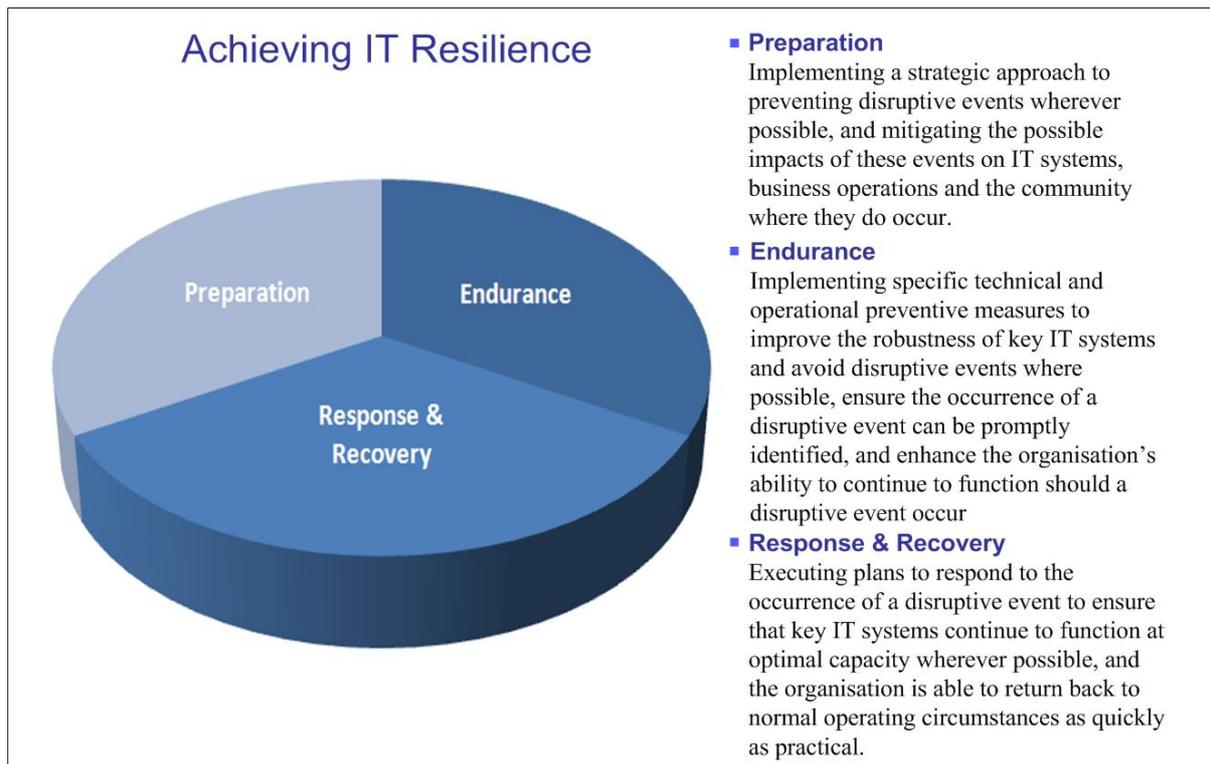


Figure 2 – Model for Achieving IT Resilience

This definition adapts and extends a number of previous definitions², and is designed to align with the specific aim of this paper to provide advice to organisations on achieving resilience of IT systems. The ensuing sections of this paper are structured in accordance with this definition, with specific actions that can be taken by organisations to achieve each component of resilience discussed.

Preparation and Endurance combine to establish practices that aim to *prevent* disruptive events wherever possible, and then to withstand such events when unavoidable. Response and Recovery is concerned with addressing situations where a disruptive event has, despite these efforts, taken place.

Ongoing reforms to legislation, relevant security standards and other regulations must also be continually monitored by organisations. Such requirements are generally established to ensure the resilience of the organisation's information assets, or information assets they hold on behalf of others in the course of their business. Compliance requirements may also be industry and/or location specific, with key sectors such as banking and finance, telecommunications and utilities subject to their own regulations.

This paper is one of two that provides guidance to organisations on achieving IT resilience. An additional CEO paper summarises the concepts discussed in this paper and is designed to provide senior executive guidance on actions that can be taken to achieve resilience.

² The definition of 'resilience' used in this paper has been adapted by explanations of the concept in papers released by the US National Infrastructure Advisory Council and the Reform Institute, a US based not-for-profit think tank. These papers can be viewed at http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf and <http://www.policyarchive.org/handle/10207/9662>

PREPARATION

Preparing organisational infrastructure to deal with a disruptive event is one of the most significant components of establishing a sufficient level of IT resilience. Proactively engaging in activities to prepare systems to deal with these scenarios is crucial so that business operations can continue should such an event occur at some point in the future. This will minimise the potential impact felt by customers and the community at large.

It is important that any preparation strategy takes into account the changing and increasingly ubiquitous approach of businesses to the use of technology. 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 process is also being affected by other factors, including:

- An increasing interconnectedness of organisations through shared networks;
- Utilisation of shared application, storage and bandwidth resources through virtualisation, Software as a Service and “cloud computing” technologies; and
- A mobile workforce with access to increasingly sophisticated hand-held computing technology.

These factors – shown in figure 2 – are of significant importance when considering organisational resilience, as the blurring of the organisation's perimeter increases the surface area of the organisation that can be affected by a disruptive event.

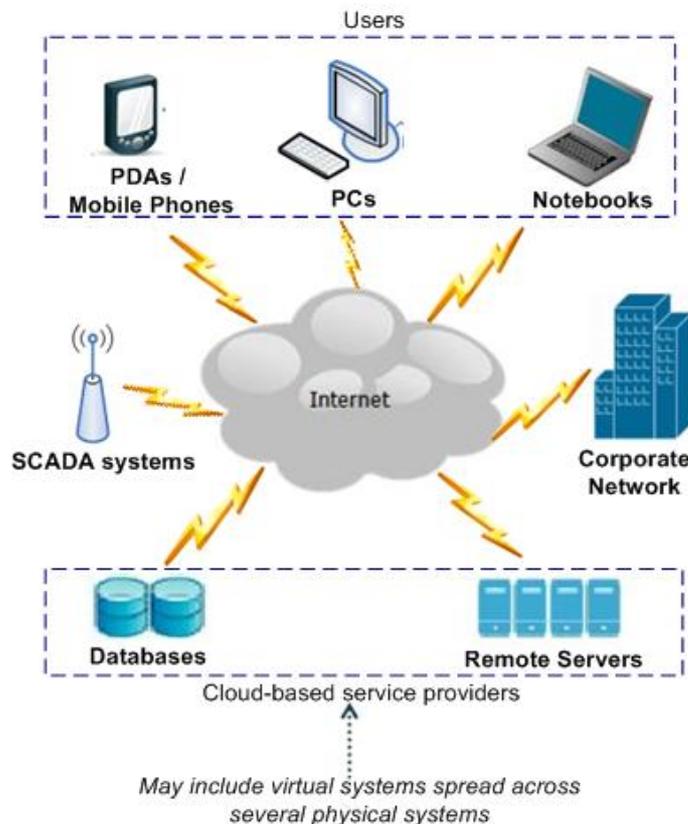


Figure 3 – Blurring of the organisational perimeter

While certain events may be sufficiently disruptive to be able to overwhelm an organisation's infrastructure regardless of its level of preparedness, implementing an appropriate strategy to manage such events can increase the resilience of important systems, minimising the negative effects of these events on organisations and the community at large.

Developing an effective strategy for achieving resilience is a significant task and one that requires extensive communications with key organisational partners, service providers, industry bodies and government. However, the result will be that your business is better equipped to continue operating normally should a disruptive event take place.

The remainder of this section discusses actions that your business should take as part of the *preparation* component of IT resilience, which include:

- Conducting a Threat Assessment
- Developing Incident Response and Business Continuity Plans
- Implementing an appropriate Governance Framework
- Integrating External Service Providers into Resilience Planning

Conduct a Threat Assessment

In order to develop a comprehensive strategy for achieving resilience, it is important to identify possible threats to the continued operation of your organisation's IT infrastructure. Performing a Threat Assessment is the most effective way to achieve this goal.

Following the AS/NZS ISO 31000 Standard for Risk Management is considered best practice. Firstly, the context of threats as relevant to your organisation is established, then risks (i.e., potential disruptive events) are identified, followed by an analysis of risk, and finally the evaluation of those risks.

Develop Incident Response and Business Continuity Plans

Developing and regularly testing incident response and business continuity plans is a critical step in pursuing resilient operations. These plans are important in order to define roles and responsibilities should a potentially disruptive event occur, and the processes to be followed in such a situation, including incident escalation thresholds and internal communication paths.

As identified in the Cyber Storm II exercise, the presence of established relationships with key organisations facilitates rapid information sharing, helping to maintain situational awareness and ensuring more effective incident response and recovery. Establishing these relationships proactively is crucial because it is difficult to create trusted relationships during the middle of a disruptive event.

In addition, developing relationships with key sources of information security intelligence can allow organisations to keep abreast of the latest security technologies, techniques and impending threats to IT systems. Groups such as CERT Australia are in a good position to predict, trace, and even work to shut down immediate threats to the IT systems of Australian critical infrastructure.

Implement an Appropriate Governance Framework

Having an appropriate governance framework in place within your business is crucial for pursuing and achieving operational resilience. The consequences of poor IT governance and subsequent IT failure can have widespread flow-on effects with regard to the overall resilience of IT systems.

There is no single leading practice model defined for IT governance. Each organisation’s security risk profile will differ and each organisation’s business objectives and practices will differ. However, key components for establishing a governance framework have been identified in a separate series of papers on IT security governance released by TISN³. These components include:

- Assigning organisational roles and responsibilities to ensure IT governance activities take place;
- Putting in place activities that are owned and operated by accountable individuals to implement and maintain governance capabilities; and
- Establishing core principles that facilitate approaches to resilience which take into account emerging threats and technologies.

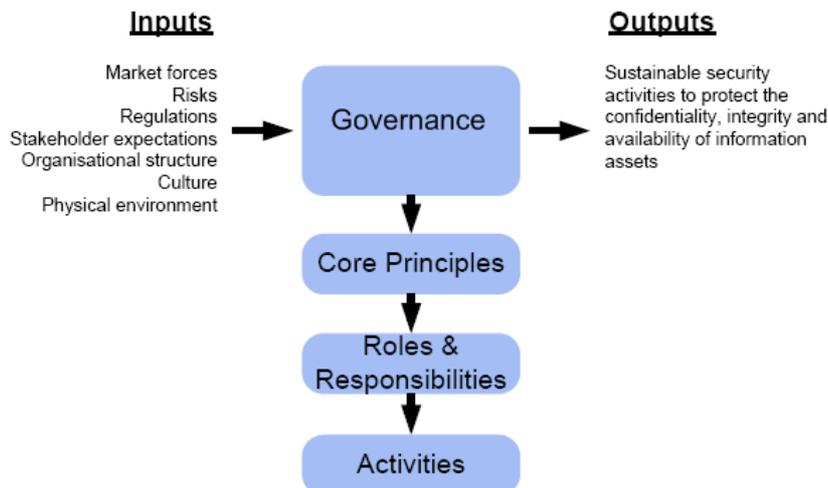


Figure 4 – Components of an IT Governance Framework

The Secure Your Information series of papers released by the Trusted Information Sharing Network (TISN) define seven principles that should underpin the enterprise’s strategy for protecting and securing its information assets as part of developing a governance framework. In addition, the TISN Resilience Community of Interest has identified eight resilience ‘enablers’ that can be used to develop a holistic approach to resilience:

Enabler	Considerations
Awareness	<ul style="list-style-type: none"> • IT leaders must be aware of potential threats to operations from <i>all hazards</i>, and have a considered plan for response. • The organisation should have an understanding of the

³ These papers can be accessed from the TISN website at http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/Publications_e-SecurityPublications

	thresholds beyond which the organisation’s response plans will be overwhelmed.
Agility	<ul style="list-style-type: none"> Established response plans must be able to adapt and evolve in an actual incident situation.
Communication	<ul style="list-style-type: none"> Internal communication channels must be clearly defined and understood. The IT team should engage with external communities of interest and advisory groups (e.g. CERT Australia) and should have mechanisms to identify emerging threats and trends.
Leadership	<ul style="list-style-type: none"> IT leaders must take ‘ownership’ of their need for resilience, identifying weaknesses and appropriate solutions.
Culture	<ul style="list-style-type: none"> Resilience is not ‘set and forget’. The culture of the IT organisation must be one that is constantly learning, and is able to adapt and innovate in times of crisis.
Change	<ul style="list-style-type: none"> As new ways of working are implemented – such as teleworking, cloud computing, software as a service and virtualisation – your IT team needs to stay on top of the implications to resilience and continuity. Such knowledge takes time to develop, so making time available above and beyond ‘business as usual’ operational tasks will be rewarded with a flexible team. Speed to change can be critical in a time of crisis – developing an ability to make rapid system changes when required is essential to manage unclear threats.
Integration	<ul style="list-style-type: none"> Resilience crosses teams within the organisation – risk, audit, IT, facilities management and more – and all of these groups need to have an open dialogue.
Interdependency	<ul style="list-style-type: none"> Your IT systems will almost certainly rely on other companies as suppliers, outsourcers, and partners. These firms are just as important to your resilience as your own internal capability and need to be engaged as such.

Integrate External Service Providers into Resilience Planning

As explained above, businesses are increasingly making use of systems and networks over which they have little or no control, especially with the increasing use of cloud computing services and Software as a Service (SaaS). In such an environment, devising a strategic approach to achieving resilience must include consideration of measures external service providers need to implement in order to secure their IT infrastructure to ensure an equivalent level of protection to that established by your organisation internally. If outsourcing arrangements are not properly managed and associated risks understood, the blurring of organisational boundaries and responsibilities can in fact reduce overall IT and organisational resilience.

Generally speaking, IT service providers are only obliged to implement IT controls in accordance with what they have been contracted to do. Failing to define and enforce stringent

requirements around security, availability and resilience on IT Service Providers will therefore have a significant detrimental impact on your organisation's level of preparedness for a disruptive event.

Contracts with IT service providers should establish key roles and responsibilities within your organisation and the service provider, and parameters should be established for the investigation and handling of incidents involving outsourced IT infrastructure.

Organisations must also understand that managerial and organisational liability for information security will often be unchanged by the outsourcing of IT functions.

More information on the management of external service provider relationships is available in a separate TISN paper⁴.

ENDURANCE

Once the task of preparation is complete, the next step in achieving a resilient IT environment is to improve the endurance of key systems by implementing a variety of measures at both technical and operational levels. The most effective way of achieving this is through pursuing a *Defence in Depth* approach.

Adopt a Defence in Depth Approach

Defence in Depth requires that mechanisms be implemented to try and prevent disruptive events, and ensure that operational capacity of IT infrastructure can be maintained should such an event occur. A Defence in Depth approach also assists with detecting attacks against systems so that an effective response can be implemented. This is important to ensure that systems are able to adapt effectively and continue functioning should the operating environment change significantly.

Defence in Depth has become increasingly important to achieve IT resilience as a result of overall business and technology trends which may weaken an organisation's control of information assets. This particularly includes the process of perimeter erosion discussed earlier in this paper.

Figure 5 provides a high level overview of the concept of Defence in Depth from a security perspective. This layered approach can also be extrapolated and applied to other areas of IT resilience.

⁴ Trusted Information Sharing Network, *Managing IT Security When Outsourcing to an IT Service Provider: Guide for Owners and Operators of Critical Infrastructure*, May 2007
[http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/\(427A90835BD17F8C477D6585272A27DB\)~Managing_IT+Security+When+Outsourcing+to+an+IT+~+Guide+for+Owners+and+Operators+of+Critical+Infrastructure.pdf/\\$file/Managing_IT+Security+When+Outsourcing+to+an+IT+~+Guide+for+Owners+and+Operators+of+Critical+Infrastructure.pdf](http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(427A90835BD17F8C477D6585272A27DB)~Managing_IT+Security+When+Outsourcing+to+an+IT+~+Guide+for+Owners+and+Operators+of+Critical+Infrastructure.pdf/$file/Managing_IT+Security+When+Outsourcing+to+an+IT+~+Guide+for+Owners+and+Operators+of+Critical+Infrastructure.pdf)



Figure 6 –Defence in Depth: A Layered Approach

Defence in Depth delivers:

- Effective risk-based decisions
- Enhanced operational effectiveness through improved resilience of IT infrastructure
- Reduced overall cost and risk and improved information security

A Defence in Depth strategy requires the in-depth understanding of system criticality, since this helps identify those systems that, if affected by a disruptive event, are likely to detrimentally affect the ability of an organisation to continue operating effectively.

The core principles of a Defence in Depth strategy are:

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

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.

More information on maintaining a Defence in Depth approach is available in a separate series of papers released by TISN⁵. Managing user access to IT systems, which is a key aspect of Defence in Depth, has also been addressed in a separate series of TISN papers⁶.

⁵ There are three separate papers on Defence in Depth available from the Trusted Information Sharing Network Website at http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/Publications_e-SecurityPublications

⁶ There are three separate papers on User Access management available from the Trusted Information Sharing Network Website at http://www.tisn.gov.au/www/tisn/tisn.nsf/Page/Publications_e-SecurityPublications

RESPONSE AND RECOVERY

Effectively executing plans developed to handle a disruptive event is important in order to ensure the proactive efforts undertaken by your business in the preparation and endurance phases are not wasted. Whatever measures have been taken in advance of a disruptive event, an organisation's ability to effectively respond should such an event occur is a crucial aspect of achieving IT resilience.

Incident response and business continuity plans will have been devised during the preparation phase. Following these plans, having established incident escalation thresholds and leveraging relationships established with key external organisations to facilitate rapid information sharing will ensure that the impact systems sustain from a disruptive event is minimised, and normal operating circumstances can be returned to as quickly as possible.

Responding and recovering from a disruptive event to IT systems can be categorised into four timeframes:

- **Immediate response** – identify that a disruptive event has occurred and identify the source and/or component responsible for it.
- **Assessment and activation** – assess the status of the disruptive event, determine the business operations affected, and determine the most appropriate actions.
- **Response/recovery** – execute the necessary actions to stop the disruptive event (where possible) and recover operations capability.
- **Resumption** – following assessment of the disruptive event's root cause and resolution of necessary issues, resume normal business operation.

In addition, undertaking a process of analysis of the success of response following resumption of normal business operations can help identify areas of potential improvement for responding to a similar disruptive event in future. This will position your organisation to strengthen its overall approach to achieving IT resilience.

CONCLUSION

Establishing a sufficient level of IT resilience is crucial to ensure that the impact of potentially disruptive events on important systems is properly managed. Following the recommendations in the three areas of resilience as outlined in this paper will ensure that organisations are able to continue operations and that the negative implications felt by customers and the community generally from a disruptive event are minimised.

Achieving IT Resilience Based on the Eight Key ‘Enablers’	
Awareness	<ul style="list-style-type: none"> • Educate users and external contractors of key risks and threats to IT resilience, and the responsibilities expected of them regarding security and acceptable usage • Track technical threats, reviewing these threats in the context of the organisation’s environment and vulnerabilities
Agility	<ul style="list-style-type: none"> • Establish, regularly test and refine incident response and business continuity plans • Determine the most appropriate actions to respond to a disruptive event based on incident response and business continuity plans • Execute the necessary actions to stop a disruptive event (where possible) and recover operations capability • Perform an analysis of any disruptive events and the success of the response process
Communication	<ul style="list-style-type: none"> • Participate in informal and formalised information sharing networks in information security both internal and external to the organisation.
Leadership	<ul style="list-style-type: none"> • Develop a strategic approach to achieving resilience that complies with legal and regulatory requirements. • Foster a Defence in Depth approach to achieving resilience that is implemented throughout the organisation • Assign IT responsibilities and ownership throughout the organisation.
Culture	<ul style="list-style-type: none"> • Complete regular reviews of systems and the effectiveness of resilience measures in place • Adjust preparatory and response measures to disruptive events based on changes in technology and the threat landscape
Change	<ul style="list-style-type: none"> • Maintain continual awareness of new technologies and services • Establish a network of sentinels who research and develop awareness of emerging threats and can provide reliable information when you need it most
Integration	<ul style="list-style-type: none"> • Develop clear incident escalation thresholds and clear internal communication paths between business areas in an organisation
Interdependency	<ul style="list-style-type: none"> • Form co-operative relationships with service providers and other relevant organisations • Define monitoring and reporting responsibilities for external service providers in engagement contracts.

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

Achieving IT Resilience – 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