Trusted Information
Sharing Network
for Critical Infrastructure Protection

WIRELESS SECURITY—OVERVIEW FOR CEOS

CEOs and Boards of Directors are ultimately responsible for protecting their organisation’s information and information systems not only from malicious & accidental damage, but from unauthorised access as well. Failure to take mandatory precautions may result in a direct violation of regulatory requirements, such as:

- Corporate governance regulation - CLERP 9 (Australia) and Sarbanes-Oxley (USA).
- 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).

As modern organisations increasingly rely on the Internet, ‘due care’ requires that controls be established to minimise the risk of:

- Significant financial loss from either direct theft of funds, information or through the application of fines associated with regulatory non-compliance.
- The loss of business through a denial of service attack against your organisations information systems.
- Significant brand damage and associated loss in consumer confidence in your company.
- Directors’ liability in the event of insufficient care being taken.

Wireless technologies benefit businesses, as they provide increased access to organisational resources—but they also increase security risks. Using public wireless networks (e.g. in airports and hotels), or wireless technologies within the organisation, provides attackers a potential avenue for stealing or tampering with an organisation’s data.

This paper provides a starting point for managing these wireless security risks.

Business benefits of wireless technologies

The benefits of wireless technologies are visible at all organisational levels as they provide greater mobility, accessibility and convenience. Technical teams have less network cabling to consider and can achieve cheaper scaling and expansion and overall greater flexibility.

Wireless technologies offer improved productivity and cost savings and as a result are being used more often.

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 judgement of users. The 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.

Revised June 2008

Business risks

While wireless technologies offer a number of benefits there are security weaknesses associated with using them which can expose an organisation’s business assets to significant risks. Without controls on the implementation and use of wireless technologies, potentially any information on your corporate systems could be broadcast, resulting in it being picked up by unauthorised parties.

Potential consequences of wireless system security breach

Direct Loss

- Financial loss through fraud
- Regulatory fines or other penalties
- Share price manipulation

Indirect Loss

- Inability to service clients
- Lost productivity
- Brand damage

A reliance on wireless networks and devices for critical functions may increase the potential for outages, as wireless infrastructure may be more susceptible to being taken offline by an attacker. Also, should a malicious outsider conduct criminal activity using your wireless systems, the organisation may face criminal investigation or need to engage resources in handling the matter.

As wireless enabled devices are often physically removed from the organisation’s premises, they will also generally be subject to a greater risk of loss or theft of information.

Resources required to secure wireless systems

Addressing wireless security related risks requires implementing controls around the people, policies and procedures, and technologies that comprise wireless systems. Implementing these controls may require purchasing new hardware, using technical specialists and developing new security policies. Co-ordination of these actions will generally be managed by your CIO or IT Manager.

Issues to raise with your CIO

A wireless security strategy should target three focal points: people, policies and procedures, and technology.

The following is a suggested list of issues to discuss with your CIO or IT Manager in developing an overall security approach appropriate to wireless which mitigates the risks relevant to your business.

People
• Raising awareness of wireless security risks across the organisation, and establishing controls to minimise them • The need for (additional) training of technical staff to control the security risks • Employee knowledge of safe usage practices for wireless networks and devices both internal and external to the organisation
Policies and procedures
• Specific inclusion of wireless technologies and devices in IT policies and usage

guidelines • Security audits to ensure adherence to policy and regulation
Technology
• Protection of sensitive information as it is sent across any network (including both organisation owned and public networks) • Whether the organisation has the necessary infrastructure to deliver high standards of wireless security and if not, whether an action plan for implementing such a system is required

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.