Trusted Information
Sharing Network
for Critical Infrastructure Protection

WIRELESS SECURITY – INFORMATION FOR CIOS

Introduction

In today’s business environment, controlling access to data is critical to long-term business survivability. Wireless is widely used because of the benefits it offers in its improved productivity, efficiency and cost effectiveness, though common with any technology there are security challenges associated with this technology. The broad range of wireless technologies is no exception - such technologies allow for access to information outside an organisation's normal perimeter.

Wireless signals are broadcast in an open and easily detected manner and will often travel well beyond the organisation’s physical security perimeter. As these technologies gain wider acceptance in the marketplace and increased adoption in your organisation, these security risks require attention by the right people and at the right levels within your organisation.

This paper, developed by the IT Security Expert Group (ITSEAG) which is part of the Trusted Information Sharing Network (TISN)[1] for critical infrastructure protection - provides information on the risks involved with using wireless technologies, and a set of basic actions your organisation can do to manage and respond to these risks. A companion paper, the *Wireless Security CIO Technical Appendix* is also available and provides more comprehensive and technically focused information covering the various types of wireless technologies, risks associated with the technology as a whole, and methods for mitigating these risks.

Benefits of using wireless technologies

Wireless technologies can offer cost advantages, availability of information on demand, geographic freedom, as well as increasing scalability and flexibility when responding to changes in IT infrastructure needs. Wireless technologies also offer several benefits to all

[1] 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 (IAAG), several Expert Advisory Groups (EAGs), and the Critical Infrastructure Advisory Council (CIAC - the peak body of TISN that oversees the IAAGs and EAGs).

The ITSEAG is one of the EAGs 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. Its members include academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security field.

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

levels of an organisation. For workers, wireless technologies provide greater mobility, accessibility and convenience. Network administrators have less network cabling and ports / jacks to consider, fewer obstacles to extending the network for cheaper scaling and expansion, and overall greater flexibility.

Businesses utilising wireless technologies often realise enhanced productivity and cost savings. As a result, these technologies have a growing presence in organisations today. Some example applications of wireless technologies are listed below:

- Enabling high mobility connectivity for devices such as mobile telephone Internet services;
- Providing metro area or wide area point to point high speed data transfer;
- Enabling connections into corporate networks from remote locations such as airport 'hot spots'; and
- Enabling the use of cordless devices such as Bluetooth headsets for mobile telephones.

This paper seeks to in general terms investigate the concerns, risks and vulnerabilities within wireless standards, and common approaches to managing them.

Overview of Wireless Security

Whilst the advantages are numerous, the erosion of the organisation's physical boundary and the increasing bandwidth capabilities raise a number of associated security risks which require consideration. Wireless networks are exposed to many of the same risks as are traditional wired networks; however there is a greater attack surface area[2] for attackers to abuse due to the nature of wireless transmissions.

The risks to unsecured wireless networks that have previously been exploited include destroying or stealing data, launch attacks that tie up network bandwidth, deny service to authorised users and to eavesdrop on conversations[3]. For example, attackers have compromised wireless systems to gain access to sensitive financial data held in an organisation's internal databases.

Protecting the information of your organisation requires the maintenance of three (3) key properties in wireless networks. These are:

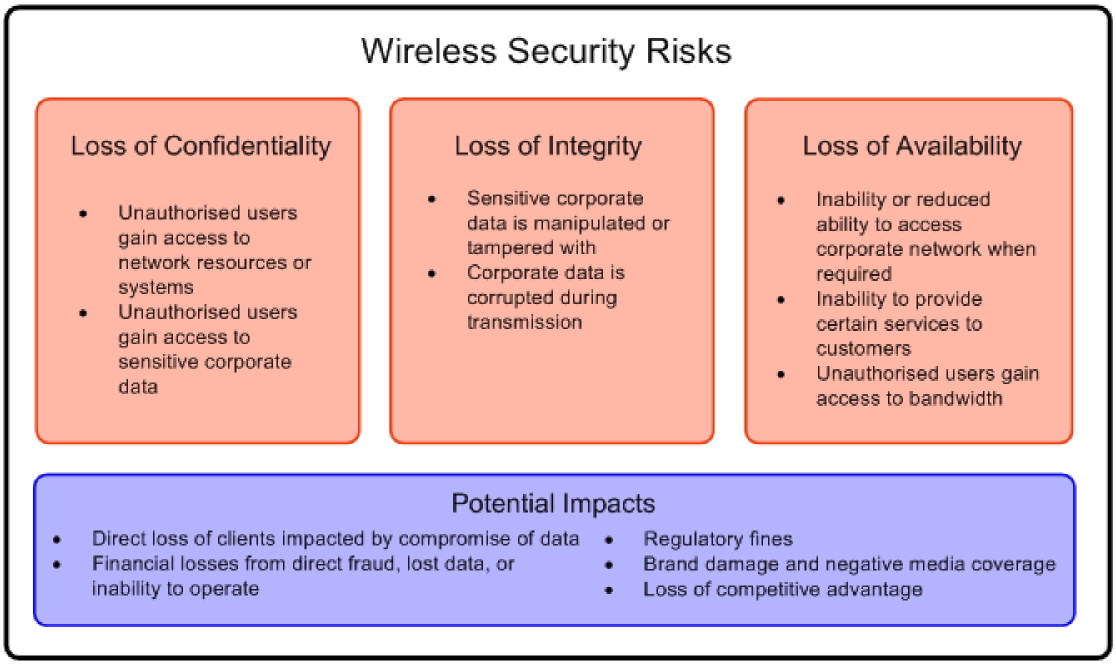
- **Confidentiality** – ensuring that sensitive information is safe, preventing eavesdropping on your enterprise data and systems, and minimising information loss due to device loss or theft;
- **Integrity –** ensuring wireless data has not been tampered with or corrupted; and
- **Availability –** ensuring that when needed, the wireless system is ready for use.

Risk Identification

Attacks on wireless technologies may adversely affect the organisation's ability to conduct business operations or satisfy information protection requirements. Key areas of risk are outlined below:

[2] The attack 'surface area' is the area of a system, application or other technology that can be subject to attack. As wireless networks have a number of additional technology components on top of the standard networking technologies, there are a greater number of elements that can be subject to attack.

[3] Page 1 Security for Wireless Networks and Devices, Shirley Raddock, National Institute of Standards and Technology http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm.



Wireless Security Risks

Loss of Confidentiality

- Unauthorised users gain access to network resources or systems
- Unauthorised users gain access to sensitive corporate data

Loss of Integrity

- Sensitive corporate data is manipulated or tampered with
- Corporate data is corrupted during transmission

Loss of Availability

- Inability or reduced ability to access corporate network when required
- Inability to provide certain services to customers
- Unauthorised users gain access to bandwidth

Potential Impacts

- Direct loss of clients impacted by compromise of data
- Financial losses from direct fraud, lost data, or inability to operate
- Regulatory fines
- Brand damage and negative media coverage
- Loss of competitive advantage

- **Loss of Confidentiality**

  Due to wireless devices transmitting messages via radio frequencies, network access can be gained without physical access to network ports or other infrastructure. Attackers can use wireless 'packet sniffers' to capture wireless network traffic which can reveal service configuration details, authentication credentials, and even the messages contained within. Loss of sensitive information can have a material impact on an organisation, ranging from the loss of client and investor confidence through to large and direct financial liabilities.

  One of the attacks that can result in a confidentiality breach is an impersonation attack, where a lack of appropriate data encryption may allow an outsider to capture traffic in transit. This in turn may allow an outsider to access the wireless network without authorisation and potentially access any internal systems connected to the network itself.

  Examples of the potential impact regarding the loss of confidentiality include:

  - Regulatory fines or other penalties;
  - Brand damage associated with negative media coverage; and
  - Direct loss of clients impacted by the loss of their data.

- **Loss of Integrity**

  A wireless connection which does not adequately secure the integrity of wireless messages could expose data or information to attackers that could exploit the system using techniques such as spoofing to inject unauthorised packets into the network, 'man-in-the-middle' attacks, and many others.

  Poorly configured connections between mobile computing devices and organisation-owned networks may leave transmitted data susceptible to manipulation, which could remain undetected by the sender and recipient.

Examples of the potential impact in the loss of a system's integrity include:

  - An inability to rely on the integrity of critical information (eg: being unable to sign off on the accuracy of financial statements); and
  - Brand loss or financial loss through direct fraud.

- **Loss of Availability**

  An attacker could stop authorised users from using the service through exploiting vulnerabilities in a wireless node to render the system inoperable, or flooding the network with traffic. Due to the nature of Radio Frequency (RF) transmission, wireless networks could also lose service inadvertently from other wireless devices that communicate over similar wavelengths.

  Outsiders may have the ability to steal services and utilise the organisation's connection bandwidth. Should a malicious outsider conduct criminal activity utilising organisation owned wireless systems, the organisation may face criminal investigation or otherwise be required to engage resources in handling the matter.

  Examples of the potential impact of loss of availability include:

  - An inability to provide services to clients, resulting in a direct loss of revenue
  - Loss of clients requiring immediate services to competitors during periods of system downtime

The accessibility of wireless connections outside of networks owned by your organisation compounds the confidentiality, integrity and availability risks to your information. Services such as free wireless 'hotspots' in cafes and airports may not be configured to provide the required level of security control that your sensitive information requires.

Protecting the organisation

In order to manage the level of risk associated with wireless technology, you should consider the following organisational assets:

- **People**
  Applying security controls to counter people related risks such as internal data theft or uploading malicious software, is critical for protecting an organisation's information and system's integrity in wireless networking environments. Similarly, the awareness and capability of staff will constitute a major factor in performing required security practices defined in organisation policies.

- **Technology**

  Securely configuring your wireless infrastructure and devices will considerably reduce risk exposure.

- **Policies and Procedures**
  Policies need to be developed that outline clear procedures and responsibilities for the use of wireless devices by staff members at all levels.

Examples of specific controls in each of these areas are detailed in the following table:

People
• Identify key roles and responsibilities for wireless security • Identify wireless user groups and their scope of usage for risk assessment • Ensure network administrators are aware of wireless security issues and risks, and have the necessary training to implement mitigating controls • Initiate awareness programs for users of wireless systems covering wireless risks and acceptable wireless usage • Initiate training of users in relevant incident response procedures
Technology
• Complete regular audits of wireless networks • System and network administrators utilise strong wireless security configurations. Information on wireless security can be sourced from the *TISN Wireless Security – CIO Technical Appendix* paper • Ensure monitoring and logging of any wireless related security alerts takes place such as failed login attempts and any unusual wireless usage • Ensure technical staff are up to date with relevant technologies and current and emerging threats • Ensure that both the operating systems and firmware of any wireless systems or infrastructure utilised in a wireless system are regularly patched with the latest security updates offered by the product vendors • Ensure corporate data is secured properly on a suitable storage device and is protected from malicious code such as viruses, worms and Trojans by applicable security software and procedures
Policies and Procedures
• Integration of wireless security controls into existing IT security policies o Ensure these policies account for any wireless requirements listed in applicable industry regulation / requirements such as the Payment Card Industry Data Security Standard (PCI-DSS) wireless encryption requirements • Ensure integration of wireless usage into Acceptable Usage policies covering wireless connectivity from both organisation owned and non organisation owned wireless networks • Coordinate regular review of wireless security policies • Develop technology risk assessment schedule to cover wireless risks • Ensure that wireless security is regularly reviewed including reviews after any significant system changes

Conclusion

It is essential that organisations have suitable protective measures for their IT systems particularly where wireless technologies are used. This paper provides the basic knowledge for managing and mitigating the risks associated with wireless technology.

Management policies and procedures should ensure that new technologies cannot be introduced without the knowledge of IT management. Good practice approaches should be utilised in the configuration of wireless technologies to mitigate external confidentiality, integrity and availability risks.

Finally, security of wireless networks or any business technologies should be viewed as an integral and ongoing consideration in an organisation's operations. Implement a secure structure which conforms to best practice advice, then maintain and update the system as necessary to track future changes in wireless technology or wireless related risks.

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