



Wireless Security – Overview for CEOs

The “backbone” of your information services infrastructure is changing and there is every possibility that “wireless” applications will increasingly feature in your information platform. It is highly likely that wireless is already in your networks or being used by your people in some form or other both inside and outside your organisation at any time of day or night. For example, your people may be accessing your information systems at 10,000 metres from specially equipped planes on business trips.

Wireless is offering new cost advantages, availability of information on demand and when needed, and flexibility in being able to respond to changes in IT infrastructure needs.

As these technologies and their associated products gain wider acceptance in the marketplace a number of security concerns need to be taken into account. They arise from the nature of the technology involved – wireless is broadcast in an open and easily detected manner and normally operates “around the clock”.

These concerns need to be addressed by the right people and at the right levels in your organisation.

Essentially the new wireless connectivity can be categorised roughly into four different types, largely based on the distance over which they operate, as follows:

ABBREVIATION	NAME	EXAMPLE	USAGE
WWAN	Wireless Wide Area Network	GSM Mobile Phone	10Kms
WMAN	Wireless Metropolitan Area Network (IEEE 802.16)	Suburb of city connected to the Internet at broadband speeds	1Km
WLAN	Wireless Local Area Network (IEEE 802.11)	Local area network on the floor of your building connecting all workstations and servers.	100m
WPAN	Wireless Personal Area Network (“Bluetooth”, Infrared)	Connecting and controlling various products and devices	1m

Everyone now talks about “hot spots”, located anywhere in a city, building or even on board a train, bus or plane, where a person may connect to the Internet and then, at the same time, to your organisation’s IT infrastructure via their wireless equipped laptop computer or even their PDA and mobile/cell phone.



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.

Issues you need to consider

There are quite a few concerns that you should be aware of and for which you should have appropriate management policies determined and responsibilities assigned.

For example there is a growing amount of enterprise databases and information which reside in employees' laptops, or wireless enabled devices. These need protection, as they can easily fall into the wrong hands. At the policy level, there needs to be policy to safeguard such information, and at the practical level, there needs to be protection (encryption) to ensure such information does not fall into the wrong hands.

The following provides a quick summary of the security issues that need to be considered in embracing this new and convenient technology.

Simply, the usual security problems of

- **confidentiality and privacy** (eavesdropping on your enterprise data and systems)
- **integrity** (including authentication of people and systems as well as data and programs used)
- **availability** (to ensure that if needed, the wireless system is there and ready for use)

With wireless we now have to add a few more concerns, which include:

- **masquerading** (illicit connection of “foreign” computers/systems into your own network)
- **insertion** (of computer viruses, spam email message and so on), and
- **bypass** (those enterprise laptops and PDAs with wireless connection are truly mobile and can be used outside the protection given by such systems as the corporate firewall, email filters, so-called “proxy-servers” that protect real enterprise addresses on the Internet).

Issues to Raise With Your CIO

The following is a suggested list of issues to discuss with your CIO in developing an overall security approach appropriate to wireless.

- Is the CIO conversant with the new technology and its place in your organisation?
It is new and appropriate education and training needs to be budgeted for and time allowed for this to be done. This applies at both the CIO executive level as well as at the information systems and network management levels since it is likely that their earlier education and training in the IT arena did not include the details of this technology nor its control, management and security.
- Is there a policy for the installation of wireless as a network medium within your enterprise, including where, when, how and for what purposes?

- Is there a policy about usage of wireless connectivity outside your own information infrastructure, for example, by sales people “on the road” at hotels, airport lounges or like “hotspots”? Has the CIO and the enterprise network manager determined the required security parameters that need to be set or additional security subsystems that are needed?

It has to be noted that nearly all laptop computers and even PDAs that are purchased today have wireless connectivity built in as a standard feature. These parameters need to be correctly configured against your security policy - this may not be obvious to or even easily and reliably done by the normal user.

Finally, is the CIO ready to brief you and your board or senior management group on your enterprise’s use of wireless technology along with any risks that have been determined and overcome?

Note:

The IT Security Expert Advisory Group* has developed a separate paper for CIOs to provide them with practical advice on how to set up and run wireless systems with minimum risk. The ITSEAG Secretariat can be contacted on (02) 6271 1426.

** The IT Security Expert Advisory group (ITSEAG) is part of the Trusted Information Sharing Network for critical infrastructure protection (TISN) which 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 (EAG), and the Critical Infrastructure Advisory Council (CIAC - which is the peak body of TISN and oversees the IAAGs and the EAGs). One of the expert advisory groups within the TISN framework is the ITSEAG which provides advice to the CIAC and the sector-based IAAGs on IT issues as they relate to critical infrastructure protection. The ITSEAG is made up of academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security field. More information on TISN can be sought from <http://www.tisn.gov.au>*