

Wireless Network SECURITY

Is your wireless network broadcasting your company's confidential data to the world? Are unauthorized users using your bandwidth?

Today's wireless networks offer users flexibility and convenience. Without careful security planning, encryption and frequent auditing, however, unauthorized users can view private data, link to network resources, carry out Trojan attacks, or steal your company's bandwidth.

Secure Enterprise Computing's Wireless Network Security Team will assess your company's wireless network to discern its current security posture, or assist you in building a secure wireless deployment from the ground up. SEC can provide recommendations and assistance to secure your confidential information and protect your firm from outside attacks.

Methodology Working with your Information Technology team, Secure Enterprise Computing will tailor a configuration to your business needs without compromising security policy or information resources. At a minimum, the final solution will have processes in place to address the following:

- **Planning and Implementation Support:** The initial rollout of wireless access will require solid detailed planning with relevant technical staff to ensure a smooth implementation and provide for ongoing support.
- **User-based authentication:** Unique for each user to mitigate the risks of an unauthorized user that has access to an authorized device
- **Secure communications:** WEP has known weaknesses and is easily exploitable. There are enhancements to this standard (LEAP / PEAP) that should be implemented in order to prevent unauthorized individuals from compromising corporate communications.

- **Accountability:** All user access should be logged and monitored.
- **Segregation:** Placing the wireless network in its own virtual local area network (VLAN) will allow administrators to control access and isolate the wireless from the wired while still allowing fully functional access for authorized users.
- **Flexibility:** Any design needs to consider non-standard configuration needs, such as public system access.
- **Manageability:** The system, once deployed, should be easily managed and upgradeable wherever possible.
- **Scalability:** The solution will be able to grow as needs on the wireless infrastructure are increased, and will support emerging standards such as 802.11g.
- **Intrusion Detection/Prevention:** A complete solution would monitor the health of authorized access points/clients and provide feedback about any unauthorized devices.

Wireless technologies, when installed, must comply with industry recognized standards and specifications. Equally as important, the solution must support and employ industry accepted security configurations, such that when data traverses the wireless network it is kept private and secure.

Secure Enterprise Computing is an established, respected and capable Information Security Professional Services organization, that focuses on needs-based solutions. We can assist your organization with a wireless configuration that will enable the business process without inviting threat.