THOMPSONNETWORKCONSULTING
7115 West North Avenue, PMB #252
Oak Park, Illinois 60302
708.214.7544
www.thompsnet.com



# A World without Wires

Wireless Local Area Networks (WLANs) increase an organization's productivity through enabling location independent Internet and office Intranet network connections. WLANs reduce the need for expensive office cabling and wiring. However, an **unprotected WLAN provides easy access to an organization's computer network**.

WLANs serve as gateways between wireless devices such as laptops with WLAN cards, the office computer network, and the Internet. A wireless device connects to a WLAN through using the WLAN identification, called an SSID. In order to access the office Intranet and Internet, a wireless device may have to provide additional authentication passwords.

A WLAN signal's range often extends beyond the office. WLANs can be an open door for attacks from hackers looking for free Internet service and access to confidential information.

**Securing the WLAN involves protecting communications with wireless devices**. This requires following best practices for limiting knowledge of the WLAN SSID, layers of authentication for wireless devices accessing the WLAN, and encrypting communications between authorized wireless devices and the WLAN.

**Thompson Network Consulting** recommends the following best practices for securing WLANs:

1. Physically place WLAN equipment in the center of office building
2. Do not use the default SSID values
3. Do not broadcast SSID
4. Enable encryption between wireless devices and WLAN
5. Configure WLAN to only support approved wireless devices
6. Place firewall in front of WLAN
7. Implement multiple layers of authentication for wireless devices

**Thompson Network Consulting offers solutions that protect confidential electronic records, ensure secure communications, and optimize computer network performance. Our solutions enable organizations to meet expected outcomes for quality service delivery.**

**Thompson Network Consulting service descriptions, security presentations, and event information are located at: www.thompsnet.com**