Vol. 5 No. 2
February 2013

BUSINESS*insights*

# Wi-Fi Best Practices

Most businesses agree that it's no longer necessary to invest in wired technology when wireless networks can be implemented more quickly for much less money. Wi-Fi or wireless LAN (WLAN) networks give your staff the freedom to take their calls anywhere, anytime within your facility and to get faster and easier access to information.

Wireless networks also provide these other advantages:

- **Simplifies your network:** Wi-Fi eliminates the complexity of connecting PCs and other devices together with cumbersome cabling, wiring, switches, adapters, plugs, pins, and connectors.

- **Provides greater flexibility:** Wi-Fi makes it easier to expand your network as your business grows.

- **Satisfies employees and visitors:** The proliferation of laptops, smart phones, tablets and wireless home networks makes the availability of Wi-Fi an expectation on the part of employees and visitors.

- **Increase customer service and satisfaction:** If your business provides customer services, offering a Wi-Fi hot spot can increase customer visits, customer loyalty and your bottom-line revenue.

To implement the proper Wi-Fi environment, you'll need to make the following determinations so it can be built and sized to serve your specific needs. You'll want to make sure you build your WLAN to support current and future demand to prevent any possible overload and costly downtime.

1. How many users do you want your Wi-Fi network to serve?
2. How large a geographic area do you need to serve and are these areas indoors and outdoors?
3. What will be the typical use of the network so you can estimate performance requirements?
4. Must the network stand on its own or enhance an existing wired network?
5. What applications need to run over the WLAN?

Once you have answers to the above questions, you can build your WLAN so it can support your specific needs.

It's important to remember, however, that Wi-Fi communications and data travel through the air. That makes a WLAN more vulnerable than a wired network if not properly secured. To help ensure Wi-Fi security we recommend that you take the following steps:

**1. Start by choosing your Wi-Fi security option:** Your choices have been Wire Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) or WPA2. First, IT professionals recommended WEP and WPA, but, over time, these have been found to be vulnerable. If your computers and network support the Enterprise version of WPA2 with the Advanced Encryption Standard (AES) algorithm, this is today's best option. The great advantage of this choice is that the encryption key is never loaded onto the computers themselves. Using this type of security helps protect your network from the threats posed by disgruntled ex-employees or stolen or lost laptops. If an employee is terminated or a laptop lost, the only thing you need to do is cancel or change user passwords -- nothing more.

(continue pg. 2)

IDeACOM® NETWORK
1-866-IDEACOM
(433-2266)
www.ideacom.org

BUSINESS*insights*

2. **Build, activate and verify firewalls:** Ensure that your network is protected by firewall technology and that it is active at all times.

3. **Prevent your computers from connecting to other networks:** Typically, Windows-based computers are set up to try to find and connect to available networks in stores, airports, residential neighborhoods and more. Many of these networks are not secure and the minute one of your company laptops connects to an unsecured network, your private information is vulnerable. Make sure this auto-connect feature is turned off on all company computers.

4. **Keep hardware system firmware, drivers and operating system up to date:** With so many threats to computer networks, developers and manufacturers are constantly updating their firmware, software and drivers to keep systems secure. Mark your calendar to periodically check for updates from your operating system, hardware and accessory vendors so you can keep your systems as secure as possible.

5. **Keep your servers and routers in a secure location:** Make sure all routers, access points, and network devices are hidden and secure so no one can plug directly into your network.

6. **Consider setting up a virtual private network (VPN) for extra security:** By installing a standalone VPN server, putting server software on your computers or using a hosted service, you can encrypt all user traffic using your Wi-Fi network.

7. **Divide your network into sections and restrict access:** By setting up individual "virtual networks" you can restrict document access by title or responsibility. Not only does this prevent a low-level employee from seeing management or financial information, but, if that computer is ever compromised, the hacker will have access only to the section of information available to that employee.

Wi-Fi simplifies your efforts to provide a flexible working environment for you and your employees. A Wi-Fi hot spot can also provide an additional benefit to customers and visitors. Just make sure that, before you enjoy all the benefits of this convenient technology, you keep your business information fully secure.

"Wi-Fi" is a trademark of the Wi-Fi Alliance and the brand name for products using the IEEE 802.11 family of standards. Only Wi-Fi products that complete Wi-Fi Alliance interoperability certification testing successfully may use the "Wi-Fi CERTIFIED" designation and trademark.

IDeACOM® NETWORK
1-866-IDEACOM
(433-2266)
www.ideacom.org