

Wireless Technology

When professionals conduct business away from their desks, they lose access to valuable network resources, which impedes the ability to respond rapidly to customer requests, to collaborate effectively in meetings, and sometimes even to close a deal. Now that wireless solutions have matured, however, companies can afford to extend their information infrastructures to workers in meeting rooms, in public areas at their main business locations, in airports and hotels on the road, and at home. A recent study conducted by NOP World—Technology for Cisco Systems® shows that wireless technology can enable workers to stay connected an additional three and a half hours a day, empowering them to respond more quickly to customers, partners, and colleagues.

Now, employees can take advantage of time between meetings and retain access to critical information resources wherever and whenever they need them. Business-critical wireless solutions extend access to applications, Web content, and communications channels to workers away from their desks, which improves employee responsiveness to customers and partners, increases business productivity, and enhances collaboration. Wireless solutions also enable SMBs to more quickly facilitate network adds, moves, and changes. Plus, if a small business is in a temporary location or plans on moving to a new location the wireless network can be easily moved.

Network managers of small and medium-sized businesses (SMBs) can extend business networks using WLAN technology to increase employee productivity. However, securing the wireless network is equally vital.

Like cordless phones, WLAN technology uses radio waves to transport data, making them open-access by design. If security is not enabled, the radio signals transporting the data are vulnerable to unauthorized receivers. Wireless access point and network interface cards (NICs) have built-in security, but units are shipped from the factory without security enabled in order to comply with interoperability rules. It is easy to successfully set up a WLAN in its default configuration, but network managers must take the necessary extra steps to apply and enforce a standardized means of securing the wireless network.

One of the main reasons that SMBs deploy wireless solutions is because of adds, moves, and changes.