



## Are Your Company's Wireless Networks Putting Your Sensitive Data at Risk?

By Stephen F. Douglas, CSP, ARM, Technology Risk Control Director  
July 2007

Since being introduced in the late 1990s, wireless networking technology has seen explosive growth.<sup>1</sup> Wireless Local Area Networks (WLANs), otherwise known as "hotspots," not only offer companies portable and flexible network-connected use of laptops, personal digital assistants (PDAs) and smartphones (mobile phones with computer-like functionality) but also other application-specific tools, such as barcode readers, point-of-sale (POS) devices, radio frequency identification (RFID) tag readers and healthcare information devices. The increase in use of wireless network technology, the rise in identity theft-related crime and inherent security weaknesses associated with wireless networks have combined to create significant threats to sensitive data housed on enterprise networks.

Wireless network security weaknesses have been implicated in several high-severity security breaches recently. The Federal Trade Commission (FTC) complaints against retailers BJ's Wholesale Club, Inc.<sup>2</sup> and DSW, Inc.<sup>3</sup> indicate security weaknesses related to wireless networks. Additionally, a recent *Wall Street Journal* article attributes the security breach that allowed the theft of 45.7 million credit card numbers from the corporate networks of TJX Companies – the parent company of Marshalls, T.J. Maxx, Home Goods and A.J. Wright retail stores – to problems with wireless networks in their stores.<sup>4</sup> This is the largest publicly announced breach of private non-public information to date and is currently being investigated by the FTC.

The primary difference between wireless networks and wired networks is also the root of the security concerns involved with use of these networks. The radio links used for network communications in a wireless network can be easily and covertly intercepted. Eavesdropping on or manipulation of these communications by an attacker becomes a much simpler task. To bring these networks to levels of security near that of traditional wired networks, strong authentication techniques and encryption that makes these intercepted signals unreadable to unauthorized parties are necessary.

Although these wireless security issues can be addressed, a recent survey by a security firm highlights the fact that many businesses have not implemented basic controls. The survey was conducted by traveling specific routes through the business and financial districts of New York, London and Paris and using a laptop with specialized software to detect wireless networks and log information about network configurations. Between 20 and 25 percent of business wireless access points in areas surveyed were open to access by anyone with a wireless device.<sup>5</sup> As demonstrated by the high-profile data breaches mentioned above, the primary risk is that sensitive corporate network data is vulnerable to unauthorized access.

The following suggestions are offered regarding the use of wireless networks by businesses and the growing threat to information security:

- **Develop a formal security policy regarding the use and deployment of wireless technology.** This policy should address user security awareness, an approval process for adding, monitoring and configuring wireless network hardware, and procedures




for registering all wireless Network Interface Cards that are used in devices connecting to the corporate network.

- **Change WLAN access point Service Set Identifiers (SSIDs) and administrative passwords from factory defaults to unique values for your business.** The SSID is a name assigned to a WLAN to allow wireless devices to distinguish one WLAN from another. Administrative passwords allow access point configuration changes that could be used to disable security. Factory default passwords are easy for attackers to access and, in most cases, are readily obtainable from published lists for specific manufacturers and models. The survey noted above also found that 24 percent of the networks in the New York City survey had at least some settings that had not been changed from default values.<sup>5</sup>
- **Disable access point SSID broadcast features and enable hardware or MAC address filtering.** When the broadcast feature is enabled, the WLAN's SSID is visible in plain text to anyone with a wireless device. If this SSID has not been carefully chosen to be private or vague, it may provide information regarding the identity of the network that could be valuable to an attacker. MAC address filtering limits access to wireless devices with MAC IDs specified by the network administrator. It should be noted that these two techniques will only prevent access by casual users who are simply looking for free Internet access. This configuration won't stop experienced attackers unless used in conjunction with strong encryption and authentication techniques.
- **Do not depend on Wired Equivalent Privacy (WEP) access as a primary means of securing wireless networks.** At a minimum, use Wi-Fi Protected Access (WPA). Stronger encryption algorithms are available but upgrades of wireless network hardware may be necessary. A Virtual Private Network (VPN) is also an option for securing wireless links. The VPN should be configured so that it must be used for all WLAN devices and so that all wireless traffic goes through a VPN device before entering the corporate network.

WEP was the first security specification introduced to address the inherent insecurity of WLANs. Shortly after the introduction of WEP, researchers began to publish papers indicating weaknesses in its encryption and message authentication mechanisms. Attack tools used to exploit these weaknesses are now widely available.<sup>6</sup> Improved security options, such as WPAs, have been available since 2003.<sup>7</sup> Widespread implementation of improved wireless security options has been slowed by lack of awareness of the problems with WEP and the fact that WEP continues to be provided as the default option on most wireless hardware.

Despite the known risks, a surprisingly small number of the business networks surveyed by RSA have implemented one of these more advanced forms of encryption – 49 percent in New York City, 48 percent in London and 41 percent in Paris.<sup>5</sup> Also of significant concern is that the cracking of WEP encryption is implicated in the breach of TJX Company's corporate data. It is believed that employee user names and passwords used to log on to the company's central database were intercepted as they were transmitted from wireless devices used to communicate price markdowns and inventory management.<sup>4</sup>

- 
- **Use VPNs for mobile user remote connections to corporate networks from public WLANs or hotspots.** VPN provides the encryption necessary to protect data in transit across public networks but mobile business users should also be educated about the risks presented by rogue hotspots. These temporary access points are set up by attackers and may look like authentic hotspots. Important security information may be gathered from users who inadvertently log on to a rogue hotspot.

Although opinions differ as to the best protection for wireless networks, lack of encryption or use of weak encryption, such as WEP and use of default wireless device configurations, are inadequate protection for business networks that may store sensitive or private non-public information. As the significant costs associated with responding to high-severity breaches is becoming clear, additional legislation that would impose full financial responsibility on companies whose security is breached is being considered. Rapid changes and increased use of wireless technology warrant closely examining your company's technical and procedural controls to ensure that wireless networks are not an open window through which sensitive data can be accessed.

**CNA works with business owners in all industries on technology issues, such as wireless network security. To learn more about how we can work with you to help you mitigate risks, please contact Stephen Douglas at [stephen.douglas@cna.com](mailto:stephen.douglas@cna.com), call us toll-free at 866-262-0540 or view our other Risk Control tools online at [www.cna.com](http://www.cna.com).**

#### REFERENCES

1. Karygiannis, Tom and Owens, Les. "Wireless Network Security: 802.11, Bluetooth, and Handheld Devices." *Special Publication 800-48*. November 2002. National Institute of Standards and Technology. July 23, 2007, [http://csrc.nist.gov/publications/nistpubs/800-48/NIST\\_SP\\_800-48.pdf](http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf).
2. *In the Matter of BJ's Wholesale Club, Inc.* Federal Trade Commission. July 23, 2007, <http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf>.
3. *In the Matter of DSW Inc.* March 7, 2006. Federal Trade Commission. July 23, 2007, <http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf>.
4. Pereira, Joseph. "How Credit-Card Data Went Out Wireless Door." *The Wall Street Journal Online*. May 4, 2007. July 23, 2007, <http://online.wsj.com/article/SB117824446226991797.html>.
5. *Wireless Security Surveys 2007 – London, New York City and Paris*. June 2007. RSA, The Security Division of EMC. July 23, 2007, <http://www.rsa.com/node.aspx?id=3268>.
6. Gast, Matthew. "Wireless LAN Security: A Short History." *O'Reilly Wireless DevCenter*. April 19, 2002. O'Reilly Network. July 23, 2007. <http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html>.
7. Frankel, Sheila; Eydt, Bernard; Owens, Les; and Scarfone, Karen. "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i." *Special Publication 800-97*. February 2007. National Institute of Standards and Technology. July 23, 2007, <http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf>.

The information, examples and suggestions presented in this material have been developed from sources believed to be reliable, but they should not be construed as legal or other professional advice. CNA accepts no responsibility for the accuracy or completeness of this material and recommends the consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situations. This material is for illustrative purposes and is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. Any references to non-CNA Web sites are provided solely for convenience and CNA disclaims any responsibility with respect thereto. CNA is a service mark registered with the United States Patent and Trademark Office. Copyright © 2007 CNA. All rights reserved.  
Tech WRLSART 073107