



## Down to the Wire

*When it comes to wireless networks, technology drives PCI compliance*

By Julie Ritzer Ross

For most merchants, deploying a wireless local area network (WLAN) yields several benefits, such as improved flexibility of POS equipment configurations and enhanced communication between disparate sites. Yet retailers and others with WLANs in place run a greater risk of violating the PCI Data Security Standard (PCI DSS) as criminals target networks to steal credit card information.

“Threats against WLAN systems are evolving just as rapidly as the underlying wireless and system technologies,” says Craig Mathias, a principal with Ashland, Massachusetts-based wireless and mobile advisory firm Farpoint Group. As merchants’ trusted advisors, ISOs can—and should—familiarize themselves with technology-based strategies for safeguarding WLANs and payment data alike.

Implementing “multiple layers” of network protection devices remains key, according to Chris Roeckl, vice president of marketing at AirMagnet, a provider of WLAN security, performance, and compliance solutions in Sunnyvale, California. The layers include intrusion detection systems, automated threat responses, and configurable intrusion alerts. Roeckl deems carefully chosen intrusion detection devices essential because they can play an important role in helping merchants comply with these six of the 12 PCI DSS requirements:

**Requirement 1:** Install and maintain a firewall configuration. Newer-generation intrusion detection systems protect cardholder data by ascertaining that only merchant-authorized wireless devices can access a given WLAN. These solutions also ensure that all devices adhere to a documented security policy that meets industry and legal standards.

**Requirement 2:** Do not use vendor-supplied defaults. Feature-rich intrusion detection solutions can identify when vendor-supplied defaults are effective on wireless devices, which should alert administrators

to security hazards that require mitigation. Such products also can verify whether encryption is used on wireless devices and whether a merchant’s wireless implementation has security vulnerabilities.

**Requirement 4:** Encrypt transmission of cardholder data and sensitive information across public networks. Better intrusion detection devices can determine whether the transmission of data over a WLAN is encrypted and alert administrators if it is not. Just as significantly, they will pinpoint alert administrators to vulnerabilities in encryption implementation.

**Requirement 10:** Track and monitor all access to network resources and cardholder data. Many intrusion detection systems have features to facilitate the tracking and monitoring of all access to a particular WLAN. Most of these products also record such data in audit logs that are stored in a secure, centrally managed database.

**Requirement 11:** Regularly test security systems and processes. Requirement 11 can be satisfied with mutually exclusive technologies, Roeckl says. One such technology is a wireless intrusion detection/prevention system that identifies all wireless devices in use. The other is a wireless analyzer that performs quarterly scans. “Some products include an intrusion detection system that regularly tests security systems and processes on wireless devices and networks, and determines if security vulnerabilities exist,” Roeckl says. “When vulnerabilities are identified, it sends configurable alerts to administrators.”

**Requirement 12:** Maintain a policy that addresses information security. Certain solutions offer compliance reports to help document and maintain a security policy that informs organizations whether their wireless network and devices conform to the PCI DSS standard, as well as other industry standards and legal requirements. Moreover, they allow security alerts to be automatically reported to the individual or

group responsible for security investigation and vulnerability mitigation.

### Maximizing Technology’s Power

Beyond leveraging the capabilities of sophisticated intrusion detection systems, merchants can take several more steps to further maximize technology to limit the risks posed by WLANs, notes Amit Sinha, fellow and chief technologist, Enterprise Wireless LAN for Schaumburg, Illinois-based Motorola Enterprise Mobility Solutions.

Rather than allowing direct Internet access to POS systems, retailers should install a firewall separating the two entities. Similarly, they also should separate payment processing devices from all other systems, such as e-mail and Web browsers. So, too, should Wi-Fi protected access encryption, wherever it is supported.

Sinha also advises default passwords and identifiers on every network management device be changed. And he advocates enabling firewall logs that can hold up to 12 months of information, as well as reviewing firewall rules to ensure unnecessary ports for inbound and outbound device connections have been disabled.

Motorola rolled out the Air Defense Wireless Vulnerability Assessment solution, which it is billing as the first technology to allow remote assess to the security of WLANs from hackers’ point of view. The solution eliminates the need to conduct on-site compliance testing, and assessments can be customized to validate what should be accessible from the wireless side.

“As WLANs take on an ever-greater role, innovative, cost-effective techniques for the proactive and efficient detection, analysis, and remediation of a broad range of threats [will be] essential to long-term success,” Mathias concludes. **TT**

*Julie Ritzer Ross is a contributing writer for Transaction Trends. Reach her at [jritzerross@gmail.com](mailto:jritzerross@gmail.com).*