By Tia D Ilori

WIRELESS NETWORKS

A Customer Loyalty Dream Can Become a Security Nightmare

Wireless technology can provide a powerful leg up when it comes to building customer loyalty within the competitive hospitality industry. For many guests, access to wireless Internet hotspots can be a deciding factor when choosing where to stay. Thanks to wireless networks, guests can speed though the check-in or check-out process rather than enduring lines. Expedited valet parking and the ability to send room service orders directly to the kitchen are two more examples of how wireless technology is being harnessed to enhance the customer experience.

Wireless technology can be a double-edged sword, however. If not properly secured, criminals can steal cardholder data, seriously damaging a business' brand. Data compromises can also carry financial repercussions and invite unwelcome legal or regulatory scrutiny.

This risk is compounded if the hotel or restaurant stores full magnetic-stripe track data, card verification value 2 (CVV2) security codes or PIN blocks, all of which are prohibited by the Payment Card Industry Data Security Standard (PCI DSS) and PCI PIN Transaction Security standards.

Because of the unique vulnerabilities in wireless networks, users should first carefully evaluate the need for the technology and fully understand the risks as well as the security requirements, before deploying wireless solutions.

Regardless of the network's purpose, implementing security controls is a wise course to follow. If wireless technology is used to transmit cardholder data or if a wireless network is connected to part of the cardholder environment (e.g., not separated by a firewall), wireless security features must be implemented.

Common Wireless Vulnerabilities

Data thieves have employed several means of attacking wireless networks and have even documented them on criminal Websites – complete with downloadable software and instructions. Here are a few of their more common methods:

Eavesdropping — An attacker can gain access to a wireless network just by listening to traffic. That guest sitting in the lobby with a laptop or other device may actually be criminal using that equipment to freely and easily intercept radio transmissions. Neither the legitimate sender nor the intended recipient has any means of knowing whether the transmission has been intercepted.

Rogue access — If a wireless network is part of the enterprise network, a compromise in one area can lead to the compromise of the rest of the system. In other words, an attacker can use a vulnerability in the wireless network to gain access to payment data elsewhere in the system.

Data thieves have employed several means of attacking wireless networks and have even documented them on criminal Websites.

Denial of Service (DOS) — Due to the nature of radio transmission, wireless networks are vulnerable to denial-of-service attacks and radio interference. Such attacks can be used to disrupt business operations or to gather additional information for use in initiating another type of attack.

Man-in-the-middle — A criminal can take advantage of an insecure wireless network to launch man-in-the-middle attacks where legitimate Internet traffic is intercepted and rerouted to fake Websites where the criminal can steal data. For example, a customer may use the wireless network to access a banking Website but instead be redirected to a criminal's spoof site that collects the user's personal banking information such as login names and passwords.

Wireless Security Strategy

Hotels or restaurants that have implemented or are considering implementing wireless technology should develop and implement a comprehensive strategy to secure it. Those strategies should ensure that they:

- Have a proper awareness of the security risks associated with the technology.

- Develop risk-mitigation strategies to protect their computing environments — compliant with PCI DSS and the PCI PIN security requirements.
- Evaluate all payment applications against the PCI Payment Application Data Security Standards (PA-DSS) posted on www.visa.com/cisp to ensure prohibited card data such as PINs and codes from the magnetic stripe are never stored or logged after transactions are complete.

PCI DSS for Wireless Networks

Several of the PCI data security requirements are directly applicable for securing the wireless environment. Some are very technical, so work with your wireless vendor to ensure these steps are taken. Details are available at www.visa.com/cisp.

TIA D. ILORI *is the compliance program manager for Visa Inc.*

Basic Precautions

1. Use network segmentation to ensure the payment card processing environment is separate from public networks, including wireless networks. This ensures that if there is a network problem, the issue is isolated.

2. Always change the vendor-supplied defaults. Default passwords for popular wireless devices are well known to hackers and often available on the Internet. Also, change the default service set identifier (SSID) on the wireless access point (AP). An SSID can be easily sniffed and does not supply any security. The SSID should not include a name or company identifier.

3. Implement Wi-Fi protect access (WPA) or WPA2 to encrypt transmissions. Never rely on wired equivalency privacy (WEP), which has well publicized vulnerabilities.

4. Use two-factor authentication for providing access to manage the wireless network. For example, requiring an authorized user to provide a password and as well as answer a security question.

5. Physically secure wireless APs.

6. Perform periodic wireless scanning to identify rogue or insecure wireless access points.