

five SECURITY Issues

ALL HOTEL OPERATORS NEED TO KNOW

The hospitality industry continues to find itself targeted for damaging data compromise events by hackers. This article looks at the top five issues facing hotel operators and what actionable steps can be taken to decrease the likelihood that your business will be stung by data thieves.

1 Remote Access

Many hotel operators and franchisors use remote management applications (RMAs).

Their ease of use in managing multiple locations makes them ideally suited to disseminate business downloads, conduct sales polls or survey inventory. Franchise operators need to be aware, however, that an improperly configured RMA is vulnerable to data compromise attack by hackers. Here are some strategies to help limit that risk:

- **Change vendor-supplied default settings.** RMAs are often packaged from vendors with default or blank passwords (of which data thieves are generally well aware). Creating unique user IDs and complex passwords (preferably unique to each franchise location) can reduce the risk of data compromise and help facilitate compliance with the Payment Card Industry Data Security Standards (PCI DSS).
- **Configure the RMA** to allow connections only from known IP/MAC addresses or configure the system so remote users must establish a virtual private network (VPN) connection via a firewall before access is granted.
- **Only turn on the hotel operator's modem when needed to allow access to franchisors** or payment application

vendors and turn off immediately after services are complete. Consult with the RMA vendor on secure configuration settings.

2 Network Security

Transaction volume, brand recognition and the potential for sensitive data retention are all factors that make hotels (particularly franchise networks) juicy targets for hackers seeking to exploit insecure networks via the Internet. It's important for hotel operators to be aware of these security practices that can help guard against network intrusion:

- **Install and maintain a firewall at all times.** Disabling a firewall can put a business at heightened risk of Internet attacks and potential system compromise.
- **Enable firewall logging and maintain firewall logs for one year with a minimum of three months immediately available for analysis.** These audit trails assist with reconstructing system events, help identify suspicious network activity and are instrumental in facilitating forensic investigations.
- **Implement strong access controls.** Access controls will help restrict inbound and outbound traffic on known ports to only traffic necessary for the cardholder data environment.
- **Routinely examine and secure all systems and networks for unknown and unauthorized software and newly added hardware devices.**
- **Ensure that anti-virus, anti-malware and anti-spyware software programs are up-to-date.**

Investigations confirm that outdated security software is often found at compromised entities. This fact underscores how critical it is to

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

install security software and new updates immediately.

- **Use outside resources to help identify new security vulnerabilities.** Visa provides a frequently updated data security alert listing malware and IP addresses identified in forensic investigations, publicly available at www.visa.com/cisp.

3 Password Management

Hotel operators need to know that passwords, designed to keep criminals out, can also be a vulnerability in the absence of proper controls. For example, Visa has been made aware of several breaches where the default database password was left blank, allowing the criminal trouble-free entry into the database, resulting in the theft of cardholder data. Compromises have also occurred when merchants permit third parties, such as vendors, to access their point of sale (POS) systems remotely for maintenance or support. Hackers subsequently gain unauthorized access through these systems because the vendor used a default password.

Examples of devices and software that use default settings include the following: routers, switches, servers, wireless access points, shopping carts, point-of-sale (POS) software, Web servers and database software.

Take these steps to safeguard against the compromise of account information caused by the use of default settings:

- Check vendor manuals and Internet resources for default settings for all devices and software, and **immediately change the default settings upon installation**. This includes changing default passwords to a unique, secure password and changing default account names to custom names as appropriate.
- **All unnecessary services should be disabled.**
- Merchants should also **ensure that all necessary security functions for all devices and software are activated.**
- **Use the latest version of remote access software** and implement the security features according to manual instructions. See the sidebar for some examples.
- **Use payment applications and versions that have been validated as compliant** with the Payment Application Data Security Standards (PA-DSS), available at <http://www.pcisecuritystandards.org/>.
- **Ensure proprietary or home-grown systems such as a property management or reservation system are compliant with payment application standards.** These commonly used systems should be PA-DSS validated or covered within the scope of a merchant's PCI DSS validation assessment.

4 Wireless Security

Thanks to wireless networks, guests can speed through the check-in process, expedite valet parking and send room service orders directly to the kitchen. At the same time, hotel operators should recognize that criminals can leverage improperly secured wireless networks to steal cardholder data and should implement strategies to thwart these efforts. Have a proper awareness of the security risks associated with the technology. Develop risk-mitigation strategies to protect computing environments—compliant with PCI DSS and the PCI PIN Security Requirements. Evaluate all payment applications against the PA-DSS to ensure prohibited

card data such as PINs and codes from the magnetic stripe are never stored or logged after transactions are complete.

5 Incident Response Plan

Despite all best efforts, data compromise events can occur and every hotel operator should have a plan in place. Prompt action must be taken by hotels or restaurants that have experienced a suspected or confirmed security breach to help prevent additional exposure of cardholder data and ensure compliance with the data security requirements. Those first steps should include:

Immediately contain and limit the exposure.

Minimize data loss. Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. Compromised entities should consult with an internal or payment card industry forensic investigator (PFI) to preserve evidence and facilitate the investigation.

Alert all necessary parties immediately.

First you will contact your merchant bank. If you do not know the name and/or contact information for your merchant bank, notify Visa Incident Response Manager immediately. The numbers and e-mail addresses for regional response management offices are found at the end of this article.

Notify the appropriate law enforcement agency.

Detailed instructions on breach response procedures can be found in Visa's "What to Do If Compromised" document which is available for download at www.visa.com/cisp. The Visa publication "Responding to a Data Breach: Communications Guidelines for Merchants," is available to merchants through their acquiring financial institutions.

TIA D. ILORI is a business leader for Visa, Inc.

Visa Incident Response Manager

U.S. – (650) 432-2978 or usfraudcontrol@visa.com
 Canada – (416) 860-3090 or CanadaInvestigations@visa.com
 Latin America & Caribbean – (305) 328-1713 or lacrmac@visa.com
 Asia Pacific – (65) 96307672 or APIInvestigations@visa.com
 CEMEA – +44 (0) 207-225-8600 or CEMEAFraudControl@visa.com

Use the latest version of remote access software and implement the security features according to manual instructions.

- Ensure that vendors accessing the system remotely change default settings in the remote access software.

- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication or complex passwords for logins.

- Enable encrypted data transmission.
- Enable account lockout after a certain number of failed login attempts.

- Configure the system so a remote user must establish a secure connection through a firewall before access is allowed.

- Ensure the logging function is enabled to monitor inbound and outbound activity.