By Tia D. Ilori

©2012 Hospitality Upgrade
This work may not be reprinted, redistributed or repurposed without written consent.

VET VENDORS to Keep Out Unwanted Guests

The highly complex nature of the hospitality industry's payment card processing environment has made it an attractive destination for the most unwelcome of guests: data thieves. As with any compromise, the brand damage and loss of customer loyalty when cardholder data is compromised can be serious.

As a whole, the industry has taken action to harden its payment processing environment. Despite the increased focus on data security, criminals are still finding ways into hotel and restaurant operators' systems. One important area of vulnerability we have seen exploited has been improperly or insecurely installed payment applications. Improper installation can lead to significant security weaknesses.

If you outsource your payment application and/or network installation and maintenance to a licensed third-party integrator or reseller, make sure you vet your vendor and ask questions to ensure your payment application and network is secure. Ultimately, ensuring the payment card processing environment is secure is the responsibility of the hotel or restaurant operator – not the vendor.

Questions to Ask Your Vendor

If you currently use or are considering using a licensed third-party integrator or reseller, initiate a discussion about how your payment card processing environment is installed and the security measures in place. Asking a few questions of your vendors should ensure the security of your network or alert you to changes that may need to be made. Some examples of key questions to ask appear in the sidebar.

What to Listen For

When listening to the responses there are three key things to listen for:

First, make sure your vendor is providing and installing software that is compliant with the latest version of the Payment Application Data Security Standard (PA-DSS). A list of validated payment applications can be accessed through the PCI Council. Second, make sure your vendor has created strong login IDs and passwords that are unique to your business. You don't want your vendor to use the same passwords across all of its clients or leave the default passwords unchanged. You should also have a strong password policy in place, requiring user passwords to be changed at a minimum of every 90 days and enforce strength criteria such as minimum password lengths.

Third, if your vendor has installed remote management software, make sure it is necessary and ask why. Remote access can be helpful, particularly if a restaurant or hotel has multiple locations that need to be managed centrally. However, it can also create a big vulnerability since a criminal who succeeds in breaking in through one location can potentially gain access to all other systems connected by a central network. Make sure your vendor has properly secured your system by protecting any outward-facing IP address (these are Internet-facing entry points to your network) with a properly configured firewall. Visa highly recommends further bolstering security by restricting connections only to known devices and using strong two-factor authentication, among other things.

Visa Best Practices and Additional Information

Outlined above are three important security areas to discuss with your vendor. We also highly recommend reviewing the complete list of best practices Visa developed for payment application integrators and resellers. These best practices cover in more detail the recommended steps vendors should take to help avoid poor implementation, maintenance and support that could lead to a data compromise.

Help keep unwelcome guests out by insisting that your payment application vendor make your system's security a priority.

TIA D. ILORI is the business leader, U.S. payment system risk, for Visa Inc.

Key Questions to Ask

Point-of-sale Vendors

- Does the payment application store cardholder data?
- Does my network have a firewall installed to protect my point-of-sale system from unauthorized access?
- Can you confirm that you did not use common or default passwords for my system?
- Have all unnecessary and insecure services been removed from the systems and databases that are part of my point-of-sale system?
- Does my payment application receive software updates in a secure manner?

Software Vendors

- How often can I expect to receive patches and how quickly will I be notified of vulnerabilities?
- What are your software upgrade policies?
- Do you deliver patches via a secure method?

Processing Vendor

- Are you PCI DSS compliant?

List of validated payment applications: https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php
List of Best Practices: http://usa.visa.com/download/merchants/bulletin-integrators-resellers-best-practices-04282011.pdf