PCI COMPLIANCE AND THE HOSPITALITY INDUSTRY

EXCERPTED WITH PERMISSION FROM:

THE BOTTOMLINE

THE JOURNAL OF
HOSPITALITY FINANCIAL AND
TECHNOLOGY PROFESSIONALS

FEATURES

PCI COMPLIANCE AND THE HOSPITALITY INDUSTRY

TASK FORCE INITIATIVES WORK TOWARD A CROSS DIALOGUE ON COMPLIANCE

By Katy Walterscheidt

Running over the next five issues, The Bottomline and the HFTP PCI Compliance Task Force feature a series of articles focusing on areas of top concern with PCI Compliance and how it relates to the hospitality industry.

Let's set the scene: It's September 2010 and *Hospitality Upgrade* is hosting its CIO Summit in San Francisco, Calif. Several hotel CIOs casually gather with Frank Wolfe, CAE, CEO of HFTP, and eventually start discussing their frustrations with credit card security in the hospitality industry. They are confused about requirements, frustrated with fines and tired of being the largest target for credit card criminals.

HFTP Decides to be an Advocate for the Industry

You see, 40 percent of all breaches are from the hospitality industry.[1] So someone needed to step up and begin the steps towards addressing the problems that the industry had. That's when Wolfe and then HFTP Global President, Terry Price, CPA, CHAE, CHTP, decided that HFTP could be the advocate that the industry so desperately needed in regards to PCI (Payment Card Industry) compliance.

Soon after the CIO Summit, HFTP announced that it was hosting a Roundtable that would bring about dialogue between all parties involved with hospitality PCI compliance. The ultimate goal would result in a best practices document that both industry professionals and credit card companies could use to better understand how PCI compliance impacts the industry.

HFTP put a call out for those interested in joining the Roundtable. The response was positive and a group was formed. HFTP needed someone to lead the group and Jeremy Rock, CHTP, president of RockIT Group stepped up to the task.

Dialogue With PCI Security Standards Council is Crucial

The first meeting of the Roundtable was in April 2011 in Dallas, Texas. Before the meeting even started, Wolfe and Rock realized that the credit card security issue was a much bigger task than just writing a best practices document. So, the Roundtable turned into a task force full of industry professionals representing more than 7,500 hotels, payment processors, consultants, resorts and QSAs.

Those present at the task force meeting discussed the issues they had with PCI compliance. The task force kept stressing the need for dialogue between the hospitality industry and the PCI Security Standards Council (PCI SSC), the global forum that represents the major card brands. So HFTP joined the council as a stakeholder and has started discussing how the PCI SSC and HFTP can work together on issues that need to be addressed.

One of the main things the task force realized is that PCI compliance for the

Katy Walterscheidt is public relations and social media manager for HFTP and the staff liaison for the HFTP PCI Task Force. She can be reached at katy.walterscheidt@hftp.org.

hospitality industry is much different than other industries. Not only are hotels one of the largest targets for security breaches, but they also have unique situations that credit card companies don't necessarily understand (We'll go into more details about this in a future article here in *the Bottomline*). So an open form of communication between the industry and the credit card brands is crucial to improving security at each property.

Deciding on the 12 Initiatives and Getting Started

The task force eventually came up with 12 basic initiatives that they felt were important to implement for the hospitality industry *(listed at right)*. The initiatives have a wide spectrum of time and effort involved, but some of them were easy for the task force to get started on right away.

First, an online repository was created for PCI compliance on the HFTP web site. Continuously updated, the repository includes links to webinars, best practices tips, a sample Self Assessment Questionnaire (SAQ) and more.

Then, the task force hosted a PCI Compliance Boot Camp at HITEC 2011 in June. Over 100 attendees discussed what PCI compliance means, how to remove card data from their property, best practices for compliance and more. The boot camp was a success and the task force plans to host more in the future.

HFTP and the task force also organized a PCI compliance special focus for *the Bottomline* magazine. That is what you see here.

In each issue — now until June 2012 — you'll find two to three articles dedicated to various topics on PCI compliance. Different experts and task force members will tackle some of the major issues hospitality professionals face with data security like end-to-end encryption, choosing a breach investigator, why the hospitality industry is unique in PCI compliance, the future of PCI compliance and more.

So be sure to check back each issue for more articles.

PCI COMPLIANCE TASK FORCE'S 12 INITIATIVES

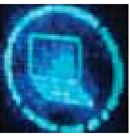
Develop industry focused certification programs	1
Develop an FAQ online forum that is updated frequently	2
Create an educational initiative targeted at owners and executives	3
Create for distribution property staff training materials	4
Develop an industry roadmap for achieving PCI Compliance	5
Educate the industry on the use of encryption technology and tokenization	6
Educate QSA's on hospitality industry technologies	7
Educate regulators on hospitality industry requirements	8
Establish workshops for the Self Assessment Questionnaire (SAQ)	9
Develop a forum to address hotel and management company issues (in regards to multiple party involvement)	10
Foster sharing of info on known threats	11
Publish a current top 10 forensic/QSAs recommendations	12

Plenty More to Come

One lesson learned from the past year is that PCI Compliance is complicated for the hospitality industry. The PCI Compliance Task Force has a long road ahead of them, but they're dedicated to making sure the industry knows how to protect themselves from breaches.

Be sure to keep up with HFTP and the PCI Compliance Task Force as they continue to implement their 12 initiatives. You can start by visiting the PCI Compliance Repository in the Resources section of the HFTP web site and by reading the following articles on PCI compliance.

1. 2010 Verizon Data Breach Investigations Report.



PCI COMPLIANCE AND THE HOSPITALITY INDUSTRY

WHERE THE RUMORS AND MYTHS END, AND THE FACTS BEGIN

By Jerry Trieber, CPA, CHAE, CFE, CFF

PCI Compliance in the hospitality environment requires an infinite number of processes to review and modify, and hefty fines for non-compliance. Manage the task by distinguishing what is important.

A term familiar to many of us in the hospitality industry today is PCI Compliance, which is a realistic goal for every hospitality enterprise. I would say that a majority of us working in areas of finance and technology for hospitality companies have viewed this as a topic top concern, trying to sort through the piles of information passed our way. To help you distinguish what is important, I hope to dispel some of the myths and rumors surrounding PCI Compliance.

The Twelve Commandments of PCI Compliance

Wikipedia.org defines the term *PCI* as an acronym for the "Payment Card Industry," the industry association comprised of "debit, credit, prepaid, ATM, and POS cards and associated businesses." In turn, the term "PCI-DSS" refers to the PCI Security Standards Council's Data Security Standards; the PCI Security Standards Council is the rule-setting body regarding credit card data security. By inference then, PCI Compliance simply means adhering to the PCI-DSS.

At its core, the PCI-DSS are comprised of 12 domains, which I have affectionately termed "The Twelve Commandments" of PCI Compliance. Each domain must be strictly followed in order to achieve PCI Compliance. The first two domains concern building and maintaining a secure network. Specifically they require installation and maintenance of firewalls to protect cardholder data, as well as the use of non vendor-supplied passwords for all hardware, software and other systems where cardholder data is stored, processed, transmitted, viewed or otherwise interacted with.

The next two concern protecting cardholder data and specifically call for the protection of such data through encryption across public networks. The two that follow require installation, use and maintenance of anti-virus software, as well as use of secure information technology systems and applications.

The next three domains concern "implementing strong access control measures" which specifically require that access to cardholder data be restricted on a business "need-to-know" basis, that each person with computer access be assigned unique access credentials and that physical access to cardholder data be adequately restricted. Next are two that require that systems where credit cards are processed are adequately monitored and that access controls are tested. The final domain requires that policies addressing information security be maintained and updated. These 12 domains constitute "The Twelve Commandments" of PCI Compliance.

Jerry Trieber, CPA, CHAE, CFE, CFF is director of field accounting for Crestline Hotels and Resorts, HFTP Global secretary and a member of the HFTP PCI Compliance Task Force. He is also a frequent speaker at HFTP educational conferences and will be speaking on this topic at the 2011 HFTP Annual Convention & Tradeshow.

Be Diligent With Your Data Management

With “The Twelve Commandments” of PCI Compliance in mind, some PCI Compliance items to consider are:

ACCESS

Review who has access to view guests’ complete credit card numbers in the property management system (PMS), point-of-sale system (POS) or gateway software (the “middleware” which captures credit card transaction information from the PMS and POS to send to the acquiring merchant bank). Only those employees with a “business need–to-know” purpose should be able to view guests’ complete credit card numbers in these systems.

IMPRINTS

Review if and/or why credit cards may be imprinted at your place of business, especially concerning merchant bank retrieval request and chargeback information request requirements. It is a myth that merchant banks require imprinted credit card numbers in order for merchants to “win” a chargeback, so stop this unnecessary practice.

STORAGE — PRINTED DOCUMENTATION

Review proper storage of registration cards (for those enterprises using paper-based processes). Under PCI, as well as federal and local privacy laws, any printed document containing personal or other private data must be physically secured with access adequately restricted at all times.

STORAGE — AUTHORIZATION BINDERS

Review where front office employees maintain “credit card authorization binders” and forms used for third party billing authorizations. If these forms are easily accessible in an accordion file, binder, bucket or other container at the front desk, then PCI Compliance may have been violated. All cardholder information must be secured, whether on paper or in a computer system.

STORAGE — SALES AND CATERING

Review where sales and catering files are stored. Do these files contain credit card information? Often, these files may contain “sticky” or other note papers where complete credit card numbers may be in written form. Note, that this is a violation of PCI rules if this information is not under lock-and-key.

STORAGE — ELECTRONIC DATA

Review sales and catering electronic systems (such as Newmarket/Delphi and SalesPro). Are credit card numbers entered in notes, comments or other such fields? These fields are not encrypted, rendering any credit card data stored in such fields accessible to hackers or employees to pilfer credit card numbers or other personal data. Credit card data must only be entered in the fields designated for such purposes in these systems.

PASSWORDS

Review if credit card data or access credentials (computer passwords) are written on a sticky note placed on employees’ computer monitors. How many times have we walked around our sales, catering and accounting offices and paid attention to the notes that abound? Passwords and other information shouldn’t be in plain sight or easily obtainable, shared or learned (by others).

SPECIAL THANKS: EXPERT REVIEWERS

The Bottomline would like to express gratitude to the following industry experts who reviewed the articles for the PCI Compliance series published in this issue.

John Edwards
Regional Director of IT, East
Dolce Hotels & Resorts

Mark Haley, CHTP
Managing Partner
The Prism Partnership, LLC

Ron Hardin, CHTP
VP of Technology
Davidson Hotels and Resorts

Separating Facts From Myths

As we can see from the above items, PCI Compliance requires a multi-disciplinary approach. Accounting, IT and operational employees must all work together to implement and maintain the requirements of PCI Compliance. However, since there is a multitude of information in the public domain regarding PCI Compliance, and since PCI Compliance requires a multi-disciplinary approach, how can the facts be separated from the myths and rumors?

MASKING NUMBERS IS ENOUGH

One myth concerning PCI Compliance is that if an enterprise's PMS or POS masks (hides) all but the last four digits of a credit card number, then the PMS or POS is PCI Compliant. Masking credit card numbers is only a small part of PCI Compliance and is guest-facing (external); the PMS or POS may not be storing data internally in a compliant manner.

ALL PMS/POS ARE COMPLIANT

Another myth is that PMS or POS vendors only sell systems that are PCI Compliant. Hotel, restaurant and other franchise brands may contact non-compliant hotels, restaurants and other businesses, as may vendors. Both may upsell items not needed or use lingo unfamiliar or confusing to even the most consummate hospitality financial and technology professional. In addition, upgrades or updates required to make a PMS or POS PCI Compliant are borne by hotel and restaurant owners, not by management companies or franchisors. Check the site: *pcisecuritystandards.org* for the only authoritative list of products and versions certified as compliant.

There is no "de minimus" valuation for the volume or dollar amount of credit card transactions required for PCI Compliance; even one credit card transaction for one dollar requires the credit card accepting-entity to be PCI Compliant.

COMPLIANCE IS COSTLY

A third myth is that PCI is costly. Although there are monetary and labor costs associated with becoming PCI Compliant, credit card issuers have fined merchants for non-compliance in amounts far outweighing compliance costs. These fines may start relatively low ($20 per month for failing to submit a required self-assessment questionnaire, network scan or other documentation of PCI Compliance), but can quickly escalate to the tens and hundreds of thousands of dollars, and even to the inability to accept credit cards for payment. In the event of a data breach, these fines, penalties and costs can escalate nearly exponentially, as can the loss of one's business reputation.

Personally, I have known hotel organizations to be fined in excess of $400,000 for PCI Compliance violations. In 2009, TrustWave SpiderLabs reportd 38 percent of investigated breaches were in hospitality; in 2010, Verizon reported 40 percent.

SYSTEMS ARE SECURE

A final myth is that hospitality technologies and systems are fairly secure and are not often breached. Unfortunately, this is one of the biggest myths. On September 9, 2010, HEI Hotels warned of a data breach affecting 3,400 customers: a PMS at a New York hotel, as well as POS systems at other hotels were breached between March 25 and April 17, 2010. In addition, on March 1, 2010, Wyndham Worldwide announced its third hack in less than 12 months.

Separating Facts From Rumors

As with myths, so too are there rumors concerning PCI Compliance.

PCI COMPLIANCE IS REQUIRED

One rumor surrounding PCI Compliance is that if a business entity (hospitality or otherwise) accepts credit cards as methods of payment, then that entity is required to be PCI Compliant under their merchant agreement. This rumor is not a rumor, but a fact. There is no "de minimus" valuation for the volume or dollar amount of credit card transactions required for PCI Compliance; even one credit card transaction for one dollar requires the credit card accepting-entity to be PCI Compliant.

FRANCHISES HANDLE COMPLIANCE

Another rumor surrounding PCI Compliance is that if a hospitality enterprise is a franchisee of a brand, then PCI Compliance is handled by the franchisor and, consequently, PCI Compliance is guaranteed. As we discussed above, this rumor is indeed a rumor. Levels of PCI compliance vary by brand and management (corporate vs. franchised locations). Each hospitality enterprise must be certified independent of brand requirements. Brands handle their proprietary systems (PMS, POS), but owners must bear the costs of upgrading to the most current "PCI Compliant" versions of those systems. The merchant, in this case the hotel, is always responsible for the costs of compliance or non-compliance.

As we have seen, PCI Compliance in the hospitality environment requires an infinite number or processes to review, many processes to modify and fines in excess of $400,000 for non-compliance. However, the rewards for complying are priceless.

PCI COMPLIANCE AND THE HOSPITALITY INDUSTRY

EVALUATING P2PE IN THE WORLD OF HOSPITALITY PAYMENTS

By Christian McMahon

Point-to-point encryption and tokenization are still evolving, so understand how to identify the technology with the right fit by understanding all your business processes, asking the right questions, choosing trusted partners and keeping yourself updated.

As every business owner now knows, credit card security is an ongoing struggle and PCI Compliance is only the starting point for data theft prevention strategies. Just like in an arms race, merchants as well as the rest of the players in the payments industry are trying to keep up with the hackers and thieves. Point-to-point encryption (P2PE) and tokenization solutions are responses to the escalating and evolving threats in the payment security landscape. As a merchant you need to understand how these technologies will affect your cardholder data environment and fit into your overall risk management and compliance strategy.

Though P2PE technology has been around for years, it is still early in its genesis in the hospitality payments world. What makes P2PE in our industry so complex are the numerous points where payment card data can enter the merchant environment, the unique lifespan of the payment cards and the number of interfacing systems that make up the merchant environment. For example, a hotel merchant may have front desk terminals, call center reservationists, back office accounting systems, multiple point-of-sale systems and retail/booking web sites. Each of these systems may have different methods of capturing, transmitting and storing payment card data. P2PE solutions will have to be flexible enough to support each point of entry and business process and will no doubt encompass both hardware and software components. *(See the Point-of-Entry diagram on page 33).*

Multiple Points of Destination

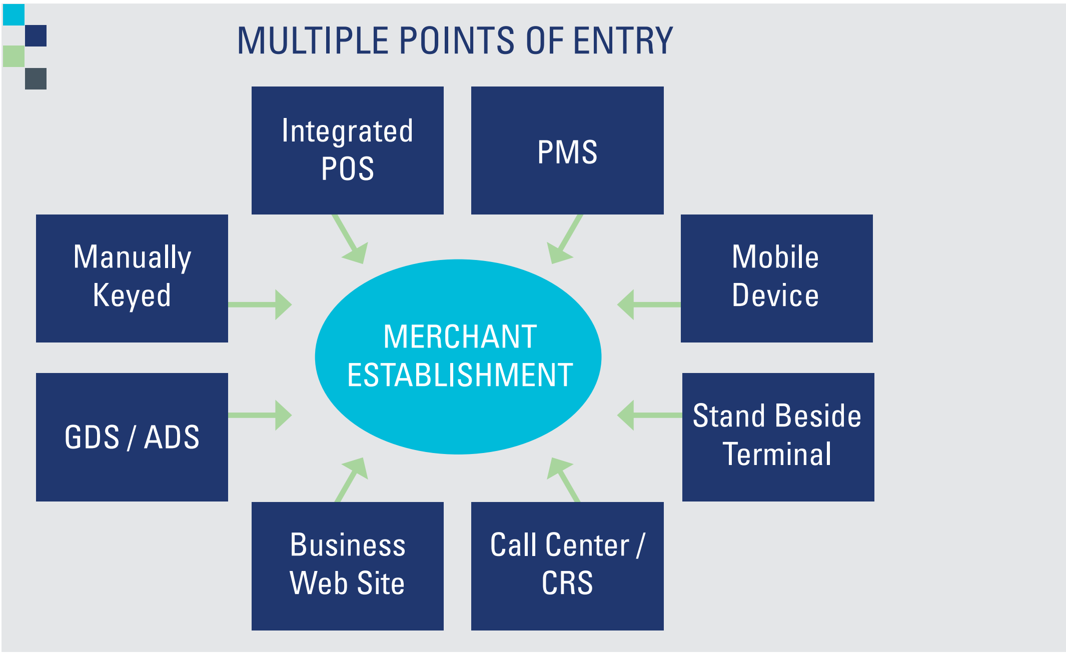
Not only are there multiple points of entry to consider, there are also multiple end points, or points of destination. The term “end-to-end encryption” or E2EE is often confused with point-to-point encryption. E2EE often is thought of on a grand scale and defined as encryption between the local entry point and the merchant’s bank. In reality though, there is no vendor today that covers this entire path. P2PE can be described as encryption from a beginning point to an end point that is connected securely to the back end banking networks. These end points can be interfaced with gateways, processing agents, banks or even the card associations. Because P2PE more accurately describes the solutions in the marketplace today, it has become the standard way of describing encryption services and is the term advocated and used by the PCI Council.

P2PE technologies work to protect and secure payment card data as it is being transmitted through and from the merchant environment. This is commonly referred to as “data in motion.” P2PE places this data in a wrapper that can only

Christian McMahon is product manager for lodging and security solutions at Merchant Link, LLC in Silver Spring, Md. and a member of the PCI Compliance Task Force. He can be reached at Christian.McMahon@merchantlink.com.

be decrypted by an endpoint that has the requisite key. The merchant should never possess or have access to the cryptographic keys or a decryption function that would allow encrypted data to be decrypted. This was pointed out in the “Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance” document issued by the PCI Council in October 2010.

The goal of P2PE technologies is to encrypt as close to the point of entry as possible and guard against thieves who attempt to install sniffing/hacking software on a merchant’s network. For example, in an online transaction, where a software-based P2PE solution is typical, the encryption should occur from the point the payment data is manually entered or received from a third party system. If the payment card data is entered from a call center or a card swipe, a hardware-based solution is typically employed. The encryption should occur as close to or within the device as possible. The encrypted payment data is transmitted to a third party vendor who hosts the decrypting mechanism, otherwise known as the host security module (HSM). At that point, the data goes out to the banking networks for authorization and payment.



MULTIPLE POINTS OF ENTRY

P2PE VS. Tokenization

When evaluating the implementation of a point-to-point encryption solution, merchants need to think about whether encryption alone is sufficient, not only from a security standpoint, but also from a practical standpoint — especially in a hospitality environment.

If P2PE protects data in motion, tokenization is its counterpart and protects data at rest by completely replacing the payment card numbers with tokens that are meaningless if stolen. Tokenization has been defined by VISA as “a process through which Primary Account Number (PAN) data is replaced with a surrogate value known as a “token.” The security of an individual token relies on properties of uniqueness and the infeasibility to determine the original PAN knowing only the surrogate value. As a reference or surrogate value for the original PAN, a token can be used freely by systems and applications.”[1] Layering P2PE and tokenization technologies can appreciably increase overall security while significantly reducing PCI scope.

Determining Your Needs

The PCI Security Standards Council has repeatedly acknowledged the ability of these two emerging technologies to protect cardholder data and reduce PCI burden and recently released guidelines on both tokenization and point-to-point encryption. Not surprisingly, P2PE vendors are offering a wide array of solutions until standards are agreed upon. Solution types include both hardware and software-based solutions, and are being offered by POS/PMS vendors, payment gateways, bank processors and even acquiring banks. A small, independent retail merchant that has limited credit card entry points may have their needs met by a simple, bank-issued, stand-alone encrypting terminal; whereas, a restaurant with both an online ordering site and POS hardware on-site may require one or more solutions. Examining your own environment and creating detailed use cases that outline data flow from initial capture to final payment can arm you with a better understanding of what you need so you can make an informed choice.

Examining your own environment and creating detailed use cases that outline data flow from initial capture to final payment can arm you with a better understanding of what you need so you can make an informed choice.

Finding a Solution

Shopping for a solution can be intimidating, and there is much to consider. The first step a merchant should take after examining the data flow in their own environment is to educate themselves on the various methods and technologies that are available. A good place to begin is by reading "Initial Roadmap: Point-to Point Encryption Technology and PCI DSS Compliance v 1.0" published by the PCI Security Standards Council in October 2010[1]. It describes in detail what to look for in a P2PE system.

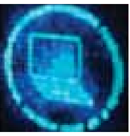
As a second step, merchants should ask their POS/PMS vendor if they are working with any companies to provide P2PE and tokenization and if those solutions are integrated or non-integrated into their POS or PMS system. Integrated solutions may require extra steps at set-up and installation, but offer greater functionality; whereas non-integrated solutions may be easier to install, but restrict choice and ease-of-use. Yet another factor to consider is device functionality, i.e. whether or not the device encompasses swiped cards, manually entered cards, etc. and whether or not the device is tamper resistant, all of which impacts the ultimate price tag.

When evaluating vendor P2PE solutions, ask probing questions such as:

- Is the P2PE solution a hardware or software solution or both?
- Is the vendor well established in the payments industry?
- Does the solution encrypt both swiped cards and manually entered cards?
- Does the solution encrypt online transactions, as well as on-site or card-present transactions?
- Has the vendor solution been evaluated by a trusted Qualified Security Assessor (QSA)?
- Is the P2PE solution integrated with the property management or point-of-sale system or is the encrypting device standalone?
- What happens if the encrypting device fails? What is the fall back scenario?
- Where is the HSM located in the solution? Where is the data decrypted exactly?
- Does the P2PE solution integrate with a tokenization system?
- Can the solution function effectively without tokenization?
- How does the encrypting device handle non-payment cards such as employee cards, gift cards and airline/membership cards?
- How does the vendor secure communication between their network and the merchant's systems?
- Is the solution tamper resistant? What happens if an attempted breach occurs?
- Does the solution support format-preserving encryption? (Format-preserving encryption refers to encrypting in such a way that the output is in the same format as the input, i.e. encrypting a 16-digit credit card number that outputs another 16-digit number. This method will more easily fit with into existing reporting, receipts, and databases.)

In the end, the purpose of both point-to-point encryption and tokenization is security, not PCI compliance. Until there is standardization across technologies to accommodate both encrypting and tokenization technologies, there will be a myriad of solutions and flavors to choose from. Even so, waiting for standardization is not an option for merchants. Thieves won't wait for a unified approach and specification. They are looking for your data now and you need to enter into the technology arena as soon as you can. Doing something is much better than doing nothing. By understanding all your business processes, asking the right questions, choosing trusted partners and keeping yourself updated, you can identify which technologies are right for your business.

1. VISA Best Practices, Tokenization Version 1.0, July 14, 2010, pg. 1



PCI COMPLIANCE AND THE HOSPITALITY INDUSTRY

WHY PCI IS EVEN MORE IMPORTANT FOR HOSPITALITY TODAY

By Bob Russo

Many of the PCI Security Standards Council initiatives of the last year have been to help a merchant understand how to continue to shrink the scope of where card data is present or stored within an organization

Looking back on this past year and all that has been accomplished and needs to be done, my mind is firmly set in the future and the next steps to increasing payment security globally.

We all know hospitality has been hit hard in recent years by credit card breaches and data theft; in fact, it was the most affected vertical according to the *2010 Verizon Data Brach Investigations Report (DBIR)*. Encouragingly though, you've also probably seen the swift action of various hospitality organizations to further educate the industry by coming together and assembling best practices to help protect cardholder data in the future. Here's what we know about the present:

- Cyber criminals continue to attack systems that store credit card data, including point-of-sale and property management systems.
- Many hospitality organizations are "ripe for the picking" due to the high volume of transactions, stored credit card numbers and employees who perhaps have not been properly trained in preventing card fraud.
- A good number of hoteliers believe they are not at risk because they only use applications and systems that conform to the latest PCI Security Standards. However, even software validated against the PA-DSS can be vulnerable if the hotel does not implement or operate them in a secure manner.

I've written previously on some of the ways to establish and propel a PCI program in your business, so I won't get into all of the specifics, but the best way to think about it is, "if you don't need it, don't store it."

I agree this can seem a bit like an oversimplification, but it works on so many different levels, and in fact, this is the basis for many talked about technologies such as encryption and tokenization. This has also been a primary focus for many of the hospitality industry trade groups. Do everything you can to eliminate data. Train your people, create the processes and then look at the appropriate technologies that help you in this effort. In many cases you can replace the data that you currently store or transmit by encrypting or tokenizing the data. This will help reduce the scope of your PCI assessment and simplify your compliance efforts.

Really, many of the Council initiatives of the last year have been to help a merchant understand how to continue to shrink the scope of where card data is present or stored within an organization. The smaller the card data environment (as long as protections are implemented properly), the more difficult it will be for crooks to target and steal this data. The other items I can't emphasize enough when speaking with hospitality organizations include:

Bob Russo is general manager for the PCI Security Standards Council.

Think Security, Not Compliance. That's basically what the first tip is about as well, but this goes further. A report on compliance is a piece of paper; valuable to many organizations, but perhaps less valuable than the peace of mind that you have when you are prepared for ongoing security.

Name an Internal Expert. One of the simplest and most effective means of maintaining ongoing compliance is through a dedicated internal resource. Through this, you can have an individual or team that not only helps prepare for a compliance assessment, but also establishes the protocols to monitor and maintain not just ongoing compliance, but security. Our Internal Security Assessor (ISA) program gives internal champions the training to know what to look for and how to keep an organization on track and within the PCI requirements for the entire year.

Implement a Risk-based Approach. Once you have your internal staff on board, it's time to set your agenda. Whether you are well into your PCI process, or just beginning, a great reference for you to consult is the PCI Prioritized Approach document *(www.pcisecuritystandards.org/security_standards/prioritized.php)*.

The Prioritized Approach provides guidance to help merchants identify how to reduce risk to cardholder data as early on as possible in their compliance journey. The tool groups together the requirements of PCI DSS into six key milestones for merchants to consider in their card data security strategy. This risk-based approach eliminates the biggest vulnerabilities first and allows you to share with your assessors, acquiring banks and the card brands on how you are progressing along your journey.

Make Security Part of Your DNA. Again, this goes to a previous bullet — think security rather than compliance. The PCI DSS is a fantastic foundation for establishing a core group of best practices that can serve as the foundation for your security efforts. Remember, the DSS is the floor, not the ceiling; you should always be looking to build additional layers of security on top of it. This layered approach will allow you to focus on the security part of your business, building it into every business project or activity you commence, and allow you to move beyond a compliance sideshow to one where you are an increasingly difficult target for the bad guys. The more difficult you make it for the bad guys, the more quickly they are likely to look elsewhere.

Resources From the PCI SSC

For our part, I also want to keep you informed on the valuable resources we are assembling and how these can help you alleviate some of the challenges of achieving and maintaining PCI Compliance.

Payments and payment technology is moving at a breakneck speed. We need you to help us address the next five years. To drive payment security forward in the midst of a rapidly evolving payments system, we will have to continue to focus on and listen to where the market is going, such as:

- Mobile guidance, further explore P2PE, cloud, virtual payment cards and new card not present formats and other technologies.
- Advanced malware has also risen to the top of the causes of breaches. We need to help organizations stay on top of a defense-in-depth strategy to counter today's threats.
- We will continue to push efforts for global collaboration, expanding our reach.
- We will need to continue to explore the ramifications of EMV (Europay, MasterCard and VISA) as expansion of that technology increases in new markets.

We'll address these and other issues in the coming years because in the midst of a changing payments landscape, the security of cardholder data must be central. Your feedback is critical in creating and maintaining strong standards for protecting all forms of cardholder data. You will help us shape what the next five years are about and how we incorporate data security in all of these initiatives.

Your peers in hospitality need you. If you've got the expertise, we need you as well. Please send us your feedback and make your industry safer. ■

PCI COMPLIANCE AND THE HOSPITALITY INDUSTRY

FOUR KEY DEFENSES AGAINST HOSPITALITY CHARGEBACKS

By Kirsten Rebello

> *Even with PCI Compliance, a hotel property can still retain the necessary cardholder information to defend against contested charges. Your best defense becomes a matter of modifying your operations to obtain necessary documentation and communicating your policies.*

Chargebacks are costly and can be a significant issue for hotel properties. Many properties are finding it increasingly difficult to protect themselves against chargebacks due to PCI concerns, a variety of payment channels and online bookings where a card is not swiped. With the landscape of payments changing every day, how does a property ensure that they are taking the proper steps to help decrease chargebacks at their business?

In the hospitality environment, there are multiple types of chargebacks that your guests may initiate. They can range from, but limited to, a cardholder disputing a charge for damage, a no show or a late cancellation charge. Whatever the chargeback reason, the losses can impact your bottom line. The best defense against chargebacks are to:

- Understand the frequent chargeback reason codes that affect your business,
- Seek guidance from a payment processor to understand payment brand rules,
- Keep good sales documentation, and
- Implement best practices through your guests' experience that keeps chargebacks from occurring.

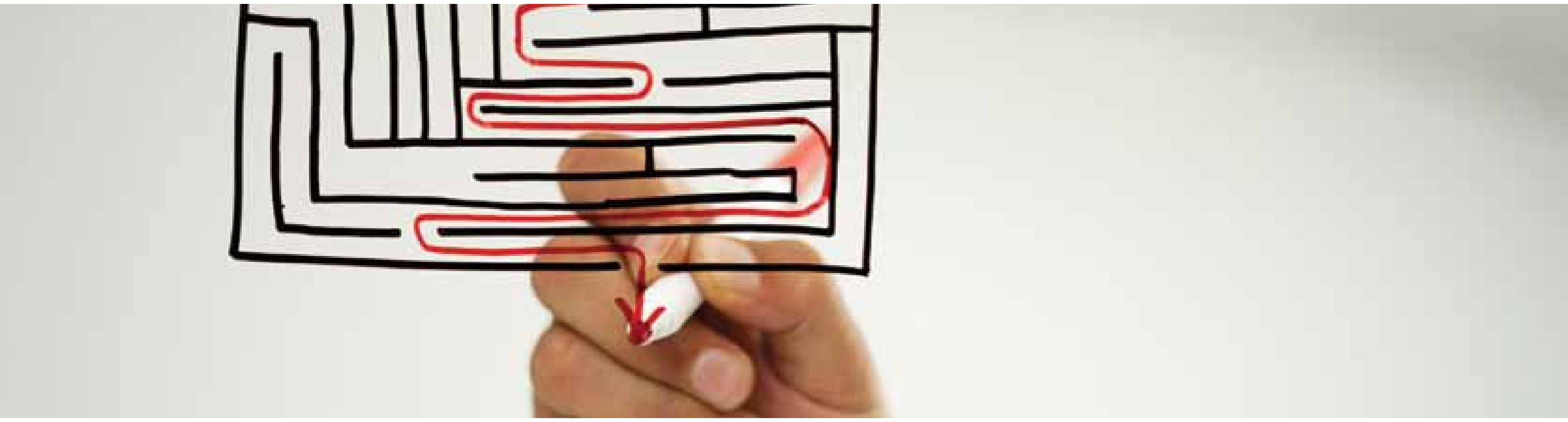
Retaining Sufficient Cardholder Information and Still Be PCI Compliant

Let's first look at PCI requirements. A common misconception within the hospitality industry is that PCI does not allow a merchant to retain cardholder data. The PCI standards do not prohibit the retention of cardholder data. They require that merchants who store, process or transmit cardholder data must implement specific controls to protect cardholder data while in their possession. The PCI DSS is comprised of 12 requirement categories that are grouped under six general headings. These requirements range from removing sensitive card data from your payment terminals, to implementing data security policies for your employees. Those requirements include:

- Build and maintain a secure network,
- Protect cardholder data,
- Maintain a vulnerability management program,
- Implement strong access control measures,
- Regularly monitor and test networks, and
- Maintain an information security policy.

(The complete list can be found at www.pcisecuritystandards.org)

Kirsten Rebello is chargeback manager for Chase Paymentech.



The misnomer in the industry is that you cannot keep cardholder information in order to be compliant, which makes it difficult to defend a chargeback. The truth is that PCI does not forbid storage of key cardholder data that is needed in chargeback processing.

According to the PCI Security Standards Council, only the Primary Account Number ("PAN"), expiration date, service code and cardholder name may be stored after authorization, and merchants must use technical precautions for safe storage. Enough cardholder data can be securely stored to enable hotels to defend chargebacks.

Frequent Hotel Chargebacks and Best Practice Tips

With a secure network, you are able to safely store the necessary data to defend chargebacks; but, you still have to properly manage these contested charges. Here are some frequent reasons for chargebacks and recommendations for handling the situation.

Delayed or Amended Charges. A delayed or amended charge may include room, food or beverage charges, taxes, rental fees and other charges, but must not include charges for loss, theft or damage such as smoking in a non-smoking room. MasterCard® and Visa® state that you cannot retain the right to charge a card at a later date nor recharge a card to collect on a debt. In addition, according to Visa and MasterCard policy, even if the cardholder signed the folio, a property is not allowed to charge a card for loss, theft, damage or smoking charges.

Hopefully the policies that your property puts in place regarding loss, theft, damage and smoking are clearly communicated to your guests to avoid a cardholder dispute. Unfortunately, if you decide to charge a guest after their stay for loss, theft damage or smoking and they initiate a chargeback, you will most likely not be able to defend that chargeback according to the payment brand rules.

Photocopies of Your Guest's Payment Card Are Not a Defense. Many hotel merchants take photocopies of the payment card and it is important to note that this is not the same as an imprint of the card and cannot be used to dispute a charge. In fact, you may get charged a fee from the card brands for doing this.

Disclose Your Cancellation Policy. Your cancellation policy should be legibly printed on all copies of the transaction receipt, reservation confirmation and online reservation site. Proper disclosure must not include a statement that waives the cardholder's right to dispute the transaction with the issuer.

Have a Clear Reservation/Checkout Page. The reservation and checkout screen should include all the cardholder's information along with the reservation information and have an affirmation button on the check out screen that requires the cardholder to "click to accept" all terms and conditions. It is important to note that this may help defend some chargebacks, but cannot be a guarantee against all chargebacks. In addition, MasterCard does not honor the existence of an online contract as defense against a valid chargeback; however, Visa does honor online contracts when properly disclosed.

No Response to a Retrieval Request. It also is important to respond to a chargeback in a timely manner along with providing supporting documentation when faced with a chargeback. When a chargeback is received, the merchant is immediately debited for the amount of the chargeback. In order to rebut the chargeback, the merchant has 39 days from the date of the dispute to send in dispute documentation for representment. From the day of the representment, MasterCard has 45 days to send in a chargeback. Visa and MasterCard have 60 days to send in a pre-arbitration.

There are hundreds of chargeback reason codes and all cannot possibly be addressed within one article. Your best defense is education and understanding how you can modify your operations to obtain necessary documentation and communicate your policies. Your payment processor should be able to help you review the common chargeback reason codes affecting your business along with providing recommendations that can help mitigate associated losses. ■

PCI COMPLIANCE AND THE HOSPITALITY INDUSTRY

COMPLIANCE AND TECHNOLOGY GO HAND IN HAND

By William Collins

By changing the way credit card data is stored, hotels can institute a first line of defense against cyber criminals.

According to the 2011 Data Breach Investigations Report, conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit, the hospitality industry ranked as the most attacked industry, accounting for 40 percent of reported incidents in 2010, with retail and financial services ranking second and third respectively. Simply put, hotels have become the hackers' number one target.

Hackers are this century's bank robbers, using their computers as weapons. Heartland Payment Systems® knows first-hand how dangerous these 21st century criminals can be. In January 2009, Heartland learned it was the victim of a security breach within its processing system during the fall of 2008. Eight months after that discovery, federal prosecutors indicted 28-year-old Albert Gonzales for this crime — as well as for the 7-Eleven, Inc., TJX and Hannaford breaches.

This incident strengthened Heartland's resolve to thwart cyber criminals and the company began leading an industry movement to help protect business owners, consumers, processors and financial institutions.

Why are Hotels at Risk?

Unlike some other industries, hotels tend to keep card data in a number of places. From central reservations, third party partners, the front desk, bar tabs, e-mails, card authorization forms, to sales and catering client files and card imprints, there are simply too many places where card data is vulnerable to theft. Additionally, PC-based point-of-sale (POS) systems and property management systems (PMS), including shared systems among chains, must be properly secured to prevent intrusions.

What is most alarming is that once a hacker has penetrated a POS or PMS, they can remain tapped into the system for days, weeks or even months, undetected. Once they are in the system it is not just guest credit card information that is at risk, but also personal information such as full names, addresses, driver's license numbers and more. While many hotels believe they need to retain credit card data for a variety of reasons, it is precisely the reason they are at risk.

By changing the way credit card data is stored, hotels can institute a first line of defense against cyber criminals. Some practices that hotels should re-evaluate are: card imprinting, credit authorization forms, accounting/chargeback reconciliation and data storage for events and catering clients. Only capturing and storing the payment data when it is absolutely necessary, can immediately lower the risk of that data falling into the wrong hands.

William Collins is executive director of vertical market strategy for Heartland Payment Systems.

Security Through Technology

As data security threats and solutions evolve, Payment Card Industry Data Security Standards (PCI DSS) continue to play an important role in safeguarding card data. In addition to meeting and keeping up with the PCI DSS requirements, hotels should also turn to advanced security technologies like encryption and tokenization.

The marketplace is filled with encryption vendors and products. To ensure hotels are getting and using the most effective technology, it is important to keep the following key features in mind.

End-to-end Encryption. Many technologies encrypt data from point-to-point, meaning information is protected at certain points of the transaction flow, but exposed at others. True end-to-end encryption protects payment card data from the moment it is swiped or hand-keyed, to and through the processing network. This technology scrambles sensitive data before it enters a merchant's system and never stores data on the system, removing the value hackers typically see in these systems. If a cyber criminal does compromise the system, he will find nothing of commercial value, and move on to his next victim.

Hardware- and Software-based Encryption. There is no such thing as safe software. Layered technologies using both hardware and software offer optimal protection for card transactions and start protecting data at the moment of card swipe.

Unique Encryption Keys and Automatic Key Management. Encryption keys, which convert sensitive account information to and from encrypted data, are a critical part of the encryption process; however, many providers share keys among several devices, creating obvious security flaws. If a hacker obtains a key to decrypt sensitive data on one system, and that key is used for other systems as well, he can easily decipher and steal data from the other machines with that same key.

Several providers rely on remote key injection to change encryption keys, which is typically costly and burdensome for merchants. In fact, many believe this to be a major obstacle in the adoption of encryption. With new technology, encryption keys can change transparently and automatically, eliminating the hassle and cost for the merchant.

Tokenization. Tokenization replaces the sensitive cardholder data obtained during a card transaction with a marker — or token — in the hotel's system, enabling management and staff to access the information they need for day-to-day business operations without leaving the full 16-digit payment account number in the clear. As the token takes the place of the original data, it does not allow the entity that stores that information to know anything about the original data or the tokenization scheme.

Unlike encrypted data, the token cannot be reversed to reveal the original data. Retrieving the original data that was replaced by the token requires a database that maintains the relationship between the token and the original data. The data is stored so when hotel staff needs to access this information to issue a refund or for another reason, they can retrieve it.

No Time Like the Present

Making the necessary investment to keep guest card data secure is a must. Although some hotels may worry about the costs associated with new or upgraded technology and wonder whether it is necessary, surely those hotels can ill afford the steep fines and legal fees that come as a result of a breach.

Hoteliers should take the time to review all the products and vendors available to them and beware of those who are eager to capitalize the hotel's need for data security by charging extra security and per transaction fees. With the right technology and security policies, the hospitality industry can take the target off its back. ■

PCI COMPLIANCE AND THE HOSPITALITY INDUSTRY

MINIMIZING DATA STORAGE TO LIMIT COMPLIANCE SCOPE AND EXPENSE

By Chris Zoladz, CIPP, CISSP, CISA, CPA

To manage credit card data storage, identify where it is kept with a credit card inventory, reduce instances where it's recorded and dispose of it securely.

In an effort to reduce the burden and cost of achieving PCI compliance, it is essential to limit the scope of your compliance efforts by eliminating unneeded card data that exists at the hotels. In addition, eliminating unneeded credit card data will reduce storage costs and the risks of the data being lost or stolen, which has costly legal implications in virtually every state in the U.S.

However, before you can eliminate unneeded credit card data you must first identify where it exists. Depending on the size and nature of your operations, the task of creating a credit card data inventory may be straightforward or more complex. You may also need to involve multiple individuals onsite to complete a credit card data inventory. Specifically, you need to think about and identify if credit card data is collected and stored:

- At one or multiple locations (e.g., hotels, corporate headquarters, reservation centers)
- In-person
- Over the telephone
- Via fax
- Online at your web site
- By service providers that you engage (e.g., outsourced web site hosting companies)
- On paper (e.g., via imprint)
- Swiped into a point-of-sale system
- Electronically from a third party travel service or via e-mail
- On backup tapes or other storage devices, either internally or by a third party service provider

In addition, you will need to address your data management. Take a look at the business purposes for collecting the card data and who uses it in the normal course of business. Also review how long the card data needs to be maintained for business or legal reasons, current data retention periods and the approximate volume of credit card data in each repository.

Once you complete this inventory exercise, document the results. There are commercial data inventory tools you can license or purchase to automate the creation of a credit card data inventory and which maintain it over time. However, if the number of locations collecting or storing credit card data is relatively small and not significantly growing or changing, an Excel spreadsheet can suffice.

Avoiding Common Credit Card Collection Pitfalls

Remembering that the compliance requirements apply to all instances of credit card data, having less credit card data in fewer electronic files and hardcopy documents is a top priority.

Chris Zoladz, CIPP, CISSP, CISA, CPA is the founder of Navigate LLC, an information protection and privacy consultancy. He can be reached at chris@navigatellc.net.

For example:

- Do not swipe a customer's credit card into a terminal and also maintain an imprint of the card or other paper record of the card number.
- Do not keep multiple versions or copies of electronic files or paper records that contain a record of a credit card transaction.
- Do not keep electronic files or paper records with credit card data that is old and no longer needed to satisfy business, legal, tax or contractual obligations.

Securely Disposing of Unnecessary Credit Card Data

Now that you have identified credit card data that is no longer needed for business or regulatory purposes, compliance requirements include, among other things, that there are processes for the secure destruction of card data. Generally, you should focus your initial efforts to those areas that contain the most card data, and thus minimize the adverse impact if the data were lost or stolen. Basically, when developing the process, think like the bad guys and realize how important it is destroy the information to the point that it is unrecoverable. But what exactly does that mean?

When it comes to paper, that means cross-cut shredding. You can either purchase cross-cut shredders, or you can contract with a service provider that will do the paper destruction for you. If you purchase your own cross-cut shredders make sure that you have enough of them and they can handle enough volume. This is so that your employees find them convenient to use, and aren't storing up paper at their desk "until they can get to the shredder." Also make sure the size of the resulting paper shred is small enough (usually 5/32" x 1" or smaller) to reduce the likelihood of a full number still being seen.

If you decide to hire a service provider for document destruction, do some research before you sign the company on. You will want the company to complete the destruction on-site at your business (many have mobile trucks). Also, make sure the price includes providing enough locked containers at your facility to store documents between shredding visits. Last, have a certificate of destruction provided, and be sure to keep it on file for 12 or more months.

These same alternatives may also work for information stored on CDs. When it comes to electronic data stored on other types of electronic devices and media (e.g., laptops, computer servers, USB drives) or in user generated files, you will need a special software package to "securely delete" the files with credit cards numbers. If you go to your local computer store, and ask for software that will securely delete electronic files, they will likely ask what strength. You should use software that is Department of Defense strength or close to it. There are also service providers such as Intechra (www.intechra.com) that can securely delete card data from electronic devices or media for you, as well as comply with Environmental Protection Agency electronic device disposal requirements.

> *When developing a process for the secure destruction of card data, think like the bad guys and destroy the information to the point that it is unrecoverable.*

For credit card information contained within packaged software systems, like your point-of-sale system, the capability to securely delete files should be a function of the system. *Don't assume, however, that your system is set up to do that right out of the box.* Contact your dealer, and have them walk you through the settings that need to be configured on your system in order to ensure that when the system deletes a file it is securely deleted from the system, and is not recoverable.

PCI COMPLIANCE AND THE HOSPITALITY INDUSTRY

IS IT GOODBYE MAGNETIC STRIPE, HELLO EMV?

By Bob Lowe

While EMV technology continues to become more wide-spread, it does not guarantee increased security at the back end

In August of 2011, Visa announced the expansion of its Technology Innovation Program (TIP) to include merchants in the U.S. The announcement referred to the evolution of point-of-sale (POS) payment infrastructure from static magnetic stripe to intelligent devices, such as Europay MasterCard Visa (EMV) chip cards and near field communication (NFC) devices like mobile phones. MasterCard has since made a similar announcement. Does this signal the end of the magnetic stripe reader in U.S.-based hotels? To find the answer to that question and understand what TIP is, we need look no further than its identical twin — EMV.

Meet EMV

EMV technology (created by the card associations and promoted and administered by their proxy company, EMVCo) is designed to replace a payment card's magnetic stripe with an embedded chip. The chip is read from and written to during a payment transaction. When countries make the transition to EMV, it is usual to include both a magnetic stripe and a chip on payments cards to ensure they can be used at any merchant location.

The driving force behind EMV is the belief that EMV is more secure. EMV technology's claim to better security rests on the premise that cards using EMV are very difficult to replicate illegally. Making a copy of a magnetic stripe card is easy by comparison. Advocates of EMV also state that EMV reduces fraud because a chip-enabled card never leaves the customer's hand. Rather than handing a card to a guest attendant who then swipes it through a reader, the guest inserts the card themselves and, if required, enters their PIN.

What EMV does not do is guarantee that the information exiting the back of an EMV terminal is any more secure than what comes out the back of current U.S. PIN debit/signature capture terminals. Both typically transmit clear text card numbers with an encrypted PIN block.

Adopting EMV

While it's expected that all merchants will be supporting EMV chip-enabled cards by 2015, it's not clear at what point the magnetic stripe will disappear. Payment industry experts predict the magnetic stripe to be removed from cards by 2015. We believe that process will be slow, given the large U.S. payment infrastructure. It's our view that EMV terminals will be first adopted in the U.S. by retailers, followed by those in F&B. Hotels will be late adopters.

Bob Lowe is vice president of business development for Shift4 Corporation. He is also member of the HFTP PCI Compliance Task Force.

When EMV chip-enabled cards are introduced into a country, Visa typically enacts a policy change that shifts fraud liability from Visa to the merchant. This shift only occurs where the fraud could have been prevented if the merchant had EMV in use. This strategy — which decreases Visa's liability — also accelerates adoption.

To further accelerate adoption, the card associations have stated that if at least 70 percent of a merchant's transactions in a single year originate from a device that is chip- and NFC-capable (which device providers are obliged to offer), then the merchant does not need to perform a Payment Card Industry Data Security Standards (PCI-DSS) audit that year. This doesn't mean the merchant can abandon attempts to be PCI-compliant — it simply means they won't need to be audited. As only Level 1 merchants (those merchants who perform more than six million Visa or MasterCard transactions in a year) need to perform an external audit anyway, that accommodation may not have much real benefit.

As it is currently implemented in Canada, EMV provides no way of determining if a transaction will complete as a debit or credit when it is started. It's only during the transaction itself that the determination is made. As we all know, the adoption of support for debit in hotels has been slow in the U.S. because debit does not support the incremental authorization flow that hotels use. Instead, a debit transaction on a guest folio at the time of check-in is an immediate payment with no ability to adjust the amount during a guest's stay. Most property management system (PMS) vendors will need to add support for debit transactions and be able to adjust transaction types after completion. Considering the system design of several PMS products, this process will be complex.

Fixing EMV

What hoteliers are really looking for is a way to reduce their PCI compliance burden and it doesn't appear that EMV will be helpful in that regard. But, there are other technologies that the PCI Council has published information about that are helpful: tokenization and point-to-point encryption (P2PE).

PCI-DSS has very strict regulations regarding the storage, processing and transmission of sensitive cardholder data (CHD) that tokenization and P2PE address very well. Tokenization and P2PE remove the PAN from the hotel merchant environment, store it in a secure place and return a piece of data that has no use in any other setting for the PMS to reference. When tokenization and P2PE are in play, tokens and encrypted data — not CHD — are what is stored, processed and transmitted by the merchant.

When properly implemented, the blend of P2PE and tokenization can dramatically reduce the hotel's PCI burden as it would no longer store, process or transmit sensitive card data. With P2PE, encryption can take place inside a magnetic stripe reader and sensitive data is passed all the way through a hotel's merchant environment without being decrypted. This means the hotel's PMS application is no longer a PCI payment application and neither is any computer or network within the business. That's the PCI nirvana hoteliers have been seeking. Smart hoteliers will move to solutions that include P2PE and tokenization ahead of supporting EMV so that their IT personnel can focus on guest-facing and revenue-generating initiatives rather than PCI-driven strategy.

EMV Endgame

We expect to see the emergence of EMV payment devices that also support P2PE through the use of encrypt at head technology. This will allow hoteliers who have already successfully removed card holder data from their environment to continue to enjoy their life after PCI status.

Will EMV spell the end of magnetic stripe readers? We believe it could. ■

PCI COMPLIANCE AND THE HOSPITALITY INDUSTRY

HOW TO CHOOSE A PCI FORENSIC INVESTIGATOR

By Jibran Ilyas

Guide to selecting a PFI firm that provides the best service during the investigation, plus questions to ask and clear guidelines on how to move forward after the investigation

The hospitality industry has been targeted by cybercriminals seeking to steal credit card information for years primarily because of the volume of transactions and the potential ability to propagate to multiple locations within the hotel chain. In fact, for the past three years, Trustwave has identified the hospitality industry as one of the top targets for cybercriminals in Trustwave's annual Global Security Reports (2009–2011).

Unfortunately, to-date the hospitality industry as a whole has been slow to identify breaches. In most cases, hotels are alerted after customers call to complain that their card has been used fraudulently or the credit card processing bank alerts the hotel about the potential credit card breach.

How Hotels Are Alerted to Potential Breaches

When a certain percentage of credit cards that have experienced fraudulent activity have been processed through a hotel's payment environment, the payment brands (i.e., Visa Inc., MasterCard Worldwide, American Express, Discover Network and JCB) will flag the hotel as the source of a potential breach and issue a Common Point of Purchase (CPP) report. The payment brands alert the hotel's processing bank, which then contacts the hotel about the potential breach. Regardless of how the breach occurred, the hotel is required to enlist a PCI Forensic Investigator (PFI) to identify the details of the breach and the necessary remediation activities. When processing banks request an official forensic investigation, only the PFIs can conduct the investigation. Additionally, hotels can only use PFI companies that are approved by PCI Standards Council.

There are presently only 15 PFI approved companies around the world. This article will serve as a guide for choosing the PFI in an event of a required forensic investigation by a credit card processing bank.

Considerations for Selecting a PFI

Eligibility. Hotels may have existing relationships with security consulting firms who offer forensic services. Hotels must ensure that the company they select is on the list of approved companies located on the PCI Security Standards Council web site (www.pcisecuritystandards.org).

If they choose a company that is not on the list of approved PFI companies, they will most likely have to repeat the investigation with an approved company, which means increased costs, and potentially degradation of evidence. The bottom line is that it's best to work with an approved company up-front.

Jibran Ilyas is a senior security consultant, incident response with Trustwave. He is also member of the HFTP PCI Compliance Task Force.

Presence. An important consideration for choosing a PFI is where the firm can conduct investigations. This is critical for hotels with multiple locations around the globe. Even if those locations are not on the suspected list, it is possible that attackers may have propagated to them through a Local Area Network. Out of the 15 approved PFI firms, there are two firms that can conduct PFI investigations in all regions. While it is not disallowed to use multiple forensic firms for a data breach, it could lead to confusion and increased costs. It is better to have one firm get a comprehensive picture of the environment rather than multiple firms knowing bits and pieces.

Reputation. Choose a company with experience in the field. The PFI list changes every year so it is important to ask the company how long it has been certified as a PFI firm. The firms that have been conducting credit card breach investigations for multiple years would most likely have many experiences with complex cases.

Also, the credit card processing banks can be asked for recommendations. Many acquiring bank have dealt with credit card breaches in the past and it's likely they have worked with some or most of the PFI firms. Though they don't select PFI firms, if asked, they may provide a short list to choose from.

Hotels should conduct their own research on the PFI firms. Many firms share their breach statistics and white papers on credit card breaches. Also, look to peers in the hospitality industry for advice and recommendations.

Timelines. When a hotel experiences a security breach, they need to act as quickly as possible. Questions for PFI firms include:

1. How long will it take to start the investigation?
2. How long will it take to complete the project?

For a single property, the project start date should be within five days of signing the paperwork, while the project completion should be within a month. The investigation for multiple locations could depend on the complexity of the case. Also, it is the hotel's right to request weekly updates on the investigations.

Most importantly, the PFI firm must allocate time for questions about the breach and its financial consequences, as well as to its reputation. It is reasonable to request weekly calls to align the parties on the investigation.

Reporting and Remediation. PFI firms are required to submit a preliminary report within five business days from the completion of the onsite visit at the suspected property. While additional analysis is required by the PFI firm following the onsite visit, a skilled PFI firm will most often have the ability to discover key information regarding the breach and assist in containment within the first 24 hours of their visit to the impacted location. Therefore, a skilled PFI firm can often assist the hotel in containing the breach prior to their departure.

Completion of the investigation results in a comprehensive final report. The delivery timeframe of this report varies with the size and complexity of the breach. The final report will outline in detail all findings uncovered by the PFI firm per PFI requirements on the PCI Security Standards Council web site (www.pcisecuritystandards.org).

Within the final report, a comprehensive list of completed and outstanding remediation steps will also be documented. In most cases, these remediation steps will mirror PCI DSS compliance requirements. Subsequent to the completion of the PFI investigation, the breached entity will be responsible for fulfilling and validating PCI DSS compliance requirements as quickly as possible. This comprehensive list will assist the hotel in fulfilling their compliance duties.

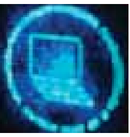
Costs. The costs of hospitality investigations depend on the scope of the investigation. The first thing an investigator will determine is the merchant ID that is experiencing fraud. For example, if the CPP report was called on the hotel restaurant's merchant ID and that restaurant environment is not connected to other areas of the network, then the investigation can be limited to the restaurant environment only and the hotel can save significant costs by not having to investigate outside of that environment.

However, it is very common for hotels to have interface systems that connect the hotel restaurants, spa and other areas within the hotel to a common property management system, so that all charges to one credit card can be consolidated and processed at the check-out time. It is important for hotels to have a complete understanding of the systems that process, transmit or store credit card data so that they can provide adequate information to the PFI firm, which will assist the PFI firm in properly scoping the engagement in order to supply an accurate quote.

The scope of the investigation could also increase based on connectivity with the corporate location and/or other franchisee locations. Hotels should ask PFI firms about the costs in the event of scope increases to encompass multiple locations and systems so that there are no surprises during the investigation.

Disclosure of Information. Per PFI contracts, firms are required to submit reports to the client, as well as the contracted acquiring bank and the impacted card brands. At the time of selecting a PFI firm, hotels should inquire about their data disclosure policy and be comfortable with their policies. Many mature PFI firms have relationships with law enforcement agencies and will share data per the authorization of the client. While it is important to share the forensic findings with law enforcement agencies to catch the attackers, the decision to share the data with any parties other than acquiring bank and card brands lies on the shoulders of the impacted client.

Without a doubt, credit card data breaches are stressful and can be expensive. Hotels should look for a PFI firm that has a great reputation and is capable of handling complex cases. The requirements in this guide are designed to help organizations within the hospitality industry select a PFI firm that can provide them with the best service during the investigation, questions to ask them, and clear guidelines on how to move forward after the investigation.



PCI COMPLIANCE AND THE HOSPITALITY INDUSTRY

COMMON MISTAKES IN DATA SECURITY: PRE-BREACH

By Douglas H. Meal, Esq.

Part I of II

Take an affirmative action approach to data security to reduce the chances of a breach occurring or to minimize the consequences of a breach should one happen.

Part II, "Common Mistakes in Data Security: Post-breach," will run in the August/September 2012 issue.

Data security breaches are both pervasive and expensive — especially in the hospitality industry. It is therefore incumbent on all businesses, but particularly those in the hospitality industry, to take meaningful action to reduce their chances of suffering a data security breach in the first place and to limit their exposure to a data security breach should they be unfortunate enough to suffer one. This topic will be presented in two separate articles. In this issue, I will discuss common pre-breach mistakes; and in an upcoming issue, I will discuss post breach mistakes.

Plainly, the best way for a company to protect itself against the enormous financial and reputational exposure presented by a data security breach is to take affirmative action, before suffering a data security breach, designed to reduce the chances of a breach occurring or to minimize the consequences of a breach should one happen. All too often, however, a company's pre-breach actions actually serve to increase, rather than decrease, either the likelihood of a company's suffering a breach or the company's costs of dealing with a breach should it incur one. In particular, data security breach victims frequently make at least one of the following crucial pre-breach mistakes.

Insufficient Empowerment of and Investment in the IS Function

While some data security breaches result from a hacker's exploitation of a security vulnerability that was neither foreseen nor reasonably foreseeable by the breached entity, in many cases the intruder exploits a deficiency in the information security measures that are in place to protect the intruded-upon network. Insufficient empowerment is best addressed by ensuring the IS function is both separate from the company's IT function and reports directly to a function that sits above the IT function. Insufficient investment is more difficult to avoid, but the best approach for avoiding the human errors that are the lifeblood of hackers is for a company to invest in sufficient IS personnel and technological support to enable the IS function to adopt a "fail-safe" approach to information security implementation, under which separate personnel check, double-check and even triple-check that any given information security measure is in fact being implemented in accordance with the information security plan that is in place. Building a quality assurance component of this sort into a company's overall information security plan would be expensive, and would not eliminate all the isolated human errors that are the source of many breaches, but doing so should substantially reduce the amount of such errors that would otherwise occur.

Douglas H. Meal, Esq. is a partner with Ropes & Gray LLP and a national leader in defending victims against the monetary claims and government investigations that data security breaches invariably generate. This information is general and educational and is not legal advice. For more information, please visit www.hospitalitylawyer.com.

Relying Unduly on an Outside Assessor

Many companies retain outside assessors to evaluate the adequacy of the information security measures that they have in place. As a general proposition, the use of an outside assessor such as a QSA is a wise decision, for the outside assessor may well identify information security deficiencies that the company in question otherwise would have left uncorrected. Having said that, companies that retain outside assessors to evaluate the adequacy of their information security measures often make the mistake of relying on those assessors unduly.

How does a company avoid making the mistake of placing undue reliance on an outside security assessor? The key thing is for the company to understand what sort of assessment it is getting from whatever outside assessor it is hiring. A standard QSA-style security assessment provides very little assurance that the company has adequate information security measures in place (as shown by the many, many companies that have suffered substantial data security breaches immediately after having been certified by a QSA as PCI DSS compliant), so companies should place very little reliance on such assessments from an information security perspective and instead should view such assessments largely as a means of satisfying contractual obligations they may have to conduct such assessments. On the other hand, an outside security assessment that goes beyond the standard review process and instead represents an effort to conduct a comprehensive evaluation of the efficacy, implementation and maintenance of a company's information security plan can be a very effective component of a company's effort to protect itself against suffering a data security breach.

Publicly Touting Your Information Security

Many companies that have suffered data security breaches in recent years made public statements, prior to the occurrence of the breach that they incurred, describing to some degree or in some manner the security measures they had in place to protect the data that wound up potentially being compromised in the breach. But, when a data security breach occurs that potentially compromises the personal information covered by statements of this sort, such statements become a focal point for the plaintiffs' class action bar and the regulatory authorities.

How does a company avoid making the mistake of publicly touting the information security measures it has in place for whatever personal information it is handling? As a starting point the company can eliminate from its web site or any other customer facing materials any discussion, or at a minimum any language that might possibly be construed as a promise or representation, as to the efficacy of the security measures it has in place to protect personal information.

An even more protective approach would be to couple the elimination of such language with a prominent disclaimer of any promise or representation, express or implied, as to the company's security measures regarding personal information. Such a disclaimer would likely enable the company to protect itself not only against the misrepresentation and deception claims described above, but also against the implied contract claims that have recently survived dismissal in consumer class actions stemming from data security breaches.

Not Having the Right Incident Response Plan in Place

The actions a company takes and fails to take in the first days and weeks following its discovery of a data security breach are actions the company will have to live with for months and years as it deals with whatever claims and regulatory investigations emerge from the breach. So what is the right sort of incident response plan? Some companies that do not have a plan go too far in the other direction when they decide to adopt one, developing extremely complex incident response plans that seek to anticipate every conceivable eventuality and control every step of the process of handling whatever eventuality actually occurs. Such plans are of limited value in actual practice, especially in the context of a major data security breach, because they are so cumbersome and rigid that the team handling the breach winds up having neither the time nor the patience to follow the plan.

The best incident response plans strike a middle ground by keeping things simple and keeping things flexible, with their primary focus being:

- Identifying the members of the incident response team, including back-ups for each team member and third-party vendors who can be called upon, such as outside counsel, a forensic investigatory firm and a public relations firm.
- Specifying each team member's role on the team.
- Setting forth a "what may happen" reminder list identifying the issues the team may need to consider depending on the nature and magnitude of the breach.
- Most important, emphasizing the criticality of getting outside expertise (be it legal, forensic or PR) involved sooner rather than later, as they will know immediately from experience how to respond to the particular situation that is being presented, making it unnecessary for the plan to try to anticipate each such situation.

In short, the plans should focus on getting the right team with the right expertise in place and on the ground as fast as possible and then giving that team the flexibility to rely on the team members' judgment and experience in making decisions as to the particular situation that has occurred.

Not Having the Right Insurance in Place

There is a wide variety of insurance products that potentially could cover at least some of the losses that a company is exposed to when it suffers a data security breach. Neither the traditional insurance products nor the newer Cybersecurity products will provide any coverage for losses stemming from a data security breach unless they are drafted so as to provide such coverage. That being the case, to the extent a company wants or expects to be able to rely on insurance coverage for protection in the event of a data security breach, it is incumbent on the company to evaluate its insurance policies before, not after, a data security breach occurs. Such an evaluation needs to focus closely on two distinct issues: coverage scope and coverage amount.

Coverage scope issues. Whether a company is looking at one or more of the traditional insurance products, or a Cybersecurity product, or some combination thereof, it should pay careful attention to whether the policy terms actually cover the potential losses that the company is worried about. One particular area that should be focused on is coverage for the cost of complying with regulatory obligations that are triggered by the breach (such as the state notification statutes) and/or the costs of responding to and resolving whatever regulatory investigations emanate from the breach. Oftentimes neither the traditional products nor the Cybersecurity products are designed to cover such costs, which is problematic given that regulatory-related costs are a staple of virtually every data security breach and hence are exactly the sort of costs that a company would presumably be expecting to protect itself against when it purchases insurance against data security breaches.

Similarly, the company should investigate whether, when a data security breach involves payment card data, the company's policies cover the costs of complying with the card brand rules that are triggered by the breach (such as paying for a card-brand-commissioned forensic investigation of the breach) and/or defending and resolving the breach-related claims for issuer fraud and fraud prevention costs that are customarily made by the card brands. The card brand liability that can result from a data security breach involving payment card data can be quite substantial and is almost always far and away the largest liability generated by such a breach, companies that do not focus on this issue before the fact are often quite surprised and disappointed to find out after the fact that they purchased data security breach insurance that does not even cover the principal liability that data security breaches tend to generate.

Coverage amount issues. A company looking to purchase data security breach insurance must evaluate not only whether the insurance has the right coverage scope, but also whether it has the right coverage amount. The evaluation should be predicated on a thoughtful analysis of the financial exposure that a data security breach would pose for the company, given its particular circumstances. A company's financial exposure to a data security breach depends on a wide range of variables, many of which may not be readily apparent to somebody not well experienced in data security breach cases. Accordingly, companies may want to consider obtaining expert outside advice to assist them in analyzing their potential data security breach financial exposure for purposes of determining the appropriate amount of data security breach insurance coverage they should seek to purchase.

Unfortunately, many companies that suffer data security breaches wait until after they are breached to undertake a rigorous analysis of whether the insurance policies they have in place are broad enough in scope and large enough in amount to protect them against at least a substantial portion of the costs they stand to incur by reason of the breach. By that time, of course, it is too late to adjust either the scope or the amount of whatever policies the company has purchased. All companies are well advised to engage in a rigorous review of the scope and amount of their insurance policies as they apply to data security breaches and to negotiate with their insurers, before a breach occurs, any adjustments to their policies that may be necessary to provide them with the insurance that they conclude they need and that they may well have thought they were already getting.

Look for part two, "Common Mistakes in Data Security: Post-Breach" in the August/September 2012 issue of *The Bottomline*.

WARNING: OUTSOURCING CAN BE A POTENTIAL SECURITY HAZARD

Be diligent when sharing sensitive data with an outside provider, because ultimately the security responsibility is yours

By Howard Glavin
CPP, CISM, CRISC, QSA,
PA-QSA, CTGA

The decision to outsource an IT process comes about when a business looks to meet specific needs without having to lay out the cost to meeting them in-house. As part of this convenience though, a company doesn't reduce its PCI liability. It fact, it generally increases, since the data is in the hands of additional parties with no contractual PCI compliance requirements forced on them. If you do decide to work with an outside service provider and give them access to sensitive data, be sure to investigate their security measures before you commit. Ultimately it is your company that is responsible for the sensitive data.

Who is Responsible in the Event of a Breach?

Who is responsible in the event of a breach is strictly based on the contract. Normally the card brands contract with the acquirers and processors. The acquirers and processors then contract with the merchants and direct contracted service providers. This part is easy to follow since it is all based on who is contracted to whom.

The next step is a lot less simple to track, as the merchants then contract with other entities for payment processing. These contracted parties are not known to the acquirers or the processors. It is common for these contracted parties to also outsource parts of their business to other service providers. This creates a daisy chain where the end liability to the contract for compliance stops with the acquirer, service providers or the card brand direct contract.

Currently for Report on Compliance (ROC) reporting, all service providers are required to be listed by the card brands. In the European Union these “service providers” are required to become registered agents sponsored by the company that was under contract to the card brands, acquirers or service providers such as processors. The U.S. has a similar process currently not mandated by VISA.

Howard Glavin CPP, CISM, CRISC, QSA, PA-QSA, CTGA is vice president of K3DES LLC.

> *It is incumbent on the company contracting with a provider to understand what the provider is certified for. Generally providers are not 100 percent PCI compliant with all 12 requirements… These partially certified companies don't generally advertise this partial certification on their web sites, nor volunteer what areas they are or are not certified for.*

In short, if your company is the one initiating the contract between the acquirer or processor, then the ball stops with your company. You have to go after the service provider you hired if you can prove or suspect them of allowing or causing the breach.

Outsourced Entities and PCI Compliance

To make it more confusing, a large number of these service providers have enacted PCI Compliance initiatives on their own, and then advertise their efforts to increase business. These service providers come in many forms and varying degrees of PCI Compliance. Generally these companies are broken into the following categories:

- Co-location data centers
- Token development companies
- Call centers
- Niche businesses catering to specific verticals:
    - » Hospitality off hours assistance
    - » Web site management
    - » Vulnerability management
    - » Network management
    - » Vendors for devices
    - » Vendors for applications
    - » Managed service for alert management
    - » Scanning companies
    - » Penetration testing companies
    - » Reservation agents
    - » Tour and cruise agents
    - » Insurance agencies with independent agents
    - » Help desk management
    - » User management
    - » Cloud computing and data storage
    - » Batch report processors
    - » Demographic firms for business growth activities
    - » Bulk mailers
    - » Shared data storage
    - » Others

It is incumbent on the company contracting with a provider to understand what the provider is certified for. Generally providers are not 100 percent PCI compliant with all 12 requirements. For example:

- Co-location data centers that only furnish ping, power and pipe are normally only certified for Requirement 9: Restricting Physical Access; and
- Others in niche markets are generally only certified for Physical Access and a minimum number of other requirements, such as user management.

These partially certified companies don't generally advertise this partial certification on their web sites, nor volunteer what areas they are or are not certified for. The fine print in the contracts will in some cases spell this out. For example, a cloud computing company may advertise that they are PCI compliant. Though, when you do review the contract and/or their actual certification scope, you find the company is only certified for physical protection, such as a co-location data center. All the remaining requirements are the burden of the individual contracting their service.

Risk vs. Reward

The decision to outsource a service for your company is not something that should be taken lightly. If you are only outsourcing to reduce your liability for PCI compliance, you may have actually increased it by involving other companies (as well as the additional companies they may have contracts with) who are not responsible for your customer data. Of course, there is a strategic advantage to outsourcing when you know what you are getting into and what data and processes they can see or impact. In any case, you are the company of record for liability. It will be your company that the headlines site and the company that was breached.

Outsourcing, when entering into this relationship, requires you to know the proper constraints and all the entities involved in your data stream that, in fact, could add to your bottom line. The amount of risk you take with these companies is up to the strength of your contract, and in any case, stops with you as the contractor.

When a company you are considering for outsourcing states they are SSAE-16 (SAS-70) or similarly compliant, this is not PCI compliance and should not be considered to be the same compliance requirements. If the company you are going to outsource with also states they are PCI compliant, investigate further and ask for the scope of the assessment performed by a third party QSA (Qualified Security Assessor) firm or done internally by an ISA (Internal Security Assessor). If they say they used a Self-Assessment Questionnaire (SAQ) and self-filed, be very cautious. They may have filed incorrectly by not knowing what the requirements actually mean, or may have reported a state they were not at when they filed the SAQ.

As of January 1, 2012, MasterCard requires all companies filing as a Merchant Level 1 and 2, Service Provider or Processor need to use a certified ISA or QSA firm for all assessments. Merchants are defined as:

- Level 1: 6 million transactions per card brand per year or if previously experienced a breach.
- Level 2: 1 to 6 million transactions per card brand per year.

Service providers have only two levels and both are required to adhere to the reporting process either using a QSA firm or an ISA that has passed the training and meets the business requirements.

- Level 1: 300,000 or more transactions per card brand per year
- Level 2: Up to 300,000 transactions per card brand per year

The other item to remember about outsourced entities, is that they are service providers who are not under contract with anyone but you in the card data process. Additionally, their cumulative number of transactions is what defines their level.

Remember that PCI compliance requires annual reporting on your anniversary date of your initial filing. For outsourced service providers, if they state they are PCI compliant and more than one year has passed since the initial filing, even if it was restricted to a small portion of the requirements, they are out of compliance.

The Final Word

Choosing to outsource part or all of your business is a decision that carries some risk. If carried out without proper due diligence, it could easily cost your company and have your reputation adversely affected on the front page headlines, when you thought all along that you had contracted it away. ■

NO END-POINT FOR COMPLIANCE

Tactics for maintaining your security initiatives

By Jeremy Rock, CHTP

If you are like most hotels and resorts, you have probably reached your saturation point with regards to PCI compliance. You've been inundated with information over the past few years on what it is and why you need to be compliant. Additionally you've undertaken your own documentation and exhaustive compliance initiatives to ensure that your property is compliant and meets the PCI requirements. More than likely you're at a point where you feel that the time has come to move on to other more important things (Like selling rooms and generating revenues to pay for the PCI compliance initiatives that were recently implemented).

However before you check the PCI compliance initiative off your to-do list, it's important to realize that becoming compliant was simply just the first stage of the requirement — *maintaining* compliance is really what the initiative is about. Reports are starting to emerge of hotels and resorts that are being breached for a second and third time. In the majority of these cases, it has been due to a lack of vigilance as it relates to ongoing compliance efforts.

So what are the things that you need to be concerned with and what should you be doing to maintain your ongoing compliance efforts? While the list is long, the following are some of the key items that you should focus on.

Intrusion detection systems (IDS) and file monitoring. These systems need to be set in place and actively monitored. If the systems are taken offline or the alerts are not followed up in a timely manner, your network could be subject to being compromised. In some cases properties have considered the ongoing expense of these "services" (some of which may be managed externally) to be too costly and have elected to remove them. In these cases, if the alert notifications or exception reports are not being acted upon or being received in a timely manner, the property or organization is at risk of being breached.

Jeremy Rock, CHTP is president of the RockIT Group based in Anaheim, Calif. He is also a speaker at HITEC 2012.

Additionally if the exception reporting tends to be filled with a number of so-called false positive responses, then these non-issues need to be addressed ASAP to ensure that the reporting is effective and concise. By remedying these items, the IT department will be able to focus on the "real" issues at hand, rather than having to sift through the large except reports that tend to get produced from traditional scans.

Changes to the network or systems. Make sure that your systems and network configuration is well documented and the information is stored in a secure, but accessible, location. It is important to document all configuration changes and to ensure that these changes are noted in the stored files. Often properties lose key IT systems personnel and much of the configuration and documentation of the systems is lost with their departure. Often the IT manager or administrator was instrumental in addressing PCI compliance at the property, and the loss of their knowledge base could be extremely detrimental to ongoing PCI compliance efforts. Incoming personnel are at a huge disadvantage when trying to get "up-to-speed" and understanding the system without detailed documentation and network configuration information.

Be careful of temporary changes to the network. Very often temporary changes tend to become full-time modifications, as properties are understaffed from a technical resource standpoint and these temporary fixes have a tendency to become permanent. An example of this is the introduction of a new application that requires that changes be made to the firewall. Unless the permanent solution is engineered in a timely manner, this change will typically become a permanent modification to the network and may affect the overall compliance of the network. Should the firewall or other network changes be permitted, then they need to be documented and their effect on PCI compliance taken into consideration. Reversing firewall changes once an application is in effect, may prove to be extremely difficult to facilitate, especially for a 24/7 environment such as a hotel or resort.

Operational policies and procedures, and the importance of regular staff training. Make sure that new procedures are added, documented and controlled. It is recommended that periodic audits of operational policies and procedures be conducted to ensure that they are being enforced operationally. Changes in personnel often lead to changes in operational procedures and a loss of compliance knowledge by key personnel. It is recommended that staff undergo regular PCI compliance education and training to ensure that the knowledge base is not diluted, and to provide updates to changes within the overall program.

Ensure that password policies are upheld. Use of generic or *stale* passwords still represents one of the easiest ways for the *bad guys* to gain access to your network. Conduct regular audits of your password policy to ensure that they are rotated and changed in accordance with your official company and operational policies and procedures.

Quarterly vulnerability scans. The importance for performing regularly scheduled vulnerability scans cannot be overstated. These scans represent a documented report for specific points in time and ultimately lead to a proactive approach to maintaining compliance. Often they can highlight deficiencies in the network and a proactive approach to correcting these vulnerabilities can prevent future breaches and data compromises.

Evaluation of new data security focused applications and the move to tokenization. Newer technologies that offer enhanced data security to the organization should be continually evaluated and considered as part of an effective ongoing PCI compliance program. One approach that appears to be having tremendous success is that of tokenization. Properties who have adopted the use of tokenization, have reportedly reduced their overall risk of data compromises considerably, as the data no longer resides at the property level. A side benefit to this is the reduced compliance reporting that results from the lack of credit card data being present onsite.

The need for an active PCI compliance officer: The importance of having someone on staff champion the maintenance of an effective PCI compliance program cannot be understated. Without having someone empowered with the necessary authority to track and maintain a compliance program, it is inevitable that the focus on this important issue will lapse. This will put the property at risk of falling out of compliance, or worse yet, suffering an actual breach.

Continue to hold regular PCI compliance meetings and formulate a way to track the compliance program and any required updates. Set goals and measure performance against these goals (e.g. regular virus updates). It is recommended that you work with your acquiring bank or processor to ensure that your property is meeting any new requirements. If required, provide your processor or acquiring bank with the quarterly vulnerability scans and compliance reports.

Scheduled reviews of the Incident Response Plan. Properties should schedule regular meetings with their incident response teams to review the properties response plans and make necessary updates based on new information being made available.

Remember the best way to approach PCI compliance is not to look at the process in terms of having a beginning and an end. Properties and organizations have an obligation to their guests to secure their credit card and personal information. Not only is this their fiduciary responsibility and the right thing to do, but it is also vital long term to the business entity. ■