



So You've Been Breached?

NOW WHAT?

If you are like me I had recently become numb to the barrage of information on PCI compliance from various trade publications, seminars, conferences, credit card processing companies and other sources that were continually pushing the importance of becoming PCI compliant. From application providers insisting on upgrades to their systems to network service providers looking to tighten the security on firewalls and segmenting the networks everyone was pushing their services in the name of PCI compliance. As a result most people have become blasé to the ramifications of not being compliant. Then it hap-

Then it happens— the dreaded call from the bank.

pens—the dreaded call from the bank. “We believe that your systems have been breached and we have multiple sources indicating that

the credit cards being transacted at your property are being compromised.” The response is usually how could this have happened? You think you run a secure and tight ship and the systems are PCI compliant and up to date.

When this information is first presented it hits you like a ton of bricks. What do we do now? Interestingly enough one of your first meetings will be with a security representative from either the acquiring bank or American Express. They will usually outline the key issues facing your property and get you on the right track. You will learn that the breach could have occurred as a result of either an electronic network compromise or through a manual breach in an internal operational policy or procedure. As a result, you will need to tackle the issue from two fronts. One targeting the network and electronic credit card data and the second was targeting operational policies and procedures. They will also provide you with some data of the cards that they believe were compromised at the property. From this the first thing that you do is try to identify where the cards were used and which merchant ID numbers were affected. They will also advise you to obtain the following assistance right away.

1 Hire a certified Forensic Assessment Firm

Once you are known to have been compromised, most card brands and acquiring banks will insist that you immediately contact an officially authorized forensic assessment company that has been officially certified by the card brands, Visa (QIRA), MasterCard (QFI), to have them assist with the identification of where your network has possibly been breached. The number one focus here is to stop the bleeding. You will soon find out that while these firms can be very effective, their services come at a price. Working with a good forensics resource will help to identify the potential breach sooner rather than later. As such, you will need to interview a few firms and make a selection in a fairly short space in time in order that they may begin their scans and assessments. (The one thing that you learn is that until you identify the source of the problem [and perform the necessary remediation work]; your guest's credit cards will continue to be compromised on a daily and real-time basis.) When interviewing the forensic firm, try to ensure that you hire someone with hospitality experience and more importantly one who has experience with remediation work. One thing that you will find out is that while forensic firms will assist with the identification of a potential breach, they usually do not facilitate the remediation due to a conflict of interest. As such, you cannot rely on the forensic firm to resolve/remediate your problems. Also hiring a forensic firm does not necessarily mean that they will be able to locate and identify how the network was breached. The forensic firms will compile a complete report for the card brands and acquiring bank to provide them with a detailed analysis of the network and potential remediation work that will be necessary to bring the property's network into compliance.

2 Hire a certified Qualified Security Assessor (QSA)

Along with a forensic assessment firm, the QSA will assist with performing an in-depth assessment of the overall PCI compliance of the property. They will

look at not only the network aspect of things, but will analyze and follow through with the properties overall operational policies and procedures to ensure that all aspects of credit card and data security are being adhered to. In addition, they will provide a GAP analysis of where the property currently stands with regards to its overall PCI compliance and in many cases offer advice for potential remediation of areas of concern. In many cases, the acquiring bank and card brands will also insist that these assessments be made, especially if the property's merchant level changes as a result of the breach from say a level 4 to a Level 1.

In speaking with Jeff Tutton, president of Intersec Worldwide (an authorized PCI - QSA firm), he said, "It is important that you identify and select a QSA and forensic auditor that has real-world remediation experience and is not simply a check-box auditor." The remediation aspect of a breach is probably the most important aspect of addressing the fallout from a network breach and working with knowledgeable and technically experienced assessors can make a huge difference to stop the bleeding and more compromise of data. To use an oil spill analogy, a compromise of your credit card data through a breach of your network can be likened to the recent oil spill in the Gulf, until the source of the leak is located and plugged, your guest and customer credit card information will continue to be compromised at a potentially enormous rate and the overall health of your business will continue to be at risk.

3 Hire an IT Network Remediation Firm

In most cases network breaches are remedied through the use of extremely knowledgeable hospitality-focused network engineer and IT resources that have extensive hands-on experience working with the various applications and programs. In many cases they actually locate the source of the breaches and have the skills to apply the necessary remediation

Armed With a team Of Professionals YOU Will begin to track down the SOURCE OF YOUR Problems

work. Often times, properties call on outsourced IT consulting firms to assist with the remediation aspect of the credit card breaches. Not only are they familiar with the various applications that are impacted by the breaches, but they are also experienced in the overall operational requirements that are also part of the overall PCI compliance requirements. From a practicality standpoint, the hiring of the IT remediation team is

probably the most important step to take once learning of a potential breach - the sooner you can identify and remediate a breach, the sooner you can stop the fallout from your guests' cards being compromised.

Armed with this team of professional (in some cases high-priced hired guns) you will begin to try and track down the source of your problems. You will need patience as in many cases it is like looking for a needle in the proverbial haystack. In many cases intruders find ways to insert malware into the network whose prime directive is to source and locate credit card numbers. This malware often works in conjunction with custom executable files that once it locates a source of data work to extract the data and upload it to Websites that encourage the mining of this highly profitable data. It should be noted that in many cases the malware and associated executable files are undetectable by most of the current antivirus and scanning software and applications. Additionally while many audits and assessments are focused on the strength of the firewalls and segmentation of the networks, most of the current hospitality compromises involve commonly known and used passwords for many of the network login's and associated applications. In other words, the perpetrators are coming in the front door with an authorized key rather than scaling the fence and breaking in via the back door.

Due to the complexity and in some cases sophistication of the cyber criminals at hand, very often it is the outsourced IT remediation team that locates and identifies the source of the breach and not the forensic assessment team. There are very good reasons for this. One reason is that the outsourced team is familiar with the applications and where credit card information may be stored and in some cases the attacks are random and unless the network is being monitored at a specific time and place, you won't be able to detect the data being compromised. Forensics usually don't have the luxury of monitoring a live network and typically take images of all of the compromised servers with them to ana-

THINGS TO DO TO AVOID A BREACH

Engage a QSA firm with experienced QSA employees to conduct an assessment for your property.

Follow the remediation recommendations and secure your network.

Network segmentation can be painful at first, but is the key to real lasting success.

Review your current policies and procedures for handling credit cards and data and ensure that they are implemented.

Ensure that all of your applications are PCI compliant (PABP or PA-DSS)

Implement an extensive password policy program (This is the major source of problems)

Limit access to the Web and social media for those positions that require access. In many cases hotels have resorted to stand-alone computer that are not attached to the network to facilitate correspondence.

Ensure that you destroy all copy machine hard drives when they are returned from a lease.

Destroy all of the data from cell phones prior to turning them in for a new phone.

Ensure that your antivirus programs and anti-malware are up to date.

lyze the data in a lab. As such, the best approach is to work with all three entities to identify and remediate any compromises.

So this is only part of the story. While all of this research is being facilitated, credit cards and sensitive data continue to be breached. In many cases even when the source of the breach is identified and corrected, you still can't be sure that the problem has been addressed. In many cases the cards take approximately two to three weeks from the time that they are extracted to the time that they are compromised. Then it typically takes another two to four weeks for the fraud to either be noticed on the cardholder's statement or for the card brands to identify fraudulent activity in its use. Basically, this can translate to a fairly lengthy time between when the property was first notified of the breach to the time that the situation was remedied. In the meantime, thousands of dollars are being compromised on a daily basis unabated.

So while the property continues to operate life becomes unbearable for some staff members. Group sales, for example, has to deal with the fall-out from large groups who attended business meetings and

conferences at the property. Almost all of the participants have their cards compromised and the group organizers are looking for someone to be accountable. Daily e-mail correspondence between sales managers can become demoralizing – especially when regular groups continue to be compromised while the forensic team is still trying to locate and remedy the problem.

Operations and rooms directors have to deal with the fall-out from guests complaining about the fact that their bank told them that their card was compromised at the property. Hotel staff members become aware of the issue and internal communication with everyone becomes a key morale factor. At this point, it becomes important to work with a communications specialist to help structure both internal and external communications with staff, guests and potentially the media.

Early on in the process, it is also important to contact your law enforcement departments to ensure that they are aware of the issue and to assist them with trying to address any potential leads with regards to resolving the crime. Due to the nature of credit card fraud, typically local authorities will only get involved if the fraud involves a staff member and is operational in nature. Usually the Federal law enforcement agencies get

PREVENTIVE MEASURES TO AVOID A BREACH:

If you're reading this and your property hasn't been breached, then it may be a good idea to take some preventive and proactive measures to minimize the overall impact should you unfortunately be the target of an actual breach:

Build an emergency SWAT team to contain a potential breach:

Legal Council

Identify a good legal team or resource to advise your property in the case that you are breached. Surround yourself with someone who is familiar with the legal reporting requirements for your state and jurisdiction.

IT Remediation Team

This is probably the most important first line of defense. Identify a qualified IT resource team who is familiar with the hospitality environment and who you can call in to help identify where the breach occurred and try to remediate the problem. Most forensics and QSAs do not or will not offer remediation services,

however some QSA firms do offer these services. It is important to note that not all QSAs are created equal, and it is most important to shut down the breach as soon as possible.

Identify an effective PCI authorized forensic firm

At this point in time, the PCI Council has only authorized 10 companies to perform certified forensic scans. Identify a company who not only has resources that are familiar with the hospitality environment, but who can potentially offer a not to exceed pricing for their services.

Identify an effective PCI Authorized QSA firm

Again the identification of a certified QSA who is familiar with remediation work and who can provide an effective assessment of the overall data security of your network, policies and procedures is of critical importance. Evaluate not only the QSA firm, but also the individual

employee (QSA) sent onsite, to ensure they have both industry and remediation experience. Ask for a resume and references. Check the employee on LinkedIn, Google the name and most importantly check the PCI Council Web site to ensure he or she is active and has a current certification in the PCI Council's QSA database lookup tool.

Retain a Public Relations specialist

Contact an effective PR specialist to consult with any potential fall-out from a public standpoint.

Identify key law enforcement agencies and individuals

Should your network or property be breached, it is likely that you will need to contact local, state and possibly federal authorities to assist with the investigation.

Create an Incident Response Plan (IRP)

Identify the key person in your organization who is responsible for managing and

maintaining the overall data security IRP in case your property is breached.

Ensure that the IRP is reviewed on a regular basis and all contact information is validated to ensure that it is up to date. When was the last time you checked your plan?

Identification of the location of all of your data

Data discovery and classification is an important yet cumbersome activity to facilitate at the best of times. Trying to identify the location of all of your data when you in a compromised environment and you are under extreme pressure is extremely challenging.

Most properties operate multiple systems that are either linked or tied to credit card or guest personnel data. As such it is imperative to identify the location of this information prior to any potential breach to not only protect the information, but also isolate it in the event that you are breached.

involved given the nature of cyber crime and it's far reaching points around the globe.

Managing communications with your acquiring bank and the card brands is extremely important. They need to try and identify the potentially breached cards once this information becomes known as they need to notify the cardholders of the potential compromise and cancel and re-issue the cards where possible. Additionally they like to be kept apprised of all developments and need to know that the property is doing all that it can to address the problem. The more the banks and card brands see the property working with them, the less likely they are to push for large fines and assessments once the incident is over.

Overall the process of undergoing a credit card breach is extremely costly, and can potentially destroy the business entity. The lost confidence from guest's can be extremely difficult to overcome, especially when a property has taken years to build up many of the relationships. The demand on management can be extremely draining when taken into consideration with the other factors affecting the operation of a hotel in a difficult economy. The bottom line is that everyone really needs to take PCI compliance seriously. For all that you have heard about the need to be compliant the last thing you want to go through is a breach.

Lastly the following question was recently posed to me during a PCI remediation meeting: If you were a

criminal which computer would you target to try and gain access to in an organization? The answer may surprise you. It's the executive administrative assistant. It is usually a computer with little or no security, but one that contains the most amount of private and sensitive data from confidential correspondence to access to all key numbers and in some cases social security numbers and corporate credit cards; this is the one computer that could impact management the most. Make sure it's secure!

Remember credit card fraud (especially in the hospitality industry) is one of the fastest growing crimes worldwide. It's not a question of if you're going to be breached but potentially when.

Given the loyalty aspect of the hospitality industry, lost guests and customer revenue could have one of the biggest impacts on the overall business. Lost revenue attributable to compromised guest loyalty could be devastating. Once guests feel that their privacy and personal data have been compromised, it is extremely difficult to regain their trust. As such, the loss of revenues (sometimes permanent) and especially group business can be difficult to replace.

JEREMY ROCK is the president of the RockIT Group, a technology consulting firm specializing in new development and refurbishment projects. He can be reached at jrock@rockitgroup.com.

THE POTENTIAL COSTS

It may surprise you, but the financial impact of a breach can sometimes be far reaching and extremely costly. In some cases they could potentially be catastrophic to the overall business entity. In addition to the list below are the associated damages and fines as well as the damage to customer loyalty:

Resource Costs to Consider

- 1 Cost to determine that a breach has occurred
- 2 Executive management
- 3 Legal Council
- 4 General Resources - personnel resources associated with identifying and researching the individuals and guests who have been impacted by the credit card breach

Hard Costs for Post-Incident Remediation

Criminal Investigation—Certified Forensic Assessment—a minimum of 40-50 hours of investigative research, imaging and detailed reporting

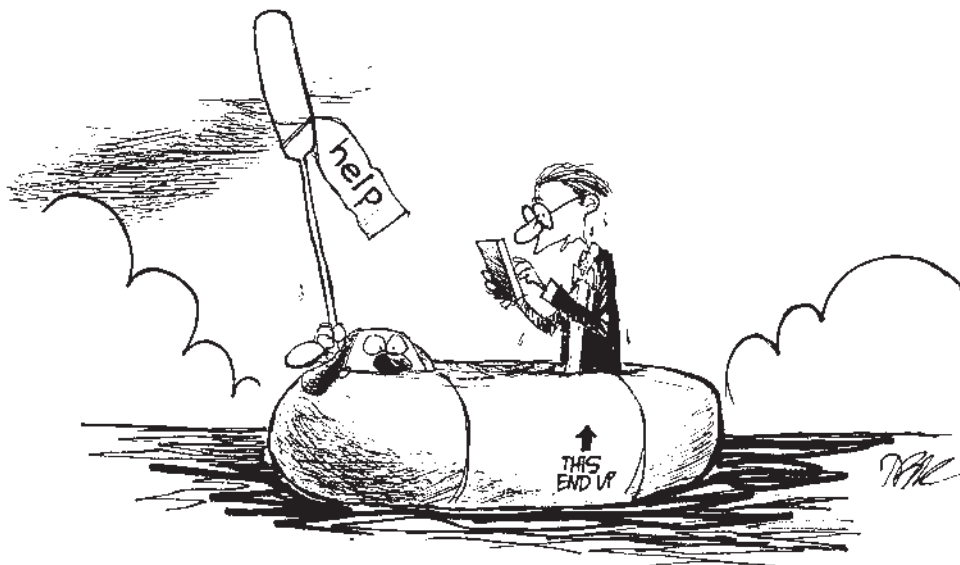
Qualified Security Assessors (QSAs)

Public relations

Customer Notification and cancellation of cards (\$25 a card)

Additional Staffing of the reservation/communications department

Cost of remediation This could be a huge ticket. The cost to remediate could take a while and usually involves outside qualified IT staff and an overall upgrade and securing of the hotel's network with hardware, software and service related costs.



"Good news, Chumley. Thanks to this new app I just downloaded, our hotel is changing tonight's reservation to whenever we wash up AND throwing in extra towels at no charge."