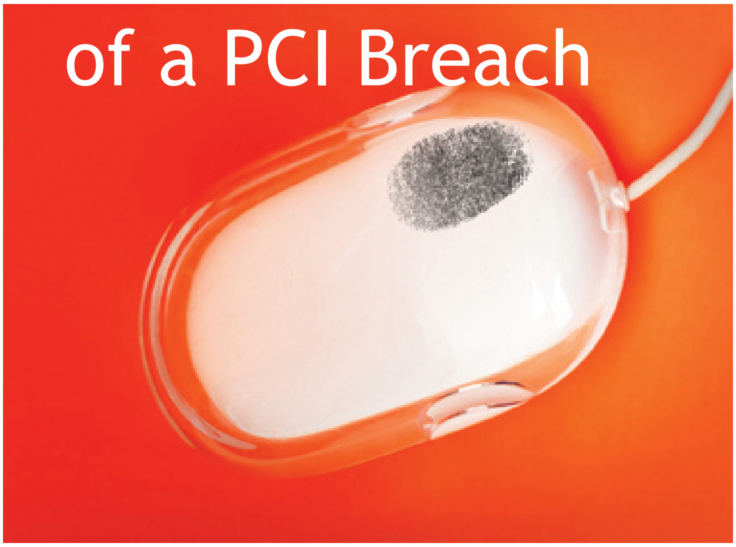
Data Security   By Mark Shelhart

The Forensics of a PCI Breach



As one of the forensic companies responding to PCI breaches, Arsenal Security Group receives hundreds of calls where it has to explain why the bank is requesting a hotel go through a forensic investigation. One of the hardest pills for its clients to swallow is that their hacker is thousands of miles away, and has broken into their POS networks, silently with no indication, bells or alarms.

If you are a regular reader of this magazine, you have seen many great articles explaining the technical side of a hacker's attack, but let's discuss all the people involved in your breach.

The Hacker

Just like a scene from the movies, there are organized criminals sitting on the other side of the world(or further) who spend their days looking for systems to break into. On the average, an attacker's laptop can easily scan 1 million IP addresses in a matter of four hours. Within those million he or she may identify over 900 systems running POS software.

So the hacker may start his day picking a major metro area to attack, out of pure preference, perhaps St. Paul today and Denver tomorrow. Halfway through the hacker's day, he faces the choice of which of the 900+ machines to begin attacking. A favorite POS brand with known default passwords? Or perhaps pick one using remote desktop protocol (RDP) instead of pcAnywhere™. Hackers make decisions of preference.

Hackers don't pick victims by name. They scan MILLIONS of computers a day looking for known PCI weaknesses.

The Executive

Have you just gotten a letter or phone call from your bank describing an account data compromise (ADC) or common point of purchase (CPP) data regarding your hotel? These are the two acronyms that you don't want to ever see, but some readers here may be experiencing this as we read.

First, discuss this matter internally. You may have an incident team, you may not. Round up the need-to-know people, and discuss the matter. Do it quickly, there is a running clock.

Call your processing bank. Not just your account representative, but the fraud team. All major banks have a team that covers ADCs. The letter you received likely has the investigator for your case.

At this point, emotions are at play and stress is high. You may feel as if your bank or the card brands are out to get you. Trust me, they're not.

Tip No. 1: Befriend your bank.

All parties above have common interests with you. No one wants consumers to feel scared to shop. And everyone wants the fraud/attack to stop.

Tip No. 2: Call a PFI company to discuss your incident.

While their motive is to be hired as your consultant, they have a wealth of knowledge that can give you direction. PFIs have the experience of working through hundreds of breaches and can be your tour guide. A good PFI is objective and discreet.

PCI forensic statistics for the past five years have shown that three factors have heavily contributed to compromises:

✗ Inadequate firewalls

✗ Default/weak passwords

✗ Remote control applications

Needless to say, your POS may have rolled off the factory line with any or all of these issues. It is never a pleasant conversation to call a vendor and explain that the company prodcut may be at least partially responsible for your compromise.

IT Personnel

Stay close to your IT staff. There are many different ways they may react, and all of them have implications in your compromise. Many tech folks take this personally. This is normal, but one thing that cannot happen at this stage is trying to cover it up. Deleting data and not sharing details only hurts everyone involved.

Catching the bad guy should not be a goal of IT. The immediate goal is to first identify the size of the breach. If only 30 customers have been breached, do you want to notify 60,000? A good incident plan means maintaining logs and systems so forensic personnel can get a good copy of information. Then work on containment.

Denial or saying it didn't happen at this point is not productive. If your bank has notified you of a potential compromise, there is usually significant research that has already been done. Work with them.

Outside Vendors

This in itself could be an entire article. While we've said trust your bank and the brands, this process often puts the merchant in a conflicted position with its outside vendors, often the POS reseller.

Cause and Effect

You may have no choice but to discuss your compromise with vendors who support you. There are some things you need to do prior to talking with your vendors.

1 **Preservation of evidence.** Just like your IT staff, outside vendors may have a knee-jerk reaction to clean up the mess. If you have to tell your vendors about your breach, preventing vendors from having access to the systems [temporarily] is a good idea.

2 **The blame game.** A vendor's defense may quickly include emails saying, "we told you about PCI" or "we told you upgrades were mandatory." Keeping any written communications is a good practice.

3 **Contract review.** When you bought your POS system, does your contract say who is responsible for security? Who installs software patches? Who changes the passwords every 90 days? Some not-so-nice vendors, even franchises, require merchants to have security settings that are in conflict with PCI. Be careful.

4 **The next guy.** How would you like it if you notified your vendor of a breach and the company's response was, "We heard of this attack before, and your system was compromised three months ago. We cleaned it up." Make sure that your contract says vendors must notify you of security issues involving your system. PCI rules are very clear on when vendors are allowed to connect and when they can make changes. You should be holding the keys to the kingdom (and for good reason).

The Others

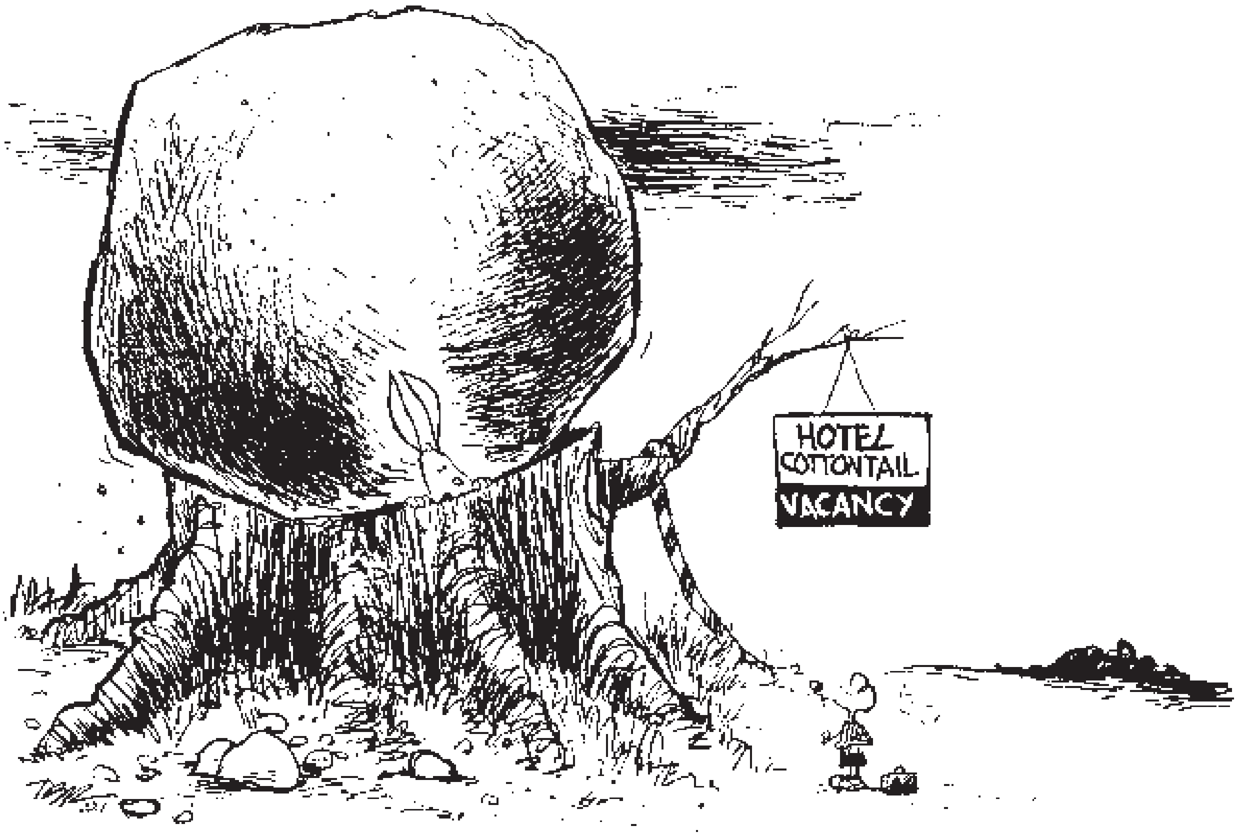
Other people are going to be aware of some of the details of the compromise. While it's a good idea to keep things on a need-to-know basis, you should keep track of who has been involved to date. Whether this is outside council or internal IT, keeping a timeline in your notebook is a good practice.

Self or Customer Detection

This article was written knowing that most fraud is detected first by the banks and the brands. If you suspect something has happened in your card processing environment, or a customer has approached you, all the suggestions above still apply. Your acquiring and processing bank is a good first call.

This article touches on the process during a compromise. If you would like to read more, Arsenal Security Group and the PCI Council recommend the Visa document, "What to do if Compromised.' Version 3 was recently released and can be found online: http://tinyurl.com/5dz724

MARK SHELHART is the vice president of forensics and incident response for Arsenal Security Group. Arsenal's PFI team has investigated hundreds of PCI compromises since 2006. He can be reached at (800) 274-5208 or mshelhart@arsenalsecuritygroup.com.



"C'mon, relax. You know, Account Data Compromise is such an ugly term. Our incident team and marketing department would prefer you think of it as a full-scale guest financial info safety evaluation and review event."