Privcap/
CONVERSATIONS
Q3 2015

Cybersecurity:
Protecting Financial Data

Keith Swiat, RSM's Northeast Regional Director, Security and Privacy explains how personal and credit card information is one of the biggest targets of cyber crime, and how merchants can protect customer data.

"With magnetic stripe data, it's a relatively trivial task to take that and transform it into fake cards."

– Keith Swiat, RSM

WITH EXPERT COMMENTARY FROM: RSM

SPONSORED BY RSM

Click to watch video
➜The Real Economy: Investing in Energy

Cybersecurity: **Protecting Financial Data**

Keith Swiat, RSM's Northeast Regional Director, Security and Privacy explains how personal and credit card information is one of the biggest targets of cyber crime, and how merchants can protect customer data.

Keith Swiat
Northeast Regional Director,
Security and Privacy,
RSM

➜BIO

Keith Swiat brings over 20 years of experience in information technology, including 10 years of experience in management and network/application security with strong technical expertise with mobile platforms. He is an advisor on best practices and compliance for software vendors developing mobile/Web/desktop applications. As an active participant in the Payment Card Industry (PCI), Keith has collaborated with standards organizations, merchants and software vendors to create new data security standards and best practices. His proven leadership skills focus on utilizing the individual strengths of team members to build productive and cohesive practices.

CONTINUES ON NEXT PAGE

How big of an issue is cyber security in the financial services industry right now?

Swiat: Cyber security is a very large issue, mainly because companies within this sector have access to very sensitive information that could be easily monetized. And because of that, cyber criminals will continue to put financial services companies on the top of their list as far as organizations are going to attack.

How much money should a financial institution invest in their cyber security?

Swiat: Well, I hate to use the consulting phrase, it depends, but it really does. It's going to take a lot less money to secure a 10 person shop than a 10,000 person organization that has multiple locations. What's more important is to look at what's at risk, at the kind of information that these organizations have and how it could be monetized, and then take that number and feed it back in to see how much an organization should spend on cyber security and security awarenes.

Cyber attacks are not as difficult to perpetrate as they appear in films and television are they?

Swiat: That is probably the most reoccurring theme. Hollywood has really glorified these attacks and breaches in hacking by portraying these crazy guys in black hoodies, going around in dark rooms. But in reality, anybody could perpetrate these attacks. There are tools freely available on the Internet to provide point and shoot functionality. I spend the most time making people aware of how easy these attacks are actually carried out.

On the flipside, isn't it easy to protect your data?

Swiat: It is. The most time and resources spent after creating a security framework within an organization is enforcing and keeping it maintained. There's a simple social engineering attack called piggybacking. That's where an intrude will follow someone into their office after they badge in at the door. If you educate your employees to not allow someone to walk in behind you, that's something that doesn't cost any money.

It really comes down to communicating and helping staff know they are responsible for helping safeguard their organization's information.

What are some of the biggest challenges for large companies with a global footprint after a breach?

Swiat: When you have a geographically diverse company, the biggest challenge is going to be time zone because, even if you have a very well-defined incident response program, you're going to be waking up people in the middle of the night and their ability to make snap judgments or decisions on what to do during a breach might be hindered. When you have these large global organizations, the clock is probably one of the biggest enemies.

Looking at all the legal issues that come into play and all of the regulatory requirements, this can be a huge challenge when you're dealing with every country that an organization does business in, and may require a lot of legal talent to pull everything together.

There's a notion that using one's debit card at a point of sale is more risky than using a credit card. Is that true or a myth?

Swiat: That's mostly a myth. It's easier to breach credit because you're only looking at the magnetic strip on the back. With a PIN debit transaction, you're looking at the magnetic strip and you also have to capture that pin. Also, for debit transactions, they have a specific encrypting key for each transaction.

Where is financial information like credit card data most likely to be breached?

Swiat: It depends on region. In the United States, we have a very high usage of magnetic stripe usage that's

CONTINUES ON NEXT PAGE

> **"With magnetic stripe data, it's a relatively trivial task to take that and transform it into fake cards."**
>
> –Keith Swiat, RSM

not protected or encrypted. When we're talking about credit card information, we see breaches where the attackers are going after large stores of credit card information that is stored on the magnetic stripe that's on the back of our credit card.

For systems that are not secure or not configured to properly safeguard that information, the data that's on the back of the card might be inadvertently stored on a server someplace within the environment, or within the actual point of sale terminals at the merchant. What happens is that, over time, those cards build up and they just amass into a big clear text file worth of credit card information.

The attackers, if they manage to get into an environment and get onto these systems and circumvent any type of physical controls that are on the systems, they could get access to these files that have this credit card information. With mag stripe data, it's a relatively trivial task to take that and transform it into fake cards. And then the attackers can then either take those fake cards and send it to organized crime to perform fraud or they could perform fraud themselves.

Do you know how much money cyber crime costs the country?

Swiat: I would imagine it is quite large because for every breach that's reported, there are probably a hundred breaches that never go detected or reported. There's probably some statistics out there where someone will raise their hand and say, 'I have this dollar amount of what it costs companies,' but that's a really kind of a foolish number to put out there.

What are some of the ways attackers can breach your IT network?

Swiat: What we've seen over the last year is an increasing amount of creativity when it comes to how attackers are getting into environments. These attacks could include many different levels of access. One of the most popular ways that we see people getting in environments is they start with a social engineering attack, whether that's email, like a phishing scam or even physical misrepresentation. You'll see people going into retail establishments, acting like they're part of a governing body or they're law enforcement or something, to get access to the systems in the back room that might have this data.

Attackers are notoriously lazy. They're going to go for the low-hanging fruit. What happens is, instead of attacking the fortified wall that is presented to the Internet, they're just going to hack a human. It's much easier to take advantage of that inherent level of trust that exists between two people when they interact, even if it's through email.

Is it challenging for you to get private equity professionals to realize that they really need to pay attention to securing their electronic files?

Swiat: Yeah, it's always a challenge. It's become easier with some of the very high profile breaches that have come up in the last year or so. That's made our job easier. Still, we have a lot of funds and portfolio companies that might be smaller firms or might be, say, a furniture store out in the middle of Pennsylvania who are like, 'We've been doing this work for 200 years. Who is going to hack a furniture company?'

The attackers are looking for just that kind of attitude. A place that doesn't think that they have much to offer is not going to secure their platform, but they may have something to offer attackers without realizing they do. We see funds take a varying level of control or connectivity into their portfolio companies, and if they have a VPN (Virtual Private Network) line into one of these small companies, that could be breached easily and there's a chance that the breach can move into the fund and then affect other companies as well.

What are the governing bodies that overlook cyber security issues?

Swiat: There are a number of governing bodies, but when we're talking about credit card information, there's an organization called The Payment Card Industry Security Standards Council. They're a group that was formed by five different card plans and they provide a framework and security standards to which all merchants should apply. They also provide security standards for applications handling credit card data, the PIN entry devices, etc.

They form regulations but when it comes to the actual enforcement of the rules, that falls on different parties, such as the acquiring bank. If there is a breach, usually the card brands will see it first in their traffic, or people are calling and reporting fraudulent activity. They'll push that down to the merchant's acquiring bank and then the acquiring bank will enforce the standard from there. ■