Five Observations of Retail Data Breaches

Why Include Encryption?

WINMAGIC®
DATA SECURITY

TABLE OF CONTENTS

RETAIL LANDSCAPE

Retailers have reason to be scared. The spate of data breaches is relentless and unforgiving. In September 2014, Home Depot, which has roughly 2,200 stores in the U.S. and more than 180 in Canada, disclosed it was working with financial institutions and law enforcement agencies to investigate "unusual activity" based on reports that hackers had stolen credit card information from customers. In late 2013, Target revealed a major breach that ultimately was believed to affect as many as 110 million customers – attackers stole credit and debit card information, as well as names, mailing addresses, phone numbers and email addresses. Initially, the U.S. retailer reported losing only magnetic stripe data on 40 million payment cards.

Across the pond, U.K. shoe store Office advised its customers in May 2014 to change their passwords for their online accounts after discovering they suffered a security breach, exposing customers' names, addresses, phone numbers, and email addresses. While the retailer said no financial data was affected, it drives home the fact that many retailers keep customer data, including credit card information, on file forever to make it easier for consumers to return and place more orders.

RETAIL LANDSCAPE

Data breach concerns run headstrong into the reality that consumers prefer plastic over cash. More and more people are switching to debit and credit cards, or even their mobile phones, to pay when they shop. Whether it's grocery shopping, purchasing big ticket items or just buying a coffee, consumers are paying with cards that require a four-digit Personal Identification Number (PIN) or nothing more than a quick tap on a Point-of-Sale (POS) terminal with the assumption their personal data and their bank balances are safe.

Based on front-line experience providing data security solutions for more than 5 million worldwide licenses, WinMagic's executive and engineering teams offer the following observations and lessons for retailers facing the uncertainty created by today's security landscape.

RAMIFICATIONS

The ramifications of these breaches can be far reaching for both the consumers and the retailer. While consumers are generally insured and will recoup money lost to fraudulent transactions, they have to deal with the agony of the process. For the retailer that was breached, it could mean its downfall depending on the breach's severity. If the breach contravened government or industry regulations, there could be serious penalties to the retailer in the form of fines leveled against it and even limitations placed on future business operations. A breach could be the basis of legal action launched by customers demanding significant compensation. All of these scenarios damage the brand of the retailer and lead to lost business over time, eroding the retailer's customer base and resulting revenues. Just doing damage control can consume a great deal of financial and human capital and negatively affect the retailer's ability to run daily operations.

1 BREACHES ARE INEVITABLE

Investigations into recent high-profile breaches show that while they were avoidable, they are representative of an increasingly sophisticated adversary. For example, the phishing email attack, where an end user is tricked by a well-disguised email, has been around for a long time. Yet it is still devastatingly effective, because hackers continue to evolve highly deceptive phishing emails. They might target one specific role within an organization with content that is carefully crafted to appeal to that role.

The end goal of the attack has shifted as well. Recent retail breaches resulted from compromised POS systems, where malware within those systems delivered credit card swipe information back to a server outside the firewall. In one hypothetical scenario, a POS system is compromised after an initial targeted phishing attack tricked a corporate user into downloading malware, getting the hacker inside the retailer's network. From there, the infection would find its way to a target POS system as programmed by the hacker.

It has been speculated if not proven that the Target breach was achieved through a program called BlackPOS installed on POS devices. Further, a Department of Homeland Security report released in August 2014 noted widespread infestation reports from seven POS system vendors of another POS malware known as Backoff, with the U.S. Secret Service estimating that more than 1,000 businesses may ultimately be infected.

The amorphous and advanced nature of today's attacks has caused many IT security pros to face the facts. It's no longer a question of whether they will be breached, but rather when. The cliché of inevitability is profiled in SC Magazine's September 2014 cover story: While organizations are still investing in security products, they are increasingly advised to invest in solutions that identify and remedy an infection, rather than solutions that stop the infection in the first place. And these same IT pros are also increasingly interested in securing the data so that even if it is compromised, it is useless to the thief.

2 DON'T MERELY RUSH TO FIX WHAT CAUSED THE MOST RECENT BREACH

Hackers are often the threats we hear about, either through launching attacks on retailers' information technology infrastructures or through phishing scams that lure consumers via email. Customer data including financial information can also fall in the wrong hands either by accident or because of malicious intent in a number of ways, both at a head office level or a retail location.

If USB devices or other removable media are moving data around, they can easily be lost or stolen. In some cases, the threat can be from a disgruntled employee. If customer data resides on a laptop computer, it too can be lost or stolen, falling into the wrong hands. And with the Bring-Your-Own-Device phenomenon, corporate data, including customer data, often finds its way onto smartphones and tablets. Data in transit through wired and wireless networks can also be intercepted by the wrong people.

IT security pros and c-level executives need to be thoughtful as they see headlines about data breaches. They should take the opportunity to evaluate their entire IT security posture.

3 PCI COMPLIANCE IS NOT NEARLY ENOUGH

The credit card industry aims to help retailers protect their systems with the PCI Data Security Standard (DSS), initially developed by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. The technical requirements of PCI DSS are an excellent start and include implementing strong access control measures, regularly monitoring and testing networks and protecting cardholder data. However, it's clear from recent breach examples that hackers are able to evade the defenses dictated by PCI guidelines.

In truth, many organizations have known this for a long time. A Computerworld story published January 6, 2010 debates the effectiveness of PCI, noting that Heartland Payment Systems—which was the victim of a large credit card data breach a year earlier—had insisted it met the letter of every PCI guideline. PCI compliance is noble, however it does not alter the reality of the current security landscape and the fact that organizations will inevitably be breached.

4 CONSIDER A COMPANY'S RISK MANAGEMENT PROFILE

In addition to rushing to evaluate POS system security and maybe conducting workshops to educate your employees on the danger of phishing emails, retail IT security teams need to evaluate the risk profiles for their systems.

For each of their systems, they should look at how those systems are vulnerable and the probability that a threat agent will capitalize on those vulnerabilities. They should then match high probability of a system compromise with the impact should that system be compromised. Systems that have a high probability of being compromised and a high probability of significant damage being inflicted because of that compromise—are those systems that need to be addressed immediately.

Conducting a risk assessment will identify other security priorities for a retail organization. It follows this logic: The hackers know that companies are rushing to secure their POS systems; they are likely to look for other ways to get into a retail organization.

Following the risk assessment, an IT security team might determine that one particular system could be easily compromised and the vulnerabilities are hard to fix. For that system, full disk encryption might be necessary. For another system with a different risk profile, two-factor authentication might be the answer. The list of possibilities is wide ranging.

5 EVALUATE THE ENTIRE SECURITY POSTURE FOR YOUR COMPANY

In addition to conducting a risk assessment, there are several key ways retailers can work toward better securing customer financial data:

Know where their business is being conducted

A retailer's customer data is spread out across corporate offices and retail locations. Data also resides online and with partners. The larger the retailer, the more locations and more devices. It's essential that retailers understand how and where customer data, especially payment information, is being accessed, handled, and most importantly, how it's being secured.

Identify data at rest

Retailers must remember it's not just customer card data being accessed on an active device such as a POS terminal that must be protected. This information is being held in many locations for customer convenience so they can easily make repeat purchases, as was the case with U.K. shoe retailer Office. Data stored on laptops or portable drives or archived on servers is often forgotten, making it a ripe target for hackers or negligent employees. This data needs to be encrypted when it is at rest so the physical theft of the devices is not a concern.

Locate data in transit

Retailers must have a clear understanding of how customer payment data is travelling through their infrastructure, as well as that of their partners. Sniffers and network traffic monitor software enables retailers to know where customer data has been, where it is going, and most importantly whether or not it is encrypted while "in flight." Technology is available to know exactly which devices are storing customer card data at any given time and allows retailers to adjust their security based on potential threats.

5 EVALUATE THE ENTIRE SECURITY POSTURE FOR YOUR COMPANY

Partner with a security expert

Ideally, retailers should focus on the core business of selling goods in stores or online rather than having to worry about managing security infrastructure. To adequately safeguard customer card data, they should recruit a data security partner who can continuously monitor and implement the most appropriate security strategies for both current and emerging security threats in real time.

Have an encryption policy

In this day and age, encryption should be mandatory, but it must be manageable. Retailers should deploy encryption with 128-bit keys (or stronger) as well as multiple rounds of testing before the policy is implemented. Retailers should be particularly focused on systems containing customer card data, such as POS terminals and other store-based systems. Once deployed, there should be an auditing of a sample of systems. Role-based controls are another critical component of an encryption policy, where only certain individuals at the retailer have the ability to control or access specific pieces of information. Routine and ongoing audits are also recommended to ensure data security and encryption policies are consistently enforced.

MANAGE SECURITY, MANAGE REPUTATION

Implementing a comprehensive security strategy does far more than help prevent, identify and remediate breaches. It means avoiding the ramifications of losing sensitive customer data, including loss of profits, legal action and punitive fines. A well-thought security strategy that includes encryption can grow and evolve with a retailer's business as it expands locations physically or grows its offerings online. It also contributes to a reputation that secures brand loyalty.

WinMagic understands encryption across networks and across devices. Most importantly, we focus on making encryption manageable, which is a key component of making any compliance and security strategy effective.

WinMagic's core product, SecureDoc, is built with the understanding that retailers collect large amounts of customer data, including payment information, as part of their ongoing operations. Storing this information makes it easier for customers to shop and allows retailers to promote sales and special offers, but industry regulations and government legislation mean this data must be protected.

SecureDoc is a complete data security and encryption solution that offers government-grade encryption to protect customer data throughout a retailer's operations. The solution encrypts data without interfering with a retail organization's staff or the customer experience. SecureDoc brings peace of mind to retailers and aids with overall regulatory compliance.

INCLUDE ENCRYPTION

WinMagic provides the world's most secure, manageable and easy-to-use data encryption solutions. With a full complement of professional and customer services, WinMagic supports over five million SecureDoc users in approximately 84 countries. We can protect you too.

WinMagic Inc.
Phone: 905.502.7000
Fax: 905.502.7001

Toll Free: 888. 879. 5879

sales@winmagic.com
www.winmagic.com

Click here to request a free evaluation ›