Ready for Battle

Anticipation and preparation are key to fighting data breaches

by M.V. GREENE

This is the first article in a three-part series examining cyber crime in retail and how the industry is responding. Future articles in this series will report specific benchmarks on the current state of retailers' challenges and techniques retailers can employ to build effective cybersecurity risk mitigation plans.

A "cat-and-mouse" game is a fitting way to describe what retailers are up against in their long-standing war with cyber criminals. Think about it in the context of serial bank robber Willie Sutton: Asked why he robbed banks, Sutton's reported response was "because that's where the money is." In a retail context, cyber criminals might say something similar — retailers' point of sale and card processing systems are "where the payment card data is."

Everyone needs to worry about it, says cybersecurity expert Mark Weatherford, a principal with the Chertoff Group security advisory firm, who calls the threat "almost unprecedented."

No merchant is unscathed: News headlines read like a Who's Who of prominent retail companies that have experienced cyber breaches.

"It really is no longer a question of if you are going to have a cyber event," says Weatherford, former deputy undersecretary for cybersecurity at the Department of Homeland Security. "The question is, when is it going to happen?

"The difference between a company with a good security program and a company with a not-so-good security program is how quickly they can discover that breach, how quickly they can mitigate it and how quickly they can get back into business," he says.

'A RECURRING PROBLEM'

"As long as keeping credit card information is integral to your business, the hackers are going to target you," says Erin Nealy Cox, executive managing director at digital risk management and investigations firm Stroz Friedberg. "The idea of retailers being a target is not just a 2014 problem. It is going to be a recurring problem."

The 2014 Data Breach Investigations Report from Verizon Enterprise Solutions reports that the vast majority of organizational data breaches stem from nine primary threat patterns: miscellaneous errors (such as sending an e-mail to the wrong person); crimeware (malicious software that seeks to gain control of internal systems); insider/privilege misuse; physical theft/loss; web app attacks; denial of service attacks; cyber espionage; POS intrusions; and payment card skimmers.

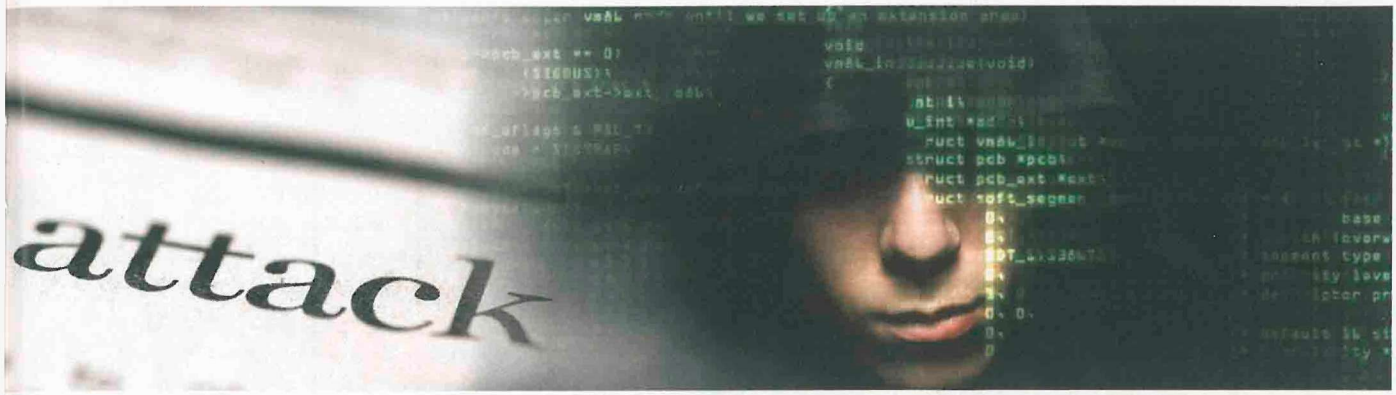
The Verizon study found that only 11 percent of data breaches occur at retailers, compared with 34 percent at financial institutions, but "the industries most commonly affected by POS intrusions are of no surprise," the report says. "Restaurants, hotels, grocery stores and other bricks-and-mortar retailers are all potential targets."

In response, retailers and other industry sectors have put in place focused cybersecurity measures to protect electronic networks, systems and processes.

Early this year, NRF organized the Information Technology Security Council, comprised of retailing's leading technology security experts. The goals of the council include networking and collaboration, education and research, and an information sharing platform tasked with providing timely notification and actionable data on critical threats.

Risks impacting retailers' information technology systems and data breaches "are at an all-time high," according to the 2014 BDO Retail Risk Factor Report. Since 2009, the number of retailers citing concerns over data security has more than doubled; nine of 10 retailers view data security as a risk to their businesses.

"We've seen a dramatic shift in the cyber crime landscape from solo hackers motivated by intellectual property



to organized criminal groups and state-sponsored actors motivated by financial fraud and cyber espionage," says Kimberly Kiefer Peretti, a former senior litigator for the U.S. Department of Justice's Computer Crime and Intellectual Property Section who assisted in the prosecution of the largest hacking and identity theft case ever prosecuted by the Justice Department. That case involved data pilfered from some 170 million credit and debit cards by a group of hackers working from 2005 to 2007. In March 2010 the leader, Albert Gonzalez, was sentenced to 20 years in prison.

Today highly sophisticated organized criminal gangs, particularly those from Russia and nations in Eastern Europe, "try to infiltrate and compromise as many systems as they can to maintain their presence and then pilfer systems over time," Peretti says.

"These criminals are often targeting confidential company information, personal information of consumers, customers and employees, and all of that creates a potential for litigation and regulatory inquires and reporting obligations," says Peretti, now a partner specializing in white collar crime and security incident management and response at the law firm Alston and Bird.

STAYING ONE STEP AHEAD

Cyber criminals targeting retail seek to breach systems by infecting them with malicious software, or malware, that captures payment card magnetic stripe information. The criminals then sell that data in bulk to other criminals — typically via underground Internet sites — who produce counterfeit cards.

Peretti says efforts to limit cyber breaches have amounted to a back-and-forth game: Going back a decade, cyber thieves would hack into retailers' systems and steal customer information stored in unencrypted databases. Retailers then began adding safeguards like network layer encryption technologies to protect internal systems and make it difficult for criminals to hack in.

> Since 2009, the number of retailers citing concerns over data security has more than doubled; nine of 10 retailers view data security as a risk factor to their businesses.
>
> **— 2014 BDO Retail Risk Factor Report**

Cyber criminals struck back, configuring ways to capture payment data in transit from the retailers' networks to payment processing systems. Retailers and the financial services sector responded with new protocols set by the Payment Card Industry Security Standard Council. Criminals then upped the ante with the ability to capture in-memory data — the very brief period between when a payment card is swiped and it moves to encryption.

Experts agree that once criminals latch onto a system that works, they will exploit it as long as they can.

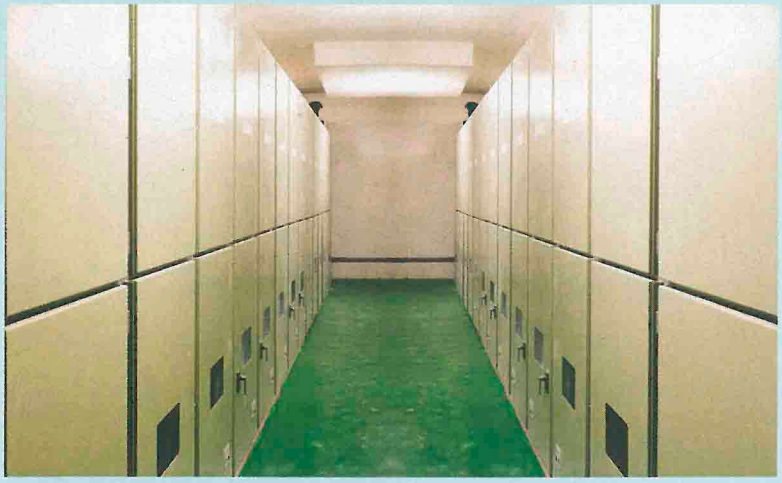
"To some extent, it always has been difficult to identify the person behind the keyboard committing a cyber attack, given the ease with which individuals can act anonymously and hide their tracks," Peretti says. "That has always been an obstacle."

This January, the FBI warned retailers to prepare for an even greater proliferation of cyber attacks via "memory-scraping" malicious software. The agency, in a widely covered unclassified report from its Cyber Division, reported that investigations of the 2013 Target breach turned up nearly two dozen additional cases involving that same kind of malware.

Peretti says retailers might need to fundamentally overhaul the way in which the industry processes payments to prevent memory-based pilfering. That likely would mean convincing the card industry to do away with magnetic stripe data on payment cards.

One technology favored by the card industry is EMV, commonly known as chip-and-PIN. Chip-and-PIN technology is designed to provide enhanced protection against lost, stolen or counterfeit cards through an embedded microchip. Using "dynamic cryptograms" to authenticate the card itself, along with an owner-supplied Personal Identification Number, EMV provides a strong deterrent to the

BIG DATA'S ROLE IN FIGHTING CYBER CRIME



Buoyed by emerging technologies, the retail industry has been moving aggressively to incorporate sophisticated new tools that enhance the shopping experience in stores and online. These initiatives have included new methods of merchandising and marketing, including mobile payments via smartphones and tablets; Wi-Fi networks in stores linked to back office systems to assist in customer ordering; micro-location technology for communicating messages to mobile devices; sensors to track customer movements and store traffic patterns; and tagging technology for inventory replenishment.

These new approaches are powered in a large degree by big data — the process of collecting, classifying and analyzing structured and unstructured marketing information to determine consumer patterns, behaviors and preferences in order to render more effective business decisions — that give retailers greater opportunities to reach their audiences.

Yet experts say retailers will need to be ever more vigilant to ensure network security as the mobile retail environment further develops.

"The store is going to become a much bigger environment of consumer data," says Erin Nealy Cox of digital risk management and investigations firm Stroz Friedberg. "Right now, the store has credit card information, e-mail addresses and they might know where you live.

"If [stores] start taking information from smartphones and have a bigger online presence so they can market better to people, they are going to be in the position of having to protect that data," Cox says. "Hackers are opportunistic: If they get into an environment where there is a treasure trove of personal identifying information, they'll grab that too."

Mark Weatherford of the security advisory firm Chertoff Group believes security intelligence can be siphoned from consumer data collected by retailers. For instance, retail IT and loss prevention specialists might be able to detect if a particular payment card number is being used in different places simultaneously by monitoring the usage of payment cards against consumer buying patterns.

Weatherford calls the ability to capture information on an event before it happens the "holy grail" for cybersecurity.

"The ability to mine this data gives the retailer the opportunity to see short-term events that can have long-term impact," he says.

types of fraudulent activities associated with the current magstripe-based system.

EMV alone is not the panacea some believe. It still leaves sensitive consumer information such as the credit card number in the open and susceptible to the same types of breaches in the news now. And without a PIN, as many U.S. card issuers are preferring (referred to as chip-and-signature), there's no proof the person trying to use the card is the person that owns the card.

Swapping out current generation payment card readers and magnetic stripe cards will mean major investments, according to Peretti. "That's a significant upgrade at significant costs to change out all the cards and terminals," she says. "We need an overhaul such that this type of crime is no longer as prolific and as easy to be conducted. It has been supporting an underground [network] for a decade."

Understanding EMV's technology and implementation shortfalls, many retailers are pursuing other, more encompassing and robust solutions, such as point-to-point encryption and tokenization technologies. Point-to-point encryption protects account data directly at the point of capture and maintains that protection through the payment process, including in memory, and is viewed as being more secure and reliable over the long term than chip-and-PIN.

Whatever solutions are adopted, dramatic action is needed to counter the criminals.

"Your whole response can't be reacting to the latest development of the hackers," says Cox. "You have to have a more holistic approach to security. We are only going to be able to get ahead if we can do a better job of having an overall better security posture that anticipates attacks instead of reacting to them." **STORES**

M.V. Greene is an independent writer and editor based in Owings Mills, Md., who covers business, technology and retail.