In data-heavy economy, breaches unlikely to end

January 29 2014

Target. Neiman Marcus. And now three other national retailers (yet to be named) have reportedly lost customers' personal data.

The Target breach alone compromised the data of as many as 110 million Americans - roughly one of every three people in the country.

The recent cascade of scams is an unwanted manifestation of the technology we carry in our pockets, the business we conduct online and the ever-growing array of devices, merchants, service providers and agencies we entrust with pieces of our identity.

Think of how often you swipe your card at the counter, fill out an online form, or even enter your user name and password into a website. Every time, you're sharing information that thieves are itching to get their hands on.

In 2012, the latest year for which widely accepted statistics are available, 621 confirmed data breaches compromised 44 million individual records. That's according to Verizon's annual Data Breach Investigation Report, considered by many to be the definitive measure of data intrusions in the industry.

Even that is not a comprehensive figure: It's limited by the number of organizations that participate, a roster that includes outfits as diverse as Deloitte and the U.S. Department of Homeland Security.

Because the number of participants changes constantly, it's also impossible to compare year-over-year stats. Thus there's no way to confirm the widespread perception that the number of breaches is growing.

But other firms that tally breaches put the number even higher.

Among veterans of the information security wars, it's widely assumed that "100 percent" of Fortune 500 companies have been hacked at some point, said Robert E. Lee, a security business partner at Intuit.

Even scarier: "It's very difficult to get a hacker out of your environment once they have a foothold," Lee said.

The beauty of being a hacker is that you only have to exploit one weakness. The problem of being in IT is that you have to protect against all potential attacks. And the points of attack just keep growing as more of our lives occur in cyberspace.

You can think about firewalls - the primary tool companies use to safeguard data - as a series of concentric circles. At each circle, a checkpoint looks at incoming information and assesses if it's OK, or not OK, to let it through.

But no matter how many checkpoints a system has, there's a vulnerability they're blind to.

"Think of them as outward-facing," said CEB TowerGroup research director Jason Malo. "You are standing on the wall, (trying to repel) someone (who) wants to come inside the castle."

The problem is, every system is hackable, and because the defenses are outward-facing, a thief who sneaks in can often harvest data undetected

for months or even years. Breaches usually go unnoticed for six to 13 months, giving malware ample time to do what it was designed to do, steal customer or company information, said Jake Kouns, chief information security officer for Risk Based Security, which runs the DataLossDB project.

"Once an attacker is inside the network, it's 'game over,' " said Adam Ghetti. He's the founder of Atlanta-based Ionic Security, which provides encryption services to banks, hospitals and other companies.

"The centralization of assets has been a protection method for centuries," said Ken Baylor, a research vice president at the information security research and advisory company NSS Labs. "Banks secured their data in vaults. Companies now centralize them in databases.

"At least with a vault, banks knew when they had been robbed," Baylor said. "With databases, a copy can be created in seconds and the company is unaware that millions of its customers have been put at severe risk."

Retailers, in particular, aren't properly protecting their in-house databases, Ghetti said.

"Retail enterprises continue to invest in, and lean heavily on, perimeter security technologies," he said in an email.

It's not as if IT folks can't come up with solutions. But businesses are caught in a tug of war between risk and reward, said Lee.

"Businesses are transferring risk to users, with the reward of higher profits for themselves," he said. "We know how to solve these problems; some companies choose not to."

Take for example, the more secure "EMV" cards, which carry an

encrypted chip rather than a magnetic stripe, and are used in most countries outside the United States.

Payment networks are pushing hard to get retailers and banks to adopt the new technology, but cost is an issue.

"Every ATM, every (point of sale) terminal, the retailers, the banks would have to pay for that." said Penny Crosman, the technology editor at American Banker.

And EMV alone wouldn't have prevented the Target breach.

The picture isn't all bleak, though. Many companies are now focusing on analytics, trying to keep track of data once it enters a system.

"I think that's where a lot of companies are starting to invest," said Malo, adding that analytics - tracking what a computer is doing inside, say, a retailer's network - is critical.

On a larger scale, the Georgia Technology Authority works with companies, law enforcement and other agencies to bolster cyber-security. For instance, the GTA is working with the Georgia Information Sharing and Analysis Center, a regional crime center that shares information across agencies both here and out-of-state.

In 2012, the GTA hired its first threat identification employee, using a grant from the U.S. Department of Homeland Security. His job is to analyze reports of suspicious online activity for patterns that suggest a significant attack is imminent.

"The No.1 concern we have is cyberthreat intelligence," said Mark Reardon, Georgia's chief information security officer. Reardon is a former director of technology at S1, one of the first firms to offer digital

banking software.

The immediate goal, he said, is to "give (potential targets) information in advance of an attack that allows them to take protective measures to either reduce or even block the impact of an attack."

In the long term, though, he said, "security is not a product that we're trying to produce; it's really a culture that we're trying to foster."

One piece of that cultural shift is moving beyond our reliance on user names and passwords to authenticate people. Three of every four network intrusions took advantage of weak or stolen credentials, according to Verizon's tally of data breaches.

"Candidly, it's tragic that you have one particular layer of security that is just so constantly exploited," said Jeremy Grant, a senior adviser for the National Strategy for Trusted Identities in Cyberspace, a White House initiative.

"When you look at the numbers, Grant said, "it makes a clear argument for why it's important to get people away from the password."

While the cyber-guardians tackle such issues, though, the cyber-crooks are working overtime to devise new lines of attack. There is an entire economy set up behind the scenes to facilitate their schemes.

Hackers share best practices and sell stolen data on eBay-like "carding" forums on the Internet. There, a thief can purchase, say, compromised card numbers from Bank A - filtered to include only its platinum members. It's that advanced.

There are also crime kits that allow novices to pick and choose attributes of malware, such as Zeus, the banking Trojan. That software infects a

person's browser, simultaneously stealing all the passwords and card numbers he or she uses online.

Most people and companies use anti-virus software, but it only guards against threats it recognizes, and the bad guys are constantly tweaking their weapons to circumvent such protections. Adding as little as a few lines of code will evade most anti-virus programs.

"The people who make a living commercially making the malicious software test them against all the (anti-virus) engines out there," said Intuit's Lee. "It's the stupidest thing in the world: Anti-virus only catches yesterday's problem."

And thieves have other tools as well: Man-in-the-middle attacks and phishing, among others, keep security employees up at night.

Given the havoc hackers create, especially the ones behind major data breaches, many people assume they're very sophisticated. Not always so. Many attacks can be attributed to off-the-shelf kits.

According to some reports by generally reliable sources, the Target breach was initiated by malware created by a Russian 20-something, with a teenager providing tech support. They reportedly didn't mount the attack themselves; someone else used malware these dudes made.

The sale of such ware is illegal, but many cyber-crimes cross international borders, which means it's tough to prosecute the perpetrators. So they continue to hatch their schemes while the victims of their hacks struggle to repair the damage.

Tory Gravitt, a senior at Kennesaw State University, has essentially been without a debit card since around Christmas. That's when her bank notified her that her information was compromised in the Target breach.

(She won't name the bank because she doesn't hold it responsible.) Unlike credit card holders, debit card holders generally find their money missing - although it will eventually be replaced - in the wake of a breach. Faced with a choice of getting a new card or tighter fraud controls from her bank, Gravitt chose the latter.

She took out a lump sum of cash, but that quickly ran out. As a result, she's been writing $50 and $60 checks to her roommate for cash.

"I had to buy groceries with a check the other day," the 22-year-old marveled. "I didn't know you could do that."

HOW TO SAFEGUARD YOUR IDENTITY ONLINE:

The following tips come from the Federal Trade Commission:

-Avoid phishing emails. Don't open files, click on links, or download programs sent by strangers.

-Be alert to impersonators. Don't give out personal information over the Internet (or by phone or mail) unless you've initiated the contact or know who you're dealing with. If a company that claims to have an account with you sends email asking for personal information, don't click on links in the email. Instead, contact company service through the company's website or by phone and ask whether they really sent a request.

-Encrypt your data. To guard your online transactions, use encryption software that scrambles information you send over the Internet. A "lock" icon on the status bar of your Internet browser means your information will be safe when it's transmitted.

-Keep passwords private. Use strong passwords with your laptop, credit,

bank, and other accounts. Be creative: Think of a special phrase and use the first letter of each word as your password. Substitute numbers for some words or letters. For example, "I want to see the Pacific Ocean" could become 1W2CtPo.

-Don't over-share on social networking sites. If you post too much information about yourself, an identity thief can find information about your life, use it to answer "challenge" questions on your accounts, and get access to your money and personal information.

-Use security software. Install anti-virus software, anti-spyware software and a firewall. Set your preference to update these protections often.

-In addition, some free services help you guard your data: Credit Karma, a lead generator that makes cash from marketing credit cards, allows you to check your information without having to ever pay for the privilege.

BillGuard, a New York City startup, crowd-sources fraudulent charges - that is, it lets consumers share information about scams and alerts participants to suspicious activity on their bank or credit card statements.

Finally, several commercial vendors, including the major credit rating agencies Equifax, Experian and TransUnion, offer identity-protection services.

For a comprehensive overview of identity crimes, look to the Center for Identity Management and Information Protection at Utica College (Google "identity crimes Utica College").

10 WORST DATA BREACHES:

The firm Risk Based Security, which tracks data breaches, tallied 2,149 known breaches in 2013, exposing over 822 million records. That makes

last year the worst the company has recorded. Three of the year's breaches made its list of the 10 largest of all time. Here's that list:

-Adobe Systems Inc.: In March 2013, Adobe lost data on 152 million customers, including credit card numbers, names and passwords.

-Shanghai Roadway D&B Marketing Services Co. Ltd: In March 2012, the firm illegally bought and sold 150 million customers' information, including names, addresses and financial information.

-Unknown organization: In June 2013, North Korean hackers obtained personal data on 140 million people, including Social Security numbers (or non-U.S. equivalents) and email addresses.

-Heartland Payment Systems: In January 2009, the fifth-largest credit-card processor lost the card numbers of 130 million people.

-Target Corp.: In November and December 2013, hackers stole 70 million customer names, addresses, phone numbers and email addresses, as well as 40 million credit or debit card numbers with expiration dates, PIN and security codes.

-TJX Cos. Inc.: In January 2007, the company lost data on 94 million T.J. Maxx customers, including names and credit card numbers.

-TRW: In June 1984, hackers obtained Social Security numbers (or non-U.S. equivalents) and financial information on 90 million people.

-Facebook Inc.: In July 2008, Facebook publicly exposed 80 million users' names and birth dates.

-Sony Corp.: In April 2011, the company lost 77 million names, addresses, email addresses, birth dates, passwords and other account

information.

-Pinterest: in August 2013, the website exposed 70 million users' email addresses.