Taming the beast: Data protection in 2014 & beyond

A comprehensive look at the threat landscape, the White House’s suggestions for data protection success, and your peers’ top 3 DLP tools
Are your data protection tools doing enough?

According to the Electronic Privacy Information Center, 90% of the world’s data was created in the past two years. The unfortunate truth is that every single byte of data has the potential to lead companies into insurmountable trouble. In the wake of massive breaches experienced at well-respected retailers like Target and Nieman Marcus, the government is responding. But does the Big Data: Seizing Opportunities, Preserving Values report address all of the business community’s concerns and weaknesses? In this e-guide, you’ll uncover the answer as our experts walk you through the:

• Current threat landscape and where weaknesses lie

• White House’s recommendations for ensuring data privacy and security

• Peer-rated top 3 data loss prevention tools to ensure comprehensive protection

Major retail breaches highlight point-of-sale security weaknesses

By Brandan Blevins, News Writer

After two major retailers, Target Corp. and Neiman Marcus, revealed that massive data breaches had compromised tens of millions of customers’ data records, everyone from consumers to politicians has asked how such spectacular security blunders could occur. But if experts’ anecdotes and insights on the numerous weaknesses in retail point-of-sale (POS) systems are any indication, it may be surprising major breaches don’t happen more often.
Minneapolis-based Target was the first major retailer to announce a breach during the 2013 holiday shopping period, initially confirming the compromise of 40 million credit and debit cards over the course of three weeks in November and December. Target's forensic investigation soon uncovered that personal data, including email addresses and telephone numbers, of up to 70 million customers had been stolen as part of the same criminal operation.

Separately, Neiman Marcus confirmed that it uncovered a breach on Jan. 1 that dates back to the same time frame as the Target breach, though the Dallas-based retailer has yet to confirm whether the two incidents are related or even how many payment cards were affected. Customers are being notified of the breach.

And more retail breaches are likely to be revealed soon. A recent Reuters report indicated that other retailers also suffered data breaches during the holiday season. Undisclosed sources told the news agency that "at least three other well-known U.S. retailers" were breached, and the attack techniques utilized were similar to those in the Target breach.

Why are attackers currently having so much success penetrating retail environments? While some may look to cast blame on weak legacy point-of-sale security, others say retailers’ security woes extend far deeper into their payment-processing infrastructures.

**Complexity reduces point-of-sale security**

Target CEO Gregg Steinhafel caused a stir in the security community following an interview with CNBC this week when he disclosed one particular aspect of the attack against his company.

"We don't know the full extent of what transpired, but what we do know is that there was malware installed on our point-of-sale registers," Steinhafel said. "That much we've established."

Though Steinhafel did not elaborate, the report from Reuters points the finger at what is known as a RAM scraper, or memory-parsing malware, which
essentially scans the memory of a computer looking for signs of track data from payment cards that may be unencrypted. Payment card giant Visa Inc. issued two warnings in 2013 related to the surge in use of such attacks to target retailers.

Blogger Brian Krebs reported Tuesday that the malware used to victimize Target was likely a variant of BlackPOS, a tiny memory-scraping program designed to sneak past perimeter defenses and install on point-of-sale systems undetected.

Patrick Townsend, CEO of Olympia, Wash.-based Townsend Security and a participant in the Payment Card Industry Security Standards Council (PCI SSC), said that such point-of-sale malware is difficult to stop. However, Townsend believes the security issues within retail environments extend further than point-of-sale terminal compromises. First and foremost, a retail environment, especially for a large company like Target, he said, can be incredibly complex.

In a typical brick-and-mortar store, according to Townsend, point-of-sale terminals are usually integrated with a cash register, which includes a complete operating system. A store will also have controllers that link terminals together.

Retailers then have payment operations at company headquarters, where payment transactions are consolidated and information is sent to a third-party payment processor. Any one of these technologies, as well as others like customer loyalty or gift card management systems, represent a potential attack surface that retailers often struggle to secure properly.

"Every one of those points could potentially be attacked and have been points of attack," Townsend commented. "So that complexity is one of the things that make it so hard to secure these environments."

According to Curt Wilson and Dave Loftus, both part of the ASERT team at distributed denial-of-service mitigation vendor Arbor Networks Inc. in Burlington, Mass., this sizable attack surface provides criminals a wide range
of possible vulnerabilities with which to exploit retailers, often enabling an attacker to compromise a Windows PC or another weak point in a network and use that as the foothold to move laterally to the desired destination. Wilson and Loftus penned a recent report uncovering an active point-of-sale malware campaign that seemingly targeted only smaller retailers.

The bulk of the activity Arbor tracked as research for its report was attributed to the venerable Dexter family of RAM-scraping malware. Wilson said it's unclear whether Dexter was used in the Target attack, though a connection is possible, especially because the Dexter source code was previously leaked.

Arbor's research into Dexter enabled Wilson to learn about the different techniques used by attackers to install such malware onto POS systems. He noted that attackers have leveraged a number of Windows-based vulnerabilities, open remote desktops connections and vulnerabilities in open wireless networks to gain access to retailers' systems, including POS terminals themselves as well as Windows PCs used at corporate headquarters.

**Spreading retail malware via central console**

Once inside a network, there are a number of ways that attackers can install malware and locate valuable information. In the case of the Target breach, Wilson suspected that attackers might have compromised a central management console responsible for pushing software updates.

Adam Meyers, vice president of intelligence for Irvine, Calif.-based CrowdStrike Inc., agreed, highlighting the difficulty that attackers would otherwise have in spreading malware to thousands of point-of-sale endpoints.

"To deploy that much software to that many point-of-sale devices, they would have had to have gotten into some sort of central management console and pushed out the malware," Meyers said.
Meyers noted that sophisticated attackers, such as those sponsored by nation-states, are more likely to infiltrate a network and stay inside over the course of months or even years, whereas typical cybercriminals would simply utilize smash-and-grab tactics to take whatever they can find. The fact that such attackers possibly used the same techniques as nation-state hackers to hit Target and other retailers "speaks to the evolution of some of these criminal actors," he said, making the detection of their activities nearly impossible without implementing stronger security practices.

How to shore up retail security
As for how retailers can improve point-of-sale security, experts say reducing the complexity of payment systems is key.

Through his research on Dexter, Wilson discovered what appeared to be a mom-and-pop retailer running multiple applications on a single computer system alongside its POS software, including those for video surveillance and employee time-clock access. He said such a situation should never occur and stressed the need for isolation and network segmentation for systems in the card data environment.

"You should not have that [point-of-sale] machine used for other applications," Wilson said. "You should not have people surfing the Web, checking email, etc., on these point-of-sale machines, or [have] systems connected to these point-of-sale machines."

Meyers also recommended that POS systems should be isolated and placed on segmented networks, not only because of the obvious Payment Card Industry Data Security Standard (PCI DSS) compliance demands, but also because of the monitoring benefits such a setup provides.

"By creating a separate segment for those devices that you have control over, you can build a bottleneck point where you're then able to monitor anything crossing over that zone," Meyers said. "So it really gives you the ability to see traffic emanating from and [returning] to your point-of-sale environment."
With the November release of PCI DSS 3.0, the PCI SSC emphasized the importance of continuous monitoring, Townsend noted, which he believes could play a key role in detecting and mitigating retail breaches. Industry studies point to evidence that a breach typically occurs up to 12 months before an actual loss of data, he said, so it's up to retailers to monitor for criminal activity before a huge data loss occurs.

"When forensics is done, in a vast majority of cases, the breach was detectable early on based on system log information," Townsend said. "So having an appropriate system logging and monitoring infrastructure in place is crucial.

"But those systems are only as good as your implementation of the collection from all your endpoints," he added. "Companies need to collect logs and monitor them, but they also need to collect them from every PC and user and server and application and Web server and payment system in the network. Those active monitoring systems are only as good as the data they have to work with."

The information stemming from the Target and Neiman Marcus breaches, as well as other smaller retail breaches in previous years, could also give retail defense teams an upper hand over attackers, according to Meyers. He wants retailers to take the intelligence gleaned from security events at other companies and apply what is learned to their own IT infrastructure. Between the success attackers are having targeting retailers and the release of the Dexter source code, experts agree that retailers must improve their point-of-sale security practices drastically if they want to avoid becoming the next Target.

"The underground economy is interested," Wilson said, "and this flurry of activity is probably going to stimulate more attacks."
White House big data initiative: A data security and privacy analysis
By Francoise Gilbert

The report *Big Data: Seizing Opportunities, Preserving Values* was published on May 1, 2014, by the Executive Office of the President in response to a request made in January 2014 by President Barack H. Obama to conduct a study examining how "big data" will transform the relationships between the government, citizens, businesses and consumers.

The report identifies five areas of focus:

- **Privacy**: Maintain privacy values by protecting personal information in the marketplace, the United States and worldwide through interoperable global privacy frameworks
- **Discrimination**: Prevent discrimination that some uses of big data may enable
- **Law enforcement**: Ensure responsible use of big data in law enforcement, public safety and national security
- **Public resource**: Harness data as a public resource, use it to improve the delivery of public services, and invest in research and technology that will further power the big data revolution
- **Education**: Recognize schools as an important sphere for using big data to enhance learning opportunities while simultaneously protecting personal data usage and building digital literacy and skills

The report concludes with a number of policy recommendations, specifically to:

- Advance the Consumer Privacy Bill of Rights
- Pass national data breach legislation
- Amend the Electronic Communications Privacy Act
- Extend privacy protections to non-U.S. persons
- Ensure data collected on students in school is used for educational purposes
- Expand technical expertise to stop discrimination
These recommendations are likely to affect the way in which companies operate, how and why they collect data, and what uses they make of the information collected. The general theme of the report and its recommendations center on finding responsible uses of big data for the benefit of individuals while respecting privacy and intimacy, and setting up better structures, disclosures or technologies to allow for these new uses. Let's take a further look at some of the main components and recommendations of the report.

**Consumer Privacy Bill of Rights**

The report furthers the White House initiative known as the "Consumer Privacy Bill of Rights" in which President Obama proposed adoption of a national data privacy law. The report suggests that the Department of Commerce draft legislative text implementing the Consumer Privacy Bill of Rights for submission by the President to Congress.

**Notice and consent**

The White House report recognizes that the traditional concepts of notice and consent, which have been a central pillar of how privacy practices have been organized, may no longer be sufficient to protect personal privacy for a variety of reasons, including the rampant over-collection of data, combination of multiple databases, the advance of technology and computing capabilities, and the difficulty in keeping data anonymous.

In the "notice and consent" framework, a company notifies a consumer in advance of the intended use of the personal data being collected, and the user consents to collection for these purposes. The company is limited to using or processing the data for the purposes that were originally identified, or perhaps similar purposes. Big data processing does not fit within this framework because most uses of big data processing technologies are outside the scope of the original notice. They are intended for the discovery of patterns or behaviors that were not contemplated in the original notice. In addition, the patterns or behaviors may result from the combination of several databases, originating from several entities.
In fact, notice and consent would be incompatible with the benefits that big data would enable, such as "new, non-obvious, unexpectedly powerful uses of data" beyond the scope and intent of the original data collection. Thus, new criteria for access to and the processing of data would have to be developed.

'Do not track'
The report recommends strengthening "do not track" tools, technologies and mechanisms to address the growing array of technologies available for recording individual actions, behavior and location data across a range of services and devices.

While there are currently numerous efforts to implement a "do not track" regime, various obstacles are delaying implementation. Concurrently, companies are resisting the implementation of "do not track" because they view the ability to analyze usage data as critical for understanding their market.

Data brokers
Key parts of the report apply specifically to data brokers. Data brokers have been the subject of intense scrutiny in the past few months, including an initiative of the Federal Trade Commission. The report encourages the data broker industry to build a portal (similar to those that have been developed by the advertising industry) relating to cookies and customer tracking. On these portals, data brokers would disclose data practices and provide methods for consumers to better control how their information is collected and used, or to opt out of certain marketing uses. The massive collection and use of personal data by data brokers -- and their dissemination of the collected information -- has been the subject of several Federal Trade Commission enforcement actions. The White House report suggestions would help sanitize some of these practices, though at this point the threat of legislation seems highly unlikely.

National data breach legislation
More than 10 years after California passed the first security breach disclosure law, the country is still divided into 47 different regimes, and
federal legislators have not been able to pass a law that would provide disclosure uniformity. The White House report on big data supports legislation to define a single national data breach standard that would impose reasonable time periods for consumer notification; minimize interference with law enforcement investigations; and potentially prioritize notifications of large, damaging incidents over less significant incidents.

Amend the Electronic Communications Privacy Act
There is no doubt that the Electronic Communications Privacy Act (ECPA), at almost 30 years old, is out of sync with the reality of today's communications based on cloud, texting, social media and other means that did not exist or were in their infancy in 1986. Numerous initiatives have been discussed already to update this aged act. The White House report supports the trend and recommends amending the ECPA to ensure that the same protection is given to online and digital content as that which is afforded in the physical world, including removing archaic distinctions between emails left unread or over a certain age.

Privacy protections for non-U.S. persons
The report takes into account the increased globalization of practices and communications along with the fact that cloud computing and other technologies allow the presence on U.S. servers of information generated by users out of the country that is intended to be used outside the United States. The report recommends that the Office of Management and Budget work with various departments and agencies to apply the Privacy Act of 1974 to non-U.S. persons where practicable, or to establish alternative privacy policies that apply appropriate and meaningful protections to personal information regardless of a person's nationality.

Interoperable global privacy frameworks
After having been the target of much criticism for its practices and lack of "adequate protection," the United States is now stepping up its efforts at communicating with the other powers worldwide and attempting to establish and participate in building bridges between the different privacy and data protection regimes.
The big data report encourages the Department of State and the Department of Commerce to engage with the European Union, the Asia Pacific Economic Cooperation (APEC), the Organization for Economic Cooperation and Development, and other stakeholders to take stock of how existing and proposed policy frameworks address big data issues. In addition, it recommends that the two departments strengthen the U.S.-European Union Safe Harbor Framework, encourage more countries and companies to join the APEC Cross-Border Privacy Rules system, and promote collaboration with respect to data flows between the United States, Europe and Asia through efforts to align Europe’s system of Binding Corporate Rules and the APEC CBPR system.

**Discrimination**

The report also focuses on the potential ability of big data to create more opportunity for discrimination based on the information that would be collected through the processing of the data. The White House recommends the federal government's lead civil rights and consumer protection agencies expand their technical expertise to be able to identify practices and outcomes facilitated by big data analytics that have a discriminatory impact on protected classes, and then develop a plan for investigating and resolving violations of law.

**Law enforcement and security**

With the recent revelations of the extensive use of personal information by U.S. and foreign government agencies, it is no surprise that the White House report would contain numerous recommendations regarding the role and scope of powers of law enforcement agencies. For example, the report recommends that the use of predictive analytics by law enforcement should receive careful policy review. Federal agencies with expertise in privacy and data practices should provide technical assistance to state, local, and other federal law enforcement agencies seeking to deploy big data techniques. Government use of lawfully acquired commercial data should be evaluated to ensure consistency with our values. Federal agencies should also implement best practices for institutional protocols and mechanisms that can help ensure the controlled use and secure storage of data.
Conclusion

Big data tools offer astonishing and powerful opportunities to unlock previously inaccessible insights from new and existing data sets. As a result, organizations are collecting and storing increasingly larger amounts of data and allowing the digital traces users leave behind to be collected, analyzed and assembled to reveal a surprising number of things about individuals. As a result, big data analytics have the potential to eclipse long-standing civil rights protections in how personal information is used in housing, credit, employment, health, education and ultimately the entire digital marketplace. The White House big data report provides a thorough analysis of the good and bad uses of big data and suggests numerous structures and safeguards that should be put in place to avoid negative or harmful consequences for individuals. It is likely that some of the proposed initiatives will be translated into new laws and regulations, which will undoubtedly create obstacles and compliance requirements for many, if not most, companies.

It is clear that big data analytics and technologies -- especially when combined with the amazing capabilities of sensors, wearable technologies and other Internet of Things devices -- create the potential for new uses of data never before envisioned. While big data has the potential for numerous positive developments -- such as in the health or the education sectors -- it is clear that structures need to be put in place to help preserve intimacy and protect personal lives. The White House big data report is an important step in the right direction, but it remains to be seen how the study and its recommendations will be implemented to preserve a reasonable balance between the different players -- and the different goals.

About the author:
Francoise Gilbert, JD, CIPP/US, is the managing attorney of the IT Law Group, and she serves as the general counsel of the Cloud Security Alliance. She focuses her legal practice on information privacy and security, cloud computing, big data and data governance. Francoise was named Best Lawyers’ “2014 San Francisco Lawyer of the Year” in the area of information technology, and was listed as one of the country’s top legal advisors on privacy matters in a recent industry survey. For the past few years, she has been repeatedly identified by Ethisphere as “an attorney who matters” in the
Taming the beast: Data protection in 2014 & beyond

Contents

Major retail breaches highlight point-of-sale security weaknesses

White House big data initiative: A data security and privacy analysis

Security Readers’ Choice Awards: Best of data loss prevention

By Robert Richardson, Editorial Director

Gold: Symantec Data Loss Prevention, Symantec Corp.

Although it's been a category of great importance to enterprises for a number of years, this is the first year we've asked readers to give the nod to their top data loss prevention (DLP) products. The margin among the award winners, we have to admit, is small, but the victory was eked out by Symantec. Readers gave Symantec Data Loss Prevention especially high marks for ease of installation, configuration and administration—this in a product category where installation in particular can quickly become hopelessly mired in the details of the various kinds of data and formats that are found on any particular enterprise IT system. Symantec also received category-leading marks from users for vendor service and support.

A recently added component to the product, called Data Insight, tackles the problem of unstructured files, which analysts predict will grow at 60% per year. The addition, which gives administrators a view into the usage patterns and access permissions for unstructured data, is an example of how vendors increasingly need to add new dimensions to their DLP products. There's no single approach to DLP that gets the overall job done. Users have found that Symantec has the mix right.

Silver winner: Websense Data Security Suite, Websense, Inc.
Websense grabbed the silver, with readers singling out high granularity and flexible policy creation, along with the product's high degree of scalability. The product is a suite that comprises a data security gateway, a tool for locating and classifying data across the network infrastructure and Websense Data Endpoint, which identifies and controls data in use on laptops, USB drives and other endpoint devices. The Websense Data Security Suite handles mobile endpoint data protection by way of Triton Mobile Security, a cloud-based product.

**Bronze winner: McAfee Total Protection for Data, McAfee, Inc.**
Readers awarded bronze to McAfee, noting the product's flexibility in creating data policy definitions. Additional flexibility comes from the broad array of products that McAfee has released in the DLP space. There are appliances for general DLP management and data discovery; separate software offerings target endpoint DLP and the management of information copied to removable media. Readers said they also liked the product's effectiveness in detecting unauthorized user activity.
Free resources for technology professionals
TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more—drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?
TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites
- SearchCloudSecurity
- SearchSecurity
- SearchFinancialSecurity
- SearchMidmarketSecurity