Business Horizons (2016) 59, 257—266

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

BUSINESS LAW & ETHICS CORNER

Why you should care about the Target data breach

Nathan Manworren [a,*], Joshua Letwat [b], Olivia Daily [c]

[a] Candidate for B.A. in Economic Consulting, Kelley School of Business, Indiana University (expected 2017)
[b] Candidate for B.A. in Accounting and Finance, Kelley School of Business, Indiana University (expected 2017)
[c] Candidate for B.A. in History and Finance, Kelley School of Business, Indiana University (expected 2017)

KEYWORDS
Cyberattack;
Cybersecurity;
Target;
Best practices;
Internet;
Malware;
Data;
Data breach;
Security;
Lawsuit;
Privacy

Abstract Data breaches are becoming more frequent and more damaging to the bottom line of many businesses. The Target data breach marked the beginning of increased scrutiny of cybersecurity practices. In the past, data breaches were seen as a cost of doing business, but Target's negligence and the scale of the data loss forced businesses and the courts to reevaluate current practices and regulatory frameworks. Businesses must make strategic use of their chief information officers, adopt cybersecurity best practices, and effectively train their employees to respond to growing security threats. They must also shape the cybersecurity narrative to influence regulatory responses to these threats.

1. The breach that changed everything

Shortly before Thanksgiving 2013, someone installed malicious software (*malware*) on Target's security and payments system. The malware was designed to steal information on every credit card used at the company's 1,797 U.S. stores. At a moment when shoppers were focused on spending for the upcoming Christmas season, malware began capturing their credit card numbers and storing that captured information on servers commandeered by the hackers. In theory, Target was prepared for the hack: six months earlier, the company had begun installing a $1.6 million malware detection tool designed to inform them of a data breach. Yet in late 2013, Target failed to respond quickly to the attack—a failure that marked the beginning of a series of challenges for Target.

Since those fateful days in late 2013, customers and banks have filed more than 90 lawsuits against Target for negligence and compensatory damages. The costs of responding to the breach have continued to mount. In numbers, Target's profit for the 2013 holiday shopping period fell 46% from the same quarter the year before; in sentiment, Target lost the trust of its customers, investors, and lenders.

* Corresponding author
E-mail addresses: nmanworr@indiana.edu (N. Manworren), jletwat@iu.edu (J. Letwat), odaily@indiana.edu (O. Daily)

0007-6813/$ — see front matter
http://dx.doi.org/10.1016/j.bushor.2016.01.002

Target is just one of many companies to be affected by data security breaches. The Target case is unique, however, in that its employees evidently worked *against* its security systems. Because of this, the Target breach will likely stand as the data loss that changed everything. This article explores the Target breach, first by examining the technology involved and then by considering the roles that Target employees and others played in jeopardizing the security of its data. The article then considers the complexity of state and federal laws as they relate to data loss and suggests that creation of a national standard is the only hope for reducing the complexity of the current regulatory system. Finally, the article considers what businesses must do to protect themselves and their customers in the changing landscape of data breach regulation.

2. Target's failure

Target was at the forefront of technology in 2013, investing in state-of-the-art security. The company was warned when the hackers attacked in 2013, but it ignored multiple alerts that something was wrong and continued selling to consumers. As a result, millions of people continued to swipe their credit cards and their information continued to be sent to hackers. The resulting loss of critical consumer data put millions of people at risk for identity theft (Riley, Elgin, Lawrence, & Matlack, 2014).

2.1. How the attack happened

The hackers were able to gain access to Target's system by stealing credentials provided by the company to Fazio Mechanical Services, a contractor that ran Target's climate systems. Target failed to segment its network to ensure that Fazio—and other third parties—did not have access to its payment systems (Riley et al., 2014). As a result, the hackers were able to exploit a connection designed to let Fazio exchange contract and project management information with Target and then used this connection to upload malware onto Target's systems, including its individual point-of-sale systems (Hosenball, 2014).

2.1.1. Point-of-sales systems

A point-of-sale (or POS) system is a type of technology used to collect a consumer's payment information. The POS system calculates the amount owed by the customer and collects the payment. The interaction between the consumer and the POS system is an extremely familiar and innocuous process that occurs countless times a day. However, there is much more to a POS system then what is visible to consumers.

POS systems are comprised of both software and hardware. The hardware includes equipment such as a cash register, credit card reader or terminal, pin pad, and monitor. The software communicates the customer's information using a central payment-processing server connected to a number of POS application terminals. When a credit card is used at the POS terminal, the terminal connects to the central payment-processing server in the merchant's corporate environment, which then provides payment authorization (Hizver & Chiueh, 2012). When people swipe their credit cards at a POS terminal, the data encoded on the card's magnetic stripe—such as the card number, cardholder name, and card expiration date—is sent with the transaction request to the payment software application and then to the company's payment processing provider (Constantin, 2014).

The malware used by the hackers was programmed to steal Target's customer data at the point of sale. So-called 'RAM scrappers' would copy customers' card information while it was still in the memory storage of Target's POS system. While payment information is encrypted when it is sent off to confirm a sale, it remains readable within the system (Constantin, 2014). Target's IT infrastructure should have identified and destroyed this malware, but it failed to do so (Smith, 2014).

2.1.2. Target's security

Target was aware of the threats posed by hackers and had deployed numerous security measures to protect its computing architecture. It had "multiple layers of protection, including five firewalls, malware detection software, intrusion detection and prevention capabilities, and data loss prevention tools" (Committee on the Judiciary, 2014). Target also performed internal and external validation and benchmarking assessments, and its security systems complied with data security standards in the credit card industry. It was even widely reported that Target used "the same security system. . .employed by the CIA, the Pentagon, and other spy agencies around the world" (Smith, 2014).

Target's sophisticated security system could and should have addressed the malware uploaded by the hackers. The system even had a function that would automatically delete malware as soon as it was detected, but Target's security team had turned off that function—just as many other businesses using the same system had done—because it often halted email and Internet traffic by incorrectly flagging data as malware (Finkle & Heavey, 2014; Smith, 2014).

2.1.3. Ignored warnings

By all indications, Target was warned repeatedly about the occurring cyberattack. Target's IT protection system was designed to send automated warnings when it detected malware (Finkle & Heavey, 2014), but Target failed to respond to these warnings, thus enabling the unheeded hackers to install malware on Target's system (Committee on Commerce, Science, and Transportation, 2014).

These automated alerts were not the only red flags the company ignored. As the malware was breaching Target's system, the hackers created a link outside the system to hold the stolen customer data so that it could be commoditized. To accomplish this, the hackers used software designed to go through Target's internal firewalls and security before reaching the Internet. Here, too, Target's security system caught this attempted breach and sent multiple warnings to the company. Once again, however, Target failed to respond to these warnings (Committee on Commerce, Science, and Transportation, 2014).

Even though Target seemed prepared for a cyberattack, the results were catastrophic. The breach compromised the financial and personal information of millions of people, and as the attack became public, Target suffered significant damage to its reputation and its bottom line.

2.2. The target on Target Corporation

With public sentiment resolutely against them, Target was left with little choice: in 2015, the company agreed to settle a class action lawsuit for $10 million, providing up to $10,000 in relief to customers with injuries stemming from the data breach (Cooney, Kurane, Walsh, & Dwivedi, 2015). In addition to the settlement with customers, Target agreed to a settlement for $67 million with Visa Inc., a $20.25 million settlement with several banks and credit unions, and a $19.11 million settlement with MasterCard Inc. (Howland, 2015).

Several months earlier, Target had sought settlement with MasterCard, who was acting on behalf of big banks such as Citigroup, Capital One, and J.P. Morgan Chase. That first proposal, however—a similar $19 million settlement offer—was rejected when it failed to gain the required 90% support from the banks.[1] The banks and credit card issuers were seen as ''send[ing] a message to merchants that they [were] unhappy with their security efforts'' and as making an example of Target to demonstrate their frustration with the lackluster data security environment currently in place (Sidel, 2015).

In the past, large banks had accepted the costs associated with data breaches—such as the expense of monitoring for fraud and reissuing cards—as a cost of doing business (Embry, 2015.) As the frequency and severity of data breaches have continued to escalate, however, judges and the public are beginning to hold retailers more accountable. As a result, the costs and uncertainty resulting from Target's data breach are still mounting.

At the end of 2015, Target disclosed that costs related to the breach had reached $290 million. Taking into account $90 million in insurance reimbursements and additional tax deductions on breach-related expenses, Target's net cost from the data breach has exceeded $100 million (Howland, 2015).

Despite the enormity of that sum, it may not create sufficient financial pressure to prompt significant changes in the ways that large companies protect customer data. In fact, the cost of Target's data breach represents less than 1% of Target's $72.6 billion in total revenue for 2014 (Target Corporation, 2015). While the company must still account for the costs of pending lawsuits and investigations, it remains unclear whether the data breach has stirred enough concern among business and government leaders to prompt significant changes in the business and regulatory environments.

Some argue that Target's costs were a result of poor public relations decisions that led to a loss of consumer trust during the holiday season rather than a result of the data breach itself. Home Depot's response to a similar case of hacking provides some support for this conclusion. In Home Depot's case, the data breach occurred in September rather than December, and the company responded to the breach within 24 hours. Unlike Target's data breach, Home Depot's was met with a public yawn (Hill, 2014), but this sort of reasoning leads businesses to treat data breaches merely as public relations problems while continuing to use lax data security practices. Businesses are likely to continue doing so until industry leaders, government regulators, and/or the public prompt the necessary transformations in businesses' approaches to data security.

3. The expansion of liability

In many ways, the Target data breach may serve as a watershed moment in cybersecurity regulation. Awareness of the behavior of Target employees laid bare the extent to which businesses are comfortable allowing employees to circumvent technology in ways that greatly expose their IT systems to data breaches.

[1] The banks representing cardholder accounts affected by the data breach.

Congress is currently considering a plethora of cybersecurity and data breach laws. Congress's considerations are structural as well as procedural as it assesses the framework of the current cybersecurity environment. Unfortunately, despite the "perilously overdue" need for regulation, significant gridlock in Congress has delayed the progress of such legislation (Sanger & Hirschfeld Davis, 2015; Shearman, 2015).

The absence of federal regulation has allowed large businesses to pass millions of dollars in data-loss-related expenses to credit card companies, insurance companies, and consumers. Target's data breach, however, is an unmistakable warning to regulators and courts about the role that businesses play in contributing to the extensive loss of data.

The lack of uniform federal regulations also means that businesses operating in multiple states must comply with a patchwork of varying state and local laws and regulations, making conformity to security rules an extraordinarily inefficient and messy process. There are 47 unique laws concerning data breaches across the country—52, when U.S. territories are included—which creates a jumble of complex, confusing, and sometimes incongruent policies and practices within a single business operating nationwide (Experian, 2015). Because of the patchwork of laws, the National Retail Federation is pushing for uniform national standards that would preempt state and local laws (Shearman, 2015). If passed, uniform national standards would reduce costs and confusion for companies, but only if they preempted state and local laws. National standards that do not preempt state and local laws would only further complicate the regulatory puzzle, and it could be years before state and local laws harmonize with federal law, if ever. Preemptive national standards would enable businesses to operate more efficiently and to spend money on bolstering cybersecurity rather than on employing compliance officers and legal consultants.

An example of incongruence in policies is the fact that, depending on the jurisdiction, companies may or may not be required to pay customers whose data is stolen even if they do not suffer economic damages as a result. In 2014, thieves stole two laptops containing unencrypted data for thousands of customers from AvMed, a medical insurance company. In response to a class-action lawsuit by its customers, AvMed agreed to pay $3 million to reimburse customers whose information was stolen, including customers who did not suffer any actual economic damage as a result of the disclosure of their information (Goodman, 2014). Like AvMed, companies in many states could be forced to pay damages for data breaches even when the disclosure does not result in actual economic damages.

The U.S. Court of Appeals for the Seventh Circuit recently continued this trend by overturning a federal court decision—a reversal that allowed plaintiffs to continue suing Neiman Marcus for disclosure of their information as a result of a data breach. In 2013, hackers stole the information of roughly 350,000 customers from Neiman Marcus. In order to bring a lawsuit, the customers had to show that they had suffered a "concrete and particularized injury that [could] be traced to the challenged conduct" (Tene, 2015). The trial court dismissed the class action lawsuit because the court found that the data breach had not caused the customers a "concrete and particularized" injury. On appeal, the Seventh Circuit reversed the lower court's decision and allowed the lawsuit to proceed. In *Remijas v. Neiman Marcus Group LLC* (2015), the Seventh Circuit Court held that the customers had standing to sue based on the potential future harm that could arise from the data breach. The Court noted that the customers were exposed to a range of potential future harms and damages, including fraudulent charges on their credit cards, the need to acquire new credit cards, the time spent reviewing bills for fraudulent charges, and the need to constantly monitor their credit score. The Seventh Circuit's decision represents a huge shift in data security law and is in direct contrast to earlier decisions that only allowed lawsuits for actual economic damages that had already occurred as the result of a data breach.

The treatment of recent data breaches creates an important precedent for future cases. The expansion of liability for the security of customer information means that companies will have to take precautions to protect and secure customer data or risk liability for actual—and even potential—damages to consumers. Consumers are beginning to use courts to hold companies accountable for failing to recognize the value of their personal and financial information and to ensure its security.

4. What is a business to do?

With liability for cybersecurity expanding in uncertain and dangerous times, cyberattacks pose increasingly serious threats to many companies. However, a few simple, prospective reforms can get these businesses moving in the right direction.

4.1. Recognize that you may already have been hacked

The Target data breach represents the beginning of an onslaught of cyberattacks that will only worsen. The harsh reality is that your data may already have been stolen. Privacy Rights Clearinghouse (2015)

estimates that over 850,000,000 financial records have been illegally obtained in the more than 4,500 U.S. data breaches made public since 2005, though actual numbers of data breaches and stolen records are unknown because businesses are not required to disclose that information. Reported numbers also only encompass financial records (such as social security and credit card numbers), so the actual number of stolen records is likely to be many times larger.

The term 'data breach' has become ingrained in the collective psyche of the United States. The *New York Times* published more than 700 articles about data breaches in 2014, compared to 125 in 2013 (Verizon Enterprise, 2015a), and the societal impact of cyberattacks will only continue to increase. Indeed, an executive from Hewlett-Packard has predicted that "[by] 2020 the U.S. will be hit with an earthquake of a cyberattack that will cripple banks, stock exchanges, power plants and communications" (Lee, 2015).

Our collective concern should not be limited to loss of data. A survey of security professionals found that nearly half (48%) believed a cyberattack will take down critical infrastructure and cause deaths within the next three years (Anand, 2015). Businesses should recognize the value of the information they hold, take steps to protect it, and realize that their data may already have been comprised by cyberattacks.

4.2. Recognize that consumers have little choice in turning over their information

Consumers put themselves at risk every day. They hand over credit card information to waiters, websites, employers, government agencies, and other parties—all of whom are capable of losing or misusing that information. Customers trust businesses to protect their data by monitoring employees and by utilizing data security systems, and consumers—like many businesses—do not recognize the constant risk of being hacked. The world is moving toward total integration of our lives into a digital existence, and many people assume that businesses collecting our information will protect it.

Pretending that a business is not at cybersecurity risk ignores the harsh realities of the current environment. No industry is immune to such attacks (Verizon Enterprise, 2015a). The U.S. Government, an entity that many reasonably think should have the greatest security of any organization, has been hacked numerous times. According to one account, hackers accessed personnel records of current and former employees, as well as "extensive information about friends, relatives and others listed as references in applications for security clearances for some of the most sensitive jobs in government" (Nakashima, 2015). Clearly, something must change, and businesses cannot wait for a regulatory response that may be months or even years away; doing so leaves businesses and their customers exposed.

5. Let's get down to business

Industry has the ability to solve the issue of cybersecurity quickly and efficiently, but it needs the proper incentives. Fortunately, the incentives are rapidly emerging. The potential for nonmarket intervention is rising as it keeps pace with the ominous growth in both the number of cyberattacks and the number of interconnected devices (Verizon Enterprise, 2015b). Wall Street is pouring millions of dollars into cybersecurity stocks, and experts predict that this trend will continue (Vardy, 2015). The case is strong—and growing stronger—for businesses to begin taking cybersecurity seriously. Companies that are willing to adapt to the challenges of cybersecurity will be more sustainable and strategically positioned than those that are not.

5.1. A shift to proactive self-regulation

As discussed above, Congress is considering a plethora of cybersecurity and data breach-specific laws. Though much of this legislation has not yet been enacted, Congress has demonstrated that it seeks to establish rules to address the issue, if only to eliminate uncertainty about which businesses will be held accountable in the future. Fortunately, there is a clear theme: national standards for cybersecurity. Companies cannot wait for government to act, however; they must be proactive, not reactive. Target, for example, is now proactively seeking to improve its image in the cybersecurity arena. The company has dedicated $5 million a year to help educate consumers about cybersecurity risks, and it is partnering with the National Cyber-Forensics and Training Alliance, National Cyber Security Alliance, and Better Business Bureau to help educate consumers about current data scams in real time (Hasnie, 2015; Target Corporation, 2014). By their actions, Target and other organizations can write the public policy narrative and persuade government to give greater deference to their opinions and practices.

Government incentives for progress in this area are underwhelming. Legal remedies for data breaches are getting easier to obtain from companies (Roberts, 2015), but they apparently have

not posed sufficient financial hardship to prompt companies to take extensive security measures. Government fines for data breaches are also too small to prod businesses to act. Even after the Federal Communications Commission imposed the highest-ever fine ($25 million) on AT&T for privacy violations, one industry observer noted (Goldman, 2015):

> As long as the fines aren't putting businesses into bankruptcy—or even serious financial peril, for that matter—executives and boards are free to decide they are better off investing the bare minimum in security and saving the rest for possible breach costs and fines.

5.2. Focus ahead: The Internet of Everything

The phrase *The Internet of Things* (IoT) refers to "machine-to-machine technology enabled by secure network connectivity and cloud infrastructure, to reliably transform data into useful information for people, businesses, and institutions" (Verizon Enterprise, 2015b). Everything is becoming linked to the Internet, which means that everything is becoming hackable (Kharpal, 2015; Learmonth, 2015). The number of connections—cellular, fixed line, satellite, and wireless—are growing exponentially. By 2020, there are projected to be 5.4 billion such connections, up from 1.2 billion in 2014, as the globe experiences 28% annual increases in connectivity (Verizon Enterprise, 2015b).

The increase in Internet connectivity will force businesses to adapt rapidly to stay profitable, which often leads to unsustainable and destructive solutions. In a swiftly expanding market where time-to-market is critical, product developers may not place a priority on security (Verizon Enterprise, 2015a). This tendency to err on the side of carelessness further increases the likelihood that hackers will continue to plague consumers and businesses. Despite the risks, businesses will continue to pursue connectivity because organizations that adopt IoT extensively are projected to be at least 10% more profitable than competitors that fail to do so (Verizon Enterprise, 2015b).

There is even greater growth potential for businesses that pursue Internet connectivity while simultaneously establishing themselves as leaders in cybersecurity. As the risks of being hacked and the number of hacking incidents grow, consumer preference for security will continue to increase. Thus, greater trust in more cybersecure businesses should yield greater profitability and return on investment.

6. Businesses need to drive the conversation

Astute businesspeople recognize the obvious incentives to begin driving the cybersecurity conversation, including the need for protection against hackers, the desire to influence the policy discussion, and the realization that securing sensitive data can result in increased profitability. Fortunately, there is a clear path to becoming a leader in cybersecurity.

6.1. Start with leadership

The Internet is, and will continue to be, a key driver for sustainable and profitable businesses. The rising value of information and technology in every industry demonstrates the need for a chief information officer (CIO) or chief technology officer (CTO) and even more importantly, the need to capitalize on the potential of the position. Corporate information and technology officers must be welcomed into a company's top-level management, regarded with respect, and empowered to do more than just technology maintenance. They must be allowed to add value throughout the organization.

There is a clear gap between current practices and best practices for organizations in terms of optimizing the CIO position. The dilemma is this: CIOs and their IT departments are becoming increasingly important to the functioning of businesses everywhere, but CIOs and IT departments have increasingly less say in the strategic and growth-oriented decisions of an organization. Put bluntly, "[t]he greater the impact on the business, the more business executives expect the CIO to just do what they tell him or her to do. . . [and not] influence the business strategy or play a major role in its growth" (Press, 2015). A global survey found this to be true for most CIOs. The percentage of CIOs who reported having a "collaborative partnership with business leaders" fell from 41% in 2013 to 28% in 2014 (Computer Sciences Corporation, 2015; Press, 2015). Another 2014 survey confirmed this growing perception that IT departments are not qualified to take part in developing business strategy (Arandjelovic, Bulin, & Khan, 2015). CIOs are perceived as tools trained to quantify and analyze risk and spit out information rather than to participate actively in strategic discussions.

The potential of the CIO to add value is enormous, and companies that capitalize on that potential will emerge as industry leaders. The current climate of weak cybersecurity is a direct result of poor utilization of the position. A 2015 report predicted that (Experian, 2015):

> Senior executives will be expected to have a better understanding of the data breach response plan, comprehension of new technologies and security protocols in the workplace and have a clearly-defined chain of response should a breach occur.

Who better to proactively handle this than CIOs, provided they are allowed to help make decisions and collaborate with other departments? The report also predicted a rise in scrutiny of executives at the highest levels and an increase in legal and regulatory scrutiny. The current culture in which CIOs are left out of strategy discussions and asked to do increasing amounts of critical work with stagnating resources[2] simply makes no sense. CIOs must be given the necessary resources and be empowered to drive change and develop strategy if companies are to successfully mitigate the risk of cyberattacks (Experian, 2015; Lawrie, 2015). Rather than shooting the messenger, companies should use CIOs to craft an effective plan to prevent a catastrophe on the scale of recent data breaches.

6.2. Develop and follow best practices

Make a plan. Take the quick wins. Then move past compliance and be strategic. Businesses that take these steps will significantly reduce the risks that they face. A codified plan of action is essential for businesses to successfully focus on several primary aspects of cybersecurity. The plan must encompass how to maintain cybersecurity, how to respond to breaches, and how to effectively manage and maximize its employees' potential. Businesses must also consider the strategy and direction of technology and data use moving forward, with a full understanding of all potential risks.

6.2.1. Collect only what you need (or will need)

Many organizations collect and hold on to data much longer than is necessary—sometimes even indefinitely. Some do it for regulatory reasons, some do it because it is cheap and easy, and some do not even realize that they are doing it. Regardless, this practice creates treasure troves for hackers, who—like most opportunistic criminals—pursue prospects with the highest payoff for the least amount of effort and risk. In many cases, the payoff can be enormous; the situation that befell Target is a prime example. The solution is to hold on to only what data is necessary and only for as long as is required to limit potential damages if a company is hacked.

Companies should take a deep dive into their data repositories, determining whether or not the data they are keeping is necessary to drive business value. If it is no longer necessary, the next step is to safely dispose of the data. The key here is to do this work in a secure manner; in other words, dispose of data utilizing the equivalent of a paper shredder for these digital data points. Finally, policies must be put in place not only to protect data but to ensure its usefulness. Companies must decide what type of data to keep and for how long before it is securely deleted (Information Commissioner's Office, n.d.).

6.2.2. Follow existing best practices

One of the most innovative and effective practices is for a company to try to hack its own systems or to hire a professional white hat hacker to do so; this is essentially a stress test of its IT infrastructure and personnel. The idea is for the company to learn its own vulnerabilities through trial by fire so that it knows exactly what it needs to fix.

White hat hackers are also useful in determining when and how the actual hackers will attack. They can take the pulse of the hacking world, learn the latest hacking techniques, and allow companies to test the security of their systems with someone they trust. They may even be able to infiltrate hacker circles on the dark web and befriend would-be attackers.

Even if all of a business's technical systems are advanced, updated, and ready to fight off hackers, Target's example demonstrates that this is not enough. One of the most powerful hacking techniques is social engineering—essentially the manipulation of employees—to gain access to credentials or technical systems. This could be as simple as calling and pretending to be someone in a position of authority so that the hacker can gain credentials and access to the system, or as complex as walking into the company's building, posing as a maintenance worker or even IT support, and inserting a malware-infested thumb drive into a computer. The reality is that as humans, we want to trust. The key is figuring out who to trust and when (Shaw, 2013). This is a critical part of a company's employee policies, procedures, and training.

6.2.3. Bolster and maintain the system

The first step to maintaining a secure system is identifying and addressing vulnerabilities. One report found that "99.9% of the exploited vulnerabilities were compromised more than a year after the common vulnerability and exposure (CVE) was published" (Verizon Enterprise, 2015a). This means that

[2] Only 26% saw material budget increases in 2015.

companies are making themselves vulnerable through inactivity. Companies should engage in comprehensive and periodic patching of their systems, with an exigent plan to address those vulnerabilities that gain media attention. This will significantly reduce risks from vulnerabilities that are easy to fix.

Maintaining a functioning IT infrastructure requires the ability to respond to vulnerabilities as they arise. Corporate decision makers should take an active role in preparing for data breaches and in planning the business's response (Experian, 2015). The Target data breach serves as an example of what happens when an ineffective response plan is in place.

Companies should also be tracking and logging all activities related to their systems, and identifying the most valuable and likely targets of attack. Monitoring enables companies to identify and address vulnerabilities, saving them the embarrassment and cost of cybersecurity breaches. Companies must have an understanding of who and what may be potential targets of cyberattacks. This information will help identify the people most in need of training and the information and data most in need of protection (Newman & Caplan, 2015).

6.2.4. Employees may be your weakest link

Employees are a company's most valuable, and also most vulnerable, asset. Employees accounted for 59% of security incidents in 2014, and in U.S. companies alone, the unauthorized use of computers by employees accounted for $40 billion in losses (Experian, 2015). The central problem is that employees are not receiving the training that they need.

As consumers of modern technology, employees can develop habits that expose businesses to hacking. One such habit is their use of passphrases. A 2014 study estimated that the average person must remember passwords for 25 distinct accounts and that up to 51% of users reuse the same password for multiple sites (Das, Bonneau, Caesar, Borisov, & Wang, 2014). In addition, one can access an increasing number of sites simply by signing into a social media account like Facebook or LinkedIn. A hacker who gains access to such seemingly innocuous social media accounts may use them to access other sites containing more sensitive information. Finally, people's passwords are often easy to discover. Researchers in a 2014 study were able to guess 30% of non-identical passwords (Das et al., 2014). Hackers who do their research and run some simple analyses like the researchers in the study could access the accounts of a significant percentage of people using the Internet.

The practice of phishing—utilizing official-looking emails and websites to defraud someone of their personal information—exacerbates the problem of lost credentials. Phishing has been on the rise since 2011, with one report finding that 23% of recipients open phishing emails and 11% click on attachments (Verizon Enterprise, 2015a). Organizations must develop policies and practices to ensure that employees do not freely disclose credentials in such events.

Employees are particularly vulnerable to phishing attacks because they receive and respond to hundreds of emails every day. On the bright side, effective training and awareness can enhance employees' technological capabilities and reduce the number of people who fall victim to phishing to less than 5%, thereby reducing a company's vulnerabilities to phishing (Verizon Enterprise, 2015a). The key is training to raise employees' technical and cybersecurity intelligence, which ultimately raises the security intelligence of consumers everywhere. Employees often introduce vulnerabilities by abusing their privilege to proprietary information—including illegally selling such information—and by introducing shortcuts for convenience that unknowingly expose companies to great risk. Companies must educate employees about secure data practices.

Training alone is not enough. Companies must also utilize big data and data analytics on their employees' behavior and data flows. This will help identify where infractions and violations of data security are occurring. The risks posed by disgruntled employees must be watched closely. Essentially, companies must trust their employees but verify their activities (Verizon Enterprise, 2015a). This is especially important given the increasing use and growing importance of cloud technologies, the Internet of Things, and mobile devices in daily business operations.

7. Cybersecurity can affect your bottom line

The Target data breach, if well heeded, can serve as a valuable lesson for businesses today. Cybersecurity threats are not about to go away. Companies need to be prepared and proactive to protect their customers, their information, their reputation, and their bottom line.

Acknowledgment

The authors wish to thank Professor Anjanette Raymond for her assistance, guidance, and feedback on this article.

References

Anand, P. (2015, July 20). When a hack could kill. *MarketWatch*. Retrieved November 25, 2015, from http://www.marketwatch.com/story/when-a-hack-could-kill-2015-07-20

Arandjelovic, P., Bulin, L., & Khan, N. (2015, February). Why CIOs should be business-strategy partners. *McKinsey & Company*. Retrieved from http://www.mckinsey.com/insights/business_technology/why_cios_should_be_business-strategy_partners

Committee on Commerce, Science, and Transportation. (2014, March 26). A "kill chain" analysis of the 2013 Target data breach. *United States Senate, 113th Congress*. Retrieved from http://www.commerce.senate.gov/public/_cache/files/24d3c229-4f2f-405d-b8db-a3a67f183883/23E30AA955B5C00FE57CFD709621592C.;1;2014-0325-target-kill-chain-analysis.pdf

Committee on the Judiciary. (2014, February 4). Privacy in the Digital Age: Preventing data breaches and combating cybercrime. *United States Senate, 113th Congress*. Retrieved from http://www.judiciary.senate.gov/imo/media/doc/02-04-14MulliganTestimony.pdf

Computer Sciences Corporation. (2015). *CSC global CIO survey 2014-2015: CIOs emerge as disruptive innovators*. Retrieved from http://assets1.csc.com/cio_survey_2014_2015/downloads/CIO_Survey_Disruptive_innovation.pdf

Constantin, L. (2014, January 13). Target point-of-sale terminals were infected with malware. *PCWorld*. Retrieved from http://www.pcworld.com/article/2087240/target-pointofsale-terminals-were-infected-with-malware.html

Cooney, P., Kurane, S., Walsh, E., & Dwivedi, A. (2015, March 19). Target agrees to pay $10 million to settle lawsuit from data breach. *Reuters*. Retrieved November 25, 2015, from http://www.reuters.com/article/us-target-settlement-idUSKBN0MF04K20150319

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X-F. (2014). The tangled web of password reuse. *Internet Society*. Retrieved from http://www.internetsociety.org/sites/default/files/06_1_1.pdf

Embry, S. E. (2015, July 6). At risk: Community banks and the recovery of losses due to merchant data breach. *Lexology*. Retrieved November 25, 2015, from http://www.lexology.com/library/detail.aspx?g=eceb0fee-7686-4f9b-bfbe-f53e6903540d

Experian. (2015). *2015 second annual data breach industry forecast*. Retrieved from http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf?_ga=1.172114915.1943093614.1418003182

Finkle, J., & Heavey, S. (2014, March 13). Target says it declined to act on early alert of cyber breach. *Reuters*. Retrieved from http://www.reuters.com/article/2014/03/13/us-target-breach-idUSBREA2C14F20140313

Goldman, J. (2015, April 10). AT&T hit with record-breaking $25 million data breach fine. *eSecurity Planet*. Retrieved from http://www.esecurityplanet.com/network-security/att-hit-with-record-breaking-25-million-data-breach-fine.html

Goodman, E. (2014, June 30). Data breach suit verdict impacts third party. *Claims Journal*. Retrieved from http://www.claimsjournal.com/magazines/idea-exchange/2014/06/30/250781.htm

Hasnie, A. (2015, July 7). Target data breach inspires new BBB Scam Tracker tool. *Fox59*. Retrieved from http://fox59.com/2015/07/07/target-data-breach-inspires-new-bbb-scam-tracker-tool/

Hill, C. (2014, September 25). Home Depot's data breach is worse than Target's, so where's the outrage? *MarketWatch*. Retrieved November 25, 2015, from http://www.marketwatch.com/story/yawn-who-cares-about-home-depots-data-breach-2014-09-24

Hizver, J., & Chiueh, T. (2012). An introspection-based memory scraper attack against virtualized point of sale systems. *Lecture Notes In Computer Science: Financial Cryptography and Data Security (Vol. 7126)*. Retrieved from https://ifca.ai/pub/fc11/rlcps11/Session2-2.pdf

Hosenball, M. (2014, February 6). Target vendor says hackers breached data link used for billing. *Reuters*. Retrieved from http://www.reuters.com/article/2014/02/06/us-target-breach-vendor-idUSBREA1523E20140206

Howland, D. (2015, December 3). Target reaches $39.4 M settlement with banks over massive breach. *RetailDive*. Retrieved from http://www.retaildive.com/news/target- reaches-394m-settlement-with-banks-over-massive-breach/410208/

Information Commissioner's Office. (n.d.). *Guide to data protection: Retaining personal data (Principle 5)*. Retrieved November 25, 2015, from https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/

Kharpal, A. (2015, March 17). Biggest hacking threat to business? Wearables. *CNBC*. Retrieved from http://www.cnbc.com/2015/03/17/biggest-hacking-threat-to-business-wearables.html

Lawrie, G. (2015, February 19). The retail CIO agenda 2015: Secure and innovate. *Forrester Research, Inc*. Retrieved from https://nrf.com/sites/default/files/The%20Retail%20CIO%20Agenda%202015_%20Secure%20And%20Innovate.pdf

Learmonth, M. (2015, January 7). In 2015, a new kind of hack to worry about: The smart home. *International Business Times*. Retrieved from http://www.ibtimes.com/2015-new-kind-hack-worry-about-smart-home-1775488

Lee, T. (2015, July 25). Forget the Ashley Madison or Sony hacks — a crippling cyberattack is imminent in the US. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2015/jul/26/cybercrime-hacking-internet-of-things-target

Nakashima, E. (2015, July 9). Hacks of OPM databases compromised 22.1 million people, federal authorities say. *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

Newman, C. A., & Caplan, S. (2015, June). New Target ruling places your company's cyber oversight in the crosshairs. *Patterson Belknap*. Retrieved from https://www.pbwt.com/publications/new-target-ruling-places-your-companys-cyber-oversight-in-the-crosshairs/

Press, G. (2015, February 23). The CIO dilemma: What new surveys say about IT's declining strategic role. *Forbes*. Retrieved from http://www.forbes.com/sites/gilpress/2015/02/23/the-cio-dilemma-what-new-surveys-say-about-its-declining-strategic-role/

Privacy Rights Clearinghouse. (2015). *Chronology of data breaches*. Retrieved from http://www.privacyrights.org/data-breach

Remijas v. Neiman Marcus Group LLC. (2015, July 20). No. 14-3122, 7th Circuit Court.

Riley, M., Elgin, B., Lawrence, D., & Matlack, C. (2014, March 13). Missed alarms and 40 million stolen credit card numbers: How Target blew it. *Bloomberg Business*. Retrieved November 24, 2015, from http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

Roberts, J. J. (2015, July 29). This court ruling just made it easier to sue companies that get hacked. *Fortune*. Retrieved from http://fortune.com/2015/07/29/data-breach-7th-circuit/

Sanger, D. E., & Hirschfeld Davis, J. (2015, June 4). Hacking linked to China exposes millions of U.S. workers. *The New York Times*. Retrieved from http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html?_r=2

Shaw, R. (2013, September 23). Social engineering: A hacking story. *Hacking*. Retrieved from http://resources.infosecinstitute.com/social-engineering-a-hacking-story/

Shearman, J. C. (2015, March 27). One step closer to a national data breach standard. *National Retail Federation*. Retrieved November 25, 2015, from https://nrf.com/news/one-step-closer-national-data-breach-standard

Sidel, R. (2015, June 2). Biggest MasterCard issuers scuttled deal on Target data breach. *The Wall Street Journal*. Retrieved November 25, 2015, from http://www.wsj.com/articles/biggest-mastercard-issuers-scuttled-deal-on-target-data-breach-1433253072

Smith, C. (2014, March 13). It turns out Target could have easily prevented its massive security breach. *Yahoo News*. Retrieved from http://news.yahoo.com/turns-target-could-easily-prevented-massive-security-breach-180005247.html

Target Corporation. (2014, January 13). Target announces $5 million investment in new cybersecurity coalition. *A Bullseye View*. Retrieved from https://corporate.target.com/article/2014/01/target-introduces-cybersecurity-coalition/

Target Corporation. (2015). *2014 annual report*. Retrieved November 25, 2015, from https://corporate.target.com/annual-reports/2014/financials/financial-highlights

Tene, O. (2015, July 24). Neiman Marcus may open the floodgate for breach lawsuits. *International Association for Privacy Professionals*. Retrieved from https://iapp.org/news/a/neiman-marcus-may-open-the-floodgates-for-breach-lawsuits/

Vardy, N. A. (2015, June 24). Cybersecurity shares continue to outclass the S&P. *MarketWatch*. Retrieved from http://www.marketwatch.com/story/cybersecurity-shares-continue-to-outclass-the-sp-2015-06-24?page=2

Verizon Enterprise. (2015a). *2015 Data breach investigations report*. Retrieved from http://www.verizonenterprise.com/DBIR/2015/

Verizon Enterprise. (2015b). *State of the market: The Internet of Things 2015*. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-things-2015_en_xg.pdf