Journal of Information Systems Education

Volume 29
Issue 1
Winter 2018

Teaching Case
Security Breach at Target

Miloslava Plachkinova and Chris Maurer

Recommended Citation: Plachkinova, M. & Maurer, C. (2018). Teaching Case: Security Breach at Target. *Journal of Information Systems Education*, 29(1), pp. 11-20.

Article Link: http://jise.org/Volume29/n1/JISEv29n1p11.html

Initial Submission:	31 January 2017
Accepted:	26 October 2017
Abstract Posted Online:	12 December 2017
Published:	21 March 2018

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Teaching Case
Security Breach at Target

Miloslava Plachkinova
Department of Information and Technology Management
University of Tampa
Tampa, FL 33606, USA
mplachkinova@ut.edu

Chris Maurer
McIntire School of Commerce
University of Virginia
Charlottesville, VA 22903, USA
maurer@virginia.edu

ABSTRACT

This case study follows the security breach that affected Target at the end of 2013 and resulted in the loss of financial data for over 70 million customers. The case provides an overview of the company and describes the reasons that led to one of the biggest security breaches in history. It offers a discussion on Target's vendor management processes and the vulnerability at Fazio Mechanical Services that was among the main causes of the breach. Further, the case introduces the incident response plan implemented by Target and discusses the aftermath of the attack. The lessons learned describe some of the steps the company took to mitigate risks in the future and to strengthen its security posture. While the breach had a significant impact on Target, the organization was able to fully recover from it and develop best practices that are now widely implemented by other retailers. The case is suitable for both undergraduate and graduate students enrolled in information security or information systems courses that discuss vendor management, security incident response, or general security program administration topics.

Keywords: Information assurance & security, Cybersecurity, Case study, Teaching case, Experiential learning & education

1. INTRODUCTION

There are numerous definitions of information security, but many of them revolve around achieving confidentiality, integrity, and availability of the information and/or systems (Anderson, 2003; Dhillon and Backhouse, 2000; Sumra, Hasbullah, and AbManan, 2015; Von Solms and Van Niekerk, 2013). These goals are important, as they provide trust and guarantee the safety of data in motion and data at rest.

Within the retail industry, information security is critical as it ensures that the organizations follow best practices and can protect the personal and financial information of the customers. As Greig, Renaud, and Flowerday (2015) point out, a focus on employee behavior is vital since an "organization's success or failure effectively depends on the things that its employees do or fail to do" (Da Veiga and Eloff, 2010). Security culture has the potential to play a significant role in this respect (Vroom and Von Solms, 2004). A strong and effective security culture is in place when every employee performs daily tasks in a secure manner and such secure behavior is considered to be 'the norm' (Von Solms, 2000). Demonstrating a strong security posture is especially important for retail companies because they rely on having positive brand recognition and gaining the customers' trust. A security breach at a big retail company can also have a domino effect and potentially impact many other corporations in a negative way. Thus, understanding the critically important factors in building a strong security culture and following best practices is essential for any retail company.

2. MOTIVATION

The authors' motivation to write this case study comes from the need to incorporate real world examples into the cybersecurity curriculum. While it is important for students to master terminology and have solid foundational knowledge, the authors believe they should also be able to apply the knowledge to actual organizational settings where information security issues arise. There has been a myriad of breaches affecting a wide range of companies and individuals (Home Depot, JP Morgan Chase, Ashley Madison, the Office of Personnel and Management, eBay, Sony, and Hillary Clinton),

but there are relatively few case studies developed solely for use in the classroom with accompanying learning objectives and teaching notes. Thus, the authors wanted to explore the recent security breach at Target due to the abundance of information available and the various angles from which the students can approach the topic.

3. EVALUATION

After drafting the case text, it was distributed to students in an information security principles course at a medium-sized, private university in the US. Thirty eight undergraduate students were presented with the case text and reflection questions (provided in the teaching notes). Students' analyses of the case and reflection questions were collected as part of a graded assignment and were evaluated using rubrics to determine whether students exceeded, met, or did not meet expectations across various learning objectives. The authors also provided students with a paper survey that included several open-ended questions. The authors asked them to describe what they liked and disliked about the case, whether any additional information should be provided, whether they have any suggestions for improvement, and what sources they used when preparing their analyses. Overall, students provided very positive feedback on the case write-up. Students expressed some concern over the discussion of vendor management processes, and therefore additional detail around the vendor management processes was added to the case.

In terms of performance against leaning outcomes, the average grade students received on this assignment was 94%, which exceeds expectations. More specifically, 1 student did not meet the expectations (<65%), 9 students met the expectations (65-89%), and 28 students exceeded the expectations (>90%). These results indicate that students were able to successfully perform the case study analysis, understand and interpret the main issues, and provide feasible and adequate solutions for improving the security practice at Target Corp. The authors evaluated the students' writing skills, as well as their ability to support their statements with additional resources, readings, and integrate previous course content in their analysis. The authors used TurnItIn to avoid any plagiarism on the assignment, and the grading rubrics were adapted from the University's College of Business recommended rubric for problem solving.

4. CASE SYNOPSYS

At the end of 2013, amid the holiday shopping season, Target became a victim of a security breach affecting over 70 million customers. Their personal and financial data was stolen through a vulnerability in one of Target's vendors – Fazio Mechanical Services. The breach was first reported by the security journalist Brian Krebs, and Target's official response came shortly after the announcement. While slightly late, the company's incident management was still successful as they were able to regain the customers' trust and maintain their status as a successful retailer. After the attack, Target implemented several steps to mitigate any future breaches. The company created a Cyber Fusion Center, provided free credit card monitoring for its customers, and implemented POS terminals with chip readers. These steps demonstrate Target's efforts to improve its security and minimize the risk of other attacks in the future.

The structure of the presented case study is as follows: Target's company profile, the timeline of the events, the company's business processes before and after the breach (including vendor management and incident response), the investigation, the fallout, and lessons learned.

5. CASE TEXT

5.1 Company Profile

With its first store opening in Roseville, Minnesota, on May 1, 1962, Target aimed to differentiate itself by providing many features of traditional department stores but provide low prices typically associated with discount retailers. The name Target was chosen purposefully as Stewart Widdess (Director of Publicity) states "As a marksman's goal is to hit the center bulls-eye, the new store would do much the same in terms of retail goods, services, commitment to the community, price, value and overall experience" (Target, 2017). The company went public on October 18, 1967, (under the name "Dayton Corporation") and began expanding across the country. Through various acquisitions and expansions into new areas of the country, Target has become the second-largest discount retailer in the United States (behind Walmart). As of February 1, 2014, Target operated 1,793 retail store locations in the United States, employed approximately 360,000 employees, and had annual revenues of $72.6 billion (Statista, 2015).

Target's slogan of "Expect more. Pay less." embodies their corporate mission of providing great value to its customers while maintaining an exceptional shopping experience. A key component of Target's strategy for creating an exceptional experience for both customers and employees is to always behave ethically and with integrity. Their efforts to be a responsible corporate citizen have earned various awards such as inclusion on Fortune Magazine's "20 Most Generous Companies of the Fortune 500" and "World's Most Admired Companies" lists (Target, 2017).

While Target has worked diligently to position itself as a leading retailer in the United States with prominent charitable values, they have certainly experienced hardships throughout their long history. Notably, in 2013, they suffered a massive data breach that exposed sensitive financial information for millions of customers. While the data breach significantly affected Target's operations, the company has recovered and has learned many valuable lessons on the importance of protecting sensitive information.

5.2 Before the Breach

Like many corporations, Target employed a staff of dedicated security professionals to implement safeguards to protect sensitive data. As part of their ongoing security efforts, Target successfully passed a compliance audit for the Payment Card Industry Data Security Standard (PCI-DSS) in September of 2013 (Riley et al., 2014). PCI audits involve a review of critical security controls and systems configurations to verify that best practices for protecting payment card information on computer systems is maintained. Target also completed the implementation of a $1.6 million malware detection tool developed by the cybersecurity company FireEye in 2013 (Riley et al., 2014). Their security operations center, with

teams of personnel in Minneapolis, Minnesota, and Bangalore, India, provided round-the-clock monitoring of cybersecurity threats on the network. While there is no method for ensuring complete protection against cybersecurity threats, Target appeared to be following industry best practices and had reasonable security controls in place.

5.3 Breach Notification and Initial Response

On November 30, 2013, security operations personnel in Bangalore, India, received a notification from their malware detection software that some potentially malicious activity was recorded on the network. The alert was shared with security personnel in Minneapolis, but no further action was taken. Another alert was raised on December 2, 2013, but again no action was taken (Riley et al., 2014). It was not until December 12, 2013, when the U.S. Department of Justice contacted Target about a possible data breach on their network, that Target began investigating the issue in earnest. The Federal Bureau of Investigation (FBI) and the Secret Service joined the investigation as well. While no public disclosure was made at the time, the independent security researcher and blogger, Brian Krebs, posted information regarding a possible breach of the Target network on December 18, 2013. On December 19, 2013, Target issued the following public statement on the matter:

> Target today confirmed it is aware of unauthorized access to payment card data that may have impacted certain guests making credit and debit card purchases in its U.S. stores. Target is working closely with law enforcement and financial institutions, and has identified and resolved the issue.
>
> "Target's first priority is preserving the trust of our guests and we have moved swiftly to address this issue, so guests can shop with confidence. We regret any inconvenience this may cause," said Gregg Steinhafel, chairman, president and chief executive officer, Target. "We take this matter very seriously and are working with law enforcement to bring those responsible to justice."
>
> Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013. Target alerted authorities and financial institutions immediately after it was made aware of the unauthorized access, and is putting all appropriate resources behind these efforts. Among other actions, Target is partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident.

Initially, Target denied that debit card PIN numbers had been stolen, but reports confirmed that encrypted PIN numbers had indeed been stolen (Finkle and Henry, 2013). Another update (Target, 2014) on the breach was provided by the company a month later, on January 10, 2014, outlining the fact that personal information (names, addresses, phone numbers, and email addresses) were also taken in this breach. While there were some critiques about the fact that the company delayed its response after initially identifying the breach, Target Chairman and CEO Gregg Steinhafel defended the decision:

> Sunday (Dec. 15) was really day one. That was the day we confirmed we had an issue and so our number one priority was ... making our environment safe and secure. By six o'clock at night, our environment was safe and secure. We eliminated the malware in the access point, we were very confident that coming into Monday guests could come to Target and shop with confidence and no risk.
>
> Day two was really about initiating the investigation work and the forensic work ... that has been ongoing. Day three was about preparation. We wanted to make sure our stores and our call centers could be as prepared as possible, and day four was about notification. (Quick, 2014)

In addition to the public response, Target sent out an email to its customers (Appendix A) on January 16, 2014, offering one year of free credit monitoring. The company provided them with information about protecting themselves and staying safe. However, the email was sent to many individuals who never had conducted business with Target, which raised speculation as to how the retailer obtained the data. One possible explanation is that perhaps the email addresses were from Amazon, a remnant from the old Amazon-Target partnership. However, when consumers asked where Target obtained email addresses for people who are not now and have never been customers of the retailer, the spokeswoman simply said, "The information was obtained by Target through the normal course of our business" (Quirk, 2014). Instead of retaining its customers and solidifying their trust with the offered incentives, Target opened another door for speculations on its processes for collecting and handling customer data.

5.4 The Investigation

As part of the incident response process, Target commissioned security professionals at Verizon to assist in the investigation into how the breach occurred. A detailed security audit was performed from December 21, 2013, to March 1, 2014, and served two primary purposes: 1) identify the root cause of the breach and 2) identify opportunities to improve the security of Target's infrastructure. While the report issued by Verizon has remained confidential, various media outlets claimed to have received information stemming directly from the report. The findings presented below have not been confirmed by Target, but have been reported by several reputable security researchers and media outlets.

The initial point of entry appears to have stemmed from hijacked credentials stolen from Fazio Mechanical Services, a third party service provider. Fazio, a supplier of refrigeration devices and services, began working with Target to support the expansion of fresh food offerings across stores in the United States. As with many other vendors and suppliers of Target, Fazio was provided access to Target's systems to handle "electronic billing, contract submission, and project management." Fazio Mechanical did not, however, "perform remote monitoring or control of heating, cooling, or refrigeration systems for Target" (Fazio Mechanical Services, 2014).

In the fall of 2013, Fazio Mechanical Services was the "victim of a sophisticated cyber-attack operation" despite

stating that their "IT system and security measures are in full compliance with industry best practices" (Fazio Mechanical Services, 2014). Industry experts believe the breach involved an infection of the 'Citadel' malware that can be used to steal logon credentials from computer systems. Despite a claim that Fazio was in compliance with "industry best practices," it has been alleged that Fazio relied on the free, non-commercial version of Malwarebytes Anti-Malware software, which does not provide real-time protection. It is not clear whether Target enforced any ongoing security reviews of its vendors to ensure compliance with security best practices.

While this attack did not appear to have an immediate impact on Fazio, it is likely that account credentials for accessing Target systems were stolen during the Fazio breach. Access to Target's systems granted to Fazio would not have allowed attackers to access customer data, however, so additional vulnerabilities inside the Target network must have allowed attackers to escalate their account privileges, traverse the network, and obtain over 40 million customer card numbers.

Further investigation revealed that there were no major obstacles to accessing point of sale (POS) terminals across the entire network once inside the internal Target network. This lack of network segmentation could allow any malicious user the ability to traverse the network and attempt to access various devices ranging from point of sale terminals to mission critical back-end systems. To illustrate the lack of segmentation, the Verizon audit team supposedly accessed a cash register after they compromised a deli counter scale that was located in a different store (Krebs, 2015).

The audit team also found significant problems with enforcement of password policies. Target maintained a password policy that included industry-standard practices, however investigators found multiple files stored on Target servers that included logon credentials for various systems. According to Brian Krebs, the audit report revealed that

> The Verizon security consultants identified several systems that were using misconfigured services, such as several Microsoft SQL servers that had a weak administrator password, and Apache Tomcat servers using the default administrator password. Through these weaknesses, the Verizon consultants were able to gain initial access to the corporate network and to eventually gain domain administrator access. (Krebs, 2015)

The use of weak passwords was apparently rampant within the Target infrastructure, and the security investigation team was able to crack over 500,000 passwords, representing 86% of identified accounts, to various internal Target systems.

Investigators also identified significant issues related to the maintenance and patching of systems. Again, Brian Krebs claims:

> For example, the Verizon consultants found systems missing critical Microsoft patches, or running outdated [web server] software such as Apache, IBM WebSphere, and PHP. These services were hosted on web servers, databases, and other critical infrastructure. These services have many known vulnerabilities associated with them. In several of these instances where Verizon discovered these outdated services or unpatched systems, they were able to gain access to the affected systems without needing to know any authentication credentials. Verizon and the Target Red Team exploited several vulnerabilities on the internal network, from an unauthenticated standpoint. The consultants were able to use this initial access to compromise additional systems. Information on these additional systems eventually led to Verizon gaining full access to the network – and all sensitive data stored at on network shares – through a domain administrator account. (Krebs, 2015)

Given the previously stated vulnerabilities, the attackers were able to access point of sale terminals and install malware directly on all machines across the network. Given the timing of the alerts triggered by Target's anti-malware software in late November and early December, it is likely that the malware was installed on the terminals at this time.

The malware contained memory-scraping functionality that allowed the attackers to intercept cardholder information before it was sent for processing by a payment processor. The PCI-DSS specifically requires payment card processors to "encrypt transmission of cardholder data across open, public networks" (Security Standards Council, 2016). However, the configuration of point of sale terminals at Target did not provide the ability to immediately encrypt cardholder data upon registering a card swipe. Because of this, card data remained in plain text within the POS terminal's memory. This data was only encrypted upon preparation for transit to external card processing systems (as required under PCI-DSS). Since the malware was installed directly on POS terminals and allowed the ability to scrape data from memory of these machines, the attackers were able to intercept unencrypted cardholder data for all card swipes registered in Target stores.

5.5 The Fallout

Target has claimed that up to 70 million individuals may have been impacted by this data breach (Target, 2015a). At the time, this was one of the top ten largest data breaches recorded (Quick et al., 2016). In the aftermath of the breach, consumer confidence in Target was impaired significantly. According to Kantar Retail, a consulting group researching consumer spending behaviors, the percentage of U.S. households shopping at Target in January 2014 was 33%. This was down from 43% for the same month the preceding year (Malcolm, 2014). In Target's annual report filed with the SEC on March 14, 2014, the company stated:

> We believe the Data Breach adversely affected our fourth quarter U.S. Segment sales. Prior to our December 19, 2013, announcement of the Data Breach, our U.S. Segment fourth quarter comparable sales were positive, followed by meaningfully negative comparable sales results following the announcement. Comparable sales began to recover in January 2014. The collective interaction of year-over-year changes in the retail calendar (e.g., the number of

> days between Thanksgiving and Christmas), combined with the broad array of competitive, consumer behavioral and weather factors makes any quantification of the precise impact of the Data Breach on sales infeasible. (United States Securities and Exchange Commission, 2014)

While it is difficult to quantify the exact impact of the breach on Target's financials, the company experienced a 1% decrease in revenues from 2012 to 2013, and its net income decreased 34.3% in that same time period. The large impact to net income was largely attributable to the additional costs associated with investigating and remediating the security breach.

The financial impacts were not limited to the few months following the breach, however. Over the course of the next two years, Target continued to incur costs related directly to the security breach. According to Target's 10-Q and 10-K filings with the SEC, the company has incurred $291 million in cumulative expenses related to this breach. Of this, approximately $90 million was offset by insurance coverage, leaving Target with a total direct cost of just over $200 million (United States Securities and Exchange Commission, 2016). The breakdown of costs reported by Target for each quarter from the announcement of the breach to May 2015 are displayed in Figure 1:

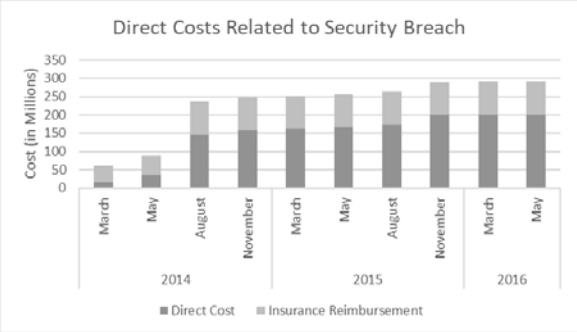

Figure 1: Cumulative Costs Related to Security Breach, by Quarter

5.6 Lessons Learned

Even though Target experienced one of the biggest data breaches in history, it is still a successful business with almost 1,800 stores in North America in 2015 (Target, 2016). While the attack did impact the company, there are some key factors that had a positive impact on Target's image. For example, customer loyalty is something that builds over time and even such a massive security flaw could be overlooked by the most devoted and dedicated individuals who associate themselves with the company. Some of them even perceived Target as a victim of the attackers and sympathized with the company during the hard times it was experiencing.

On Target's end, the company invested heavily in improving its cybersecurity operations, and in 2015 created the first Cyber Fusion Center, which is dedicated to preventing similar attacks from happening again. Brian Cornell, chairman and CEO of the company, said:

> Data security is a top priority at Target, so we continue to invest heavily in top talent, as well as technology, and focus on continually evaluating and evolving our processes as the landscape changes. It's an important part of the $1 billion Target plans to invest in technology and supply chain this year. (Target, 2015b)

Brad Maiorino, Target's Chief Information Security Officer, added:

> We've got teams of Cyber Security analysts working round the clock. They use a mix of human intelligence, analytics and state-of-the-art technology to detect, investigate and contain threats to our business. Much of the work they do takes place in our newly opened Cyber Fusion Center (CFC). (Target, 2015b)

Another improvement that Target made was adding chip readers with PIN codes for customers. In fact, Target became the first major U.S. issuer to use chip and PIN credit cards in 2015 (DiGangi, 2015), even as most card issuers in the United States were issuing less secure chip and signature cards. The addition of an EMV chip makes a card more difficult and more expensive to counterfeit. However, adding a PIN code on top of the EMV chip makes it even less likely that card information can be stolen and used to make unauthorized purchases.

Last but not least, the attack impacted Target's profits and caused some top management turnover. Target's CEO at the time of the breach, Gregg Steinhafel, a 35-year employee of the company with the last 6 at the helm, resigned in May 2014. The CIO was also replaced with Bob DeRodes, an executive with a very strong background in information security. The Target board of directors was also under significant pressure. A proxy firm, Institutional Shareholder Services, had recommended that investors oust seven board members. The firm said the board failed to protect the company from the data breach. The board members were able to convince shareholders to re-elect them, however, although the message to them was clear that future data security breaches were considered to be their responsibility (Basu, 2014). The full press release from Target regarding the managerial changes is available in Appendix B.

Although Target never shared directly any lessons learned, the examples above illustrate the company's ambition to improve its security practices and offer more protection for its customers. Taking responsibility for the breach at the highest level was something that is still uncommon in organizations of such scale. Overall, the breach enforced many new rules and practices with regards to information security, as both retailers and customers were now aware of the consequences of such an attack.

6. CONCLUSION

While the security breach at Target impacted a single corporation, it is important to note that such breaches have now become part of our everyday lives. It is not a matter of if, but when a breach will occur. Thus, the authors believe that

the lessons learned from Target are valid and can be generalized to other organizations as well. For instance, the breach stimulated other retailers such as Wal-Mart and Home Depot to install chip readers on their POS terminals. Such best practices show that others realize the importance of strengthening their security posture and providing better protection against individuals with malicious intents. Further, Target demonstrated that they have the capacity to recover from such serious events due to having up-to-date disaster recovery/business continuity plans. These best practices should be followed by others who want to prepare themselves for the inevitable.

In conclusion, this case study provides an objective view of the events surrounding the 2013 Target breach and outlines both the adequate and inadequate actions taken by the corporation. The authors' goal is to increase students' knowledge on how major organizations are impacted by such attacks, what can be done to limit these breaches in the future, and how to be better prepared to respond when they happen. The case study adds value to the cybersecurity curriculum as it requires students to put into practice the knowledge they gained from the classroom and apply it to a real world scenario. The case study reveals the complexity of the security breach and its impact on the business processes and customer trust – factors that any business professional should understand before going to the industry.

7. ACKNOWLEDGEMENTS

Research reported in this publication was supported by the Sykes College of Business Faculty Collaboration Grant at the University of Tampa for the 2016-2017 academic year.

8. REFERENCES

Anderson, J. M. (2003). Why We Need a New Definition of Information Security. *Computers & Security*, 22, 308-313.

Basu, E. (2014). Target CEO Fired – Can you be Fired if your Company is Hacked? Retrieved Ocober 29, 2017, from https://www.forbes.com/sites/ericbasu/2014/06/15/target-ceo-fired-can-you-be-fired-if-your-company-is-hacked/#709e3f37c9fa.

Da Veiga, A. & Eloff, J. H. (2010). A Framework and Assessment Instrument for Information Security Culture. *Computers & Security*, 29, 196-207.

Dhillon, G. & Backhouse, J. (2000). Technical Opinion: Information System Security Management in the New Millennium. *Communications of ACM*, 43, 125-128.

DiGangi, C. (2015). Target Becomes First Major U.S. Issuer to Use Chip & PIN Credit Cards. Retrieved January 31, 2017, from http://blog.credit.com/2015/10/target-becomes-first-major-u-s-issuer-to-use-chip-pin-credit-cards-127551/.

Fazio Mechanical Services. (2014). Statement on Target data breach. Retrieved January 31, 2017, from http://faziomechanical.com/Target-Breach-Statement.pdf.

Finkle, J. & Henry, D. (2013). Exclusive: Target Hackers Stole Encrypted Bank PINs – Source. Retrieved January 31, 2017, from http://www.reuters.com/article/us-target-databreach-idUSBRE9BN0L220131225.

Greig, A., Renaud, K., & Flowerday, S. (2015). An Ethnographic Study to Assess the Enactment of Information Security Culture in a Retail Store. In *Internet Security (WorldCIS), 2015 World Congress* (61-66).

Krebs, B. (2015). Inside Target Corp., Days After 2013 Breach. Retrieved January 31, 2017, from http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/.

Malcolm, H. (2014). Target Sees Drop in Customer Visits after Breach. Retrieved January 31, 2017, from http://www.usatoday.com/story/money/business/2014/03/11/target-customer-traffic/6262059/.

Quick, B. (2014). Target CEO Defends 4-day Wait to Disclose Massive Data Hack. Retrieved January 31, 2017, from http://www.cnbc.com/2014/01/12/target-ceo-defends-4-day-wait-to-disclose-massive-data-hack.html.

Quick, M., Hollowood, E., Miles, C., & Hampson, D. (2016). World's Biggest Data Breaches. Retrieved January 31, 2017, from http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

Quirk, M. B. (2014). Non-Target Customers Wondering how Target got Contact Info to Send Email about Hack. Retrieved January 31, 2017, from https://consumerist.com/2014/01/17/non-target-customers-wondering-how-target-got-contact-info-to-send-email-about-hack/.

Riley, M., Elgin, B., Lawrence, D., & Matlack, C. (2014). Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It. *Bloomberg Businessweek*, 13.

Security Standards Council. (2016). PCI DSS Quick Reference Guide. Retrieved January 31, 2017, from https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf?agreement=true&time=1476207333578.

Statista. (2016). Total Number of Target Stores in North America from 2006 to 2015. Retrieved January 31, 2017, from https://www.statista.com/statistics/255965/total-number-of-target-stores-in-north-america/.

Sumra, I. A., Hasbullah, H. B., & AbManan, J. B. (2015). Attacks on Security Goals (Confidentiality, Integrity, Availability) in VANET: A Survey. In *Vehicular Ad-Hoc Networks for Smart Cities* (51-61): Springer, Singapore.

Target. (2014). Target Provides Update on Data Breach and Financial Performance. Retrieved January 31, 2017, from https://corporate.target.com/press/releases/2014/01/target-provides-update-on-data-breach-and-financia.

Target. (2015a). Data Breach FAQ. Retrieved January 31, 2017, from https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ.

Target. (2015b). Inside Target's Cyber Fusion Center. (2015). Retrieved January 31, 2017, from https://corporate.target.com/article/2015/07/cyber-fusion-center.

Target. (2016). Target through the Years. Retrieved January 31, 2017, from https://corporate.target.com/about/history/Target-through-the-years.

Target. (2017). Awards and Recognition. Retrieved January 31, 2017, from https://corporate.target.com/about/awards-recognition.

United States Securities and Exchange Commission. (2014). *FORM 10-K*. Retrieved January 31, 2017, from https://www.sec.gov/Archives/edgar/data/27419/000002741914000014/tgt-20140201x10k.htm.

United States Securities and Exchange Commission. (2016). *FORM 10-Q*. Retrieved January 31, 2017, from http://investors.target.com/phoenix.zhtml?c=65828&p=irol-SECText&TEXT=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9maWxpbmcueG1sP2lwYWdlPTEwOTYwNzg0JkRTRVE9MCZTRVE9MCZTUURFU0M9U0VDVElPTl9FTlRJUkUmc3Vic2lkPTU3.

Von Solms, B. (2000). Information Security – The Third Wave? *Computers & Security*, 19, 615-620.

Von Solms, R. & Van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, 38, 97-102.

Vroom, C. & Von Solms, R. (2004). Towards Information Security Behavioural Compliance. *Computers & Security*, 23, 191-198.

AUTHOR BIOGRAPHIES

Miloslava Plachkinova is an Assistant Professor of Cybersecurity in the Sykes College of Business at the University of Tampa, FL. She holds a Ph.D. in Information Systems and Technology from Claremont Graduate University, CA. She is a Certified Information Systems Security Professional (CISSP), a Certified Information Security Manager (CISM), and a Project Management Professional (PMP). Dr. Plachkinova's research focuses on information security and healthcare. She investigates how human behavior leads to data breaches, and her work in the healthcare field investigates security and privacy issues in mobile health (mHealth) and electronic health records (EHR) on the cloud. Dr. Plachkinova also has extensive industry experience working for both the private and the public sectors.

Chris Maurer is an Assistant Professor in the McIntire School of Commerce at the University of Virginia. He received his Ph.D. from the University of Georgia and was previously an Assistant Professor at the University of Tampa. His research interests include cybersecurity controls, the impact of cybersecurity breaches, enterprise systems, and IT-business alignment. His previous research has appeared in journals and conference proceedings including *MIS Quarterly Executive*, the *International Conference on Information Systems*, the *Americas Conference on Information System*, and the *Hawaii International Conference on System Sciences*.

APPENDIX A – Email to Target Customers

Dear Target Guest,

As you may have heard or read, Target learned in mid-December that criminals forced their way into our systems and took guest information, including debit and credit card data. Late last week, as part of our ongoing investigation, we learned that additional information, including name, mailing address, phone number or email address, was also taken. I am writing to make you aware that your name, mailing address, phone number or email address may have been taken during the intrusion.

I am truly sorry this incident occurred and sincerely regret any inconvenience it may cause you. Because we value you as a guest and your trust is important to us, Target is offering one year of free credit monitoring to all Target guests who shopped in U.S. stores, through Experian's® ProtectMyID® product which includes identity theft insurance where available. To receive your unique activation code for this service, please go to creditmonitoring.target.com and register before April 23, 2014. Activation codes must be redeemed by April 30, 2014.

In addition, to guard against possible scams, always be cautious about sharing personal information, such as Social Security numbers, passwords, user IDs and financial account information. Here are some tips that will help protect you:

- Never share information with anyone over the phone, email or text, even if they claim to be someone you know or do business with. Instead, ask for a call-back number.
- Delete texts immediately from numbers or names you don't recognize.
- Be wary of emails that ask for money or send you to suspicious websites. Don't click links within emails you don't recognize.

Target's email communication regarding this incident will never ask you to provide personal or sensitive information.

Thank you for your patience and loyalty to Target. You can find additional information and FAQs about this incident at our Target.com/databreach website. If you have further questions, you may call us at 866-852-8680.

Gregg Steinhafel

Chairman, President and CEO

Source: https://consumermediallc.files.wordpress.com/2014/01/targetemailgrab.png, Accessed on January 31, 2017.

APPENDIX B – Target Press Release

"Today we are announcing that, after extensive discussions, the board and Gregg Steinhafel have decided that now is the right time for new leadership at Target. Effective immediately, Gregg will step down from his positions as Chairman of the Target board of directors, president and CEO. John Mulligan, Target's chief financial officer, has been appointed as interim president and chief executive officer. Roxanne S. Austin, a current member of Target's board of directors, has been appointed as interim non-executive chair of the board. Both will serve in their roles until permanent replacements are named. We have asked Gregg Steinhafel to serve in an advisory capacity during this transition and he has graciously agreed. The board is deeply grateful to Gregg for his significant contributions and outstanding service throughout his notable 35-year career with the company. We believe his passion for the team and relentless focus on the guest have established Target as a leader in the retail industry. Gregg has created a culture that fosters innovation and supports the development of new ideas. Under his leadership, the company has not only enhanced its ability to execute, but has broadened its strategic horizons. He also led the company through unprecedented challenges, navigating the financial recession, reacting to challenges with Target's expansion into Canada, and successfully defending the company through a high-profile proxy battle. Most recently, Gregg led the response to Target's 2013 data breach. He held himself personally accountable and pledged that Target would emerge a better company. We are grateful to him for his tireless leadership and will always consider him a member of the Target family. The board will continue to be actively engaged with the leadership team to drive Target's future success and will manage the transition. In addition to the appointments of the exceptional leaders noted above, we have also retained Korn Ferry to advise the board on a comprehensive CEO search. The board is confident in the future of this company and views this transition as an opportunity to drive Target's business forward and accelerate the company's transformation efforts."

Source: http://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/#6abeced46e61, Accessed on January 31, 2017.

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 2574-3872