The Implementation of EMV Chip Card Technology to Improve Cyber Security Accelerates in the U.S. Following Target Corporation's Data Breach

Dahli Gray[1] & Jessica Ladig[2]

[1] Keiser University, Ft. Lauderdale, Florida, USA

[2] Premier Baths, Inc., Port Orange, Florida, USA

Correspondence: Dahli Gray, DBA, CPA, CMA, CFE, CGMA, Keiser University, 1900 W. Commercial Blvd., Ft. Lauderdale, Florida, 33309, USA. Tel: 443-465-4559. E-mail: DGray@KeiserUniversity.edu

Received: February 18, 2015 Accepted: February 27, 2015 Online Published: March 2, 2015

doi:10.5430/ijba.v6n2p60 URL: http://dx.doi.org/10.5430/ijba.v6n2p60

Abstract

This study explored the adoption of the Europay, Mastercard, and Visa (EMV) standard for authenticating debit and credit card transactions among corporations in the United States, in response to high profile cybercrimes. According to the research, the Target Corporation data breach in 2013 appears to be the event that motivated the technological change. Target Corporation was the victim of cybercrime through a chain of events, several U.S. organizations have suffered severe financial losses due to data breaches, and U.S. technology is vulnerable regarding debit and credit card transaction processing. Further, U.S. organizations other than financial institutions (e.g., banks) do not typically bear the financial burden for fraudulent transactions, and hesitate to invest in costly new security measures, such as machines that accommodate EMV chip cards, which are debit and credit cards with embedded microchips for added security.

Keywords: data breach, internal controls, target, EMV chip cards

1. Introduction

In February 2013, U.S. President Obama signed an executive order to establish a national framework to strengthen cybersecurity (USDHS 2013). However, this did not prevent massive data breaches such as the one experienced by the Target Corporation. As anticipated by President Obama, most organizations were slow to adopt cybersecurity improvements because they did not perceive benefits to outweigh costs (USDHS 2013, 4). As noted by PricewaterhouseCoopers, "Claims by businesses that they are unaware of cybercrime risks and the need to invest in updated cybersecurity safeguards have become increasingly unconvincing" (PricewaterhouseCoopers, 2014, 5).

The national framework published in February 2014 provided a set of "standards and best practices to help organizations manage cybersecurity risks" (NIST 2014). Also in February 2014, Target announced it would upgrade its proprietary credit cards ("REDcard") and debit and credit card readers in each U.S. store with EMV chip card technology by early 2015, more than six months ahead of previous plans. "The accelerated timing is part of a $100 million effort to put in place chip-enabled technology in all of Target's nearly 1,800 U.S. stores" (Target 2014b).

An increasing number of cybercrimes are committed in America. A major data breach happened at Target toward the end of 2013. The problem could be that the U.S. had not changed to embedded chip debit and credit cards. Most other countries have already adopted this new technology because it allegedly reduces fraud activity. The numerous attacks in the U.S. over a short period suggest the country's payment processing technology is vulnerable and weak. Advanced technology has proven to reduce the risk of a breach; thus, the U.S. should increase its efforts to provide a secure payment processing structure. Otherwise, consumers may stop using debit and credit cards if they their personal data continue to be at risk.

The Target breach affected more than 70 million customers (Clark, 2014). Information technology (IT) personnel missed opportunities to alert Target executives about data protection issues or company executives ignored guidance received. This study examines the Target data breach and shows how accounting-focused legislation (e.g., the

Sarbanes-Oxley Act of 2002) and internal controls investment and development cannot compensate for a failure to invest in technological advancements, such as EMV technology──debit and credit cards with embedded microchips and machines that read the embedded chip cards.

This study suggests Target's IT professionals missed opportunities to recommend improvements (e.g., changing to EMV chip cards) that would have helped to ensure suitable data protection. The study presents evidence that became available after the Target data breach that suggests resources (e.g., time and funds) invested in building customer confidence did not replace the need to invest in systems such as EMV chip card readers. In July 2014, Wal-Mart and Sam's Club were the first retailers in the U.S. to adopt EMV chip card readers. The following sections include a literature review, research analysis, conclusions, and research limitations and proposals for future research.

2. Literature Review

2.1 Introduction

Security breaches have increased over the past decade, particularly in the years 2013 and 2014. These breaches affect millions of customers worldwide and cost billions of dollars. Outdated technology and security measures are partly responsible, including the Payment Card Industry Data Security Standard (PCI DSS), which supports using magnetic strip debit and credit cards instead of the latest technology (EMV chip cards).

2.2 PCI DSS

"Data breaches at Target and Neiman Marcus have once again shown that compliance with the Payment Card Industry Data Security Standard (PCI DSS) is no guarantee against an intrusion" (Vijavan, 2014). "The PCI DSS requirements for merchants, vendors, and security consulting companies … [were] created to mitigate data breaches and prevent payment cardholder data fraud" (PCI, 2014). However, data breaches have multiplied. It is possible that without the PCI DSS requirements, data breaches would have been even more numerous. It would be difficult to test this; however, events speak for themselves. An example is the data breach experienced by Home Depot in September 2014, which was one of the biggest data breaches in retailing history affecting more than 60 million customers (Perlroth, 2014). Stolen customer data appeared on the "black market" and the data could potentially cause $3 billion in illegal purchases (Creswell & Perlroth, 2014).

2.3 Target Corporation

Harris (2014) examines whether Target will change to EMV chip cards, whether Target changed security measures after prior breaches at other companies, and Target's reaction in the aftermath of its data breach. The article focuses on how Target plans to improve its payment processing system technology. It reviews Target's plan of action by examining a letter written by the retailer to its shareholders and filed with the Securities and Exchange Commission. It hypothesizes Target will overcome its data breach by improving its security systems and possibly changing to EMV chip card technology.

Target has doubled staff in its IT security department, spent millions of dollars on security improvements, and is trying to recover from the security breach by moving toward a more secure payment processing system, such as using EMV chip cards for the company's proprietary credit card, the REDcard. Target reported it made security improvements to its payment processing system prior to the 2013 breach to address cybercrime activity, and it continues to look for better solutions to protect confidential information and payment processing systems (Harris 2014). Such research findings confirm updating technology and improving security measures will reduce the risk of a future data breach. The letter from Target to its shareholders has limited information on what actions the retailer is taking after the resignations of the chief executive officer and the chief information officer. The replacements for these two positions will have a major effect on how Target will move forward.

Following the data breach, the press examined Target, questioning how Target handled the aftermath of the data breach. Significant events that took place from the day the data breach occurred until the end of February 2014 indicate Target is in a vulnerable state and is not coping with the data breach aftermath well (Clark, 2014). Clark's (2014) work indicates Target could have handled the situation differently, and points out Target and the investigators of the data breach announced different conclusions. Other concerns relate to the hundreds of layoffs, Target's efforts to boost workplace morale, and the fact that customers would have preferred to hear about the data breach from the company itself. Clark (2014) outlines the significant events that occurred over the five-month period ending February 2014, but does not elaborate further, leaving unresolved questions including why Target did not initiate installation of technology to accommodate both magnetic strip cards and EMV chip cards.

2.4 Fraud Reduction

Groenfeldt (2014) examines whether changing to EMV chip cards in the U.S. would be beneficial, whether changing to EMV chip cards would actually reduce fraud, and discusses the challenges faced by Americans if the U.S. does not adopt EMV chip cards. The article investigates transactions in the U.S. conducted with EMV chip cards (Groenfeldt 2014). Adopting EMV chip cards without installing appropriate technology to read the chip cards does nothing to reduce fraud. EMV chip cards have both an embedded microchip and a magnetic strip. Machines in the U.S. currently only read the magnetic strip and do not process the embedded microchip, which means chip cards used on current machines in the U.S. currently provide no additional protection against fraud. Other countries already embrace EMV chip card technology, but the U.S. has not yet installed appropriate equipment to read the embedded chips (Groenfeldt 2014). The continued increase in cybercrime suggests current technology used in the U.S. is vulnerable and needs updating to reduce fraud (Chandler, 2014).

2.5 Credit Unions and Costs

The next issue to examine is the damage the Target data breach has caused—how the breach affected the credit unions that issued the compromised cards, and the estimated total cost of Target's data breach (Morrison, 2014). A survey conducted by the Credit Union National Association (CUNA) estimated the costs of reissuing the compromised Target debit and credit cards. The survey covered 1,112 credit unions and detailed the number of cards impacted, the number needed to be re-issued, and the cost of reissuance for each card. Morrison (2014) suggested Target's data breach had a significant effect on credit unions, causing millions of dollars in costs. CUNA's survey also shows credit unions have experienced overextended call center traffic as a direct result of the breach, and some credit unions will either not reissue new cards or are being selective about which cards will be reissued (Morrison 2014). In this context, the credit unions survey has not shown how non-reissuance of cards affects customers (Morrison 2014).

2.6 Was Target Responsible for the Data Breach?

Yadron, Ziobro, and Barret (2014) examined how Target's security system was hacked, and whether Target conducted any internal audits of its information systems. Target seemed to have known about its system weaknesses prior to the data breach (Yadron et al., 2014). The retailer received a favorable audit report regarding its information systems just months before the breach occurred; however, according to Yadron et al. (2014), investigators found other vendors also connected to the remote server used by Target's payment processes. Hackers used one of these other vendor's connections to install malware. Then the hackers navigated through the system network to gain access to Target's payment terminals (Yadron et al. 2014). Target must have been aware of security vulnerabilities within its system because an audit would have identified weak applications and processes (Yadron et al. 2014). Management should have acted on any known information system vulnerabilities.

2.7 Small and Mid-Sized Entities

Large corporations, such as Target, may be more desirable to hack than small and mid-sized organizations (SME) resulting in two concerns (Miller, 2014): First, are SMEs as vulnerable to attacks as large corporations? Second, are SMEs possible gateways to gain access to large corporations? The answer to both questions is yes. In the case of Target, hackers used a small vendor to gain access to the corporation's system. Hackers are able to use a connection between an SME and a large organization to achieve a data breach. Further, large corporations generally tend to experience more security breaches than smaller organizations; however, this does not mean SMEs are not equally susceptible. Miller (2014) provides useful insights about how a data breach can affect numerous organizations.

2.8 Security Awareness

Boose (2014) considers two questions related to security awareness. First, did the data breach at Target affect other organizations' information security budgets? Second, did the Target data breach have an impact on executives' security awareness? A survey addressed these two questions. Attendees at an RSA information security conference completed a survey that compared Target's security breach with Edward Snowden's leak of highly classified documents. The survey results suggest Target could have prevented its data breach by observing the challenges faced by other organizations, and improving system measures and controls accordingly (Boose, 2014). Further, the survey identified concerns organizations have following a security breach. Organizations can learn from the experiences of other hacked organizations (e.g., Neiman Marcus, Sony, and Michaels). Thus, the experience of one organization could influence the preventive measures taken by another.

2.9 Embedded Chip Technology

Europay, Mastercard, and Visa formed a joint venture, EMVCo LLC, in 1999 to facilitate global acceptance of secure payment transactions──the inter-operation of integrated circuit cards and compatible point of sale and automated teller machines (EMVCo, 2014). Today EMVCo is comprised of six equal members: American Express, China UnionPay, Discover, Japan Credit Bureau (JCB), Mastercard, and Visa──Europay merged with Mastercard in 2002 (EMVCo, 2014). The company manages the EMV global standard for authenticating debit and credit card transactions worldwide, which includes using debit and credit cards embedded with microchips and machines that read the cards. Dozens of banks, merchants, processors, and vendors support the standard globally (EMVCo, 2014). Rutledge (2014) examines the process a consumer can expect when using an EMV chip card, and suggests debit and credit cards with embedded microchip technology are safer and more secure than magnetic strip cards. Rutledge (2014) demonstrates how the new technology is used and describes how card issuers have the option to choose whether the cards require a personal identification number (PIN) or a signature. The recommendation is to use a PIN in combination with a microchip for added authentication. The microchip encryption changes with each transaction, thereby making it more difficult for hackers to retrieve information (Rutledge 2014). Consequently, the chip-and-PIN system allows card usage without the dissemination of information to others. However, U.S. consumers might raise questions relative to its usefulness, timeliness, and completeness. In contrast, consumers and merchants have used magnetic strip cards for decades and know exactly how it operates. However, another consideration is that outside the U.S. (especially in Europe), retail payment processing frequently uses EMV technology. For example, U.S. travelers abroad frequently experience automated payment machines in airports and train stations, etc. that do not accommodate magnetic strip debit and credit cards. Therefore, upgrading to the global EMV technology standard would aid U.S. travelers abroad as well.

2.10 Biometrics

Finally, a biometric system could be an alternative to chip-and-PIN cards. Bidgoli (2012) questions whether biometric measures can be used for debit and credit cards, shows how biometrics are applied in real case scenarios, and recommends organizations incorporate these security measures to help reduce risk. For example, hackers can steal PIN numbers, but biometrics requires a fingerprint or palm print, which makes fraud difficult; thieves would not possess the cardholder biometrics required to use the debit or credit card (if stolen). The results of Bidgoli's (2012) study are inconclusive. Biometrics provides a unique identifier; however, there are concerns about using fingerprints. First, scanning fingerprints can be difficult and some individuals may refuse (for a variety of reasons) to provide biometrics. In addition, biometric measures would not resolve fraud activity associated with card transactions where the purchaser is not present (e.g., online transactions).

Payment-processing procedure in the U.S. needs to improve. The Target data breach is a good example of a significant security issue related to the use of magnetic strip cards. EMV chip card technology is costly to implement but the results confirm the process is more secure. The data breach at Target affected other organizations. Understanding how Target's data breach occurred, and how the company handled the aftermath, could make organizations stronger and wiser. Further, new technology in general can improve the payment process system and reduce the risk of fraud. This study suggests there are measures a country can take to reduce the amount of fraud that occurs. Upgrading to EMV chip card technology should significantly reduce the amount of fraud in the U.S. Nonetheless, further investigation is needed──why was Target a data breach victim, and why, as of July 2014, are Wal-Mart and its subsidiary Sam's Club the only large U.S. organizations to adopt EMV chip card technology?

3. Research Analysis

The research analysis section of this study addresses two concerns: why Target was a victim of a data breach, and why, as of July 2014, Wal-Mart and its subsidiary Sam's Club are the only major U.S. organizations to adopt EMV chip card technology. With regard to why Target was a data breach victim, one could first question why the retailer did not implement change after numerous security breaches had happened to other companies during the prior decade. A change in technology could have prevented the type of breach Target experienced. Global Payments, Inc., a company that provides electronic processing services to organizations, had already had a similar breach. An estimated 1.5 million U.S. debit and credit cards were exposed and it cost the company almost $100 million (Kitten 2013), despite the fact that the processing systems at Global Payments, Inc. underwent a regular compliance test and had passed each time. Thus, there is a growing concern that compliance standards are outdated in the U.S., whereas other countries can confirm the success of their compliance standards.

3.1 The Security Breach at Sony

Another breach prior to Target's was at Sony, a major electronics retailer that provides a digital media service called the PlayStation Network. The breach exposed the confidential information of more than "100 million customers and resulted in a 23-day closure of the PlayStation Network" (Goodin 2011, 1). Such a closure would significantly affect any company's sales and profits. Hackers alleged Sony's security measures were weak and easily accessible. Further, these hackers, known as Lulz Security, stated the data Sony stored was not encrypted (Goodin 2011); in fact, it was stored as plain text, which is easy to steal with little effort (Goodin 2011, 1). One could wonder why these forewarnings did not result in changes that could have prevented future data breaches, such as the one at Target.

3.2 The Breach at Target

Change in a company can be good as long as it benefits the overall organization. Thus, an organization should ensure each decision-making unit works toward a common goal, such as preventing a security breach. Further, executives observe activities within a company and make decisions based on facts and relevance. The IT security staff at Target warned management about suspicious activity. Management decided to ignore the activity, thereby causing Target to experience one of the largest security breaches of all time (Harris 2014).

3.2.1 The Changes Introduced at Target

Since the data breach, Target has made significant changes. The number of IT staff doubled and the company's entire IT system was upgraded (Harris 2014). In addition, two highly ranked executives resigned. "Six months before the attack, Target began installing a $1.6 million malware detection tool made by the computer security firm, FireEye, whose customers also include the CIA and the Pentagon" (Riley, Elgin, Lawrence, & Matlack, 2014). The detection software at Target spotted the intrusion and immediately notified the corporate office. However, managers did not respond to the possible threat. Thus, in theory, Target could have prevented the data breach from happening. Riley et al. (2014) comment that Target is possibly attempting to mislead when it says it did not know of the data breach until the U.S. Department of Justice notified the retailer in mid-December. The security software Target had installed was able to detect the malware on both November 30, 2013 and December 2, 2013 (Riley et al. 2014).

3.3 Why Wal-Mart Is the Only Major U.S. Retailer to Adopt EMV Chip Card Technology

The second topic explored in this section is why Wal-Mart is the only major retailer in the U.S. to adopt EMV chip card technology; the company also began issuing new cards in July 2014. Retailers are concerned about implementing EMV chip card technology because banks are not convinced this is the best move (Chandler 2014). New technology would require new equipment and the issuance of new cards. This is a significant cost to both retailers and banks. The latter would rather absorb the costs of fraud than invest a significant amount of money in new technology (Chandler 2014). In addition, adopting EMV chip cards could potentially cause a shift in fraud liability from card issuers to merchants (Weisbaum, 2014). Consequently, retailers in the U.S. did not start installing EMV chip card point of sale terminals until 2014.

3.3.1 Concerns about Fraud Reduction

There have been some concerns in the U.S. about whether EMV chip cards will actually reduce fraud. Miller (2014) points out EMV chip cards will make physical retailers more secure but online merchants will not benefit from the new technology that reads the chip cards. Sam's Club was the first retailer to implement technology to read EMV chip cards in the U.S. (Weisbaum, 2014). Other retailers are not far behind. Target announced in its 2013 annual report it "plans an investment of approximately $100 million to equip our proprietary REDcards and all of our U.S. store card readers with chip-enabled smart-card technology by the first quarter of 2015" (Target 2014a, 23). "Visa, MasterCard, American Express, and Discover want the U.S. converted to chip-based credit cards by October 2015. After that date, they say, fraud losses will shift to the retailer if they don't have point-of-sale payment terminals that read smart cards" (Weisbaum, 2014). Considering the amount of fraud the U.S. has experienced in the past year, retailers should be willing to update to the latest technology.

3.3.2 Who Bears the Financial Burden of Fraudulent Transactions?

In the U.S., banks are the main organizations that issue debit and credit cards. They typically bear the financial burden of fraudulent transactions and enjoy protection and support from the federal government. There is also no established method to write off losses, and card users and retail merchants where breaches occur (e.g., Target) are not held responsible for the costs. Because financial intermediaries (banks) have assumed most of the financial burden, this resulted in merchants (e.g., Target, Michaels, and Sony) lacking motivation to invest funds in EMV chip card technology. However, the U.S. is moving toward making merchants at least partly responsible for the financial

losses resulting from fraud. This helps explain why Wal-Mart and its subsidiary Sam's Club changed to EMV chip card technology in July 2014.

3.3.3 The Role of Accountants and IT Professionals

Accountants and IT professionals also have a significant role to play; they help design, implement, and maintain internal control systems and procedures to assure data security, which should help prevent, detect, and resolve data breaches, fraud, and errors. From the legislative perspective, the Sarbanes-Oxley Act of 2002 helps protect data. It mandates the improvement of internal control systems and procedures that fail to protect organizations and individuals from data breaches.

3.3.4 Organizations' Failure to Report Small Data Breaches and Fraud

Organizations tend not to report small data breaches or fraud occurrences. Such reports can prove embarrassing to organizations and reduce consumer confidence because data breaches result in the loss of real assets. Target's approach to addressing consumer confidence issues has been to advertise free credit reporting services. Such an attempt to build consumer confidence without making tangible technological changes reflects the idea that improving consumer attitudes instead of improving technology resolves problems. However, this study suggests the answer to resolving data breach problems in the U.S. is to invest in new technology.

3.4 Addressing the Shift in Liability

"Major credit card issuers have published detailed schedules [called EMV Key Dates Chart-Card Networks] about the upcoming shift in liability" (Kossman, 2014, 1). They include major U.S. credit card merchants including Visa, MasterCard, American Express, and Discover that want to make the transition to EMV chip card technology as smooth as possible. Each key date includes an explanation. For instance, fuel dispensers must comply with EMV chip card technology by October 2017, otherwise liability for fraudulent transactions at fuel dispensers will shift from the card issuer to the merchant (VeriFone Systems, Inc. 2013).

3.5 Future Adoption of EMV Chip Card Technology

Together, the research results suggest upgrading to EMV chip card technology should reduce fraud activity in the U.S. "EMV technology will not prevent data breaches from occurring, but it will make it much harder for criminals to successfully profit from what they steal" (Kossman, 2014, 1). Hesitation in the U.S. to change to EMV chip card technology may have been partly to blame for the significant increase in cybercrime over the past decade. Most countries have moved to EMV chip card technology, a situation that makes the U.S. an easy target. However, the U.S. is now heading toward adopting EMV chip card technology, starting with Wal-Mart and Sam's Club.

4. Conclusion

The purpose of this study was to determine the status of the U.S. after the Target Corporation data breach in 2013, relative to upgrading to EMV chip card technology. This technology can help to reduce data breaches, such as the one at Target. The study found that despite the cost of changing to EMV chip card technology, the U.S. is moving in that direction to help prevent future data breaches. EMV technology uses embedded microchips in debit and credit cards to distinguish transactions using encryption codes. Target plans to change to the new technology in 2015. Wal-Mart and Sam's Club made the change 2014. This study suggests many further technological changes will occur in the year 2015, and recommends relevant professionals stay well informed about how the new technology will affect consumers.

There are some limitations to the study, including the inability to answer some questions left unresolved because of ongoing investigations or upcoming changes. First, is there a connection between the Target and Neiman Marcus data breaches? Research suggests these breaches are similar. Second, how does Target plan to move forward? In Target's 2013 annual report (Target 2014a), words such as "suffer" and phrases such as "if efforts are unsuccessful" are used in the context of descriptions about Target's future. This suggests Target could be unsure about how to move forward. For example, Target suggests it may need to offer more promotions and incentives to increase sales and establish a better relationship with its customers (Target 2014a, 10). Finally, it is reasonable to ask whether EMV chip cards will completely replace magnetic strip cards. Many countries have already changed to EMV chip card technology. Future research should explore the aforementioned topics regarding Target's future.

In conclusion, Target was a victim of a security breach because the U.S. was vulnerable to attack; the U.S. hesitated to change to EMV chip card technology because of the high cost of investment required. However, the U.S. is finally taking action by requiring merchants to change to EMV chip card technology by the end of 2015. If an organization does not change by the deadline, it will be liable for financial loss due to fraudulent activity. However, EMV chip

card technology should bring value to the U.S. because it has already done so in other countries. With the introduction of such technology, future research could test the theory that EMV chip card technology can actually reduce fraud in the U.S. As Kim and Vasarhelyi (2012) recommend, based on their research findings, a fraud detection model "using fraud/anomaly indicators to detect potential fraud and/or errors on real data" could also be beneficial for the efficient identification of cyber fraud.

References

Bidgoli, H. (2012). The introduction of biometrics security into organizations: A managerial perspective. *International Journal of Management, 29*(2), 687-695. Retrieved from http://search.proquest.com/docview/1020691093?accountid=35796.

Boose, S. (2014). Survey finds Target breach had greater impact than Snowden leaks. *Tripwire.* Retrieved from http://www.tripwire.com/state-of-security/top-security-stories/survey-finds-target-breach-larger-impact-snowden-leaks/

Chandler, S. (2014). The dysfunctional state of America's credit cards. *CNBC.* Retrieved from http://www.cnbc.com/id/101327705

Clark, M. (2014). Timeline of Target's data breach and aftermath: How cyber theft snowballed for the giant retailer. *International Business Times.* Retrieved from http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056

Creswell, J., & N. Perlroth. (2014). *The New York Times.* Retrieved from http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html

EVMCo, LLC. (2014). *EVMCo corporate website.* Retrieved from http://www.emvco.com/

Goodin, D. (2011). PlayStation Network breach will cost Sony $171m. *The Register.* Retrieved from http://www.theregister.co.uk/2011/05/24/sony_playstation_breach_costs/

Groenfeldt, T. (2014). US credit card fraud is spiking ahead of EMV secure chip introduction. *Forbes*. Retrieved from http://www.forbes.com/sites/tomgroenfeldt/2014/07/17/us-credit-card-fraud-is-spiking-ahead-of-emv-secure-chip-introduction/

Harris, E. A. (2014). Target gives a defense of its efforts on security. *The New York Times.* Retrieved from http://www.nytimes.com/2014/06/03/business/target-defends-its-oversight-of-customer-data.html

Kim, Y., & M. A. Vasarhelyi. (2012). A model to detect potentially fraudulent/abnormal wires of an insurance company: An unsupervised rule-based approach. *Journal of Emerging Technologies in Accounting, 9*(1), 95-110. http://dx.doi.org/10.2308/jeta-50411

Kitten, T. (2013). Global closes breach investigation: Processor says expenses less than originally reported. *Bank Info Security.* Retrieved from http://www.bankinfosecurity.com/global-closes-breach-investigation-a-5684/op-1

Kossman, S. (2014). 8 FAQs about new EMV credit cards. *Fox Business.* Retrieved from http://www.foxbusiness.com/personal-finance/2014/07/10/8-faqs-about-new-emv-credit-cards/

Miller, J. A. (2014). How the Target breach has affected small business data security. *CIO.* Retrieved from http://www.cio.com/article/2451283/data-breach/how-the-target-breach-has-affected-small-business-data-security.html

Morrison, D. (2014). Target breach: CUNA survey updates detail system cost. *Credit Union Times.* Retrieved from http://www.cutimes.com/2014/02/13/target-breach-cuna-survey-updates-detail-system-co

National Institute of Standards and Technology (NIST). (2014). Framework for improving critical infrastructure cybersecurity. *NIST.* Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

PCI Security Standards Council (PCI). (2014). About the PCI Security Standards Council. *PCI.* Retrieved from https://www.pcisecuritystandards.org/organization_info/index.php

Perlroth, Nicole. (2014). Home Depot data breach could be the largest yet. *The New York Times (blog)*, September 8, 2014 (6:58 p.m.). Retrieved from http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/?_r=0

PricewaterhouseCoopers (PwC). (2014). US cybercrime: Rising risks, reduced readiness. Key findings from the 2014 US State of Cybercrime Survey. *PwC, CERT® Division of the Software Engineering Institute at Carnegie Mellon University. CSO magazine. United States Secret Service.* Retrieved from http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

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

Rutledge, N. (2014). How to use a chip-and-PIN or EMV credit card. *LowCards.com.* Retrieved from http://www.lowcards.com/chip-pin-emv-credit-card-25177

Target. (2014a). *Target 2013 Annual Report*. Retrieved from https://corporate.target.com/annual-reports/pdf-viewer-2013?cover=6725&parts=6724-6726-6727-6730-6728

Target. (2014b). Target accelerates implementation of chip-enabled smart card technology to protect consumers from fraud. *Target.* Retrieved from http://pressroom.target.com/news/target-accelerates-implementation-of-chip-enabled-smart-card-technology-to-protect-consumers-from-fraud

United States Department of Homeland Security (USDHS). (2013). Executive Order 13636: Improving Critical Infrastructure Cybersecurity. *USDHS.* Retrieved from http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf

Vijavan, J. (2014). After Target, Neiman Marcus breaches, does PCI compliance mean anything? *Computer World.* Retrieved from http://www.computerworld.com/article/2486879/data-security/after-target--neiman-marcus-breaches--does-pci-compliance-mean-anything-.html

Weisbaum, H. (2014). Chip-enabled 'smart' credit cards coming to America. *CNBC*. Retrieved from http://www.cnbc.com/id/101743883#

Yadron, D., P. Ziobro, & D. Barret. (2014). Target warned of vulnerabilities before data breach. *The Wall Street Journal.* Retrieved from http://online.wsj.com/news/articles/SB10001424052702304703804579381520736715690