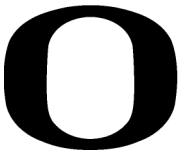
Presented to the Interdisciplinary Studies Program:



UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Best Practices to Obtain and Maintain PCI Compliance

CAPSTONE REPORT

Jennifer Blackwell
Senior Product Marketing Manager
CompTIA

University of Oregon
Applied Information
Management
Program

Fall 2018

Continuing and Professional
Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-271

Approved by

_____

Dr. Kara McFall
Director, AIM Program

Best Practices to Obtain and Maintain PCI Compliance

Jennifer Blackwell

CompTIA

Abstract

PCI developed security standards to guide merchants in ensuring sensitive cardholder data is protected. However, data breaches continue, affecting the data of billions of customers and negatively affecting revenue and consumer confidence. Merchants must determine the best approaches to not only obtain, but also maintain PCI compliance. This annotated bibliography considers best practices published from 2004 to 2018 to assist IT departments in implementing security procedures to securely process payment card transactions.

Keywords: security, data, PCI compliance, DSS, payment card, breaches, security standards, requirements, merchants

Table of Contents

Abstract 3

Introduction to the Annotated Bibliography 6

Problem 6

Purpose 11

Research Question 11

Audience 11

Search Report 12

Annotated Bibliography 17

Historical High-Exposure Breaches 17

History of PCI DSS 29

Best Practices of PCI Compliance 35

Conclusion 49

Historical High-Exposure Breaches 49

History of PCI DSS 50

Best Practices of PCI Compliance 52

Final Thoughts 54

References 55

Introduction to the Annotated Bibliography

Problem

The Payment Card Industry (PCI) Security Standards Council (SSC) was formed in 2004 (Liu et al., 2010) by American Express Company; Discover, Inc.; JCB International, Ltd.; MasterCard, Inc.; and Visa, Inc. as a global forum to develop and publish a set of Data Security Standards (DSS) to serve those that work with credit cardholder data (PCI Security, n.d.). The PCI SSC's main priorities are to assist merchants, vendors, and institutions with discerning and implementing the security policies set within the DSS as a means of creating a secure card-processing solution and providing protection against fraud and data breaches (PCI Security, n.d.). For the purpose of this study, fraud is defined as "activity that uses confidential personal (and often financial) information for unlawful gain" (Cheney et al., 2012, p. 131) and a data breach is defined as an incident where financial and personal information is compromised (Manworren, Letwat, & Daily, 2016).

Vulnerabilities to fraud and breaches can appear in numerous places within the entire credit card transactional ecosystem, such as in a point-of-sale device or mobile device, or even during transmission of data to the service provider or financial institution (PCI DSS, 2018). The PCI standards, which were updated in May 2018 to version 3.2.1, are designed as basic security best practice measures that should likely already be in place for an organization that stores, processes, or transmits sensitive cardholder data (PCI DSS, 2018). The high-level requirements are designed for the following objectives:

1. Build and maintain a secure network and systems.
2. Protect cardholder data.
3. Maintain a vulnerability management program.

4. Implement strong access control measures.
5. Regularly monitor and test networks.
6. Maintain an information security policy (PCI DSS, 2018).

Validation of PCI compliance happens annually through either a Qualified Security Assessor (QSA) (PCI DSS, 2018), who is "responsible for the performance of the PCI data security assessment" (Liu et al., 2010), or through self-assessment by the merchant (PCI DSS, 2018). There are four levels of validation into which merchants fall based on annual card transaction volume (PCI Compliance Guide, n.d.). Level 1 merchants process over six million annual transactions (PCI Compliance Guide, n.d.) and must conduct an annual audit with a QSA, perform self-assessments on a regular basis and perform scans quarterly in order to maintain PCI compliance (Liu et al., 2010). Level 2 merchants process one to six million annual transactions, Level 3 merchants process 20,000 to one million annual transactions, and Level 4 merchants process fewer than 20,000 annual transactions (PCI Compliance Guide, n.d.). Level 2, 3, and 4 merchants must conduct annual self-assessments and perform quarterly scans in order to maintain PCI compliance (Ataya, 2010).

There are penalties for noncompliance with PCI's standards, which are at the discretion of the payment brand and range from between $5,000 to $100,000 per month; the payment brand levies the fines on the acquirer (PCI Compliance Guide, n.d.). The acquirer is typically the bank, or any entity used by the merchant to process payment card transactions, who sends the payment request to the payment brand (Ataya, 2010). The acquirer informs the merchants of the requirements for DSS compliance (Ataya, 2010) and, should a merchant be in noncompliance, the acquirer typically passes any fine from the payment brand on to the merchant and has the right to increase the transaction fees or even terminate the relationship with the merchant (Morse

& Raval, 2008). According to the PCI Compliance Guide, penalties for noncompliance are often not widely publicized and can be crushing for small to medium sized businesses (n.d.).

PCI claims that full compliance with their Data Security Standards aids in mitigating vulnerabilities and protecting cardholder data through a continuous process of assessing business processes for payment processing for potential vulnerabilities, repairing vulnerabilities, and reporting compliance records to the acquiring bank and payment brand (PCI DSS, 2018). Since 2009, almost all large merchants annually validate compliance with DSS (Sullivan, 2010). However, more than eleven billion records breaches have occurred between 2005 and 2018 (Privacy Rights Clearinghouse, n.d.). In 2013 and 2014 alone, three of the U.S.'s largest breaches occurred, with a combined total of 674 million records affected (Hemphill & Longstreet, 2016). The magnitude of these breaches contributed to a dramatic increase of the annual cybercrime cost to the retail industry, from an average of $4.5 million in 2013 to an average of $8.6 million in 2014, a 91 percent increase (Hemphill & Longstreet, 2016). A 2018 report by the Ponemon Institute found that the global average cost of a data breach rose from $3.62 in 2017 to $3.86 million in 2018, a 6.4% increase (Poneman Institute, 2018).

PCI compliance does not ensure that a company will avoid a breach (Van Oosten, 2018). A data breach at Heartland Payment Systems that occurred in 2007 went undiscovered until October of 2008 and compromised payment cards affecting 130 million records, which was the largest of its time (Sullivan, 2010). The breach was due to eight-year old SQL code from an online form that contained a vulnerability (Cheney, 2010). However, Heartland was certified as PCI compliant by a QSA when the breach occurred, and Heartland had been given this certification a few times with the vulnerability present (Cheney, 2010). Global Payments, Inc. experienced a breach in 2012 affecting around 1.5 million payment card records, although the

company conducted successful routine PCI compliance tests (Gray & Ladig, 2015). Global Payments, Inc. revealed that the breach was likely due to unauthorized account access (Privacy Rights Clearinghouse, n.d.). Target Corporation experienced a security breach in November and December 2013 that affected over 70 million customers, despite the fact that Target had passed a PCI audit successfully (Plachkinova & Maurer, 2018) and had implemented a malware detection tool at a cost of $1.6 million (Manworren et al., 2016; Plachkinova & Maurer, 2018). The breach occurred through a vulnerability in a third-party vendor working with Target through which credentials were stolen (Pigni, Bartosiak, Piccoli, & Ives, 2018; Plachkinova & Maurer, 2018). Neiman Marcus experienced a breach at the same time as Target in 2013 that exposed 1.1 million records of retail consumers' payment cards (Privacy Rights Clearinghouse, n.d.), even though they had implemented security measures that exceeded the PCI standards of the time (Vijayan, 2014). It is believed that that the database breach at Neiman Marcus occurred in July 2013 but was not completely contained until January 2014 (Privacy Rights Clearinghouse, n.d.).

One cause of breaches for merchants that have obtained PCI compliance is the failure to maintain PCI DSS practices after an annual audit (Van Oosten, 2018). As early as 2011, the annual Verizon PCI Compliance Report (later renamed the Verizon Payment Security Report) disclosed that only 21 percent of organizations surveyed maintained compliance with standards from their previous assessment (Willey & White, 2013). The most recent Verizon Payment Security Report disclosed that in 2017 a little more than half (52.5%) of the merchants that Verizon assessed during an interim validation preserved all DSS compliance requirements since their last audits (Van Oosten, 2018). While this favorable trajectory looks promising over the findings from the 2011 assessments, the 2017 number actually dropped by 3 percent from 2016 when 55.4% of merchants maintained PCI DSS practices since their annual reviews (Van

Oosten, 2018). Verizon also noted that the number of controls that merchants fail to apply rose from 13% in 2016 to 16.4% in 2017 (Van Oosten, 2018).

Compliance with PCI DSS is not currently required or regulated by the federal government, although the federal government maintains involvement in compliance through the Federal Trade Commission (FTC) Act to evaluate breaches and impose sanctions on organizations that participate in unfair trade practices (Willey & White, 2013). Breaches of personal data can be considered unfair trade practices; therefore, the FTC consults the DSS to evaluate potential violations (Willey & White, 2013). A violation identified by the FTC can be interpreted as a failure by the organization to comply with PCI DSS, which is a failure to take the necessary steps to protect personal cardholder information (Willey & White, 2013). For example, the FTC filed a complaint against TJX, Inc., claiming the company violated the law by failing to take the necessary steps to provide the appropriate level of security when storing personally identifiable information (PII) (Morse & Raval, 2008). Although not federally regulated, a few states – Minnesota, Nevada, and Washington – have passed laws requiring the retail industry to comply with PCI DSS, and should a data breach occur, allow for civil action against the merchant if noncompliant during the breach (Willey & White, 2013).

The problems that complicate the effort to thwart cybercrimes that result in data breaches and fraud are multifaceted (Cheney et al., 2012; Manworren et al., 2016). Cybercrime is on the rise (Manworren et al., 2016); PCI DSS is not regulated or mandated by the government (Cheney et al., 2012; Hemphill & Longstreet, 2016; Manworren et al., 2016; Willey & White, 2013), and there is no foolproof security methodology that aids organizations with best practices to meet and maintain DSS compliance and protect end-user data effectively (Hemphill & Longstreet, 2016).

Purpose

When evaluating the PCI DSS framework, Morse and Raval (2008) stated that "external threats and internal vulnerabilities must be addressed on an ongoing basis in order to provide adequate security" (p. 13). The purpose of this annotated bibliography is to identify best practices for merchants in establishing and maintaining PCI compliance. These best practices are intended to inform a positive approach to compliance so that merchants who handle cardholder data can determine the appropriate course of action to obtain and maintain compliance. Literature sources are presented that provide insights into the history of PCI DSS, describe historical high-exposure breaches, and provide best practices in obtaining and maintaining PCI compliance.

Research Question

Main Question. What are the best practices for merchants to obtain and maintain compliance with PCI DSS?

Sub-Questions. (1) How can merchants adopt a proactive stance in maintaining PCI compliance once they obtain initial compliance? (2) What lessons can merchants learn from high-profile breaches to develop effective security programs?

Audience

Willey and White (2013) assert that "data security is not a concern in a vacuum; it comes to life when people and organizations attempt to establish policies and systems necessary to protect information" (pg. 186). Whether a small business has just made the decision to start accepting card payments or an established enterprise is concerned with a potential breach, it is imperative that the Information Technology (IT) departments managing the security frameworks have taken the time to not only become familiar with PCI's DSS requirements to obtain and maintain compliance, but have also researched the best practices to set the appropriate courses of

action (Cheney et al., 2012). Therefore, the primary audience members for this study are IT employees who work along the cybersecurity pathway, as well as IT Directors, Chief Information Security Officers (CISOs), and Chief Information Officers (CIOs).

The individuals who work in cybersecurity may include systems administrators, security engineers, software engineers, security analysts, or security architects (National Initiative for Cybersecurity Education, n.d.). These individuals perform the hands-on tasks to configure and secure systems and networks; process and store PII; perform system and data analysis; and plan, design, and implement the secure solutions to maintain resilient frameworks (National Initiative for Cybersecurity Education, n.d.). Exposure to best practices enables the individual contributors to become familiar with and be aware of real-world security issues that other organizations within and without their industries continue to face.

The IT Directors manage the oversight of the staff, set direction and timelines for staff, and inform the CISO or CIO of status and activities (Peppard, Edwards, & Lambert, 2011). The CISO oversees the IT security policy, establishes disaster recovery (DR) plans, and investigates security breaches (Karanja & Rosso, 2017). The CIO ultimately determines the strategy and growth for technology at an organization, creates the culture in the IT department, and approves the technology budget (Peppard, Edwards, & Lambert, 2011). Executives and higher-level managers will benefit from best practices from a compliance and financial impact perspective, as accountability likely lies at this level (Hooper & Mckissack, 2016).

Search Report

Search Strategy. In this study I examined the history of PCI and what compliance entails to meet the requirements in DSS. Secondly, I delved into specific issues that merchants who process credit card payments continue to face since the standards were developed. Finally, I

focused on the best practices that organizations can implement to meet compliance. The purpose of this literature review is to develop an outline of critical best practices that organizations can implement to not only meet and maintain compliance, but also create a more resilient network against breaches.

I conducted searches for historical scholarly literature on PCI history, breaches, and PCI implementation on Google Scholar and the University of Oregon Library databases. I also consulted media results, including audio and live recordings, for additional resources on PCI topics. These results yielded more general concepts regarding implementation issues and were focused by industry, as these recordings were often from industry conferences. This strategy was used as a synthesis of potential overlap and gaps.

Search terms.

I searched for literature sources to answer the following questions;

- What is PCI? What is DSS?
- How can organizations comply with the standards?
- What issues with compliance are companies still facing?
- What breaches can teach us lessons?
- Does the threat of breaches only concern large merchants?
- Did merchants pass compliance before a breach?
- How do small businesses approach compliance?
- What are the baseline compliance tactics?

Keywords.

I used the following keywords during my search for sources:

- Payment Card System or PCI,

- Security Standards Council or SSC,
- Data Security Standard or DSS,
- PCI breaches,
- PCI compliance breaches,
- PCI noncompliance,
- PCI best practices,
- Implement PCI,
- Baseline PCI,
- PCI tips,
- PCI guidelines, and
- Basic PCI security controls

Search engines and databases.

I used the following search engines and databases to identify sources:

- Google Scholar,
- University of Oregon Library databases:
  - IEEE (Institute of Electrical and Electronics Engineers),
  - JSTOR (Journal Storage),
  - Business Source Complete, and
  - Academic Search Premier.

Documentation Approach. I used multiple techniques for data collection including bibliographic management software, browser bookmarking, and saving files locally to a computer. I used a Microsoft Excel file for task management and to keep a running record of search strategies by categories. I included columns for search terms, notes, platform used, date

found, and source. This strategy enabled me to prevent duplicate efforts as well as potentially highlight efforts that developed over time. I also captured articles that I rejected in the file, along with the reason for rejection.

Reference Evaluation Criteria. I used the list of criteria from the Center for Public Issues in Education on *Evaluating Information Sources* to evaluate references: authority, timeliness, quality, relevancy, and (lack of) bias (Center for Public Issues, n.d.).

- Authority. I deemed authors as authoritative if their articles were peer-reviewed and by confirming the authors' credentials, with a preference for authors with advanced degrees and other published works on the topic. I also reviewed how often the source has been cited by other authors in the same field; I considered authors who are cited by others to be more credible.
- Timeliness. re determined to be current if published within the last fourteen years, or when PCI SSC was formed 14 years ago; I therefore excluded publication dates older than 2004.
- Quality. I determined references to be of high quality by examining the grammar, spelling, punctuation, and structure of the information or document and eliminated those sources that had multiple errors in these areas.
- Relevancy. I determined that references were relevant by considering whether the content was appropriate to the research topics of the history of PCI, high-profile breaches, and the identification of best practice in PCI compliance.
- (Lack of) bias. I reviewed each reference for bias by looking for cited sources that are not selling related products or services. In one case I identified and used reports compiled by Verizon, a telecommunications organization, after noting the

use of the reports by other sources I had already identified as authoritative and unbiased.

Annotated Bibliography

The following Annotated Bibliography includes references that investigate the history of PCI DSS; historical high-exposure breaches; and best practices of PCI compliance. References assist in highlighting key gaps in PCI compliance, oversight, and related concerns; potential solutions to obtain compliance; and approaches to determine best practices for organizations that process credit card data to meet PCI requirements. Each annotation includes these elements: (a) a full bibliographic citation, (b) an abstract from the author, and (c) a summary examining relevance to this study.

Historical High-Exposure Breaches

Cheney, J. S. (2010). Heartland Payment Systems: Lessons learned from a data breach. *SSRN Electronic Journal,* 1-36. https://dx.doi.org/10.2139/ssrn.1540143

Abstract. On August 13, 2009, the Payment Cards Center hosted a workshop examining the changing nature of data security in consumer electronic payments. The center invited the chairman and CEO of Heartland Payment Systems (HPS or Heartland), Robert (Bob) Carr, to lead this discussion and to share his experiences stemming from the data breach at his company in late 2008 and, as important, to discuss lessons learned as a result of this event. The former director of the Payment Cards Center, Peter Burns, who is acting as a senior payments advisor to HPS, also joined the discussion to outline Heartland's post-breach efforts aimed at improving information sharing and data security within the consumer payments industry. In conclusion, Carr introduced several technology solutions that are under discussion in payment security circles as ways to better secure payment card data as they move among the different parties in the card payment systems: end-to-end encryption, tokenization, and chip technology. While HPS has been very supportive

of end-to-end encryption, each of these alternatives offers its own set of advantages and disadvantages.

Summary. Cheney writes about Heartland Payment Systems, which receives and stores payment information. In 2009 the company experienced a high-profile breach, which occurred even though Heartland had passed PCI compliance and put great efforts into developing and using strong data security methods as a top business priority. Heartland's CEO, Robert Carr, spoke at a security workshop about how more must be done to increase security within the payment card industry, focusing on strategic objectives that create a collaborative and sharing environment and advance secure solutions to protect consumer data. Carr discussed how the data breach occurred when criminals compromised data as they infiltrated and moved around Heartland's network, known as data in transit. Carr also noted they had recently been assessed by a QSA but used the talking point to highlight that compliance as a minimum standard is not enough. He stressed the importance of information sharing among banks and financial services providers, as well as the need for leadership support for end-to-end encryption. Carr shared his strong belief that it is imperative that the payment card industry come together to contribute to and strengthen data security procedures and learn from past mistakes. He advocated for those companies that experience high-profile breaches to put forth more effort to influence the development of greater security enhancements to payment systems. This article was relevant to this discussion largely due to the overview of the data breach at Heartland and the descriptions of the impact to the bottom line of an organization that experiences a breach and the resulting negative effect on consumer confidence, which addresses how merchants learn from high-profile breaches.

Cheney, J. S., Hunt, R. M., Jacob, K. R., Porter, R. D., & Summers, B. J. (2012). The efficiency and integrity of payment card systems: Industry views on the risks posed by data breaches. *Federal Reserve Bank of Chicago Economic Perspectives, 36*(4), 130–146. Retrieved from https://www.phil.frb.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussion-papers/2012/D-2012-Efficiency-and-Integrity-of-Payment-Card-Systems.pdf

Abstract. To examine the adequacy of existing efforts to prevent, manage and mitigate data breaches and other fraud in card-based payment systems, the authors conducted 17 interviews of various payment industry participants in 2009. This article documents the insights gained from the interviews, which consider the need for greater cooperation, sharing of relevant information and innovation to stay ahead of the criminals that perpetrate payment card fraud with increasingly sophisticated methods.

Summary. The authors of this article explain that more consumers are using payment card systems, and the networks that process information must constantly evolve and make improvements on ease of use. The article focuses on the threat that payment fraud poses because it can deteriorate operational performance and will increase operational costs to merchants, as well as societal costs. However, the authors note that eliminating payment fraud entirely is not possible and the payment card industry must balance the cost between preventing and mitigating fraud. The authors provide some specific figures for credit card fraud losses, which in 2010 were $3.56 billion. Finally, the authors summarized industry interviews that they conducted with payment system participants, where they gleaned insights such as the fact that mobile payments were emerging at the time of publication (2012), that merchants must focus on developing a better

understanding of potential risks to payment systems, and how there is an increase in fraud committed internally by employees or even contractors. The authors highlight the greater need for merchants to collaborate and share risk management practices to stay on top of the latest threats. The authors also state that there might be an opportunity for the federal government to have a greater role in enforcement by improving processes for disabling sites that sell stolen consumer data or sharing how merchants can actively address new security threats as they arise.

Overall, the article was not a means of directing the conversation towards federal regulation; however, the authors note that it is a topic that they would like to see explored further. The information the authors received in response to their interviews suggests that the sharing of information about risk management techniques among merchants can create a more secure network, thus creating a better payment security standard to mitigate the risk of breaches. The main focus of this article was ultimately on the lessons learned from discussing payment trends, sharing of information among merchants from their experiences, and potential federal governmental governance, which could lead to an increase in consumer confidence.

Hemphill, T., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society,* 44, 30-38. https://doi.org/10.1016/j.techsoc.2015.11.007

Abstract. Managing effective security of personal customer data located in computer networks has become a strategic business and public policy issue for the U.S. retail sector. The article discusses the global credit card payment industry self-regulation regime established by the Payment Card Industry Security Standards Council (“Council”)

to combat cybercrime, comparing and evaluating the Council's existing standards regime to the theory and practices found in the industry self-regulation literature. A review of national cybercrime trends in both the volume and financial impacts (“losses”) of electronic financial record breaches on the U.S. retail sector is presented. After identifying the primary areas of retail electronic records breach vulnerability, an improved industry standards framework is developed that proposes to enhance security and minimize data privacy compromises through the adoption of recommended pure industry self-regulation (improved “security standard”) and market force mechanisms (mandatory “cyber liability insurance coverage”). The article concludes with a discussion of the implementation of the proposed industry self-regulation and market force framework; its current limitations; and what technology advancements may bring in the future to provide more effective security and protection for consumers' personal data and financial transactions.

Summary. Hemphill and Longstreet note that for as long as organizations have stored data on networks or systems, there has been an accompanying threat of hacks or breaches. Hackers exploit vulnerabilities, which in the case of retail transactions can exist at the client computer, the server, or during the transmission of data. The authors explain that Target’s data breach occurred because of a third-party vendor’s vulnerability, which approved remote access to the network to allow for software updates on their system. This vulnerability allowed hackers to plant malware on Target's system.

Since the card payment industry has established its own set of standards through the PCI SSC, which developed the DSS, the authors argue that the industry is defined as self-regulating. Therefore, they assert that the most effective security policy an organization

can develop is to ensure that merchants are not responsible for confidential data by not housing this data on their networks. A key idea within this article is the "Retail Customer Information Security Framework" proposed by the authors, which specifies that retailers can store baseline data that is considered public, such as a name and address; however, personal data like a birthdate must be considered at risk, and perhaps the retailer only stores the month and day, not the year. Another example from the framework is for retailers to encrypt data during storage and transmission and, even when the data is decrypted for use, retailers should adhere to a small window of use. This framework renders the data less usable or entirely unusable by a cybercriminal should a breach occur. The authors assert that this framework is still considered self-regulation but allows for the use of personalized marketing activities for the consumer while improving the retailer's security standards.

The authors conclude the article by outlining the impact of cybercrime and breaches, reporting the total amount of customer financial data that was compromised in 2013 and 2014 as a combined 674 million records across only six retail companies in the U.S. They note that while it is hard for merchants to stay on top of ever-evolving cybercriminal tactics, the authors believe that there are some trending methods for risk management, such as embedding a biometric reader into the card that can only be activated by the owner on a biometric pad or by using a fingerprint at the point of sale (POS). The authors highlight that these methods are still in their infancy and implementation is not yet defined, but they believe that the card payment industry will continue to make these types of shifts to protect PII.

This article was relevant to the study because the authors provide tips for secure storage and use of data, a framework for merchants to ensure they are securely handling customer data, and potential trends in combating breaches.

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons, 59*(3), 257-266. https://doi.org/10.1016/j.bushor.2016.01.002

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.

Summary. The authors detail the 2013 Target data breach to provide readers with real-world examples for organizational lessons. The authors described how the attack happened: hackers gained access to Target's system by going in through a third-party company, Fazio Mechanical Services. The hackers stole Fazio's credentials because Target did not limit vendor access to any of their systems; in the case of the breach, the hackers used Fazio's credentials to access Target's payment systems.

The authors also focused on cybersecurity regulation and note that as more of these breaches occur, consumers are turning to the court system to hold organizations accountable for not protecting PII. The authors assert that the industry must look inward and start to invest more in self-regulation by developing and following best practices. The

authors provide examples of best practices, including that organizations should invest in cybersecurity training for their employees so that they can identify and mitigate the latest hacking techniques, and that organizations should emphasize the importance of training employees on cybersecurity practices.

This article is relevant to this study because it reviews the mistakes from the Target breach, one of the most significant of its time, but also goes a step further and discusses often overlooked security practices that are fairly easy for organizations to implement across the organizations. Some of the authors' suggestions on additional security practices include: (a) proactively self-regulate, (b) hire strong CIOs to lead security initiatives, (c) develop a response plan, (d) only keep necessary data, (e) attempt to hack the network through penetration testing to identify vulnerabilities, (f) address vulnerabilities found, and (g) train and monitor employees on cybersecurity practices. This article was not necessarily meant to provide step-by-step best practices; however, it highlights some basic concepts that support the theory that organization must invest in cybersecurity practices.

Plachkinova, M., & Maurer, C. (2018). Security breach at Target. *Journal of Information Systems Education, 29*(1), 11-19. Retrieved from http://jise.org/Volume29/n1/JISEv29n1p11.pdf

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.

Summary. Plachkinova and Maurer developed this case study as a means of examining a real-world example of a high-level data breach as part of a cybersecurity curriculum that students could apply to actual security solutions once on the job. The case study and accompanying questions were distributed to thirty-eight university students and detailed the high-profile breach that occurred in 2013 at Target. The authors attempted to synthesize the results from students to understand if the learning objectives were achieved, which were to provide an objective view of the detailed events, allowing students to fully understand if the actions taken post breach were truly effective. The authors' goal was to increase the knowledge of the students and ongoing audiences of how organizations can be impacted by data breaches, how organizations can limit breaches, and how organizations can be better prepared to reduce risk and respond appropriately.

A key finding from the case study included the loss in consumer confidence following a data breach that will likely result in a decrease in revenues that could take years for an organization to recover from, as was the case with Target. Key findings of how

organizations can limit breaches include investing in cybersecurity and continuous security improvements, adding chip readers for customers, and taking responsibility for breaches should they occur. Key recommendations for how organizations can be better prepared to reduce the risk of data breaches and respond appropriately to attacks include strengthening an organization's stance on security and better protecting against cyber criminals by taking actions such as installing chip readers with personal identification numbers (PINs) on POS terminals.

This case study is relevant to this study due to the overview of the before, during, and after actions of the Target breach as a means of a post mortem. Before the breach, Target had invested in cybersecurity and employed a robust security staff to protect sensitive data, as well as passed a compliance audit. Once the breach occurred, security operations received an automated security notice of potential activity, which was simply shared with other operations teams in other locations, but no action was ever taken until the U.S. Department of Justice was notified of a potential breach and reached out to Target directly. The aftermath of the attack was that the company learned that the data of 70 million individuals was compromised, and Target took a major hit financially. The case study highlighted the real complexity of security breaches and how they impact consumer confidence. Target experienced a 1% decline in revenues and 34% decline in net income during the aftermath because shopping was down 10 percentage points.

Sullivan, R. J. (2010, Spring). The changing nature of U.S. card payment fraud: Industry and public policy options. *Economic Review [Kansas City], 95*(2), 101-133. Retrieved from https://www.kansascityfed.org/NXTTd/YXRNR/PUBLICAT/ECONREV/PDF/10q2Sullivan.pdf

Abstract. As credit and debit card payments have become the primary payment instrument in retail transactions, awareness of identity theft and concerns over the safety of payments has increased. Traditional forms of card payment fraud are still an important threat, but fraud resulting from unauthorized access to payment data appears to be rising, and we are only beginning to get a sense of the dimensions of the problem. Thus far, the role of public policy has been to encourage the card payment industry to limit fraud by developing its own standards and procedures. Whether this policy stance is sufficient depends on the effectiveness of industry efforts to limit fraud in light of the dramatic shift toward card payments. Sullivan provides an overview of card payment fraud in the United States. He develops a preliminary estimate of the rate of U.S. card payment fraud and suggests that such fraud is higher than in several other countries for which data are available. The U.S. payment industry is taking steps to combat payment fraud, but progress has been slowed by conflicts of interest, inadequate incentives, and lack of coordination. Thus, policymakers should monitor the card payment industry to see if it better coordinates security efforts, and if not, consider actions to help overcome barriers to effective development of security.

Summary. Sullivan's article examines how the emergence of electronic card payments initially resulted in high levels of security vulnerabilities because cyber criminals were able to commit fraud through not only stolen card numbers, but also by obtaining personal data that is typically required to make a purchase. Sullivan reported that the monetary value of fraud losses from counterfeit cards has risen steadily. Sullivan notes that from 2005 to 2010, 494 million records of sensitive data were compromised. He

reports how the increase of data breaches and their monetary impact lead to the formation of the PCI SSC and subsequent development of the DSS.

Sullivan examined some initiatives that were being developed at the time the article was published, which were to: (a) put more efforts into addressing a weakness in the DSS by requiring the encryption of sensitive card data either during transmission over public networks or providing end-to-end encryption, or (b) replace card account numbers with token numbers or tokenization, which happens after authorization of a card payment, thus allowing a merchant to store transaction information without storing card payment numbers. The aim of these initiatives was to attempt to make the merchants less of a target to cyber criminals because sensitive data that could be stolen would not be stored or transmitted. However, Sullivan highlights that there are barriers within the security industry that must be overcome before stronger security standards are established, such as the fact that there are no real incentives for all merchants to put forth the same efforts to establish security standards or policies.

One solution Sullivan presented is for the card payment industry to collectively pursue robust security efforts and perhaps develop a membership-style industry with buy-in and consequences if a merchant fails to abide by the standards. Sullivan highlights that governance is the best approach for success, as long as the standards are effective and flexible enough for both enterprise and small businesses.

This article is relevant to this study because Sullivan highlights that the DSS is an important first step made by the payment card industry and notes how the industry is attempting to improve the security of card payments; however, Sullivan also notes that

there are still weaknesses within the DSS and recommends that more efforts be made to be more effective.

History of PCI DSS

Ataya, G. (2010). PCI DSS audit and compliance. *Information Security Technical Report, 15*(4), 138-144. https://doi.org/10.1016/j.istr.2011.02.004

Abstract. PCI DSS compliance involves responding to a series of requirements imposed by the credit card industry. To succeed, organization must implement strict information security management processes and should master the risks related to the protection of credit card sensitive data. There are many actions that could be accomplished beforehand to ease the audit process, to reduce the effort and time consumed by the audit engagement and to ensure audit conclusions reflect the exact risk posture of the organization.

Summary. Ataya examines the management of the DSS by the acquiring banks and the importance of compliance by the merchants, noting that merchants that attempt compliance are in high-standings by the acquirer and seen as taking the time to protect PII. The author briefly outlines the requirements for compliance, as well as additional activities that organizations can implement to reduce the risk of a breach, such as implementing internal controls. These controls include: (a) think beyond the firewall and aim to improve the network perimeter, (b) continuously monitor for data breaches, (c) encrypt sensitive data, (d) regularly self-assess using security standards like COBIT or ISO27002, (e) evaluate risk assessments and determine gaps, (f) continuously review security policies and apply to all vendors, (g) run forensic analyses, (h) review configurations, (i) monitor user access and restrict periodically, and (j) isolate systems that store sensitive data from other systems. This article is important to this study because

the author emphasizes the necessity of establishing information security governance to design, implement and manage an organization's overall security program, with emphasis on the auditing portion of PCI compliance. The author asserts that establishing a governance structure and associated policies is a means of enabling ongoing analysis of compliance by the merchant.

Ataya also outlines the requirements that are most troubling for the majority of merchants during PCI compliance audits after implementation in order of frequency encountered: requirement 3 - protect stored data, requirement 11 - regularly test security systems and processes, and requirement 2 - do not use vendor-supplied defaults for system passwords and other security parameters. This information is particularly important to IT teams that might need to understand where potential security weaknesses lie. This article is relevant to this study as it details the audit process with which merchants must comply on a quarterly basis, the importance of establishing a security governance structure and associated policy for an organization's overall security program, potential compliance requirements issues, and the importance of continued assessment of security controls. Although the author did not go into great detail on how to exactly implement the best practices, Ataya promotes a proactive stance to maintain compliance.

Liu, J., Xiao, Y., Chen, H., Ozdemir, S., Dodle, S., & Singh, V. (2010). A survey of payment card industry data security standard. *IEEE Communications Surveys & Tutorials, 12*(3), 287-303. https://doi.org/10.1109/SURV.2010.031810.00083

Abstract. Usage of payment cards such as credit cards, debit cards, and prepaid cards, continues to grow. Security breaches related to payment cards have led to billion-dollar losses annually. In order to offset this trend, major payment card networks have founded

the Payment Card Industry (PCI) Security Standards Council (SSC), which has designed and released the PCI Data Security Standard (DSS). This standard guides service providers and merchants to implement stronger security infrastructures that reduce the risks of security breaches. This article mainly discusses the need for the PCI DSS and the data security requirements defined in the standard to address the ongoing security issues, especially those pertaining to payment card data handling. It also surveys various technical solutions, offered by a few security vendors, for merchant companies and organizations involved in payment card transaction processing to comply with the standard. The compliance of merchants or service providers to the PCI DSS are assessed by PCI Qualified Security Assessors (QSAs). This article thus discusses the requirements to become PCI QSAs. In addition, it introduces the PCI security scanning procedures that guide the scanning of security policies of a merchant or service provider and prepare relevant reports. We believe that this survey sheds light on potential technical research problems pertinent to the PCI DSS and its compliance.

Summary. The authors discuss how the PCI SSC was formed and why developing the DSS was so important based on increased credit card usage and continued breaches. The authors explain the transaction process, which includes the transaction flow, the clearing, and the settlement. The authors provide details of the security standards by outlining the six categories of compliance: (a) build and maintain a secure network and systems, (b) protect cardholder data, (c) maintain a vulnerability management program, (d) implement strong access control measures, (e) regularly monitor and test networks, and (f) maintain an information security policy. The authors also go into detail to explain the twelve

security requirements and the meaning and importance of each. The twelve security requirements are:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect cardholder data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need to know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for employees and contractors.

The authors outlined seven PCI compliance solutions from well-known vendors as a means of highlighting potential solutions for ease of implementation and monitoring. However, Liu et al. were careful to point out that these products likely address only partial DSS requirements; therefore, the authors compare service providers to highlight which requirements have a higher focus per vendor. Key findings include that most vendors will address requirements 3 (protect stored cardholder data), 4 (encrypt

transmission of cardholder data across open, public networks), 7 (restrict access to cardholder data by business need to know), and 10 (track and monitor all access to network resources and cardholder data), which according to the 2018 Verizon Payment Security Report, requirements 3, 4, and 7 are the most commonly passed requirements. Another highlight was that only one of the vendors, Secure Works' iSensor IPS/IDS, actually addressed all twelve requirements. Finally, the authors detail the QSA's job role and responsibilities, which are to perform compliance validation assessments using audit procedures designed from the DSS.

This article is relevant to this study as it provides an outline of how to understand and implement a more secure infrastructure to mitigate risk, as an important first step in obtaining PCI compliance. The authors highlight the fact that the DSS framework is meant to provide consistent standards and more effective practices that can create more secure transaction data to better protect all stakeholders. This article provided an informative outline of the standards and requirement trouble areas and gave context to the quarterly and annual audit process for the audience to reach a greater grasp of the overall PCI compliance topic.

Morse, E. A., & Raval, V. (2008). PCI DSS: Payment card industry data security standards in context. *Computer Law and Security Review, 24*(6), 540-554. https://doi.org/10.1016/j.clsr.2008.07.001

Abstract. In recent years, the payment card industry has dealt with the matter of consumer liability for unauthorized charges. However, risks to consumers from identity theft and related use of personal data present new challenges for cardholders and those who profit from their usage, including merchants, banks, and payment card companies.

This article examines the varying and sometimes complementary roles that legal obligations and private ordering play in incentivizing security measures to protect consumers. It shows that, in the legal environment within the United States, which lacks comprehensive legal protections for consumer privacy and security, private ordering rooted in economic incentives within the payment card industry can also bring about enhanced security for consumers. The Payment Card Industry Data Security Standards ("PCI DSS") have emerged from private ordering, although threats of legal liability have also influenced their development and implementation. The article evaluates the basic framework of PCI DSS and raises issues for further development as the government, the legal system, and the industry cope with security threats in this environment.

Summary. Morse and Raval assert that both merchants and the payment card companies must develop and address solid security standards that protect consumer data and note that in the early days of credit card development the law influenced emerging and unforeseen issues that affect consumers, such as unauthorized charges or identity theft, by providing consumer protection legislation for unauthorized charges. The authors note that the PCI SSC has gone a step further to protect consumer rights with no-liability policies for unauthorized charges, resulting in consumer protection from having to pay for unauthorized charges on their credit cards. The authors contend that regulation by the federal government in the area of personal data protection is actually lacking and assert that even though the PCI SSC developed the DSS to mitigate risks of security breaches, the model could use great improvement and can be costly for merchants when unauthorized charges occur and consumers dispute charges. Areas in the DSS that they believe need to be improved include the lack of independent legal authority by the PCI

SSC to enforce the DSS, as well as QSA assessments or self-assessments, which are open to interpretation. The authors discuss the regulatory environment that the card payment industry operates within, which includes information on: (a) privacy legislation, (b) FTC enforcement, (c) state-specific provisions, and (d) common-law claims, and note that fines can be used as measures of adherence to, as well as an assessment of, overall data security standards.

This article's relevance to this paper is based on the background information regarding the formation of the DSS and the context it provides for the multi-dimensional financial and legal frameworks of the card payment industry in relation to consumers, merchants, acquiring banks, and payment card associations. The theme of risk management for merchants was paramount to this study to fully understand the scope of the impact to all parties when data breaches occur.

Best Practices of PCI Compliance

Blue, J., Furey, E., & Condell, J. (2017). A novel approach for secure identity authentication in legacy database systems. In *2017 28th Irish Signals and Systems Conference (ISSC)* (pp. 1-6). Killarney, Ireland: IEEE. https://doi.org/10.1109/ISSC.2017.7983624

Abstract. Information systems in the digital age have become increasingly dependent on databases to store a multitude of fundamental data. A key function of structured databases is to house authentication credentials that verify identity and allow users to access more salient personal data. Authentication databases are frequently a target of attack as they potentially provide an avenue to commit further, more lucrative crimes. Despite the provision of industry standard best practice recommendations from organizations such as Open Web Application Security Project (OWASP), Payment Card Industry Security

Standards Council (PCI-SSC), Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineers (IEEE), often practical security implementations within industry flounder. Lacking or substandard implementations have cultivated an environment where authentication databases and the data stored therein are insecure. This was demonstrated in the 2016 exposure of a breach experienced by Yahoo where approximately one billion user credentials were stolen. The global technology company was found to be using obsolete security mechanisms to protect user passwords. Dated implementations such as these pose serious threat as they render authentication data highly vulnerable to theft and potential misuse. This paper offers a novel solution for securing authentication databases on non-compliant Apache servers. The method applies the recommended best practice mechanisms in the form of salt, one-way encryption (hashing) and iterations to both pre-existing and newly created passwords that are stored on insecure systems. The proposed solution can be implemented server-side, with little alteration to the existing infrastructure, unbeknownst to the user. It possesses the potential to improve system security, aid compliance, preserve privacy and protect users.

Summary. The authors of this article sought to present a potential solution for the security of older and noncompliant legacy databases through some best practice techniques. A very common form of identity verification is the use of usernames and passwords; before there was so much focus on cybercrime, this data was housed in plaintext in legacy databases, which have been successfully hacked by criminals. The authors discuss the immediate need for a solution to protect this type of sensitive data; they describe the ensuing solution as a “salt, hash and iteration” password protection process that maintained confidentiality with no data loss (p. 3). In order to hack the

password, a cybercriminal would have to somehow reverse engineer the saved password back into plaintext. The authors provide an example of Apache web servers using a system configuration such as PHP and MySQL, where the system administrator would create a table storing password information that assigns a series of numbers and letters or random strings for the password that cannot be deciphered to remove the plaintext password. The system would store a second password of random strings in a separate table; a cybercriminal would therefore have to know both passwords in order to gain access to the data.

Although this article was specific to the application of security practices to usernames and passwords stored in legacy databases, the practices still align with PCI standards and are a form of best practices compliance for specific web application forms.

Gray, D., & Ladig, J. (2015). The implementation of EMV chip card technology to improve cyber security accelerates in the U.S. following Target Corporation's data breach. *International Journal of Business Administration, 6*(2), 60-67. https://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.

Summary. The authors used the Target data breach that occurred in 2013 and affected 70 million customers as a baseline argument to explain why merchants in the U.S. are now slowly adopting the Europay, Mastercard, and Visa (EMV) chip card technology. The authors note that while this technology may not entirely reduce the cybercrime of stolen payment card data, it can reduce data breaches. The authors do point out that there is an associated cost to make the change to the chip card technology with the addition of debit and credit cards that are embedded with microchips and the actual machines that will read the cards.

This article was written in 2015 when Visa, MasterCard, American Express, and Discover gave notice to U.S. merchants to convert to chip-based credit cards by October 2015. If a merchant did not make the conversion by the deadline and fraud occurred as a result, these card companies warned that the liability would land on the party that was not EMV-compliant – in other words, the merchant. The card payment industry made the move to chip technology to help prevent future data breaches.

EMV technology includes the use of an embedded microchip within the debit and/or credit card, and the card companies recommend that the card also use a PIN, which is used to distinguish each transaction through encryption codes and makes it harder for hackers to gain access to this information. The authors noted that other countries, mostly in Europe, had already adopted the use of EMV technology; therefore, U.S. citizens traveling abroad would be able to use their card payments in the same manner with no

hiccups. The authors argue that the U.S. waited too long to invest in the change to EMV technology and therefore experienced massive data breaches such as with Target breach in 2013.

Knowles, W., Baron, A., & McGarr, T. (2016). The simulated security assessment ecosystem: Does penetration testing need standardisation? *Computers & Security, 62*, 296. https://doi.org/10.1016/j.cose.2016.08.002

Abstract. Simulated security assessments (a collective term used here for penetration testing, vulnerability assessment, and related nomenclature) may need standardisation, but not in the commonly assumed manner of practical assessment methodologies. Instead, this study highlights market failures within the providing industry at the beginning and ending of engagements, which has left clients receiving ambiguous and inconsistent services. It is here, at the prior and subsequent phases of practical assessments, that standardisation may serve the continuing professionalisation of the industry, and provide benefits not only to clients but also to the practitioners involved in the provision of these services. These findings are based on the results of 54 stakeholder interviews with providers of services, clients, and coordinating bodies within the industry. The paper culminates with a framework for future advancement of the ecosystem, which includes three recommendations for standardisation.

Summary. The authors describe simulated security assessments such as penetration testing that is conducted as part of a vulnerability scan to detect vulnerabilities on the network where a potential bad actor or criminal may attempt unauthorized entry. PCI's DSS has twelve requirements and includes vulnerability scans in requirement 11, which is to regularly test security systems and processes. Specifically, requirement 11.2 and

requirement 11.3 mandate internal and external quarterly vulnerability scans and internal and external annual penetration testing, respectively. As Ataya also noted, requirement 11 is the second most frequent cause of trouble for merchants in maintaining compliance, and according to the 2018 Verizon Payment Security Report, it is the most frequent. With the DSS in mind, the authors propose that specific standards should be developed for a simulated security assessment.

The authors begin by examining well-known certifications that certify that an individual who has passed an exam possesses the knowledge, skills, and ability to perform penetration testing, such as the Certified Ethical Hacker (CEH) or the Offensive Security Certified Professional (OSCP) certifications. However, these certifications are developed by two separate educational bodies and test to different skills. Knowles, Baron, and McGarr argue that the guidelines for how to conduct an assessment have not been developed out of formal standards by cybersecurity institutions, but rather have been presented as self-described guidelines by the security community at large, like the Penetration Testing Execution Standard (PTES). The PTES formed as a community that developed and provided penetration testing guidelines over seven stages: (a) pre-engagement, (b) intelligence gathering, (c) threat modelling, (d) vulnerability analysis, (e) exploitation, (f) post-exploitation, and (g) reporting. However, these seven stages are not technical guidelines that describe specifically how to conduct a pen test, but instead are presented as concepts.

The authors conducted 54 interviews within the security assessment community to gather the thoughts of the respondents on the details of penetration testing like scope, methodologies, terminology, and vulnerability scoring and found that there is great

ambiguity about what it truly means to conduct a penetration test. The authors also discovered that various companies use diverse metrics for vulnerability scoring, which makes it difficult to track actual improvements in performance over time. Another key finding was that the results of penetration tests often do not produce lists of priorities or categorizations, associated root cause analyses, and recommendations for improvements, which makes it difficult to prioritize and address the issues that must be addressed. The authors conclude that standardization must come from the security assessment community is and will arise through continued discussion.

Ukidve, A., Smantha, D., & Tadvalka, M. (2017). Analysis of payment card industry data security standard [PCI DSS] compliance by confluence of COBIT 5 framework. *International Journal of Engineering Research and Applications, 07*(01), 42-48. https://doi.org/10.9790/9622-0701014248

Abstract. The Payment Card Industry Data Security Standard (PCI DSS) aims to enhance the security of cardholder data and is required when cardholder data or authentication data are stored, processed or transmitted. The implementation of enabling processes from COBIT 5 can complement compliance to PCI DSS. COBIT 5 assists enterprises in governance and management of enterprise IT and, at the same time, supports the need to meet security requirements with supporting processes and management activities. This paper provided analysis of mapping of COBIT 5 supporting processes to PCI DSS 3.0 security requirements. It also presents domains which support the simultaneous application of COBIT 5 and PCI DSS 3.0 which would help create collaborations within the enterprise.

Summary. The authors explain how the framework or governance designed within Control Objectives for Information and Related Technology (COBIT) version 5 can assist merchants that store, process, and transmit sensitive card payment data to comply with DSS. COBIT 5 was developed by the Information Systems Audit and Control Association (ISACA) and is aimed at providing organizations with a detailed framework that can assist with meeting security requirements by assessing risk and identifying vulnerabilities. It can provide guidance for IT teams who are analyzing or auditing their enterprise internal controls by providing recommendations for governance that cover principles like meeting stakeholder needs or covering the enterprise from end-to-end. The authors demonstrate in the article how they have directly mapped all twelve of the DSS requirements to the supporting processes found within COBIT 5.

The authors classify PCI requirements 1 (install and maintain a firewall configuration to protect cardholder data) and 2 (do not use vendor-supplied defaults for system passwords and other security parameters) as the mapping of network processes. To secure, control, and monitor the network, the authors note that firewalls must be implemented to block any unwanted access that may occur between networks. The authors assert that vendor-defined, system defaults pose a security risk because they are easy for a cybercriminal to find on the internet. COBIT 5 addresses these requirements through processes such as establishing and maintaining a configuration model or developing solution components, which means to document authentication standards.

The authors classify PCI requirements 3 (protect stored cardholder data) and 4 (encrypt transmission of cardholder data across open, public networks) as the protection of cardholder data, which includes data deletion and encryption practices. COBIT 5

addresses these two requirements with processes that include managing end-point security, managing user identity and logical access, and managing network and connectivity security. The authors classify PCI requirements 5 (use and regularly update anti-virus software or programs) and 6 (develop and maintain secure systems and applications) as vulnerability management and note that COBIT 5 maps to these requirements through processes such as protecting against malware or establishing a test environment. They assert that these requirements are important because criminals attempt to exploit vulnerabilities in order to compromise sensitive cardholder data.

The authors classify PCI requirements 7 (restrict access to cardholder data by business need to know), 8 (assign a unique ID to each person with computer access), and 9 (restrict physical access to cardholder data) as access control measures, or the authentication method of defining who has access to which data or systems. The authors assert that COBIT 5 maps to these requirements through processes such as managing user identity and logical access, defining reference architecture, and defining information data and system ownership.

The authors classify PCI requirements 10 (track and monitor all access to network resources and cardholder data) and 11 (regularly test security systems and processes) as monitoring and testing of networks and note that COBIT 5 maps to these requirements through processes such as ensuring the traceability of information events and accountabilities and identifying and reporting control deficiencies. They state that systems must be tested regularly or scanned for vulnerabilities or signs of attacks. Lastly, PCI requirement 12 is to maintain a policy that addresses information security for all personnel, which is an important step to ensure security awareness within the

organization. COBIT 5 maps to this requirement through processes such as defining the organizational structure and establishing roles and responsibilities.

This article was relevant to this study through its application of a framework to establish a rigorous risk management approach to establishing and maintaining PCI compliance. The authors suggest that many organizations comprehend risk analysis within a type of governance and management approach of applying a framework. However, maintaining security compliance is not always addressed in this same manner. The authors suggest that the COBIT 5 processes, when applied, can greatly increase the chances of implementing and maintaining PCI compliance requirements.

Willey, L., & White, B. J. (2013). Teaching case do you take credit cards? Security and compliance for the credit card payment industry. *Journal of Information Systems Education, 24*(3), 181–188. Retrieved from https://www.learntechlib.org/p/168011/

Abstract. Security is a significant concern in business and in information systems (IS) education from both a technological and a strategic standpoint. Students can benefit from the study of information systems security when security concepts are introduced in the context of real-world industry standards. The development of a data security standard for organizations operating within the credit card payment industry serves as an excellent example of a real-world security standard that lends itself to classroom study. The establishment and requirements of the Payment Card Industry Data Security Standard (PCI DSS), and the associated consequences for noncompliance, represents a businesslike approach to the organizational protection of data that students will find interesting and one to which they will relate. Everybody uses credit cards! Incorporating the topic of PCI DSS into an activity allows students to learn and apply PCI DSS concepts to a business

setting. Just asking "If everyone uses credit cards, why don't all businesses accept them?" will start a process of exploration for the class. A hypothetical business teaching case, Blue Mountain Jams (BMJ), illustrates the challenge of PCI DSS mandates for small businesses. Small business is given some leeway in self-assessment under PCI DSS to document compliance after the decision is made to accept credit card payments. That leeway gives students the opportunity to learn and analyze the PCI DSS requirements and compliance methods and to determine the best course of action for a business that has made the decision to start accepting credit cards.

Summary. The authors discuss the importance of allowing students in the fields of business and IS to be exposed to real-world security concepts related to the PCI DSS guidelines, as the topics are highly relevant in today's business environment. Through this case study, students are introduced to the DSS requirements and exposed to the consequences of noncompliance, namely the liability and costs associated, which include the bottom-line financial loss from a fraudulent charge, associated costs of the notification obligation response to consumers, additional internal systems monitoring for continued activity, potential reissuing of cancelled cards, as well as the loss of consumer confidence and trust.

The authors apply the concepts in a business setting, noting the challenges of complying with the standards for small businesses. According to the authors, small businesses are not held to the same scrutiny as enterprise companies, which makes it easier for students to comprehend the basics to better understand the best approach for any business that will start to accept payment in this form.

Willey and White outlined the PCI DSS Requirements against the rates of compliance by percentages over a three-year period; the table highlighted the fact that organizations often have certain requirements that are easier or harder to implement. As an example, requirement 10, tracking and monitoring access, and requirement 12, maintaining security policies, are more difficult for organizations to implement. On the other hand, requirement 5, using and updating anti-virus software, and requirement 9, restricting physical access, are easier for organizations to implement. This case study would also be informative for junior-level system administrators who may be implementing DSS requirements for the first time to understand where there is likely to be oversight and noncompliance.

Yulianto, S., Lim, C., & Soewito, B. (2016). Information security maturity model: A best practice driven approach to PCI DSS compliance. *2016 IEEE Region 10 Symposium (TENSYMP)* (pp. 65-70). https://doi.org/10.1109/TENCONSpring.2016.7519379

Abstract. A successful of PCI DSS implementation depends on the capability of the organization's information security in providing the effective safeguard of their information asset, while cardholder data security is the main concern. Many organizations failed to comply with the standard, and this eventually results in fines or even termination of the ability to process credit cards. Clearly, an evaluation mechanism or tool used to measure the current state of the organization's information security is needed. In this paper, an Information Security Maturity Model for PCI DSS (ISMM-PCI) with four maturity level - None, Initial, Basic and Capable - was proposed. The ISMM-PCI utilizes the use of quantitative and qualitative analysis, enhancing the PCI DSS to ISO/IEC 27001 mapping, and focuses on improving the quality of people, process and

technology. The model assists the organizations to easily identify the key success factors and gaps (point of weaknesses), provides the guideline to better manage information security and formulate the best strategy for the enhancement, improving the overall information security state by selecting the best security countermeasures (controls) to protect their information assets from the emerging cyber-attacks, while achieving PCI DSS full compliant. The main advantage of ISMM-PCI over other ISMMs is its ease of use. The comparative analysis of the case results affirms the statement. ISMM-PCI may be used by a wide range of organizations regardless of the size.

Summary. Yulianto, Lim, and Soewito discuss how organizations that attempt to put forth standard security efforts to comply with the twelve requirements as designed by the PCI and who employ best practices of document processes are still not doing enough to protect end user data. The authors highlight some of the PCI DSS requirements that are tougher for organizations to address and implement, including securely transmitting, processing, and storing cardholder data; and how organizations should move quickly to address any internal or external factors that could lead to a breach.

The authors present an evaluation tool that can be used to determine the state of needed security measures and gaps in compliance; the tool maps directly to the PCI DSS and highlights four maturity levels: (0) None, (1) Initial, (2) Basic, and (3) Capable. The proposed model is adapted from various forms of other IS maturity models' foundations, and has three components: management, evaluation, and awareness. The model is framed as a matrix where a user can document internal and external factors related to security for the organization, as well as the organization's strengths, weaknesses, opportunities, and threats (SWOT). The user can then analyze this information to identify the maturity of an

organization in reaching its security objectives. The model allows an organization to define the weaknesses and gaps in meeting its security objectives based on the maturity level defined by the matrix, which allows the organization to put its main focus on fixing the weaknesses and gaps with an executable action plan. The model assumes that an organization is working towards an in-depth and comprehensive IS program and cyber defense overall, including identifying, developing and implementing policies, structures, personnel and physical security. The authors assert that this tool can be used as a best practice to improve the overall state of security of any size organization, enable stronger risk management, and aid in fully complying with DSS.

Conclusion

The references in the Annotated Biography section of this study examine potential best practice approaches to obtain and maintain Payment Card Industry (PCI) compliance, while considering past high-profile breaches and the history of PCI Data Security Standards (DSS). The PCI standards, which are meant to aid in mitigating risk, require that merchants not only achieve full compliance, but also maintain compliance on a quarterly or annual basis (PCI DSS, 2018). As demonstrated by some high-profile breaches, obtaining 100 percent compliance does not mean that an organization will not incur data security breaches (Cheney, 2010; Gray & Ladig, 2015; Plachkinova & Maurer, 2018; Van Oosten, 2018; Vijayan, 2014). Organizations can mitigate the risk of exposure by learning the lessons from past high-exposure breaches and maintaining best practices in PCI compliance (Cheney, 2010; Cheney et al., 2012; Manworren et al., 2016; Plachkinova & Maurer, 2018).

Historical High-Exposure Breaches

Data breaches affect numerous sensitive cardholder records and result in significant financial losses for the organizations that suffer the breaches and a negative impact on consumer confidence (Cheney, 2010; Cheney et al., 2012; Hemphill & Longstreet, 2015; Plachkinova & Maurer, 2018; Sullivan, 2010). Research on the Heartland data breach that occurred in 2009 after the company was certified as PCI compliant (Cheney, 2010) highlighted that 130 million records were compromised (Sullivan, 2010), half of its market capital was lost, $32 million was spent on settlement costs and additional legal fees (Cheney, 2010), and it was the fourth costliest records breach in U.S. history (Hemphill & Longstreet, 2015). Multiple authors reported on the Target data breach that occurred in 2013, after it too was certified as PCI compliant (Plachkinova & Maurer, 2018), where 70 million customers were affected and over $290 million in lost sales was

reported (Hemphill & Longstreet, 2015; Manworren et al., 2016; Plachkinova & Maurer, 2018). The hackers gained access to Target's payment system by going through a third-party company, Fazio Mechanical Services; the hackers stole Fazio's credentials because Target did not limit vendor access to their systems (Manworren et al., 2016; Plachkinova & Maurer, 2018). Manworren et al. (2016) point to the Target data breach as a turning point in increased scrutiny of the cybersecurity practices of retailers in the U.S. due to the scale of the number of records compromised and Target's negligence that led to the breach.

Target was one of six retail companies in the U.S. that were responsible for a combined total of 674 million records that were compromised in 2013 and 2014 (Hemphill & Longstreet, 2015). These breaches highlight the fact that organizations must implement an effective and proactive security policy beyond the minimum standards to protect their finances and consumers (Manworren et al., 2016).

History of PCI DSS

The PCI Security Standards Council (SSC) was formed in 2004 and subsequently developed the DSS with six categories of compliance: (a) build and maintain a secure network and systems, (b) protect cardholder data, (c) maintain a vulnerability management program, (d) implement strong access control measures, (e) regularly monitor and test networks, and (f) maintain an information security policy, which is designed to guide merchants to better protect against breaches affecting cardholder data (Liu et al., 2010). There are twelve security requirements that apply to any system components that are connected to cardholder data:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

3. Protect cardholder data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need to know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for employees and contractors (Ataya, 2010; Liu et al., 2010).

Of the twelve PCI DSS security requirements, Ataya (2010) identifies the requirements that are most troubling for the majority of merchants during PCI compliance audits after implementation, in order of frequency encountered: requirement 3 - protect stored data, requirement 11 - regularly test security systems and processes, and requirement 2 - do not use vendor-supplied defaults for system passwords and other security parameters.

Although not federally regulated, there are consumer protection policies in place in the case of unauthorized charges (Morse & Raval, 2008). Morse and Raval (2008) note that the PCI SSC has gone a step further to protect consumer rights with no-liability policies for unauthorized charges, resulting in consumer protection from having to pay for unauthorized charges on their credit cards. There are also penalties for noncompliance with PCI's standards, leveled largely on the merchants (Ataya, 2010; Morse & Raval, 2008).

Morse and Raval (2008) contend that regulation by the federal government in the area of personal data protection is actually lacking and assert that even though the PCI SSC developed the DSS to mitigate risks of security breaches, the model could use great improvement and can be costly for merchants when unauthorized charges occur and consumers dispute charges. Areas in the DSS that they believe need to be improved include the lack of independent legal authority by the PCI SSC to enforce the DSS, as well as QSA assessments or self-assessments, which are open to interpretation.

Best Practices of PCI Compliance

Multiple authors stressed the critical need for organizations to take additional protective measures to greatly increase the security of their systems and the likelihood of obtaining and maintaining PCI compliance (Blue et al., 2017; Gray & Ladig, 2015; Yulianto et al., 2016). Ukidve et al. (2017) recommend following defined security standards by implementing a framework from COBIT 5, which assists organizations in governance, management of IT, and meeting security requirements with supporting processes and management activities. Yulianto et al. (2016) note the need for an evaluation tool to measure the current state of an organization's information security practices in order to highlight and resolve issues. Knowles et al. (2016) identify the need for penetration testing as part of the network vulnerability scans required by PCI DSS and recommend standardizing the approach taken for the scans to avoid ambiguous or inconsistent results.

A best practice that multiple authors recommended is for merchants to simply not house data on their networks so they are not responsible for confidential data (Hemphill & Longstreet, 2016; Manworren et al., 2016). An additional best practice with widespread support is for merchants to install POS terminals with chip readers to read PINs because payment cards with

this feature are likely more secure due to the use of encryption codes for each transaction, which makes it harder to access this data and thus reduces losses (Cheney, 2010; Cheney et al., 2012; Gray & Ladig, 2015; Plachkinova & Maurer, 2018; Sullivan, 2010). While there was an additional cost for merchants to transition to the chip technology because of the need to purchase machines that accommodate the chip cards, Visa, MasterCard, American Express, and Discover gave notice to U.S. merchants to convert to chip-based credit cards by October 2015, with a warning that merchants who did not meet the deadline would be liable for any fraud that subsequently occurred (Gray & Ladig, 2015). Gray and Ladig (2015) assert that the motivation for this technology change was the massive data breach suffered by Target Corporation in 2013.

Multiple authors agreed that end-to-end encryption is an important measure that organizations can employ to better secure data (Cheney, 2010; Sullivan, 2010). Research also indicates that data breaches can be reduced with the use of encrypting authentication such as the "salt, hash, and iteration" password protection process (Blue et al., 2017, p. 3). An additional recommendation is the use of tokenization, or replacing card account numbers with random numbers after authorization of a card payment, thus allowing a merchant to store transaction information without storing card payment numbers (Cheney, 2010; Sullivan, 2010).

Research also focused on the importance of education and training. Willey and White (2013) note the importance of teaching security concepts in both business and information systems education and recommend that the history and requirements of PCI DSS and consequences for noncompliance be used as case studies in teaching students the concepts. Manworren et al. (2016) recommend that organizations invest in employee cybersecurity training, as employees may be the weakest link in the card payment chain.

Final Thoughts

The scholarly sources within this study highlight the importance of adhering to and investing in best practices to obtain and maintain PCI compliance. Merchants who comply with the standards are less likely to experience a security breach, which not only affects an organization's bottom line, but likely disrupts consumer confidence (Cheney, 2010; Cheney et al., 2012; Manworren et al., 2016; Plachkinova & Maurer, 2018). With cybercrime on the rise and vulnerabilities constantly being exposed, it is imperative that organizations take a proactive stance to maintain compliance (Ataya, 2010; Manworren et al., 2016). Organizations that adopt the best practices that suit their security policy needs will protect their own financial interests and maintain consumer confidence by constantly reducing risk (Cheney, 2010; Gray & Ladig, 2015; Manworren et al., 2016; Plachkinova & Maurer, 2018).

References

Ataya, G. (2010). PCI DSS audit and compliance. *Information Security Technical Report, 15*(4), 138-144. https://doi.org/10.1016/j.istr.2011.02.004

Blue, J., Furey, E., & Condell, J. (2017). A novel approach for secure identity authentication in legacy database systems. In *2017 28th Irish Signals and Systems Conference (ISSC)* (pp. 1-6). Killarney, Ireland: IEEE. https://doi.org/10.1109/ISSC.2017.7983624

Center for Public Issues Education. University of Florida. (n.d.). Evaluating information sources. Retrieved from https://canvas.uoregon.edu/courses/120122/files/5706985/download?wrap=1

Cheney, J. S. (2010). Heartland payment systems: Lessons learned from a data breach. *SSRN Electronic Journal,* 1-36. https://dx.doi.org/10.2139/ssrn.1540143

Cheney, J. S., Hunt, R. M., Jacob, K. R., Porter, R. D., & Summers, B. J. (2012). The efficiency and integrity of payment card systems: Industry views on the risks posed by data breaches. *Federal Reserve Bank of Chicago Economic Perspectives, 36*(4), 130–146. Retrieved from https://www.phil.frb.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussion-papers/2012/D-2012-Efficiency-and-Integrity-of-Payment-Card-Systems.pdf

Gray, D., & Ladig, J. (2015). The implementation of EMV chip card technology to improve cyber security accelerates in the U.S. following Target Corporation's data breach. *International Journal of Business Administration, 6*(2). https://doi.org/10.5430/ijba.v6n2p60

Hemphill, T., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society,* 44, 30-38. https://doi.org/10.1016/j.techsoc.2015.11.007

Hooper, V., & Mckissack, J. (2016). The emerging role of the CISO. *Business Horizons, 59*(6), 585-591. https://doi.org/10.1016/j.bushor.2016.07.004

Karanja, E., & Rosso, M. A. (2017). The chief information security officer: An exploratory study. *Journal of International Technology & Information Management, 26*(2), 23–47. Retrieved from https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1299&context=jitim

Knowles, W., Baron, A., & McGarr, T. (2016). The simulated security assessment ecosystem: Does penetration testing need standardisation? *Computers & Security, 62*, 296. https://doi.org/10.1016/j.cose.2016.08.002

Liu, J., Xiao, Y., Chen, H., Ozdemir, S., Dodle, S., & Singh, V. (2010). A survey of payment card industry data security standard. *IEEE Communications Surveys & Tutorials, 12*(3), 287-303. https://doi.org/10.1109/SURV.2010.031810.00083

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons, 59*(3), 257-266. https://doi.org/10.1016/j.bushor.2016.01.002

Morse, E. A., & Raval, V.. (2008). PCI DSS: Payment card industry data security standards in context. *Computer Law and Security Review, 24*(6), 540-554. https://doi.org/10.1016/j.clsr.2008.07.001

National Initiative for Cybersecurity Education. (n.d.). *Cybersecurity Career Pathway.* Retrieved from https://www.cyberseek.org/pathway.html

Payment Card Industry (PCI) Compliance Guide. (n.d.). PCI FAQs. Retrieved from https://www.pcicomplianceguide.org/faq

PCI Data Security Standard (DSS). (2018, May). (Rep. No. V3.2.1). Retrieved from https://www.pcisecuritystandards.org/document_library

PCI Security. (n.d.). Overview. Retrieved from https://www.pcisecuritystandards.org/pci_security/

Peppard, J., Edwards, C., & Lambert, R. (2011). Clarifying the ambiguous role of the CIO. *MIS Quarterly Executive, 10*(1), 31–44. Retrieved from http://www.som.cranfield.ac.uk/som/dinamic-content/media/ISRC/Clarifying%20the%20Ambiguous%20Role%20of%20the%20CIO.pdf

Pigni, F., Bartosiak, M., Piccoli, G., & Ives, B. (2018). Targeting Target with a 100 million dollar data breach. *Journal of Information Technology Teaching Cases, 8*(1), 9-23. https://doi.org/10.1057/s41266-017-0028-0

Plachkinova, M., & Maurer, C. (2018). Security breach at Target. *Journal of Information Systems Education, 29*(1), 11-19. Retrieved from http://jise.org/Volume29/n1/JISEv29n1p11.pdf

Ponemon Institute. (2018, July). Cost of a data breach study 2018. Retrieved from https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018/

Privacy Rights Clearinghouse. (n.d.). Data breaches. Retrieved from https://www.privacyrights.org/data-breaches

Sullivan, R. J. (2010, Spring). The changing nature of U.S. card payment fraud: Industry and public policy options. *Economic Review [Kansas City], 95*(2), 101+. Retrieved from

https://www.kansascityfed.org/NXTTd/YXRNR/PUBLICAT/ECONREV/PDF/10q2Sullivan.pdf

Tutton, J. (2010). Incident response and compliance: A case study of the recent attacks. *Information Security Technical Report, 15*(4), 145-149. https://doi.org/10.1016/j.istr.2011.02.001

Ukidve, A., Smantha, D., & Tadvalka, M. (2017). Analysis of payment card industry data security standard [PCI DSS] compliance by confluence of COBIT 5 framework. *International Journal of Engineering Research and Applications, 07*(01), 42-48. https://doi.org/10.9790/9622-0701014248

Van Oosten, C. (2018, September 25). *Verizon 2018 payment security report* (pp. 1-52). Retrieved from https://enterprise.verizon.com/resources/reports/payment-security/2018/

Vijayan, J. (2014, January 24). After Target, Neiman Marcus breaches, does PCI compliance mean anything? Retrieved from https://www.computerworld.com/article/2486879/data-security/after-target--neiman-marcus-breaches--does-pci-compliance-mean-anything-.html

Willey, L., & White, B. J. (2013). Teaching case do you take credit cards? Security and compliance for the credit card payment industry. *Journal of Information Systems Education, 24*(3), 181–188. Retrieved from https://www.learntechlib.org/p/168011/

Yulianto, S., Lim, C., & Soewito, B. (2016). Information security maturity model: A best practice driven approach to PCI DSS compliance. *2016 IEEE Region 10 Symposium (TENSYMP)* (pp. 65-70). https://doi.org/10.1109/TENCONSpring.2016.7519379