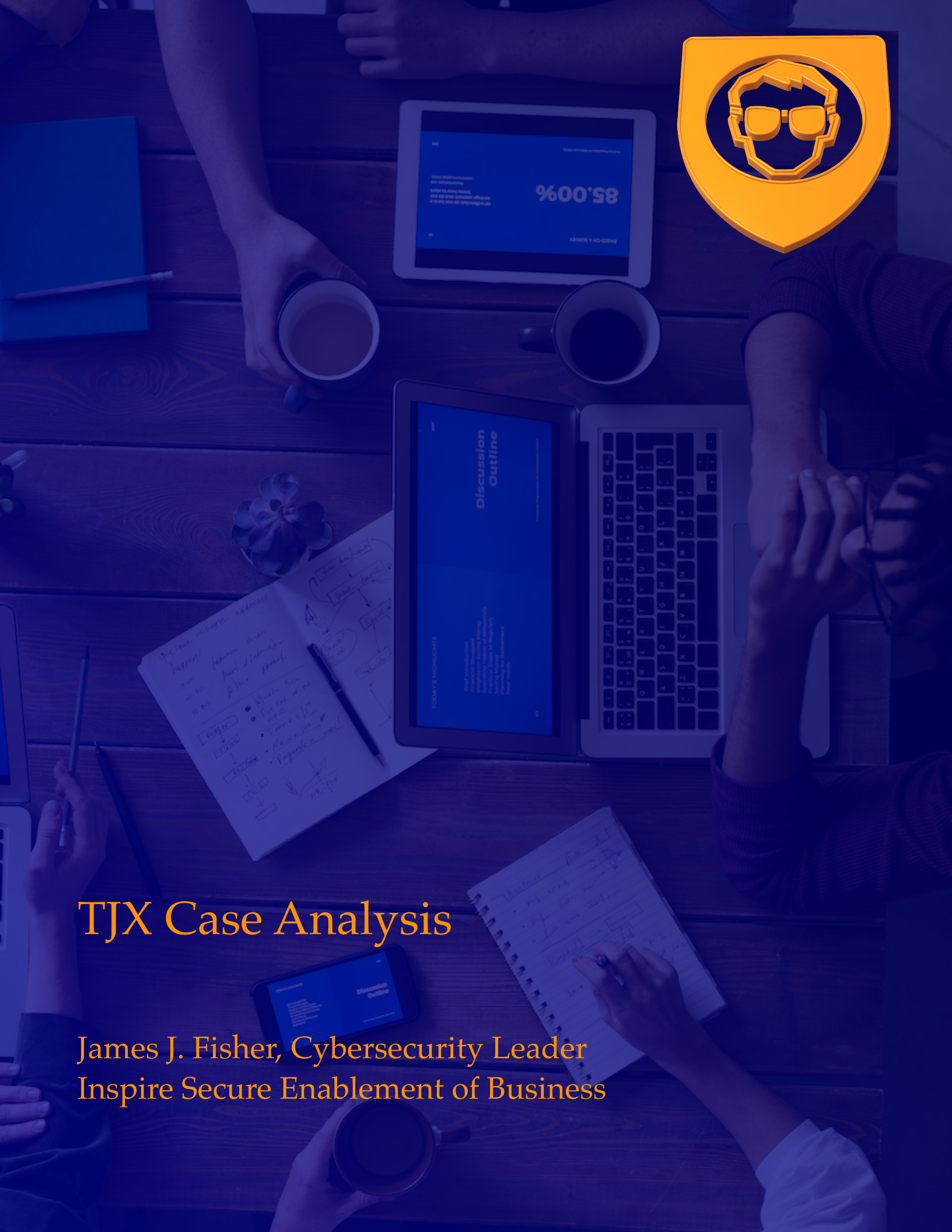

TJX Case Analysis

James J. Fisher, Cybersecurity Leader
Inspire Secure Enablement of Business

Abstract

This paper is an evaluation of the TJX Companies, Inc. breach as publicly notified on February 21, 2007. The evaluation will include an analysis of the failure points in leadership, management, and user adoption. The analysis will encompass issues related to managing, governing, and funding cybersecurity, including policy development and access control. Part of the breach was a breakdown in processes, including compliance and audit practices, as well as failures in the deployment of technology.

Keywords: information security, hacking, breach, poor governance, mismanagement of technology, audit practices, compliance practices, user community, cybersecurity budgeting

Note: This is not a peer-reviewed research paper. Do not use as a primary or secondary source within a thesis, dissertation, or research paper. If a reasonable perspective for research is found and a viable research perspective is being considered, please reach out to the author: jjfisher@jamesjfisher.org.
Updated: July 3, 2025

Introduction

The TJX Companies, Inc. (TJX) suffered a significant cybersecurity breach of its retail operations. The company operates T.J. Maxx, Marshalls, HomeGoods, A.J. Wright, and Bob's stores in the United States, Winners and HomeSense in Canada, and T.K. Maxx in Europe, with 2,400 stores and 125,000 associates at the time of their widely publicized cybersecurity breach (Chandrasekhar, 2008). As a Fortune 500 company headquartered in Framingham, Massachusetts, they are considered a discount retailer positioned between unbranded discount stores and department stores, offering full retail pricing (Chandrasekhar, 2008). For TJX, operational efficiency and the relationships with their vendors at scale are a critical part of their business model (Chandrasekhar, 2008). In this segment of retail stores, information quality is crucial in maintaining tight margins and ensuring the entire value chain is connected (Chandrasekhar, 2008). This paper will review the TJX breach, providing a focused discussion on management failure, governance, cybersecurity, and various weaknesses that contributed to the breach.

Background

On December 18, 2006, TJX learned they were hacked by finding suspicious software, altered files, and data integrity issues as their first suspicions of a compromise (Chandrasekhar, 2008). The compromise included segments of their network that processed credit cards, debit cards, checks, and merchandise returns, affecting all eight company brands in the United States, Puerto Rico, Canada, the United Kingdom, and Ireland (Chandrasekhar, 2008). Doing what was smart, TJX called in General Dynamics Corporation and IBM, and they confirmed the compromise and breach on December 21, 2006, and the compromise was still active (Chandrasekhar, 2008).

During the planning and containment phases of the incident response, the Secret Service was notified, which presented TJX with the option not to make a formal notification that would impede the investigation (Chandrasekhar, 2008). Under advisement of the Secret Service, TJX notified contracting banks, credit card companies, debit card companies, and check processing companies (Chandrasekhar, 2008). It wasn't until February 21, 2007, that TJX made its public breach announcement, concerning the timing, scope, and other details, including the fact that the breach had been occurring periodically since July 2005, right up to January 2007 (Chandrasekhar, 2008).

TJX noted that no customer data was stolen, at least no personally identifiable information (PII), despite maintaining and storing significant amounts of PII within its merchandise return system (Chandrasekhar, 2008). Part of the disclosure included deleting records and retaining them for extended periods, and the data may have been stolen during credit card approval processes (Chandrasekhar, 2008). Unfortunately, at this juncture, TJX was unable to precisely identify the stolen data and its quantity (Berg, Friedman, & Schneider, 2008; Chandrasekhar, 2008). TJX was storing large amounts of PII on their systems in the US and Europe with a stated practice of encrypting the data (Chandrasekhar, 2008).

The investigation by the Secret Service eventually revealed a fraud ring operating through Eastern European residents that was passing the breached data back to a group in Florida (Chandrasekhar, 2008). The group was operating a well-known type of plain card-style fraud against credit cards and bank accounts linked to debit cards, deriving value from the hacks they perpetrated (Chandrasekhar, 2008). This included purchasing store gift cards with the stolen credit and debit cards to maximize the value of those cards before they were terminated (Chandrasekhar, 2008). The attack perpetrated against TJX was fairly significant in that it used multiple attack vectors to achieve its goal.

Management and Governance in the Breach

Before the 2005 breach, top-level management at TJX had undergone changes, driven by the model for discount retailers, and refocused on profitability through sales growth (Chandrasekhar, 2008). This new focus had produced financial results by January 2007, even

though margins were low, net income as a percentage of sales had increased (Chandrasekhar, 2008). The inference is that executive leadership prioritized profitability over the cybersecurity of their mission-critical systems. This is made more evident by the absence of an executive manager overseeing the organization's cybersecurity.

It was not until after the breach there was a focus on cybersecurity and a cybersecurity head. Post breach, TJX hired a Chief Security Officer (CSO) who was a former Chief Information Officer (CIO) at a smaller Canadian retailer (Chandrasekhar, 2008). According to the literature, TJX executive management downplayed the scope and size of the breach during the hiring process (Chandrasekhar, 2008). Additionally, the new CSO was informed that the position had been newly created specifically for the former CIO (Chandrasekhar, 2008). It can be inferred that, even while the breach was unfolding, executive management did not understand or take the matter as seriously as needed and were taking measures to shift the responsibility to someone else. There were also issues with the then-CIO, Paul Butka, who was not supporting the continued conversation; TJX was not prioritizing the security of mission-critical systems.

The CIO of TJX had numerous options to address cybersecurity issues, but he chose to focus his attention elsewhere. During this time, Wired Equivalent Privacy (WEP) was known to be vulnerable, and the CIO opted for a conservative approach to cybersecurity investments (Xu, Grant, Nguyen, & Dai, 2008). He was aware of TJX's current sales growth, the risks involved in maintaining WEP, and knew that he could maintain PCI-DSS compliance with WEP. Additionally, he had been separately forewarned by staff about the issues (Xu et al., 2008). Wi-Fi Protected Access (WPA) was emerging as part of the IEEE 802.11i protocol specification and was widely adopted for wireless communications to replace the older WEP protocol. In his emails, the CIO believed the risk was small or negligible, and the money allocated for the upgrades towards WPA could be redirected to other priorities, as WEP was still compliant with PCI-DSS (Xu et al., 2008). It was a significant governance failure and a failure to heed staff concerns. The breach then caused a reactive decision by executive management to force the IT organization to immediately begin upgrading the wireless security infrastructure and expending the money earmarked to be saved by the CIO (Xu et al., 2008).

User Community

The article by Chandrasekhar (2008) does not explicitly discuss the user community of TJX. When reviewing the overall conversation and discussion, the user community as a whole is not addressed as a concern, considering the 125,000 associates who worked for TJX at the time of the breach. The same is true of the article by Berg et al. (2008). Likewise, Xu et al. (2008) do not provide detailed information about the overall user community, but rather note that specific senior IT personnel voiced concerns about the continued use of WEP within wireless systems. System tampering is mentioned by Chandrasekhar (2008), which has implications across the user community.

One of the main areas that Chandrasekhar (2008) discusses is the USB exploit of kiosk systems. For early versions of the PCI-DSS, mandating cybersecurity awareness was always a requirement. What was not present in the requirements was training staff on how to check systems for tampering. Berg et al. (2008), Chandrasekhar (2008), and Xu et al. (2008) did not discuss whether a strong cybersecurity awareness program was in place or if it was even compliant with the PCI-DSS. This leaves lingering questions. Were TJX personnel provided cybersecurity awareness training? If not, then how did they continue to recertify each year? How were TJX associates supposed to know what to look for concerning fraud and system tampering? Were personnel trained in incident response, and would they even know who to contact if something suspicious was noticed? Anecdotally, the author of this paper found no relevant material to analyze across multiple articles and journals that could provide answers to these questions. Granted, Chandrasekhar (2008) noted that executive management brought the Secret Service in; however, this does not mean the overall user community is aware of what to do in these situations, how to recognize suspicious activities, or what their responsibilities are.

Process Weaknesses Impacting Security

TJX had some material weaknesses within its processes that impacted the cybersecurity of its systems. This included their cybersecurity, governance, and audit practices. As an organization that followed the Payment Card Industry-Data Security Standard (PCI-DSS) and was recertified multiple times during that period, it can be challenging to understand why this incident occurred. Chandrasekhar (2008) notes that the PCI-DSS is a strong cybersecurity blueprint for retailers; however, this is not entirely accurate. Upon reviewing the PCI-DSS during that period, many of the requirements could have been met; however, the organization would still not have been secure. This is partly due to the PCI-DSS's narrow focus on only credit cards. It does not cover debit cards, checks, or PII, and is also only contractually obligated. Likewise, card processors like First Data and Chase Payment Tech are not required to be PCI-DSS compliant.

Many of the authors referenced refer to PCI-DSS Qualified Security Assessors (QSAs) as auditors; however, they are not auditors, but rather assessors, and the PCI-DSS assessment is not an audit. Berg et al. (2008) compares Statement on Auditing Standard (SAS) 109 requirements to auditing an organization which fails to realize a PCI-DSS assessment is not an audit and the assessment doesn't audit the "books" but assesses the organization to PCI-DSS requirements and does not include debit cards and checks within the assessment even if internal accounting controls under the AICPA do. The PCI-DSS is not a financial audit and is not treated as one, nor does it assess or audit backend accounting practices as AICPA controls would. The Sarbanes-Oxley Act (SOX) controls related to the AICPA should have had a greater impact on the cybersecurity of TJX systems, particularly in maintaining information.

Chandrasekhar (2008) notes deficiencies in not purging data, as some of the stolen data was five years old, dating back to 2002. The bigger problem here is that TJX is a publicly held organization, so SOX compliance takes precedence over PCI-DSS compliance. By law, then, some information must be maintained for at least seven years. Under the PCI-DSS, there is no specific period specified for data removal as a requirement, except that organizations must maintain a data retention policy that includes the purging of data; however, the timeframe is left to the organization's discretion (PCI Security Standards Council, 2008). Chandrasekhar (2008) does not specify in his article what that policy or procedure is, so it is speculative whether it was ineffective or not, regardless of a breach, when considering other factors, such as missing details. For instance, if disk encryption was used to secure relevant information that had to be maintained for seven years under SOX compliance, keeping data that is five years old in that encrypted space meets both sets of compliance rules, even though disk encryption is a weak control and would not need to be purged for another two years.

Technology's Role in the Breach

In the article by Berg, Friedman, and Schneider (2008), it was suggested that three significant areas of vulnerability were present at TJX with inadequate wireless network security, improper storage of customer data, and failure to encrypt customer data. This was echoed by Chandrasekhar (2008), who noted that handheld systems and potentially point-of-sale systems were using WEP on their wireless systems. WEP is notoriously easy to crack, and many cybersecurity professionals are aware of this, as noted by Berg et al. (2008), Chandrasekhar (2008), and Xu et al. (2008).

Although both Berg et al. (2008) and Chandrasekhar (2008) criticize TJX for using WEP in their wireless systems, it was technically permissible under the PCI-DSS. The PCI Security Standards Council (2008) under Requirement 4.1.1 of the PCI-DSS version 1.2.1 clearly states that new implementations of WEP were prohibited after March 31, 2009, and in-place installations of wireless had until June 30, 2010, to migrate to the newer standards under IEEE 802.11i. Although TJX should have tried to move towards a more secure wireless environment, there was no clear impetus under the PCI-DSS to do so between 2005 and 2007, considering it wasn't until the 2008 standards removal was noted and use extended into 2010, if not a new implementation (PCI Security Standards Council, 2008). Encryption in transit is not the only encryption issue presented.

Encryption of data at rest is another area of concern. Chandrasekhar (2008) does not delve into relevant specifics, such as the algorithms TJX was utilizing or across which systems, other than those supposedly related to terminals and merchandise returns. Berg et al. (2008) suggest in their article that nothing was encrypted or the encryption keys were stolen. Chandrasekhar (2008) does mention the compromise could have included access to the encryption keys and the tools for decrypting data. Berg et al. (2008) make a significant leap in suggesting that encryption is a be-all and end-all method to keep people out of data. This isn't entirely true, and the scope of encryption within the PCI-DSS at the time of the breach may have included the use of disk encryption rather than file or column-level encryption. According to PCI-DSS version 1.2.1 requirement 3.4.1, it is acceptable to use disk encryption if it is not directly tied to the operating system (PCI Security Standards Council, 2008). This creates an odd situation in that logical access to the data is then decrypted for anyone with logical access permissions, without needing any keys; however, if you pulled the disk drives out, walked off with them, and tried to read the data later, it would be unintelligible, and keys would be required. Chandrasekhar (2008) notes that usernames and passwords of associates were pilfered during the wireless attacks, which suggests the intruders didn't need access to encryption keys if disk encryption was being used over either file or column-level encryption. Even if improper storage were not present, this would still be a problem because the control itself remains weak.

Berg et al. (2008) note that improper storage was a significant issue within the TJX breach. Chandrasekhar (2008) indirectly mentions TJX maintaining PINs for cards and complete track data, as does Berg et al. (2008). If true, this would be a significant failure on TJX's part, as the entire portion of requirement three of the PCI-DSS is dedicated to ensuring that retailers do not store the whole track or any portions of the track of the magnetic stripe, even if encrypted (PCI Security Standards Council, 2008). Likewise, it is a significant failure of the QSA and PCI-DSS assessment company for not finding it and having the IT organization remediate immediately (Chandrasekhar, 2008). More issues arise that Chandrasekhar (2008) notes, but Berg et al. (2008) do not, such as problems with kiosks, firewalls, and log files.

TJX had kiosks during the breach where USB drives were plugged into those systems, allowing the intruders to turn them into remote terminal systems (Chandrasekhar, 2008). Additionally, Chandrasekhar (2008) notes that the firewalls were not configured to defend against traffic from those remote terminals. Chandrasekhar (2008) does not understand how firewalls work, and the kiosks would be allowed to communicate based on firewall rules because they are supposed to. They can't defend against attacks or anomalous behavior because that is not what firewalls are designed to do. Likewise, why didn't the IT organization lock down USB ports in a consistent manner across all their kiosks, since physical port hardening and securing access to the BIOS of certain types of systems is a fundamental cybersecurity principle? There are tools available that have been in place before the breach, which would have locked the ports down and monitored activity on them. Of course, maintaining logs would have been helpful as well.

Maintaining logs is a practice within the PCI-DSS that comes with some caveats. Although TJX reported 46 million and the banks reported 94 million, this discrepancy suggests that TJX was unaware of the full extent of the problem (Chandrasekhar, 2008). This can be explained as or be suggestive of a poor log management process. Granted, logs provide a wealth of information for forensic analysis; however, PCI-DSS requirements focus on three months of online data with at least a year archived (PCI Security Standards Council, 2008). The standard essentially states that organizations are not obligated to retain their logs for more than a year, and this is a compliant practice, even if it is not a best practice.

Conclusion

When looking back and from the outside, it is easy to see failures. It is much harder to see them when you're inside, working and trying to make sound decisions for the benefit of the organization. There is no doubt the IT organization failed TJX, but so did executive management. Within this paper, it is recommended that TJX should have done these potential items:

- Maintain a governance program to control IT and Cybersecurity investments, ensuring forward innovation that reduces risk.
- Separate IT and cybersecurity into separate organizations to avoid conflicts of interest and ensure that IT does not prioritize less critical tasks over cybersecurity.
- Train personnel, train IT personnel, and train executives in cybersecurity-related topics, common credit card scams, terminal tampering, and system tampering, in addition to annual cybersecurity awareness training.
- Understand and realize that compliance with PCI-DSS does not make a company secure.
- Reduce information collected, stored, and retained to only that which is vital for business function, and encrypt at the file or column level using a hardware security module that can securely store encryption keys.
- Ensure that all systems do not capture or retain the full magnetic stripe contents of all card types, reducing information to the absolute bare minimum needed to approve, authorize, and track a card transaction.

The key point that applies to all organizations, not just TJX, is the recommendation of segmentation and isolation. The PCI-DSS explicitly states that organizations should segment and isolate their cardholder data environment or CDE (PCI Security Standards Council, 2008). While it is not a mandatory requirement, it is a principle that holds true. Segmented and isolated environments within a defense-in-depth strategy greatly enhance the difficulty for intruders to penetrate deeply into organizations, giving cybersecurity operations more time to detect and respond to threats.

References

Chandrasekhar, R. (2008). Security breach at TJX. London, Ontario: Richard Ivey School of Business.

Berg, G. G., Freeman, M. S., & Schneider, K. N. (2008). Analyzing the TJ Maxx data security fiasco: Lessons for auditors. *The CPA Journal, 78*(8), 34-37.

PCI Security Standards Council (2008). *PCI DSS requirements and security assessment procedures* (ver. 1.2.1). PCI Security Standards Council. Retrieved from https://www.pcisecuritystandards.org/document_library

Xu, W., Grant, G., Nguyen, H., & Dai, X. (2008). Security breach: The case of TJX Companies, Inc. *Communications of the Associate of Information Systems, 23*(31), 575-590.

As a cybersecurity leader, author, and researcher, James is passionate about developing and delivering effective programs. He focuses on assessing and understanding current maturity levels and capabilities and then creating short- and long-term strategies, goals, budgets, metrics, and roadmaps to progress toward higher maturity. The emphasis is on aligning the cybersecurity strategy with the business and technology strategy and integrating it with portfolio, program, and project management.

Background

James is a cybersecurity professional who started in information technology in 1995 and moved into cybersecurity in 2005. James has worked with or within many different industry sectors, including healthcare, FinTech, marketing, skilled trade unions, business process outsourcing, high-end retail, publishing, and manufacturing. Additionally, James has worked with DoD/Fed prime and subcontractors. He was even a paperboy.

Education

James received a Master of Science in Information Assurance and Security in April 2016 (from Capella University), a double major Bachelor of Science in Management and IT Management in March of 2006 (from Kaplan University), a vocational diploma as a Networking and Systems Support Specialist in June of 2000 (from Ridley-Lowell Business and Technical Institute) and a Certificate in the Essentials of Government Contract Management in August of 2013 (from Villanova University). And he cannot say he is done yet because of his philosophy and passion for lifelong learning.