RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
MARCH 2021

DOI: 10.5281/zenodo.4639612

The Second Round of Information Security Challenges at TJX Companies

Courtney Gatlin-Keener, MBA[1], Ryan Lunsford, PhD[2]

[1]DBA Student, University of the Incarnate Word, USA, cgatlin@student.uiwtx.edu
[2]Professor and DBA Chairman, University of the Incarnate Word, USA, lunsford@uiwtx.edu

ABSTRACT: This descriptive case study summarizes TJX Companies (TJX), highlighting the considerable success its off-price retailing business has experienced in the United States and abroad. TJX traces its roots to small-town Massachusetts as far back as the early 20th century through its precursor company, Zayre Corporation. With over 4,500 stores globally, TJX is renowned as a dominant off-price retail business giant, positioned in the top 300 in the Fortune Global 500 annual rankings of the world's largest companies with over $40B in sales and a market value of over $62B. TJX's resilience and sustainability result from its sophisticated value proposition comprised of its business model flexibility and opportunistic purchasing. Despite their financial performance, business niche dominance, and growth and expansion prospects, an unexpected ethical dilemma was recently uncovered. Based on UpGuard's third-party report, it was discovered that despite the purported recovery from a 2007 TJX data breach debacle and supposed enhancements in its digital infrastructure, there are still significant issues related to TJX's network security. It appears as though TJX, despite having a previous opportunity to reconcile, is still, even today, unable to provide adequate customer data protection. Thus, it is recommended that TJX configures its Domain Name System Security Extensions (DNSSEC) and bolster the security of its digital transactions by implementing point-to-point encryption (P2PE) and tokenization, payment card industry (PCI) validated P2PE solutions from its store chains to the banks and PCI-compliant firewalls. Additionally, they should revise their current business model to integrate consumer information protection into its key activities and include a reliable and secure digital infrastructure as a critical resource for the business. This case study will identify best-practices that organizational leaders in a number of industries might adopt and apply within their companies to benefit from the many lessons learned after studying TJX's many challenges and successes.

KEYWORDS: TJX Companies, data breach, information security, TJ Maxx, Marshalls, HomeGoods

Introduction

A carefully-deliberated, strategic business model is a crucial success factor for any organization; however, an especially innovatively-designed model may lead to additional business sustainability (Wirtz 2011; Bocken, Short, Rana & Evans 2014). The TJX Companies (TJX) have uniquely captured the essence of the model, enabling it to make its way into the top 300 of Fortune Magazine's Global 500 companies of 2020. The TJX corporate profile at Fortune (2020) Global 500 pictures the group of companies as consistently dominant over the years as an off-price discount retailer of fashion and home goods, with 2019 sales reaching $41.7 billion. Fortune (2020) Global 500 deems the previous year's performance of TJX to be bigger than comparable retail brands, Macy's and J. C. Penney, combined. As 2020 came to a close, there were practically no remaining ghosts of the past that haunted TJX in the notorious 2007 consumer security data breach, which led to a class-action suit on behalf of its American consumers and a settlement costing TJX over $200M in 2008, among others (Berger-Montague 2018). It was not, however, an easy recovery for TJX. Nevertheless, equipped with an innovative business model, a well-planned business trajectory, and able leadership, the TJX group of companies coasted along a bumpy market ride in the aftermath of the information security breach to increase its sales by 7% in 2019 (Fortune 2020). Surprisingly, even with what was regarded as one of the three most prominent data breaches on record in the US, which resulted in the exposure of 94 million consumer credit card details, the TJX stock prices did not plummet for more than a day (Khrisna 2019; Hovav & Gray n.d.; Yahoo Finance 2021a). This

case study examines the salient details leading to the current success of TJX, despite its infamous credit card data debacle in 2007, and concludes with an analysis of how the company can continue its incredible off-price deals and the planned trajectory for growth and expansion while ensuring the privacy and security of consumer data.

Background of TJX Companies

TJX officially began as TJ Maxx in 1977; however, its roots may be traced back further to two Feldberg brothers, Max and Morris, when they established Zayre Corporation in Framingham, Massachusetts, as an apparel wholesale firm in 1919 (Laulajainen 2012; TJX 2021a). After a decade of operations, the wholesaling business was steadily declining so, in 1929, the brothers ventured into a chain of retail stores specializing in women's apparel (Laulajainen 2012). They capitalized on several innovative decisions through the post-World War II era when the population migrated to the suburbs in large numbers. The brothers identified early on that the traditional department store that catered to suburban America's needs was quickly sifting away from geographically downtown locations and resolved to shift their strategic business model to one of discounting (Laulajainen 2012).

The discount strategy proved successful, and Zayre Corporation earned fame for its discount operations throughout the eastern United States. By the early 1960s, apparel stores flourished north of the Buffalo-New Haven Connecticut line, as discount stores began to spatially disperse as far as Boston, Chicago, Miami, and Washington, DC (Laulajainen 2012). In 1976, Zayre Corporation, in another innovative decision, recruited the Marshalls' general merchandising manager, Bernard Cammarata, to launch a new chain of stores, with the off-price retailing format for family apparel and home goods. Thus, TJ Maxx was born, and the initial chain of stores opened in 1977 (TJX 2021a).

By the late 1980s, the Zayre Corporation was restructured into the TJX Companies with its initial three brands, TJ Maxx, Hit or Miss, and Chadwick's of Boston (TJX 2021a). In 1990, TJX acquired Winners Apparel of Canada, followed by the introduction of HomeGoods two years later. In 1994, TJX introduced off-price retailing to the UK and Ireland via TK Maxx as Europe's lone major off-price apparel and home fashions retailer. In 1995, TJX acquired Marshalls and sold Hit or Miss. In 1996, Brylane purchased Chadwick's of Boston (TJX 2021a; Wall Street Journal 1996). In the new millennium, TJX introduced off-price home fashions in Canada via HomeSense (TJX 2021a).

Leadership has undoubtedly been a key factor for the longstanding success of TJX and its dominance in the off-price retailing sector. As off-price discounters, TJX struck a mine of opportunities to dominate their niche of major brands at significantly lower prices with the able guidance of the most competent leaders of their own time: Bernard Cammarata, Carol Meyrowitz, and Ernest Herrmann (Davidson 2009; Parker 2020; Sarkar 2017). Founders Max and Morris Feldberg possessed an eye for promising talent, having invited then Marshall's general merchandising manager, Ben Cammarata, to lead Zayre's restructuring as off-price discount retailers, TJX Companies (Sarkar 2017).

Carol Meyrowitz was CEO of TJX during its most challenging time in 2007 when the globally dominant off-price discount chain was rocked by a humongous credit card security breach crisis (Davidson 2009). Her promotion as CEO was providential because her leadership steered the company back to its value-driven business trajectory after surviving the data breach debacle and the global economic downturn combined, which was TJX's most tempestuous disturbance in its over 40-years of history (Davidson 2009). She turned in higher sales records, higher share prices, and expanded the TJX chains' presence in areas where consumers manifested heightened interest in low-priced options.

The current CEO, Ernest Herrmann, rose from the ranks as a former purchaser of merchandise and took over from Meyrowitz in 2016 with a keen focus on enhancing the chain's

physical market presence (Parker 2020). Herrmann applies a positivist approach when examining the business environment by visualizing threats as new opportunities. He acquired considerable experience in sourcing/purchasing TJX inventory and is not a reckless and impulsive buyer. Instead, Herrmann's inventory replenishment approach calls for moderation not to purchase considerable volumes in shorter periods (Parker 2020).

TJX suffered a credit card security data breach perpetrated by unscrupulous hackers who cracked Marshalls' web equivalent privacy (WEP) security code in 2006 (Xu et al. 2008). Despite the credit card security fiasco, depleted financial resources due to costs associated with the data breach, and significant decline in sales, TJX weathered the storm of the 2007 security mess. Currently, TJX has 3,290 stores in the US, 513 stores in Canada, 672 stores in Europe, and 54 stores in Australia (TJX Companies 2019).

TJX Companies' Best Practices

Business model flexibility. TJX's flexible business model is perhaps, its chief sustainable competitive differentiator (Lewis & Dart 2014). As TJX has grown to over 4,500 stores globally, they have successfully leveraged more than 1,100 associates in their product buying offices that have developed a vendor network of more than 21,000 suppliers (TJX Companies 2019). The benefit to TJX is that they can reliably replenish their stores with fresh and exciting brand-recognized merchandise of high quality. TJX buyers operate year-round to secure market opportunities as they nimbly adjust to ever-changing consumer preferences. TJX buyers consider a variety of non-traditional purchasing opportunities, including less-than-full assortments of items, styles, and sizes in varying quantities (TJX Companies 2019).

When Zayre restructured to become TJX, its goal was to retain its discount retail business model with a twist by concentrating on the off-price retail model. As explained in Baird et al. (2020), off-price stores are one of the variations of discount stores with moderate width and shallow depth of merchandize assortment, appropriately called specialty stores, selling merchandise of average or good quality at low prices and lower continuity (Baird, Meyer & Green, 2020; Michmann & Mazze 2001). TJX, as an off-price discount retailer, purchases its products from major brand manufacturers' canceled orders, closeouts, irregulars, overruns, return orders, and seconds. It also makes purchases from other retailers' closeout merchandise and end-of-season sales. While some off-price retailers develop a reputation of selling damaged items and previous years' styles, TJX offers top-quality and in-season product offerings up to 60% less than traditional department store retailers (Donellan 2014).

Opportunistic purchasing. TJX uses the term opportunistic buying to describe its purchasing strategy and tactics, which sustainably differentiates them from traditional retailers (TJX Companies 2019). Their overall buying strategy supports their efforts in the delivery of their value proposition. The key features of TJX's opportunistic buying strategy include: 1) a frequently refreshed mix of branded, designer, and other quality products at prices generally lower than traditional retail stores, 2) year-round merchandise procurement from 100 countries facilitated by 1,100 buying associates located in 12 countries across four continents, and 3) the purchase of substantially discounted merchandise through closeouts from brand manufacturers and other retailers, manufacturer overruns, order cancellations, and unique products from brands and factories. To ensure that benefit from these features is maximized, buying associates continuously look for exciting goods throughout the year to stock inventory for either the current or an upcoming season. When opportunities present, some merchandise may also be purchased as future stocks, referred to as packaway, for goods perceived to possess TJX's ideal combination of brand, fashion, price, and quality. TJX also seeks to acquire private labels or TJX-licensed brands developed by the corporation when viable (TJX Companies 2019).

Pricing. TJX offers excellent value to consumers through "quality, fashionable, brand name, and designer merchandise" at retail prices ranging from 20% to 60% below retail price of

department stores, specialty shops, and major online retailers, courtesy of its excellent opportunistic buying strategy (TJX Companies 2019). Being an everyday sale day at TJX store chains, there is practically no need to designate a sale/super sale day or engage in promotional coupons to increase sales. TJX can also flexibly adjust its prices in response to economic cycle fluctuations to strategically maintain its pricing difference relative to traditional retailers (TJX Companies 2019).

Inventory management and distribution. To permit the creation of a treasure hunt experience among consumers in TJX stores, the company frequently refreshes their merchandise to motivate consumer interest in frequent visits for the best off-price deals of designer apparel and other popular brands. Using state-of-the-art information technology (IT) system for inventory management and distribution, TJX regularly offers new and fresh off-price selections of apparel and home fashion items. TJX applies creative IT solutions in planning, purchasing, monitoring, pricing markdown, distribution center storage, processing, handling, and shipping of specialized inventory items custom-tailored to the local preferences and demographics. Inventory turnover in TJX store chains is rapid and usually sells on computer-estimated time to generate automatic replenishment schedules in organized and timely schedules. To achieve this synergy of operations, TJX invests in its supply chain with the triune purpose of continuous operations at low inventory levels, automated deliveries, and merchandise allocation to thousands of TJX stores precisely and efficiently (TJX Companies, 2019).

Dilemma

TJX's five-year cumulative stock performance compares favorably to the S&P 500 and Dow Jones apparel retailer indices (TJX Companies 2019, "TJX Stock Performance"), and its potential for growth and expansion appears promising. However, TJX has identified potential challenges in its statements of significant risks (TJX Companies, 2019). While most of the risks acknowledged in the 10-K SEC filing are relatively normal operational issues that most corporations face, there is one specific risk that poses an ethical dilemma to the business. The risk is stated as "compromises of our data security, disruptions in our information technology systems, or failure to satisfy the information technology needs of our business could result in material loss or liability, materially impact our operating results or materially harm our reputation" (TJX Companies 2019).

TJX is wise to account for possible attempts by unscrupulous entities to access personal or sensitive information fraudulently or steal money by breaching the company's data security system through one or more of a range of manipulative actions that can compromise the privacy and confidentiality of consumer data, including account takeovers, digital and physical skimmers, denial-of-service attacks, employee malfeasance, exploitation of system vulnerabilities, malware, phishing, ransomware, or social engineering (TJX Companies 2019). However, the 117-page global corporate responsibility report did not address how the corporation secures and protects consumer data privacy (TJX Companies 2020b). To be clear, this case study does not say that TJX is negligent in securing and safeguarding its clientele base's data privacy. Rather, if any consumer data security and protection measures are in place, such measures were not included in the report.

TJX's website expressly states in its Privacy Notice how it protects consumer information. Nevertheless, two paragraphs of basic data security information and a disclaimer of corporate liability for alteration, destruction, disclosure, loss, misuse, or unauthorized access of consumer information is not "data security" and "protection measures."

Discussion and Analysis of the Data Protection Issue

2007 Credit Card Data Breach. For two days in 2005, hackers outside Marshalls in St. Paul, Minnesota aimed what was described in Xu et al. (2008) and confirmed in Schneider (2009) as

a "telescope-shaped antenna" to the direction of Marshalls to fraudulently intercept the store's wireless transactions broadcasted via the wireless network. By listening to the transactions through the networks, the hackers cracked Marshalls' wired equivalent privacy (WEP) network security code. They illegally accessed consumers' credit card and bank account information, and in the process, stole 45.7 million transactions recorded in the centralized corporate database. The hackers compromised sensitive corporate information and the privacy and security of about half a million consumers. TJX did not immediately publicly disclose the data breach but did report the violation to authorities. The corporation's public relations executive announced the data security breach in January of 2007 (Xu et al. 2008; Schneider 2009).

TJX had some foreknowledge of their potentially insufficient network security technology by various IT security firms (Xu et al., 2008). At least one IT security firm, Newbury Networks, made efforts to discuss IT security-related issues, but TJX declined their offer. At the time of the hacker intrusion into the TJX network system, the WEP security standard was in-place throughout the stores' chain. The release of the first Payment Card Industry Data Security Standard (PCI DSS 2017) occurred in 2004 to motivate credit card companies to practice due diligence in processing credit card payments. The standard was also issued to facilitate retailers' and consumers' protection against the risk of cracking, credit card fraud, and other threats and vulnerabilities (Xu et al. 2008).

Despite the possibility of fines for non-compliance, merchants, in general, did not readily adopt PCI DSS. Nevertheless, although Visa permitted TJX to operate provided that it would continue to enhance its data security and protection, TJX decided to delay compliance (Xu et al., 2008). Duvall (2007) is adamant that the data breach could have been avoided if TJX had collected less information from consumers and stored the information securely. The investigation into the TJX data breach found that 1) there was a failure on the part of TJX to manage the intrusion risk vis-a-vis the amount of unnecessary data it collected and stored longer than necessary, 2) TJX was too slow in securing their weak encryption standard in use into a more substantial encryption standard (the time-lapse was required for the hackers to feast on TJX's extensive collection of unnecessary information, such as driver license numbers, 3) TJX failed to adopt an adequate intrusion monitoring system, and 4) TJX did not comply with the PCI DSS requirement (Xu et al. 2008; Duvall 2007).

How TJX Protects Consumer Data Security 2021: A Third-Party Report. According to the third-party security report on risk and attack surface management platform by UpGuard on January 11, 2021, TJX received a "B" rating, which indicates a 2.6 times more likely probability of data security breach than an A-rated company (Gurman, 2020). Strengths of TJX's website security provided by UpGuard (2021) are its secure sockets layer (SSL), traffic via the hypertext transfer protocol secure (HTTPS), and its non-vulnerability to FREAK, Logjam, Heartbleed, Poodle, and CVE-2015-1635 or IIS HTTP.sys Remote Code Execution. There is support for SSL, a strong SSL algorithm, a valid SSL certificate that does expire within 20 days, matching hostname and SSL certificate and the SSL certificate is not in the revoked certificates list. However, several weaknesses were observed in the website, such as insecure SSL/transport layer security (TLS); exposure of its X-Powered-By, ASP.NET, and ASP.NET version headers.

UpGuard (2021) also provided strengths of TJX's email security, which are: its enabled Sender Policy Framework (SFP) with correct syntax, strict filtering, and non-use of ptr mechanism; use of the email authentication policy and reporting protocol, Domain-based Message Authentication, Reporting & Conformance (DMARC). However, its DMARC policy is set to p=none, where the domain owner requests no specific action to be made on emails that fail the authentication protocol, a weakness in email security. In terms of network security, two observations were made: first, there were no open ports, which is a security strength, but the Domain Name System Security Extensions (DNSSEC) is not enabled, which is a weakness (UpGuard 2021).

Implications of TJX's Data Security Stance

With the information available, it may be concluded that there was a little improvement in the data security approach of TJX between 2007 and 2021. For a company that had already experienced a data breach first hand and paid a considerable settlement amount on the damages inflicted by their lapse in security, it appears that TJX may not realize the ethical ramifications. Technically, DNSSEC is a set of specifications that extends the DNS protocol by adding cryptographic encryption for responses emanating from authoritative DNS servers. Functionally, DNSSEC protects the network from unscrupulous hackers' manipulation to control target computers to fraudulent websites (Constantin 2020). Sadly, for TJX, their network is still NOT adequately protected against hackers and intrusion because their DNSSEC is NOT enabled. This means that "an attacker can redirect a user to a potentially malicious site without the user realizing it" (Internet Corporation for Assigned Names and Numbers 2019).

It appears as though TJX did not learn its lesson on the importance of network security to protect consumer data, or perhaps, that it does not take consumer data protection seriously since the 2007 data breach.

Conclusions and Recommendations

The prospects for TJX's continued success appear to be optimistic from several perspectives. Their business model flexibility and opportunistic purchasing have them well-positioned to demonstrate reliable financial performance and strong prospects for continued expansion. Its best practices in opportunistic buying, pricing, and inventory management and distribution coupled with experienced and dedicated personnel, many of whom were home-grown talents trained and groomed for future leadership, are critical for sustained performance.

However, of continued concern is how TJX leadership positioned the company to be vulnerable to data compromises. Unscrupulous cyberworld entities are often as knowledgeable or more than honest technology experts. With appropriate and updated standards and preventive policies to deter data breaches now in place by authoritative bodies, Culnan and Williams (2009) suggest that "organizations have a moral responsibility to these individuals [i.e., consumers] to avoid causing harm and to take reasonable precautions toward that end." Therefore, it is a moral imperative for businesses to enhance consumer data security and protection beyond mandatory compliance to standards, policies, and regulations. Instead, companies need to create "a culture of integrity that combines a concern for the law with an emphasis on managerial responsibility for the firm's organizational privacy behaviors" (Culnan & Williams 2009).

The TJX breach was possible because TJX failed to exercise reasonable procedures to protect consumer information. Specifically, the storage and transmission of sensitive data without encryption (i.e., as clear text) and the inability to deter wireless and unauthorized access to its networks due to a failure to detect access and follow up on security warnings. As revealed in the UpGuard (2021) third-party report of TJX network security, another data breach is likely because its DNSSEC is not enabled. It is recommended that TJX bolster its network security by enabling DNSSEC. As much as DNSSEC records deter unauthorized parties from forging documents that guarantee the domain identity, it is highly recommended that DNSSEC be configured in the TJX domain. To reinforce the level of protection of a well-configured DNSSEC of the TJX domain, the following actions might also be considered by TJX and other business organizations using post of sale (POS) systems, based on input from the payments platform, CardConnect (n.d.) of the Financial Services Technology. 1) Combine point-to-point encryption (P2PE) and tokenization to better protect consumer information and considerably narrow the scope and associated costs of PCI compliance, 2) implement a PCI-validated P2PE

solution from its storefronts to financial institutions, and 3) install PCI-compliant firewalls to protect sensitive data for consumers and organizations.

TJX and its stakeholders' shared interest is to improve their current business model to comprehensively protect consumer information protection (Key Activities) and add a secure digital network (Key Resources). Incorporating this imperative to protect consumer information in the TJX business model is vital for the TJX leaders and personnel to create a culture of integrity that emphasizes responsibility for information and privacy protection.

The resolution of TJX cybersecurity vulnerabilities identified in the UpGuard (2021) report is crucial. For the TJX website's security, it is recommended that the TJX main server disable versions of SSL/TLS older than 1.2 as these outdated protocols are not secure. The TJX server configuration should remove the X-Powered-By header to ensure hackers are not given easy access to TJX server's technology. Likewise, the TJX server should also be configured to support HTTP Strict Transport Security (HSTS) to protect consumers who visit the website from man-in-the-middle attacks, where hackers covertly intercept or alter digital communication between two parties (Swinhoe, 2019). Additionally, the website header which exposes ASP.NET should be reconfigured, and the header should be removed. For TJX email security, it is recommended that the DMARC policy be migrated to p=quarantine and later to p=reject, so that email messages received which fail authentication can be appropriately addressed.

TJX Companies has realized remarkable achievements since its founding in 1977, as evidenced by its 4,500 stores globally that sell more than $40B annual in the off-price retailing sector. TJX's continued success will continue to depend on its business model flexibility and opportunistic purchasing. TJX survived a 2007 data breach debacle and, after suffering an additional compromise, needs to commit to systematically safeguarding customer data. They should revise their current business model to integrate consumer information protection into its key activities and include a reliable and secure digital infrastructure as a critical resource for the business.

References

Baird, T., Meyer, E. C., & Green, W. L. 2020. "Discount stores." *Encyclopedia.com.* https://www.encyclopedia.com/social-sciences-and-law/economics-business-and-labor/businesses-and-occupations/discount-stores.

Berger-Montague. 2018, March 17. Case No. No. 1:07-cv-10162-WGY: TJX companies retail security breach litigation. https://bergermontague.com/cases/tjx-companies-retail-security-breach-litigation/.

Bocken, N., Short, S., Rana, P., & Evans, S. 2014. "A literature and practice review to develop sustainable business model archetypes." *Journal of Cleaner Production* 65: 42-56. https://doi.org/10.1016/j.jclepro.2013.11.039.

CardConnect. (n.d.). Cyber attacks: Preparing and protecting your business. https://cardconnect.com/launchpointe/payment-security/cyber-attacks.

Constantin, L. 2020, July 30. "What is DNSSEC? And how it prevents redirection to rogue websites." *CSO Online*. https://www.csoonline.com/article/3569277/dnssec-explained-why-you-might-want-to-implement-it-on-your-domain.html?page=2.

Culnan, & Williams. 2009. "How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches." *MIS Quarterly* 33(4): 673. https://doi.org/10.2307/20650322.

Davidson, A. (Ed.). 2009. 1000 CEOs: Proven strategies for success from the world's smartest executives. Penguin.

Donnellan, J. 2014. Merchandise buying and management (4th ed.). Bloomsbury.

Duvall, M. 2007, September 25. "TJX breach could have been avoided." *Baseline Magazine.* https://www.baselinemag.com/c/a/Business-Intelligence/TJX-Breach-Could-Have-Been-Avoided.

Fortune. 2020, August 8. *Global 500: TJX*. https://fortune.com/company/tjx/fortune500/.

Gurman, S. 2020, January 8. "What are cybersecurity ratings? Security Ratings & Cybersecurity Risk Management." *SecurityScorecard*. https://securityscorecard.com/blog/what-are-security-ratings.

Harkins, M. W. 2016. "Corporate social responsibility: The ethics of managing information risk." In *Managing Risk and Information Security: Protect to Enable* (pp. 129-137). Apress.

Hovav, A., & Gray, P. n.d. "Managers, do not panic: A longitudinal study of the TJX information security breach." *Research Gate.* Available at https://researchgate.net/profile/Anat_Hovav/publication /318661530_Managers_Do_Not_Panic_A_Longitudinal_Study_of_the_TJX_Information_Security_Breach.

Internet Corporation for Assigned Names and Numbers (ICANN). 2019, May 3. *DNSSEC – What is it and why is it important?* https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en.

Khrisna, M. 2019, July 30. "Equifax hack: 5 biggest credit card data breaches." *Investopedia.* https://www.investopedia.com/news/5-biggest-credit-card-data-hacks-history/.

Laulajainen, R. 2012. "Spatial strategies in retailing." Springer Science & Business Media.

Lewis, R., & Dart, M. 2014. *The new rules of retail: Competing in the world's toughest marketplace*. St. Martin's Press.

Michman, R. D., & Mazze, E. M. 2001. *Specialty retailers: Marketing triumphs and blunders*. Greenwood Publishing Group.

Parker, G. 2020, April 8. "10 things you didn't know about TJX CEO Ernie Herrman." *MoneyInc.* https://moneyinc.com/tjx-ceo-ernie-herrman/.

Payment Card Industry Data Security Standard (PCI DSS). 2017, September 5. "PCI compliance guide: Frequently asked questions." *PCI Compliance Guide.* https://www.pcicomplianceguide.org/faq/#1.

Sarkar, S. 2017. "The supply chain revolution: Innovative sourcing and logistics for a fiercely competitive world." American Management Association Communications (AMACOM).

Schneider, J. W. 2009. "Preventing data breaches: Alternative approaches to deter negligent handling of consumer data." *Boston University Journal of Science and Technology Law*, 15(2). http://www.bu.edu/jostl/files/2015/02/Schneider_WEB_152.pdf.

Swinhoe, D. 2019, February 13. "What is a man-in-the-middle attack? How MitM attacks work and how to prevent them." *CSO Online.* https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html.

TJX Companies. 2004, January 31. The TJX companies, Inc. United States Securities and Exchange Commission (SEC). https://www.sec.gov/Archives/edgar/data/109198/000095013504001661/b49914tje10vk.htm

TJX Companies. 2019. "2019 annual report." https://www.tjx.com/docs/default-source/annual-reports/tjx-2019-annual-report.pdf

TJX Companies. 2020a, February 1. The TJX Companies, Inc.: Form 10K. United States Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/109198/000010919820000004/tjx-20200201.htm

TJX Companies. 2020. Global corporate social responsibility report. https://www.tjx.com/docs/default-source/corporate-responsibility/tjx-2020-global-corporate-responsibility-report.pdf

TJX Companies. 2021b. Privacy. https://www.tjx.com/privacy

TJX. 2021a. Our history. https://www.tjx.com/company/history

UpGuard. 2021, January 13. TJX companies security report and data breaches. https://www.upguard.com/security-report/tjx

Wall Street Journal. 1996, October 22. "TJX's Chadwick's will be sold to Brylane in $223 million deal." https://www.wsj.com/articles/SB845932359560305500

Wirtz, B. W. 2011. Business model management: Design, process, instruments. Springer Nature.

Xu, W., Grant, G., Nguyen, H., & Dai, X. (2008). Security breach: The case of TJX Companies, Inc. Communications of the Association for Information Systems, 23. https://doi.org/10.17705/1cais.02331.

Yahoo Finance. 2021a, January 8. TJX Companies, Inc: Stocks. https://finance.yahoo.com/quote/TJX/.

Yahoo Finance. 2021b. TJX Companies, Inc.: Analysis. https://finance.yahoo.com/quote/TJX/analysis?p=TJX.