Cyber Safety:
A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks

Hamid Salim
Stuart Madnick

Working Paper CISL# 2014-12

September 2014

Composite Information Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks

Hamid M. Salim
MIT Sloan School of Management
and Engineering Systems Division
hamid.salim@sloan.mit.edu

Stuart E. Madnick
MIT Sloan School of Management
and Engineering Systems Division
smadnick@mit.edu

Abstract
If we are to manage security risks more effectively in today's complex and dynamic cyber environment, then a new way of thinking is needed to complement traditional approaches. According to Symantec's 2014 Internet Security Threat Report, in 2012 more than ten million identities that included real names, dates of birth, and social security were exposed by a *single* breach. In 2013 there were *eight* breaches that *each* exposed over ten million identities. These breaches were recorded despite the fact that significant resources are expended, on managing cyber security risks each year by businesses and governments. In this paper we examine why traditional approaches for managing cyber security risks are not yielding desired results, and propose a new approach for managing cyber security risks. This approach is based on a model for accident or incident analysis, used in Systems Safety field. The model is called System-Theoretic Accident Model and Processes (STAMP). It is rooted in Systems Thinking and Systems Theory. We analyzed the largest cyber-attack at the time, reported in 2007 on a major US based retailer, using STAMP to understand the effectiveness of this approach. Our analysis revealed insights both at systemic and detailed level, which generated specific recommendations. The lessons learned from this analysis can be extended to help us to address the ongoing challenges to cyber security.

1 Introduction
Cybercrime has impacted a broad cross section of our society including individuals, businesses, and governments. Increasingly our lives are tightly coupled with the internet via multiple devices because of an ever expanding cyber ecosystem[1], where more of our personal information including financial, medical, shopping behaviors, photos, and emails are stored. With cloud computing we often don't even know where our confidential information is stored or how safe and/or secure is it. The cyber environment is continuously evolving as the world continues to become more connected every day contributing to increasing complexity, which involves systems comprising of complex hardware and software. This also introduces more opportunities for hackers to exploit new vulnerabilities, and companies continue to expend resources in millions of dollars to defend themselves. This paper attempts to understand reasons contributing to limited efficacy of traditional approaches, and our research attempts to answer the question: *Is the System-Theoretic Accident Model and Processes (STAMP) methodology effective in identifying causal factors leading to a cyber-attack?*

1.1 Limitations of Traditional Methods
Existing cyber security approaches are traditional and lack innovation. Most efforts – specifically technical, are implemented with a central theme of creating a secure fence around

[1] We view the cyber environment broadly including Internet- and Web-based services as well as other computer controlled situations, such as credit card readers, process controllers, etc.

technology assets of an organization. While this approach is essential for addressing vulnerabilities rooted in technical infrastructure, it also limits systemic thinking for three main reasons.

First, the focus is on security technology and not viewing cyber security as a risk to be addressed holistically at an organizational level, which includes people, processes, contract management, management support, and training to name a few dimensions. Second, this narrow focus on security technology reinforces a dominant perception that cyber security is Information Technology department problem. Third, within the context of the cyber ecosystem, focusing only on a technical solution is not holistic because it ignores or attaches less importance to interactions with other systems/sub-systems operating beyond an organizational boundary.

1.2 Holistic Approach to Cyber Security

We argue that limitations of technical approaches are not because of inherent problems with those approaches, but because technical approaches address only a subset of cyber security risks. Therefore, cyber security needs a holistic approach, and to create a holistic strategy organization need to go beyond security technology, to also understand and address non-technical risks contributing to the cyber security problem. Savage and Schneider [1] summarize this point by highlighting that cyber security is a holistic property of a system (the whole) and not just of its components (parts). They further emphasize that even small changes to a part of system, can lead to devastating implications for overall cyber security of a system.

The above discussion highlights the fact, that people are an essential dimension of any successful holistic cyber security strategy. In our complex cyber ecosystem, we constantly interact with systems and sub-systems, which are dispersed geographically. This human-technical interaction represents a sociotechnical system, which amalgamates technology with people to form systems [2]. This technical interaction with human behaviors adds to the complexity of the cyber ecosystem. Further adding to this complexity are the interdependencies which exist between systems and subsystems of our global digital ecosystem.

As a first step towards applying STAMP, cyber security needs to be viewed holistically from the lens of *systems thinking*. "Systems thinking is a discipline for seeing wholes. It is a framework for seeing interrelationships rather than things, for seeing patterns of change rather than static 'snapshots'." [3]. Systems Thinking is suited for cyber security because it allows practitioners to understand a system of interest and its interdependencies holistically, while taking socio-technical aspects into account. The STAMP model embodies Systems Thinking in a socio-technical context.

2 Literature Review

In our research, we studied Chain-of-Events Model and its derivative method Fault Tree Analysis (FTA) both of which are generally used for investigating cyber-attacks. We also looked at a widely used framework for cyber security best practices published by Information Systems Audit and Control Association (ISACA) called Control Objectives for Information and Related Technology (COBIT) 5[2] for Information Security, and an information security standard published by The International Organization for Standardization (ISO) and The International Electrotechnical Commission (IEC) called ISO/IEC 27002[3]. A brief discussion of

[2] http://www.isaca.org/COBIT/Pages/info-sec.aspx
[3] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533

these models and standards is presented next, followed by an introduction to System-Theoretic Accident Model and Processes (STAMP).

2.1 Chain-of-Events Model

First generation accident models attributed cause of an accident to a *single* risky behavior or a circumstance leading to risky behavior [4]. Second generation accident models incorporated *multiple* causal factors and associations among them for determining causes of an accident [4]. Different from these models, where the cause of a failure is usually attributed to a single event, Chain-of-Events Model chronologically arranges causal factors forming an event chain [4], where multiple events are included to understand causal factors behind a loss. The goal of Chain-of-Events Model is to manage risk of a future cyber-attack by implementing counter-measures, driven by eliminating an event(s) and/or intervening between events in a chain, so that the chain is broken. In this model, some events or environmental aspects are designated as proximate, root, or contributory. Risky behaviors and circumstances leading to such behaviors are used to help understand underlying causal factors, which led to a loss.

The Chain-of-Events Model is simple to understand and reasonably easy to create. Casual factors can be identified quickly based on an event chain and environmental factors or conditions, enabling counter measures to be implemented in a timely manner. But, this simplicity is deceiving and Chain-of-Events Model lacks completeness, therefore it is ineffective in explaining *why* accidents happen and how to prevent them [5]. Some shortcomings of Chain-of-Events Model are discussed next within the context of cyber security.

2.1.1 Limitations of Chain-of-Events Model

First, determination of causal factors is dependent upon the choice of events (unsafe acts or risky behavior) and related conditions[4] (environmental factors). Choice of these events and conditions is subjective, with the exception of any physical event that directly precedes the loss or is involved with a loss [5]. Second, it is impossible to determine a terminal point when traversing back from an accident event [4], because there is no fixed standard to make this decision. Third, the Chain-of-Events Model by design promote linear causality relationships [5] [6], making it very challenging to account for non-linear causalities that may contribute to cyber security risk. Fourth, Chain-of-Events Models helps manage risk of future cyber-attacks based on already discovered and addressed vulnerabilities that have been exposed after a cyber-attack. Sixth, Chain-of-Events Model lacks in accounting for systemic factors including management deficiencies and/or structural weaknesses of an organization, because learning from this model can be limited due to arbitrary choice of events and conditions, further, relevant causal factors can be excluded because of their non-linearity [5].

2.2 Fault Tree Analysis (FTA)

Fault Tree Analysis (FTA) is based on the Chain-of-Events Model is a top down method for studying causes of hazards in a system [7], which uses a tree structure and Boolean logic for its construction. FTA's simple to understand tree format enables a high level understanding of a system, without need for a detailed analysis allowing for timely detection of scenarios leading to hazards. Tree construction requires an in-depth understanding and details of a system, highlighting system inefficiencies/issues and facilitating improvements by an analyst. Events

[4] Events have finite duration, and conditions persist until an event occurs resulting in new or different conditions [5].

and their relationships are depicted graphically, making it easy to understand system logic and detect issues during analysis [7].

Some of FTA's limitations that are in addition to the inherited shortcomings of Chain-of-Events Model. First, an effective fault tree can only be created after a product has been fully designed for any consequential analysis, because constructing a tree requires detailed knowledge and understanding of system design and operation. Generic trees can be created without full knowledge of detailed system design but their effectiveness will be limited [7]. Second, for software systems FTA can only be used for verification, because the software code must already have been created to generate a tree [7]. Third, systems in software and hardware intensive cyber ecosystem are composed of many subsystems by multiple vendors and in many instances across geographies, limiting scope of software verification only to systems where analysts are able to exercise full control. Fourth, in the design stage of software development lifecycle, FTA may be used for early detection of issues [7]. But the specifications of software logic must be documented in detail for FTA to be effective, which is in itself a challenge because most organizations lack documentation of systems and/or documentation is not reflective of software changes, which have been implemented over time.

2.3 COBIT[5] 5 for Information Security

COBIT 5 is a business framework for governance and management of enterprise IT developed by Information Systems Audit and Control Association (ISACA). Two main limitations of COBIT 5 are, first it is not meant for causal factor analysis, therefore additional methods or models would be needed *after* COBIT 5 has been implemented. Second, COBIT 5 ability to integrate with other standards due to its generality would require broader in-house expertise to manage an integrated framework of multiple standards.

2.4 ISO/IEC 27002

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly prepare international standards through a formal structure comprising of committees. ISO/IEC 27002 demonstrates general principles and guidelines for information security management in an organization. Standards incorporate lessons from past experiences accumulated over many years [8], making them a valuable tool for managing cyber security risks. But the main limitation, specifically in the context of a complex and dynamic environment like cyber is the static nature of standards. That is, in general standards are slow to update, for example, second edition of ISO/IEC 27002 was published in 2013, eight years after the publication of the first edition [9]. This lag makes it impossible for standards to accurately reflect changes taking place with reference to technology, and therefore, expose organizations to greater cyber security risks.

2.5 System-Theoretic Accident Model and Processes (STAMP)

"Accidents are complex processes involving the entire sociotechnical system. Traditional event-chain models cannot describe this process adequately" [5]. In light of this statement, and in the context of cyber security, our research highlights that in general, cyber security risks stem from the cyber ecosystem, which is a complex and dynamic sociotechnical system

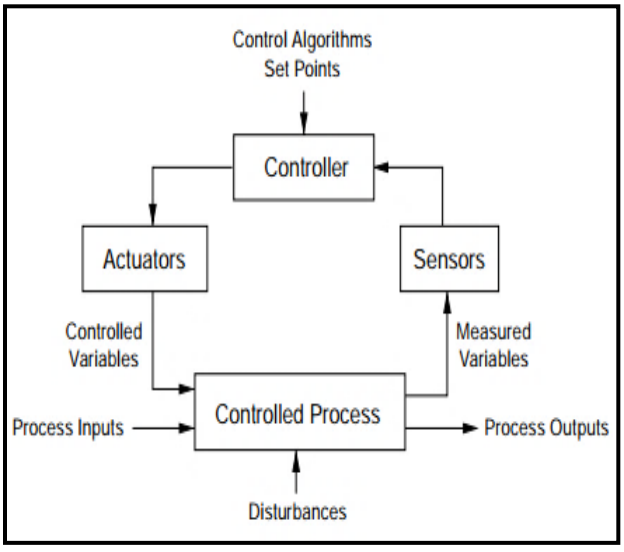
[5] COBIT is an acronym for Control Objectives for Information and Related Technology, now widely referred by the acronym only. Source: http://en.wikipedia.org/wiki/COBIT

composed of many subsystems spread across the globe. System-Theoretic Accident Model and Processes (STAMP) enable understanding accidents holistically.

2.5.1 STAMP Framework

In STAMP, to understand causal factors leading to an accident requires understanding *why* a control was ineffective. In STAMP focus is not on preventing failure event(s) but to implement effective controls for enforcing relevant constraints. This is the foundation of STAMP model, with (1) *safety constraints, (2) hierarchical safety control structures, and (3) process model* as core concepts, which are discussed next.

In STAMP safety constraints are the foundation. Missing constraints or lack of enforcement of relevant constraints leads to elevated cyber safety risks, which may cause loss event(s). Therefore to manage cyber safety risks, defining constraints requires careful analysis and thought. Second core concept in STAMP is the hierarchical safety control structure. In STAMP systems are viewed as hierarchical structures where a higher level imposes constraints over the level immediately below it, governed by a standard control loop depicted in Figure 2.1. The constraints at a higher level control behavior at lower level. Processes at lower level of hierarchy are managed by control process that operate between levels, and enforce relevant constraints upon the level below. When these control processes are ineffective in controlling lower level processes and safety constraints are violated, then a system suffers an accident. Four factors may contribute to inadequate control at each level of a hierarchical structure. The four factors are missing constraints, inadequate safety control commands, commands incorrectly executed at a lower level, or inadequate communication or processed feedback with reference to constraint enforcement [10]. Each level in the control structure is connected by communication channels needed for enforcing constraints at lower level and receiving feedback about the effectiveness of constraints. As shown in Figure 2.2, downward reference channel is used for providing information in order to impose constraints. And the upward feedback channel is used to measure effectiveness of constraints at the lower level.



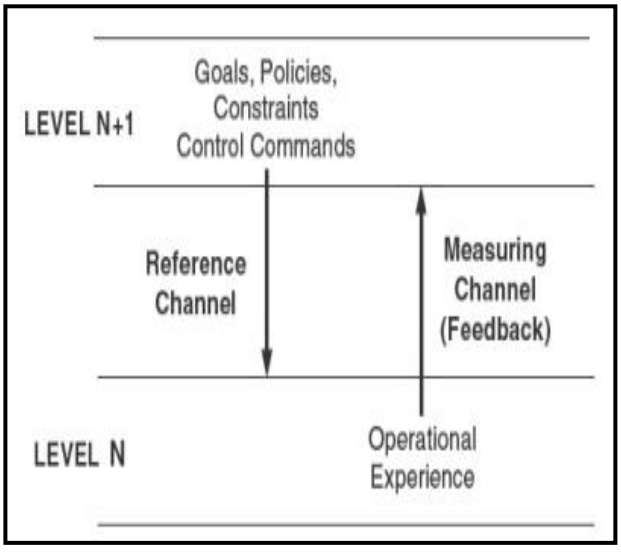


Figure 2.1: Standard control loop [11].

Figure 2.2: Communication channels in a hierarchical safety control structure [10].

Third key concept in STAMP is process model. There are four conditions necessary to control a process. These are shown in

Table 2.1, with corresponding STAMP context.

Conditions for Controlling a Process	STAMP Context
Goal	Safety constraints to be enforced by each controller.
Action Condition	Implemented via downward control channel, in STAMP context communication between hierarchical control structures.
Observability Condition	Implemented via upward feedback channel, in STAMP context communication between hierarchical control structures.
Model Condition	To be effective in controlling lower level processes, a controller (human – mental model, or automated – embedded in control logic) needs to have a model of the *process being controlled* – STAMP context.

Table 2.1: Conditions required for controlling a process and corresponding STAMP context.

A human controller's mental model or an automated controller's embedded model must contain the same information with reference to relationships between system variables, the current state of those system variables, and means by which the process can update those system variables. Any variance between the controller's process model, and the controlled process or the system being controlled will often result in a loss, see Figure 2.3. According to Leveson [10], "In general accidents often occur, particularly component interaction accidents and accidents involving *complex digital technology or human error*, when the process model used by the controller (automated or human) does not match the process".

STAMP can be used both for hazard analysis (Ex ante) and accident analysis (Ex post), see Figure 2.4. In hazard analysis the goal is to understand scenarios and related causal factors that can lead to a loss, and implement countermeasures during design and/or operation of a system to prevent losses. This method is called *System-Theoretic Process Analysis (STPA)*. The second STAMP based method called *Causal Analysis based on STAMP (CAST)* is used to analyze accidents. The goal is to maximize learning and fully understand why a loss occurred. The focus of this paper is CAST.

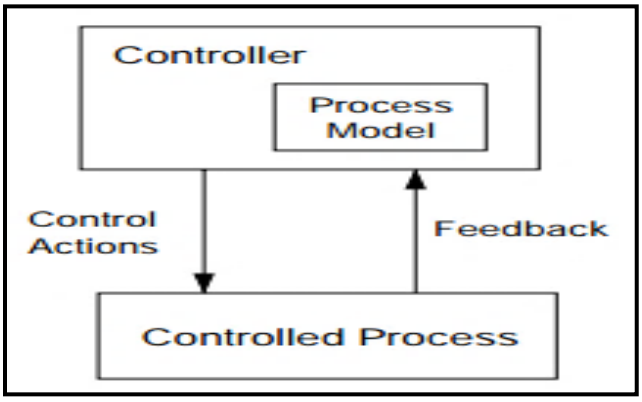


Figure 2.3: Controller with a process model [10].

2.6 Causal Analysis based on STAMP (CAST)

CAST is used for accident and incident analysis. CAST allows an analyst to go beyond a single failure event and analyze a broader sociotechnical system to understand systemic and non-systemic casual factors [12]. Goal of CAST is to understand *why* the loss occurred and implement countermeasures to prevent future accidents or incidents. CAST also places an emphasis on people's behaviors and what caused a certain behavior that led to an accident or incident [12]. Process for analyzing accidents is composed of nine steps. The steps do not imply that analysis should be carried out in this order or that a step must be completed before starting the next one. For example, recommendation(s) can be a result of identifying hazard(s) in Step #1. CAST steps are listed below in Table 2.2:

No.	Step	Brief comment(s)
1	Identify the system(s) and hazard(s) associated with the accident or incident.	a. Steps 1-3 form the core of STAMP based techniques. b. With reference to step 3, the control structure is composed of roles and responsibilities of each component[6], controls for executing relevant responsibilities, and feedback channel.
2	Identify the system safety constraints and system requirements associated with that hazard.	
3	Document the safety control structure in place to control the hazard and ensure compliance with the safety constraints.	
4	Ascertain the proximate events leading to the accident or incident.	In order to understand the physical process, events chain will be used to identify basic events leading to an accident or incident.
5	Analyze the accident or incident at the physical system level.	This step is start of analysis, and helps identify role each of the following played in events leading to an accident or incident. a. Physical/operational controls. b. Physical failures. c. Dysfunctional interactions/communications. d. Unhandled external disturbances.
6	Moving up the levels of the hierarchical safety control structure, establish how and why each successive higher level control allowed or contributed to the inadequate control at the current level.	After physical deficiencies have been identified, next step is to investigate why those deficiencies existed. This requires understanding higher levels of hierarchical safety control structure. According to Leveson [12], "fully understanding the behavior at any level of the sociotechnical safety control structure requires understanding how and why the control at the next higher level allowed or contributed to the inadequate control at the current level". This step is the core of CAST analysis requiring an analyst to focus on the overall sociotechnical system with a diagnostic mindset focused on *why* the controls were deficient. This is in contrast to Chain of Events Model where the focus is on a failure event and analysis stops once a failure event is identified.
7	Analyze overall coordination and communication contributors to the accident or incident.	This step examines coordination/communication between controllers in the hierarchical control structure.
8	Determine the dynamics and changes in the system and the safety control structure relating to an accident or	Most accidents/incidents occur when a system migrates towards a higher risk state *over time*. Understanding the dynamics of this migration towards less safe and secure environment will help with

[6] Components can be electromechanical, digital, human, or social. *Source:* [5]

	incident, and any weakening of the safety control structure over time.	implementing appropriate countermeasures.
9	Generate recommendations.	CAST is a comprehensive approach, and as a result, list of recommendations can be long. Many factors can drive which recommendation to implement depending on a particular situation. Decision factors can include cost, effectiveness, and/or practicality of a particular recommendation.

Table 2.2: CAST steps for analyzing accidents [12].

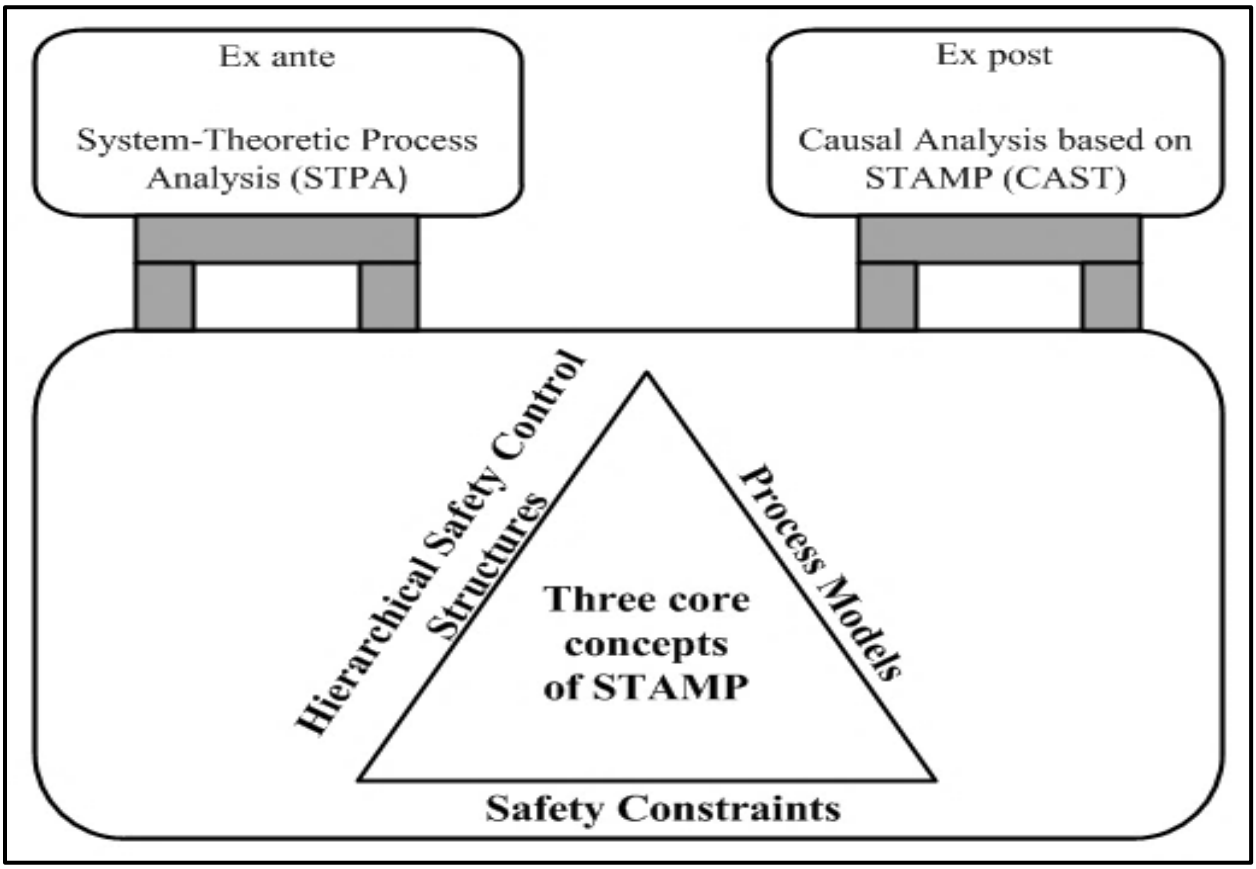


Figure 2.4: System-Theoretic Accident Model and Processes (STAMP), and STAMP based hazard analysis (STPA) and accident analysis (CAST).

3 TJX Cyber-Attack

This section presents highlights of the TJX cyber-attack that was one of a series of attacks, executed as part of operation *Get Rich or Die Tryin'* and continued for five years until 2008.

As the 2006 holiday season was coming to a close and US retailers were busy tallying their numbers, TJX, a leading US based off-price retailer, was working with the authorities to address and contain breach of its computer systems. On January 17, 2007, TJX announced that it was a victim of an unauthorized computer systems intrusion. The breach was discovered on December 18, 2006, and payment card transaction data of millions of its customers had been potentially stolen. The cyber-attack suffered by TJX was at the time the largest in history on any US corporation, measured by number of payment cards stolen.

The cyber-attack highlighted operational and IT related strengths and weaknesses of TJX, which will be studied further using STAMP in section 4, key observations are briefly

discussed in this section. The goal of STAMP analysis is to understand *why* the weaknesses existed and if/how they contributed to the TJX cyber-attack, and also if, counter-intuitively, any of the strengths of TJX played a role that resulted in increased cyber security risks.

3.1 Wireless Network Technology

TJX was one of the early adopters of Wi-Fi technology and was in use by over 2400 stores worldwide by the end of 2006. Managing technical infrastructure of this scale is a complex process. But TJX was at the forefront of technology to achieve operational efficiencies and maintain competitive advantage. However, there were also two distinct issues with TJX wireless technology that contributed to an increased risk of a cyber-attack.

- Improper configuration of the Access Point (AP) at Marshalls stores allowed hackers to gain access to in-store network without any need for credentials. Open authentication provided hackers an opportunity to decrypt WEP encryption key and gain access to TJX corporate servers in Framingham, MA.
- A deprecated WEP encryption algorithm was in use at Marshalls stores, which had publically known vulnerabilities. A more secure encryption algorithm WPA was available in 2003, but was not in use at TJX.

Given TJX's experience with technology infrastructure, the question is why TJX was lagging in keeping up with Wi-Fi technology even though WEP was publically known to have vulnerabilities. STAMP will be used in an attempt to answer this question.

3.2 Monitoring of networks

Hackers were able to install a VPN connection on the TJX corporate server and freely move around within the TJX network without being detected. Further, TJX came to know about the breach only after it was informed by a credit card company of fraudulent transactions appearing on customer statements. Understanding factors that led to TJX not being able to detect the cyber-attack also will be explored using STAMP.

3.3 Retention of customer information

During the TJX cyber-attack, hackers found payment card data that was at least two years old. This raises the question of why a retailer was storing customer information which was not required after the payment was approved by a credit card company. Related to this question is what type of information could a retailer ask for with reference to a payment transaction. STAMP will be used to understand why information was retained and what were the TJX policies regarding retention and type of information.

3.4 Use of Actual Customer Information for Troubleshooting

TJX was using actual payment card customer data for system maintenance. STAMP will be used to analyze this issue in an attempt to gain an understanding, with reference to system maintenance process that exposed customer information to risk of loss.

3.5 Compliance with PCI-DSS and Credit Card Rules

TJX was out of compliance with PCI-DSS standards and credit card rules. It is important to understand why this was the case, what is the process for implementing and monitoring of standards, or if there is misalignment of incentives between credit card companies and TJX. Credit card transactions are complicated involving multiple parties and sometimes it is not

clear which party is responsible for enforcing payment processing standards. This topic will also be analyzed using STAMP.

4 STAMP/CAST Analysis of TJX Cyber-Attack

In this section, the TJX cyber-attack is analyzed using the nine step CAST framework.

4.1 Step #1: System(s) and Hazard(s)

4.1.1 System(s)

TJX cyber-attack resulted in loss of millions of customer's payment card data, and as a result TJX also incurred financial losses amounting to over $170 million. Payment card data was stolen from the TJX payment card processing server. To understand why the hackers were able to steal so much of information without detection for a period of over one year, the system for analysis is ***TJX payment card processing system*** used for processing customer purchases and merchandise returns at TJX retail stores.

4.1.2 Hazard(s)

The hazard that is to be avoided is that ***TJX payment card processing system allows for unauthorized access***. Unauthorized access can be malicious, that is with intent to do harm, or non-malicious, that is, data is accessed unknowingly or by mistake. An example of non-malicious access may be the following. An employee who is not authorized to view salary data may be able to do so because of a system misconfiguration or vulnerability.

4.2 Step #2: System Safety Constraints and System Requirements

4.2.1 System Safety Constraints

1. TJX must protect customer payment card and other information from unauthorized access.
2. TJX must provide adequate training to technology staff for managing TJX security technology infrastructure.
3. Measures must be in place to minimize losses from unauthorized access to TJX payment card processing system, those can include:
   - 3.1. TJX must communicate and interact with payment card brands to minimize losses.
   - 3.2. TJX must inform and seek support from law enforcement and private cyber security experts.
   - 3.3. TJX must provide support to TJX customers whose payment card data or other information may have been stolen.

4.3 Step #3: TJX Hierarchical System Safety Control Structure

Hierarchical system safety control structure is comprised of two parts – system development and system operations. Safety control structure includes roles and responsibilities of each component, controls for executing those responsibilities, and feedback to gauge effectiveness of controls [12].

Figure 4.1 shows the overall TJX system safety control structure. Dotted arrows and dotted boxes indicate development part of the control structure, and solid arrows and solid boxes indicate operational part. Each box (dotted or solid) represents a component. Dashed rectangle labeled as *System Boundary* indicates the boundary of the system to be analyzed, components enclosed within this boundary will be analyzed. Numbers represent control structures with control and feedback channels forming a loop. Physical process (discussed in

forthcoming sections) is identified by dashed oval. The components nomenclature together with the control structure, depict a general view of a typical large corporation like TJX.

Solid bold arrows (loop #16, loop #17, and loop #18) indicate interactions between development and operation parts. The first interaction is between Project Management and Operations Management (loop #16), which generates high level system needs, and Request for Proposals (RFP). Project Management provides feedback in the form of reports. The second interaction is between Systems Management and Payment Card Processing System (loop #17) where the focus is system testing, implementation, and maintenance. Feedback includes test results, issues log, and change requests. Third interaction is between Systems Management and TJX Retail Store System (loop #18). This is the post implementation, technology support and maintenance loop, where TJX Retail Store System is provided with services related to all technologies at a retail store. Feedback is provided by monitoring reports and system logs.

4.4 Step #4: Proximate Event Chain

Event chain analysis is not capable of providing critical information with reference to causality of an accident – in this case TJX cyber-attack, but basic events with reference to the cyber-attack are identified for gaining an understanding of the physical process involved in the loss [12].

Normally in STAMP proximate[7] implies a short time horizon generally ranging from hours to a few months. But in the context of cyber security, causal factors underlying a cyber-attack may have been in place long before the actual loss occurred. The TJX case illustrates this, because the cyber-attack started eighteen months before it was detected, and as discussed in the forthcoming sections of CAST analysis, contributing causes were in place since 2000 when TJX moved from wired to wireless communication network – five years before the cyber-attack. Therefore, in the context of cyber-security and specifically in this paper *proximate* can also mean a longer time horizon generally in the range of 1-2 years. Proximate events leading to the TJX cyber-attack are summarized below. Note that there were multiple incidents and accidents involved in the cyber-attack. Accidents are indicated by a '*'[8] in the event chain that contributed to loss of *payment card information*, at the *physical process level*, which is the loss being analyzed and discussed in next section.

1. In 2005 TJX decided not to upgrade to a stronger encryption algorithm and continued using deprecated WEP encryption.
2. In 2005, hackers use war-driving method to discover a misconfigured AP at a Marshalls store in Miami, FL.
3. Hackers join the store network and start monitoring data traffic.
4. In 2005, hackers exploited inherent encryption algorithm weaknesses at TJX Marshalls store, and decrypted the key to steal employee account and password.*
5. Using stolen account information, hackers accessed corporate payment card processing servers in Framingham, MA.

[7] Merriam-Webster defines proximate as not being distant in time, space, or significance.
[8] ***** implies a loss from the perspective of TJX and not from computer system, because the system was executing commands as directed – albeit by hackers.

6. In late 2005 hackers downloaded previously stored customer payment card data (*not* current transactions) from TJX corporate transaction processing servers in Framingham, MA using Marshalls store Wi-Fi connection in Florida.*
7. In 2006 hackers discovered vulnerability, that TJX was processing and transmitting payment card transactions without encryption.
8. In 2006 hackers installed a script called 'blabla' on TJX corporate servers to capture unencrypted payment card data.
9. In 2006 hackers installed a dedicated VPN connection between TJX server in Framingham, MA and a server in Latvia controlled by hackers. Then using TJX corporate servers as staging area, hackers created files containing *current* customer payment card data., and started downloading the files to the Latvian server.*

4.5 Step #5: Analyzing the Physical Process

In this step, loss at the physical process level is analyzed. As shown in Figure 4.1, the physical process in the hierarchical control structure is the TJX Retail Store System. The goal of this step is to determine why the physical controls were ineffective in preventing the system from transitioning into a hazardous state that eventually led to the cyber-attack. As part of the analysis, several factors will be considered that include [12]:

- How physical and operational controls contributed to an accident, and why were they not effective in preventing the system hazard.
- What were the physical failures (if any) involved in the loss.
- Were there any dysfunctional interactions.
- Were there any communication and coordination flaws between the physical system and other interacting component(s).
- Were there any unhandled disturbances.

4.5.1 TJX Retail Store System

The physical process TJX Retail Store System is the subject of analysis, and is a part of four control loops as shown in Figure 4.1 and discussed below. The retail store physical process is the only direct touch point of TJX with its customers for processing payment card transactions and merchandise returns. Customers present their payment card information for purchases, and store processes transactions via Payment Card Processing System. For merchandise returns without a receipt additional customer information like driver's license number is also required. General focus with reference to transactions is purchase transactions, because in case of merchandise returns with a receipt customer information has already been recorded by TJX by way of a purchase transaction.

TJX Retail Store System acts on TJX customers (loop #12) by way of credit decisions, and input is received from the customer in terms of payment card data. Information flows are in the context of customer payment card transactions as shown in Figure 4.1. There are additional information flows involved in interaction with the customer, which include Stock Keeping Unit (SKU) for adjusting inventory after a return or when a purchase is made, and cash transactions, but are not relevant to CAST analysis per Step #2, which identified TJX payment card processing system for analysis.

A transaction at the physical process level is initiated after a customer presents a payment card to the TJX Retail Store System (Point of Sale (POS) terminal) to make a payment for a purchase (loop #12). The magnetic stripe at the back of the card that contains

customer information is read by swiping the card through POS card reader. The customer information is then transmitted from the POS terminal to a computer located within the TJX Retail Store System over the stores Wi-Fi network. The payment card data is then transmitted from TJX Retail Store System to the Payment Card Processing System (loop #9) housed at TJX corporate headquarters in Framingham, MA, for credit decision by the customer's bank via Fifth Third Bancorp (loop #11). If the transaction is approved by the bank, then the transaction is processed and receipt printed for the customer, otherwise, the transaction is cancelled and customer is notified.

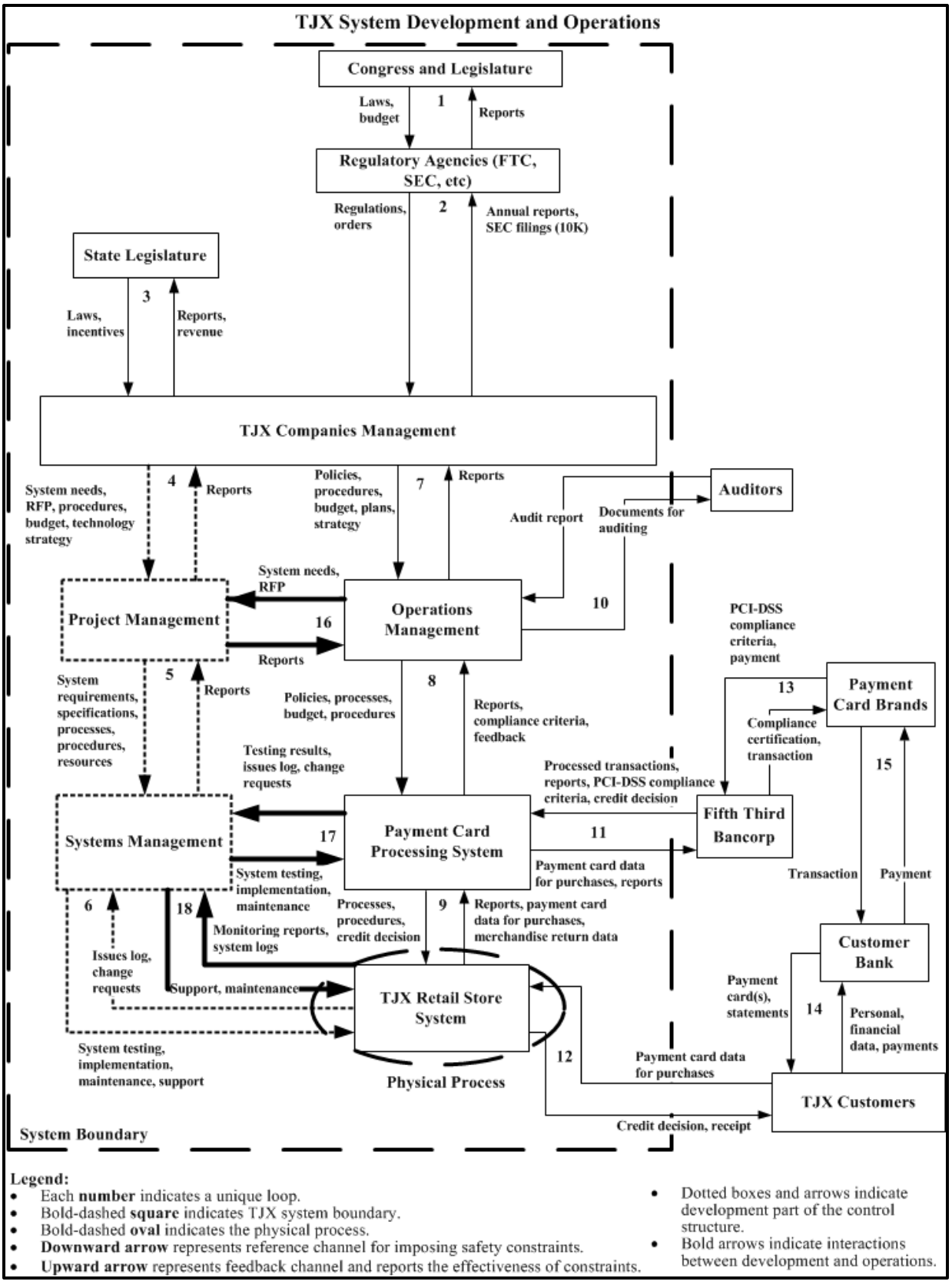


Figure 4.1: TJX system development and operations hierarchical control structure.

4.5.1.1 Inadequate control/feedback

4.5.1.1.1 Security Technology Management Capabilities

The TJX store was targeted because of the method hackers were using to find vulnerable business Wi-Fi networks. War-driving specifically looks for Wi-Fi networks which allow anyone to join without authentication. TJX store network fell in this category, because its Access Point (AP) was incorrectly configured and opportunities for correct install during implementation (loop #6) and maintenance/support (loop #18) were missed as shown in Figure 4.1. This contributed to weakening of control by Systems Management over the physical process both via loop #6 and loop #18, and further, there was inadequate feedback from the physical process to Systems Management during support and maintenance phase (loop #18), because the AP at the retail store either did not report misconfigured parameters or there was no system to capture this information by the Systems Management.

4.5.1.1.2 Monitoring

After joining the TJX Retail Store System Wi-Fi network, hacker's presence was never detected. This is despite the fact that they were downloading large amounts of data from TJX corporate server in Framingham, MA, using Wi-Fi network at the physical process level in Miami, FL. Inadequate or lack of feedback with reference to loop #18 in Figure 4.1 needs to be analyzed further to understand causes underlying the weakened control, because Systems Management via loop #18 was responsible for monitoring.

4.5.1.1.3 Encryption technology

At the time when the cyber-attack was initiated in 2005, TJX was using deprecated version of Wi-Fi encryption algorithm called WEP at the physical process level. Software utilities for decrypting WEP key were freely and publically available. Hackers in addition to taking advantage of the AP misconfiguration also exploited inherent weaknesses in the WEP encryption algorithm to steal TJX employee account and password at the physical process level. To understand why Systems Management did not replace the deprecated encryption algorithm at the physical process level via loop #18, higher levels of the control structure would need to be analyzed. CAST analysis of the physical process is summarized in Figure 4.2.

Safety Requirements and Constraints Violated:

- Prevent unauthorized access to customer information.

Emergency and Safety Equipment (Controls):

- Security technology at the store included the following barriers to prevent unauthorized access.
    - AP authentication for devices requesting to join stores Wi-Fi network.
    - WEP encryption for in-store Wi-Fi communication network.
    - Use of account id/password by store employees for accessing corporate servers in Framingham, MA.

Failures and Inadequate Controls:

- Access Point (AP) misconfiguration
    - Hackers used Marshalls store AP to join the store network. They were successful because the AP was configured incorrectly with a default setting of *open authentication* that allowed connections to anyone within range without authentication. Changing the default setting at implementation time would have served as a strong deterrent, because the technique of war-driving used by hackers specifically needed open connection setting to be

successful.

- Inadequate or lack of monitoring of stores Wi-Fi network for unauthorized access and/or data traffic at the physical process level.
    - Hackers joined the store network without authentication and downloaded large amounts of data, but their presence was never detected by TJX. There were no tools to perform scan of Wi-Fi network and gather data, related to high traffic or active connections with unknown account names for further analysis.
- Inadequate implementation/maintenance of processes and/or procedures at the physical process level.
    - Weaknesses in implementation and monitoring may be due to missing processes, procedures, adequate documentation, or checklists.
    - Further, during TJX cyber-attack investigation, it was revealed that the stores were collecting customer information that was not required to make a purchase or a return. For example, it was a common practice to ask for driver's license numbers when making returns. Apparent lack of process and/or procedures with reference to data collection policy exposed more of customer information to hackers.
- Inadequate encryption technology used at the physical process level.
    - TJX stores were using deprecated encryption WEP, and never upgraded to a more secure encryption until the cyber-attack was discovered in December, 2006.

Physical Contextual Factors:

- TJX was an early adopter of first generation Wi-Fi technology at over 1200 retail stores in 2000. Vulnerability in the Wi-Fi technology was known since 2001 but an updated version was not available until 2003. Therefore, TJX and retail industry in general were using vulnerable technology for approximately two years. TJX did not suffer a cyber-attack during this time possibly reinforcing a naïve sense of confidence and security with WEP encryption algorithm, even though other retailers relatively quickly switched to the second generation encryption.
- Wi-Fi technology became available in 1999 and TJX implemented it in 2000, requiring a significant learning curve, training, and a new knowledge base in a short span of time. This may have contributed to lack of preparedness in implementing and upgrading Wi-Fi networks.
- Assuming that monitoring was activated at the physical process level, Systems Management's process for selecting monitoring criteria was a challenge, because by the year 2005 there would be over 2000 retail stores generating system logs on a daily basis.

Figure 4.2: CAST analysis of TJX Retail Store System (Physical Process Level).

4.6 Step #6: Analysis of Higher Levels of the Hierarchical Safety Control Structure

In Step 5, three key control/feedback inadequacies at the physical process level were highlighted that contributed to the cyber-attack. First, AP was incorrectly configured, second, Wi-Fi network monitoring was inadequate, and third deprecated encryption was in use for processing payment card transactions. To understand why these inadequacies existed at the physical level, both development and operational components at higher levels of the TJX hierarchical safety control structure need to be analyzed. Understanding behavior at any level of a sociotechnical safety control structure requires investigating control at the next higher level [12].

4.6.1 Payment Card Processing System

Moving one level up from the physical process in the hierarchical control structure, along the operational part from TJX Retail Store System to Payment Card Processing System as shown in Figure 4.1(loop #9), note that TJX physical process is controlled by Payment Card

Processing System. This control is exercised by way of processes related to TJX Retail Store System operation, procedures that include guidance on handling customer information, and customer credit decisions related to purchase transactions. Payment Card Processing System receives feedback via reports that include daily merchandise inventory, merchandise sales and return, and accounting, in addition to customer payment card data for credit decisions, and merchandise return data.

Payment Card Processing System is responsible for receiving customer payment card data from the physical process level, transmit it to Fifth Third Bancorp for a credit decision, and inform the physical process of credit approval or denial. If the credit is approved, then Payment Card Processing System performs further actions related to customer payment card data including accounting of approved transaction within TJX systems. This further processing requires customer payment card data to be stored on TJX corporate servers per PCI-DSS requirements. Further, customer information is also stored for merchandise returns without a receipt.

Ensuring that customer payment card data is secure as it flows through TJX systems is a shared responsibility of Payment Card Processing System and other components in the control structure. In the context of Payment Card Processing System securing payment card data implies conforming to payment card brand standards and rules for transaction processing, that cover both technology and business aspects related to payment card processing. Payment Card Processing System interacts with Fifth Third Bancorp[9] bank (loop #11) as shown in Figure 4.1. It is also responsible for ensuring that TJX is in compliance with PCI[10]/PCI-DSS[11] requirements and not in violation of any payment card brand rules[12].

Payment Card Processing System also interacts with Systems Management (loop #17) by way of systems testing, implementation, and maintenance. Feedback is in the form of testing results, issues log, and change requests. This link is to ensure that systems are subjected to rigorous testing, conform to PCI-DSS, and TJX internal policies which include customer data retention timeframe, for secure processing of payment card transactions by way of incorporating them during system design.

4.6.1.1 Inadequate control/feedback

4.6.1.1.1 Compliance with PCI-DSS

At the time of cyber-attack in 2005, TJX was not PCI-DSS compliant, which is a requirement for any entity accepting payment card(s) and therefore was in violation of payment card brand rules. In order to be compliant a merchant must satisfy *all* twelve requirements of PCI-DSS and its sub-requirements comprising of approximately eighty pages [13], requiring a significant effort on part of merchant. As an example, TJX was in violation of the following requirements and sub-requirements:

- *Requirement 3*: Protect Stored Card Holder Data [13]
    - *Sub-requirement 3.1*: Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes. These include

[9] After mergers and acquisitions the name has changed to Vantiv (http://www.vantiv.com/).
[10] Payment Card Industry (PCI) Data Security Standard name was the first standard known as PCI from 2004-2006.
[11] PCI was called Payment Card Industry (PCI) Data Security Standard (DSS) – PCI-DSS starting from its second version in 2006.
[12] PCI-DSS will be used through rest of the thesis with an implicit understanding that until 2006 it was referred to as PCI.

limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements…

Hackers stole payment card data that was from 2003 and TJX did not cite any of the reasons mentioned in the sub-requirement above, in its 2007 Form 10K Securities and Exchange Commission (SEC) filing [14] for retaining the information. In general PCI-DSS does not allow for storing authentication data after a transaction has been approved, which was not the case at TJX. In 2005, hackers downloaded payment card data that was two years old from TJX corporate servers. In addition to being in violation of PCI-DSS standard, TJX Operation did not have a formal data retention policy, or was inadequate and not communicated to retail stores. This weakened Payment Card Processing System's control over customer data. In general companies have policies where they archive and store data off-site, otherwise it is disposed of by automated scripts as part of maintenance schedule.

- *Requirement 4*: Encrypt transmission of cardholder data across open, public networks [13]. TJX was storing and transmitting customer payment card data to the Fifth Third Bancorp without encryption as reported in its 2007 Form 10K Securities and Exchange Commission (SEC) filing [14].

To understand why TJX was out of compliance, it will help to gain a high level understanding of the role a bank plays in the credit approval process and payment card transaction flow from TJX to Fifth Third Bancorp, as shown by their interaction in Figure 4.1 (loop #11). Any payment card transaction flows through multiple entities and systems before a credit decision is made. For example, VISA transaction flow is shown in Figure 4.3 and definition of each entity is shown in Figure 4.4. All major credit cards in general have a similar transaction flow.

In 2005 Fifth Third Bancorp was a major acquirer bank and responsible party for ensuring PCI-DSS compliance by merchants it contracted with for processing payment transactions. Based on CAST analysis, the following issues have come to light.

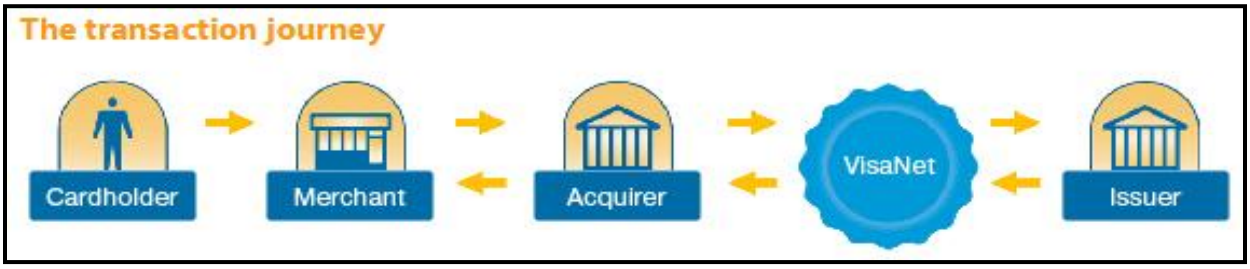


Figure 4.3: VISA transaction flow [15].

- There is a potential for conflict of interest/role between Fifth Third Bancorp and TJX when it comes to enforcement of PCI-DSS. Because TJX is a customer of Fifth Third Bancorp, Fifth Third Bancorp leverage is limited for rigorous enforcement of PCI-DSS. Further PCI-DSS is not legally required to be implemented by State (with the exception of State of Nevada) and Federal governments, limiting Fifth Third Bancorp options to primarily following up with TJX via written communications. During this communication period TJX remained exposed to cyber security risks.

- It is very difficult for Fifth Third Bancorp to gain deep insights into TJX systems to validate and verify that PCI-DSS has been implemented, because it has no regulatory role. Further, it is almost impossible for Fifth Third Bancorp to exercise meaningful influence during the design of TJX systems for PCI-DSS compliance, because system design is internal to TJX. For these reasons implementing PCI-DSS is the responsibility of TJX, which is required to submit yearly reports with reference to compliance status.
- According to PCI-DSS, Fifth Third Bancorp is not responsible for auditing TJX with reference to PCI-DSS compliance. Therefore, TJX is not under any pressure to comply fully, but fines can still be imposed by payment card brands in case of a data breach or loss. Further TJX Company auditors also do not audit specifically for PCI-DSS compliance. These factors may have contributed to the flaws in Payment Card Processing System that allowed unencrypted storage and transmission of customer payment card data.

4.6.1.1.2 Payment Card Processing System and Systems Management Interaction

Because Payment Card Processing System was sending unencrypted customer data to the bank, PCI-DSS requirement were not incorporated during the system design, weakening loop #17. There could be at least four possible explanations for this oversight. First, PCI-DSS requirements were not effectively communicated to system development, second, quality assurance process with reference to encryption testing was inadequate, third, there was systemic lack of awareness with reference to PCI-DSS requirements, and fourth, there was lack of clarity on roles and responsibilities with reference to PCI-DSS implementation between development and operations. Analysis of higher level components is needed to understand why this oversight occurred and for what reason. CAST analysis of Payment Card Processing System is summarized in Figure 4.5.

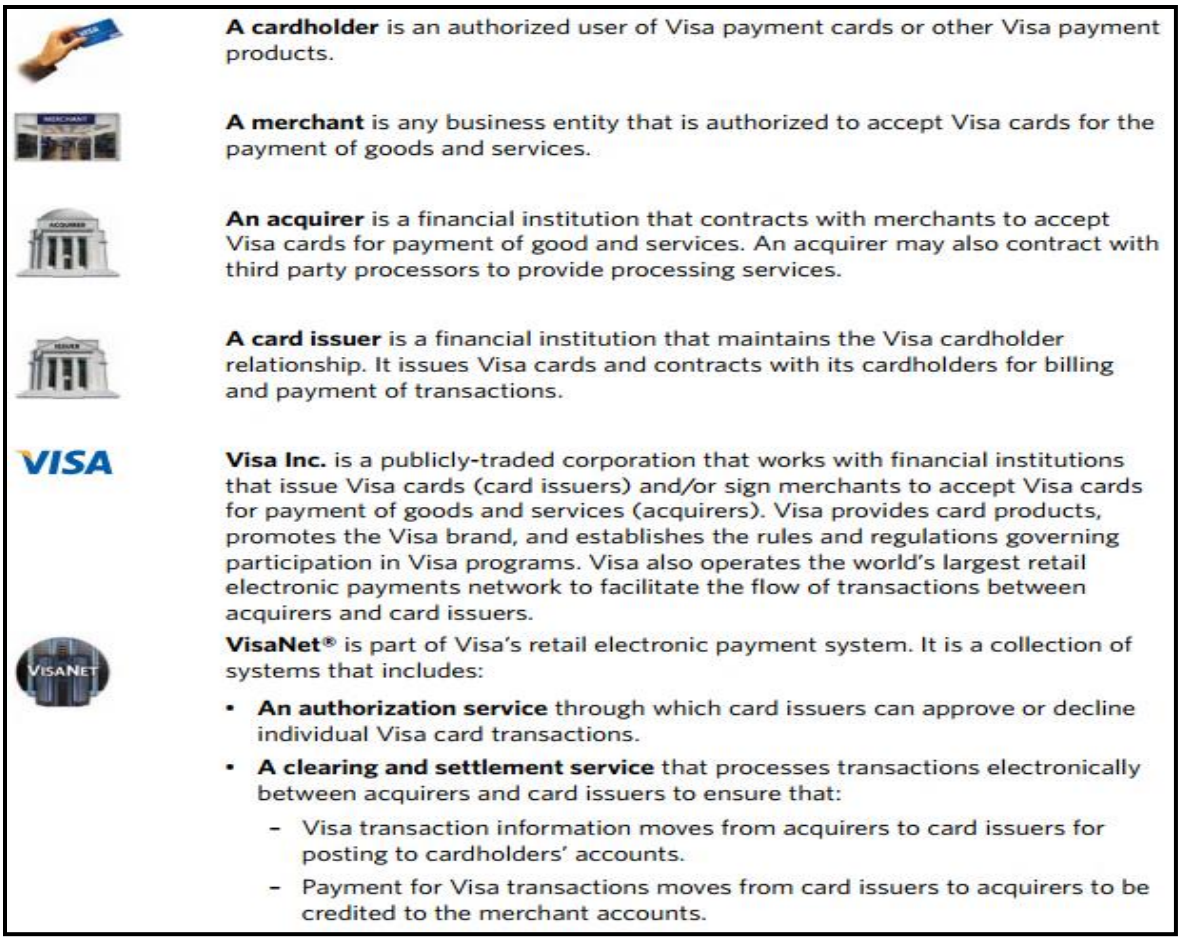


Figure 4.4: VISA transaction flow entity definitions [16].

Safety-Related Responsibilities:

- Ensure that customer payment card transaction data is encrypted during transaction processing and storage (if there is a need) on TJX servers. Specifically, Payment Card Processing System should encrypt all payment card data as it is being processed and sent to customer's bank.
- Ensure that payment card transactions flowing through TJX systems are PCI-DSS compliant. That is, all systems used for payment card processing must conform to PCI-DSS standard.
- Design, communicate, and implement customer data retention process and procedures consistent with PCI-DSS standard and TJX polices.
- Ensure that all new systems and updates to existing systems pass rigorous testing per PCI-DSS criteria, TJX policies, and TJX business rules.

Context:

- At the time of TJX cyber-attack announcement in early 2007, TJX was not in compliance with PCI-DSS which was formalized in 2006 [17], or with the first generation version of standard that was required prior to 2006. Understanding why TJX was not in compliance will require analyzing higher level components in the control structure.
- Compliance with PCI-DSS is required for anyone conducting business using any one of major payment card brands (VISA, MasterCard, etc.).

Unsafe Decisions and Control Actions:

- Inadequate compliance with PCI-DSS.
- Retained more customer payment card information than needed and for longer periods than required for processing payment card transactions and merchandise returns, in violation of PCI-

DSS.

- Inadequate testing of systems/lack of awareness of PCI-DSS
    - Hackers exploited a design flaw in payment card processing system, where payment card data for an instant was stored and transmitted unencrypted to the bank. According to PCI-DSS policy, payment card data must be encrypted for these operations. There are three plausible explanations for this flaw, (1) Systems Management was not aware of the PCI-DSS encryption requirement, (2) testing was inadequate, and (3) since 2004 when PCI-DSS was established TJX had been lacking in full implementation of PCI-DSS. Visa gave TJX opportunities to improve its security while continuing to allow TJX to process Visa transactions. A year later, in late 2005 Visa contacted Fifth Third Bancorp an acquirer for TJX with reference to PCI-DSS compliance. Visa vice president for fraud control Joseph Majka expressing concern issued a warning to Fifth Third Bancorp that TJX needed to be fully compliant with PCI-DSS. According to Majka's memo, "Visa will suspend fines until Dec. 31, 2008, provided your merchant continues to diligently pursue remediation efforts, this suspension hinges upon Visa's receipt of an update by June 30, 2006, confirming completion of stated milestones" [18]. But as discussed, Fifth Third Bancorp had limited influence on TJX with reference to enforcement of PCI-DSS, and Visa had already granted TJX suspended fines until 2008, creating conditions where TJX was exposed to cyber security risks because of these dynamics.
- To implement effective fraud management system, TJX was collecting additional information (including driver's license numbers, names, and addresses) for merchandise returns without receipts. According to TJX, unique identifier (a driver's license) helped determine if a particular customer is making excessive returns without a receipt, and served as a deterrent by allowing TJX to keep track and inform customers that further returns without a receipt would not be accepted. While customer names and addresses might be helpful and acceptable to achieve the goal of fraud management, including driver's license numbers exposed TJX customers to great risk. Because all these pieces of information can enable hackers in creating false identification with valid information.

Process Model Flaws:

- General belief within TJX that Fifth Third Bancorp's compliance with PCI-DSS implies compliance by TJX.
- Inadequate understanding of full scope of PCI-DSS with reference to its technology and business attributes.

Figure 4.5: CAST analysis of Payment Card Processing System.

4.6.2 Operations Management

Next level up in the control structure along the system operations part is Operations Management. Related to the Payment Card Processing System, the role of Operations Management is to provide policies, processes, and procedures for secure handling of customer information, customer data management guidelines (retention, disposal, archiving), compliance with PCI-DSS, and budget for resources needed to implement policies. Payment Card Processing System provides PCI-DSS compliance status, and reports that include accounting, inventory, and sales, as shown in Figure 4.1 (loop #8). Operations Management interacts with the auditors, from which it receives audit reports, and provides business documents for auditing (loop #10). Operations Management also interacts with Project Management (loop #16) for initiating system design by way of communicating system needs and Request for Proposals (RFP), and receives feedback in the form of reports that include project status, and proposals for projects. This interaction serves as a bridge between operations and development with reference to translating business needs and incorporating them within TJX systems. For

example, with reference to PCI-DSS Operations Management can use this interaction to incorporate PCI-DSS requirements in TJX systems.

4.6.2.1 Operations Management and Project Management Interaction

Because TJX was storing customer payment card data for longer than needed in violation of PCI-DSS standard and other information (driver's license numbers, names, and addresses) not required per PCI-DSS was also being collected and stored, the data retention and collection needs were not effectively or incorrectly communicated by Operations Management weakening loop #16. Further, lack of management support with reference to PCI-DSS had propagated a soft view on compliance with PCI-DSS. CAST analysis of Operations Management is summarized in Figure 4.6.

Safety-Related Responsibilities:

- Develop and communicate polices for customer information management.
- Ensure compliance with audit report recommendations.
- Ensure compliance with payment card processing rules, TJX policies, and business rules.
- Provide resources for maintaining a robust payment card processing systems.

Context:

- Because PCI-DSS implementation is not audited formally by external company auditors, non-compliance would not appear in annual audit report.
- Executive management changes noted below, corporate staff reductions, and cut in senior executive salaries in 2005-2006 may have contributed to lack of focus on policies, processes, procedures, and may have led to resource constraints.
    - 2005 – CEO resigns, new President named [19].
    - 2006 – New CEO named [20].
- Focus on rapid expansion of business during 2005-2007, may have contributed to diversion of resources resulting in lack of focus on internal processes.
- Although TJX Operations Management was responsible for PCI-DSS compliance it could not make it a high priority activity without the support of senior TJX management. In the context of TJX organization there was loose compliance and priority was given to cost savings over allocating resources for PCI-DSS compliance [18].

Unsafe Decisions and Control Actions:

- Between 2005 and 2007, for merchandise returns without a receipt TJX was collecting customer information like driver's license numbers. The objective was to control excessive returns by the same customer, and because the customer did not have a receipt so this was not a payment card transaction and therefore was not governed by PCI-DSS. The TJX internal process for collection and storage of customer information for returns without receipt, exposed customers to increased risk of identity theft. It is plausible, that TJX lacked a robust process for managing returns without receipt and deter customers who returned merchandise frequently.
- Inadequate or lack of policy guidance provided with reference to protection and use of customer information.

Process Model Flaws:

- Lack of understanding led to PCI-DSS being viewed as non-critical.
- Belief that PCI-DSS compliance is a technology issue.
- Soft view on compliance with PCI-DSS enabled lower level components of control structure to not view PCI-DSS as critical to payment transaction security.

Figure 4.6: CAST analysis of Operations Management.

4.6.3 TJX Companies Management (System Operations Part)

Next level up is TJX Management which controls Operations Management and is responsible for setting companywide policies, plans, procedures, strategy, and budgets. With reference to Payment Card Processing System, policies, plans, and procedures include responding to audit recommendations, compliance with PCI-DSS, handling of customer information by TJX, and ensuring that security technology infrastructure at TJX is robust. Additionally, TJX Companies Management is also responsible for overall business strategy and designing general business polices based on State and Federal laws and regulatory requirements. To support its business goals and strategy, TJX Management prioritizes and allocates resources across the company. Feedback is in the form of reports (loop #7), that include audit reports, financial statements, and sales report. CAST analysis of TJX Companies is shown in Figure 4.7.

Safety-Related Responsibilities:

- Ensure that resources are available and measures are implemented for protecting TJX information assets and technology infrastructure from cyber-attacks.
- Ensure compliance with all State and Federal laws, regulatory agencies, and retail industry standards.

Context:

- Executive management changes noted below may have shifted focus away from operational details.
    - 2005 – CEO resigns, new President named [19].
    - 2006 – New CEO named [20].
- Focused on rapid business expansion nationally and internationally during 2005-2007, may have contributed to less focus on existing processes.
- In 2006 TJX reduced corporate staff and cut its senior executive salaries [21], as part of its strategy for profitable growth by reducing costs. This may have created uncertainty within TJX impacting communications.
- No executive level role existed with exclusive responsibilities for cyber security risk management.

Unsafe Decisions and Control Actions:

- Inadequate or lack of policy related to protection and use of customer information.
- Safety culture non-existent. Priority given to cost savings at the expense of security infrastructure upgrades contributing to increased level of cyber security risk [18].

Process Model Flaws:

- Inadequate or incorrect understanding with reference to cyber security risks to TJX.
- Inadequate communication of priorities with reference to protection of customer information.
- Flawed view of security technology infrastructure.
    - Did not have information with reference to inadequacies highlighted at the physical system level.
- Unaware or not completely aware of PCI-DSS compliance issues.
- General lack of awareness on retail industry happenings with reference to well publicized cyber-attacks and prevailing WEP encryption issues.

Figure 4.7: CAST analysis of TJX Companies Management.

4.6.4 Regulatory Agencies

Next level up in the control structure is Regulatory Agencies, which enforce laws enacted by congress, address complaints of the public against businesses (for example, inadequate protection of consumer information by businesses), issue orders to businesses with reference to cyber security, and investigate and/or provide support to businesses in case of a cyber-attack. Regulatory Agencies control TJX by way of regulations, orders, and receive feedback via

quarterly and/or annual reports, as shown in Figure 4.1 (loop #2). An example of such an order to TJX is when Federal Trade Commission (FTC) initiated an investigation to ascertain if provisions of Federal Trade Commission Act have been violated that may have contributed to the TJX cyber-attack. Based on its investigations, FTC issued an order to TJX in 2008 with reference to company's payment card processing practices. An excerpt from the FTC decision [22] and order with reference to TJX information security policies is shown in Table 4.1; CAST analysis of Regulatory Agencies is summarized in Figure 4.8.

"IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."

Table 4.1: Excerpt of Federal Trade Commission's order to TJX [22].

Safety-Related Responsibilities:

- Ensure that companies and organizations are aware of their obligations with reference to payment card processing standards.
- Ensure compliance with provisions of laws enacted by US congress.
- Hear consumer complaints with reference to handling of personal information and issue orders to strengthen controls to protect public's private information.

Context:

- Most cyber security standards are voluntary and regulations written broadly [23], providing ample opportunities for misinterpretation.
- At the time of TJX cyber-attack, regulations existed for health insurance industry (The Health Insurance Portability and Accountability Act of 1996 (HIPPA)) and finance industry (Sarbanes–Oxley Act of 2002 (SOX)), but not for overall retail industry with reference to handling of customer information [23].

Unsafe Decisions and Control Actions:

- Inadequate regulation with reference to payment card processing and handling of customer information by the retail industry.

Process Model Flaws:

- In general, cybercrimes are seldom discovered while in progress due to inherent complexities in systems and there is not enough information in the wake of a cyber-attack that can identify regulatory weaknesses from a holistic perspective. Further forensic investigations have their own limitations. In case of the TJX cyber-attack, forensics experts from three major security companies tried to identify the hackers while they were still on TJX systems, but were not successful. These factors hamper learning from weaknesses in existing regulations in real time.

Figure 4.8: CAST analysis of Regulatory Agencies.

4.6.5 State Legislature

At this same level Massachusetts State Legislature also controls TJX Management by enacting laws, and providing incentives for businesses to stay competitive as a major regional economy. It receives revenues and feedback as shown in Figure 4.1 (loop #3). CAST analysis for State Legislature is summarized in Figure 4.9.

Safety-Related Responsibilities:

- Enact and/or review regulations for protecting information required for making purchases.
- Identify and regulate information that merchants can collect, and provide guidelines and standards with reference to retention period for business use.

Context:

- TJX is headquartered in MA contributing to state revenue and creating jobs.
- While protecting the public, state legislature wants to be business friendly and stay competitive for attracting businesses to the state. Balancing these opposing roles and responsibility poses challenges with reference to enforcement of regulations.

Unsafe Decisions and Control Actions:

- Lack of oversight of PCI-DSS compliance by businesses in Massachusetts.
    - PCI-DSS is a law in State of Nevada[13], but not in Massachusetts.
- Lack of regulation with reference to collection and retention period of customer information with reference to purchases or returns.

Process Model Flaws:

- Unaware of PCI-DSS compliance status of TJX.

Figure 4.9: CAST analysis of State Legislature.

4.6.6 Congress and Legislature

At the highest level of the control structure is Congress and Legislature, which provides a structure for businesses to operate nationwide by enacting laws and receives feedback from its agencies and businesses as shown in Figure 4.1 (loop #1). With reference to cyber security, US Congress is very actively involved and has laws on the books, and its agencies investigate data breaches. For example, US Secret Service was involved in investigating the TJX cyber-attack. CAST analysis of Congress and Legislature is shown in Figure 4.10.

Safety-Related Responsibilities:

- Protect US interests against cyber-attacks.
- Enact laws to prosecute cybercriminals.
- Provide resources for fighting cybercrime.

Context:

- Lobbyists campaign for less regulation.
- Cyber-attacks can be launched from anywhere in the world, making it challenging to enforce US laws and prosecute cybercriminals.

Unsafe Decisions and Control Actions:

- Inadequate laws with reference to payment card security standards.

Process Model Flaws:

- None.

Figure 4.10: CAST analysis of Congress and Legislature.

4.6.7 Systems Management

Along the system development part of the control structure moving up the hierarchical control structure, Systems Management controls the TJX Retail Store System (physical process) technology infrastructure including security technology (loop #6) in Figure 4.1. The control is exercised by way of system testing, maintenance, support, and implementation. Feedback is in the form of issues log and change requests. A second control (loop #18) in Figure 4.1 is for ongoing maintenance and support of systems at the physical process level. Feedback for loop

[13] *Source:* http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

#18 includes monitoring reports and system logs. CAST analysis of Systems Management is summarized in Figure 4.11.

4.6.7.1 Inadequate control/feedback

4.6.7.1.1 Monitoring of Wi-Fi network

In general most technologies including databases, websites, and computer networks have a monitoring process as part of maintenance plan. For example, general practice for databases is to use automated scripts for monitoring database connections, long running queries, etc., and most technologies have maintenance tools embedded within the install which generally require to be activated. At the TJX physical process level, hackers were connected to the Wi-Fi network but their presence was never detected. Monitoring networks is not complicated, and in case of TJX hackers joined the network that was open to anyone, accounts not belonging to TJX could have been easily identified if a report was produced based on scan of network connections. Lack of monitoring with reference to unauthorized connections and missing feedback were contributing factors that weakened control and provided inadequate feedback.

4.6.7.1.2 Security technology operations

Per the CAST analysis of the physical process, it was revealed that the AP was configured incorrectly, which was the vulnerability that allowed access to hackers in the first place. At the physical process level, AP was doing its job by providing Wi-Fi connectivity – albeit to anyone within range of AP, it was the responsibility of Systems Management to implement and maintain technology. A lack of proper configuration points to inadequate training, specifically in managing security technology.

4.6.7.1.3 System maintenance

TJX was in the practice of using actual customer payment card data for resolving system issues and ongoing maintenance [14]. This practice points to lack of guidance and policies with reference to use of actual payment card data for routine maintenance and problem solving.

Safety-Related Responsibilities:

- Must implement and maintain security technology per TJX requirements, that can include:
  - Policy for password format and expiry.
  - Configuration parameters for security technology, for example, access point (AP).
- Must monitor stores Wi-Fi network for unauthorized usage.
  - Usage implies unauthorized connections and data traffic. Any account id not created by Systems Management, that is using the network should trigger an alert. Further, unusual amount of data traffic generated should also trigger an alert.
  - Additional criteria for alerts can include time and/or duration of a network connection, for example, if an account id is joining the network when the store is closed or is connected for long periods of time.
- Effectively communicate to management current TJX security technology infrastructure requirements, in view of prevailing external security technology environment and industry trends.

Context:

- In 2005, there were over 2000 retail stores to support and monitoring of system logs can be a complex task, which would require resources to implement a robust monitoring system.

Unsafe Decisions and Control Actions:

- Inadequate or lack of monitoring with reference to networks.
- Misconfiguration of access points (AP) at retail stores.
- Use of deprecated WEP encryption technology.

- Inadequate monitoring of TJX corporate servers for unauthorized access and installation of malicious software.
- Performed inadequate testing of payment card processing systems.
- Use of actual customer payment card data for resolving system issues, leading to retention of sensitive customer information unrelated to a purchase transaction.

Process Model Flaws:

- Unaware of retail industry standards.
    - As discussed in the CAST analysis of the physical process, there were several weaknesses at that level, which included misconfigured AP and lack or inadequate monitoring of systems at the physical process level. PCI-DSS covers both of these and other issues mentioned at the physical process level. Further implementing and monitoring of security/other technology at the physical process level is the responsibility of Systems Management. Therefore, a plausible explanation here is that even if there was an absence of training or install procedures, more detailed knowledge of PCI-DSS may have prevented some or all issues at the physical process level.
- Missing or incorrect process/checklist for implementing/maintaining security technology infrastructure.
    - AP at Marshalls store was configured to grant access to network without authentication, a checklist of desired configuration parameters accessible across Systems Management might have helped in preventing AP misconfiguration.

Figure 4.11: CAST analysis of Systems Management.

4.6.8 Project Management

Next level up along the development part is Project Management that controls Systems Management as shown in Figure 4.1 (loop #5). Project Management reports to the TJX CIO. The control variables are system requirements – generated from system needs provided by Operations Management and TJX Management, specifications – generated based on system requirements, processes – based on company guidelines, procedures for execution, and resource allocations for projects. Feedback is in terms of reports which include, project status, system performance, technology assets inventory, and status of existing technology infrastructure with reference to age and need for upgrades. CAST analysis of Project Management is summarized in Figure 4.12.

Safety-Related Responsibilities:

- Incorporate PCI-DSS security standards and TJX business rules in the design of payment card processing systems.
- Perform rigorous testing of systems in collaboration with internal TJX customers.
- Conduct periodic reviews of security infrastructure and maintain updated documentation related to configuration parameters and installation procedures.
- Provide adequate training to personnel for maintaining and operating security technology infrastructure.

Context:

- Project Management is a cost center because it has a support role and not directly contributing to sales. Being a cost center, funding is always a challenge and therefore focus on cost savings can lead to inaccurate cyber security risk assessments. This is evident in the memo from the CIO where upgrade from deprecated encryption algorithm was delayed in favor of cost savings [18].
- Lack or inadequate executive management support for implementing PCI-DSS standards, because cost was favored over critical security upgrades [18].

- TJX was using weak encryption algorithm WEP for approximately two years without a breach, while an updated version WPA was under developed. This may have reinforced a false sense of security and contributed to lack of urgency with reference to upgrading to a stronger encryption algorithm.
- TJX was one of the early adopters of the new Wi-Fi technology – implemented it within a year, which would have required significant investments in infrastructure and training. It is plausible that the pressure of seeing ROI on investments may have conflicted with providing rigorous training leading to inadequately trained people managing security technology infrastructure. Additionally, because the Wi-Fi technology was so new there was no accumulated knowledge base to draw upon in order to avoid mistakes.

Unsafe Decisions and Control Actions:

- Decision not to upgrade to a stronger encryption algorithm and continued to use deprecated WEP, for over two years.
- Inadequate systemic understanding of PCI-DSS impact, that led to use of deprecated encryption algorithm, AP misconfiguration, and transmitting unencrypted customer information to name a few issues.
- Lack of policy or inadequate communication with reference to use of actual customer payment card data as a test dataset for resolving system issues. Therefore exposing customer payment card data to increased cyber security risks.

Process Model Flaws:

- Lack of/inadequate awareness or understanding of PCI-DSS details.
    - This is evident from data retention period issue, and storage and transmission of unencrypted customer information.
- Inadequate general knowledge of prevailing security issues within retail industry. There were a few other cyber-attacks by the same group of hackers on retailers in the same general geographical area as TJX.

Figure 4.12: CAST analysis of Project Management.

4.6.9 TJX Companies Management (System Development Part)

Next level up is TJX Companies Management that controls Project Management and is responsible for providing system needs, RFP, procedures, technology strategy, and budget for Project Management. It receives feedback in form of reports that include financial, system proposals, and project status as shown in Figure 4.1 (loop #4). Control on Project Management is exercised by TJX Companies Management in the context of the office of Chief Information Officer (CIO). CAST analysis of TJX Companies Management in this context is shown in Figure 4.13.

Safety-Related Responsibilities:

- Ensure that TJX business needs are met by technology solutions.
- Ensure that measures are implemented for protecting TJX information assets and technology infrastructure against cyber-attacks.
- Ensure compliance of technology with retail industry standards and business rules.

Context:

- CIO under constant pressure to keep costs in check while balancing business needs.
- Executive management changes in 2005-2006, reduced corporate staff, and cut in senior executive salaries [21], may have contributed to additional pressure on the CIO with reference to cost containment.
- No dedicated role for cyber security risk management existed. CIO is responsible for all

companywide technology projects including cyber security.

Unsafe Decisions and Control Actions:

- Safety culture non-existent. Priority given to cost savings at the expense of security infrastructure upgrades contributing to increased level of cyber security risk [18].
- Lack of effective communication at TJX Management level with reference to support needed from the business to implement PCI-DSS.
- Decision to not upgrade to a stronger encryption algorithm.

Process Model Flaws:

- Inaccurate or incorrect understanding of TJX security technology with reference to exposure to cyber security risks.
- Lack of communication explicitly addressing customer information management.
- Inadequate general knowledge of prevailing cyber security issues within retail industry.
- Inadequate understanding of PCI-DSS compliance with a focus on technology attributes only [18].

Figure 4.13: CAST analysis of TJX Companies Inc. Management.

4.7 Step #7: Coordination and Communication

CAST analysis has revealed five key coordination and communication weaknesses that contributed to the TJX cyber-attack and are discussed below.

- Payment Card Processing System is controlled by Operations Management (loop #8), and interacts with Fifth Third Bancorp (loop #11). Fifth Third Bancorp is responsible for ensuring that TJX is compliant with PCI-DSS and was relying on TJX to satisfy all twelve requirements of PCI-DSS. On the other hand, in general at TJX there was a lack of needed support from executive management with reference to PCI-DSS, a general prevailing view that PCI-DSS compliance is a technology issue, view that First Third Bancorp compliance implies TJX compliance, and finally TJX continued activities that were in violation of PCI-DSS.

  This conflict in views with reference to PCI-DSS responsibilities between First Third Bancorp and TJX contributed to lack of coordination in fully implementing PCI-DSS at TJX, and hampered communications between development and operations. Further, it is logical to assume that signals of soft view on PCI-DSS from senior management would be taken as tacit approval for weak or no compliance with PCI-DSS at lower levels, exacerbating communication and coordination issues.
- Cyber security risk posed by use of WEP was well understood within TJX [18], but because PCI-DSS was not a priority and viewed as technology project, the risks were not effectively communicated at the executive level. Further, there was no dedicated role within TJX that was responsible for managing cyber security risks companywide. In other words there was not a single role that would coordinate activities related to cyber security risk management across TJX.

  Specifically, in Figure 4.1 Payment Card Processing System was receiving compliance criteria from Fifth Third Bancorp (loop #11) that was being passed onto Operations Management via feedback channel (loop # 8). From here on it is not clear what level of details did TJX Management Company received or were explained to them with reference to PCI-DSS compliance, but as is evident from the CIO memo [18] (see Table 4.3 which is discussed later) there was a degree of awareness at the executive level and compliance was viewed more of a technology issue. Also, as is evident from the staff responses to the CIO memo with reference to postponing security technology upgrades in favor of costs as

shown in Table 4.2, parts of system development were very aware of the risks posed by continued use of deprecated encryption algorithm. But communication appears to be inadequate at the executive level, most likely due to lack of focus, priority, and awareness, because at the executive level CIO was the only technology representative and responsible for all of TJX technology programs, with cyber security as one of several initiatives during a period of high growth and profits in early/mid 2000.

IT staffer Lou Julian response:	*"Saving money and being PCI-compliant is important to us, but equally important is protecting ourselves against intruders. Even though we have some breathing room with PCI, we are still vulnerable with WEP as our security key. It must be a risk we are willing to take for the sake of saving money and hoping we do not get compromised."*
IT staffer Richard Ferraioli response:	*"The absence of rotating keys in WEP means that we truly are not in compliance with the requirements of PCI. This becomes an issue if this fact becomes known and potentially exacerbates any findings should a breach be revealed."*

Table 4.2: Staff responses to the TJX CIO memo **[18]**.

It is plausible to conclude that CIO was prioritizing budget spending with projects that had the greatest impact on the bottom line, and because CIO was representing a cost center and not revenue generating function, therefore question of CIO's influence at executive level is also a factor, contributing to lack of proliferation of PCI-DSS requirements throughout TJX.

- Disconnect between the views of CIO and his staff, and a general tendency of the executive management to view cyber security as a technology issue contributed to lack of coordination/communication between system development and system operations during system design. For example, in loop #16 with reference to PCI-DSS, Operations Management was aware of the compliance criteria but due to lack or inadequate support from executive management those system needs were either not communicated to Project Management or communicated in incomplete form. For this reason, those needs never fully flowed down to Systems Management (loop #5) for integration during system development and testing of Payment Card Processing System via loop #17. This break in communication and lack of coordination in views exposed Payment Card Processing System to greater cyber security risks, which included unencrypted transmission of customer payment card information.
- TJX lacked or there were inadequate capabilities with reference to a central shared knowledge database housing compliance requirements, specifically PCI-DSS requirements. Visibility and availability of compliance requirements across the organization may have contributed to better communication with reference to PCI-DSS compliance.
- Another coordination and communication issue was within the Systems Management component that is responsible for both implementation and maintenance/support of systems at the physical process level. As shown in Figure 4.1, loop #6 is concerned with testing and implementation of systems, and loop #18 is responsible for providing ongoing support and monitoring in the post implementation phase. Based on the CAST analysis of the physical process which revealed weak controls it can be concluded that there is lack of coordination and communication between implementation and maintenance teams.

4.8 Step #8: Dynamics and Migration to a High-Risk State

According to Leveson, most major accidents are a result of migration of a system to a high-risk state over time. Understanding the dynamics of migration will help in redesigning the system [12]. This CAST step discusses some operational and behavioral aspects revealed during analysis that contributed to the TJX cyber-attack.

A major change that contributed to the cyber-attack was TJX's move from wired to wireless networking (Wi-Fi) in 2000 in a short span of one year – Wi-Fi became available in 1999. At that time cyber security risk was at its lowest level because vulnerabilities in the wireless WEP encryption algorithm were unknown to everyone – experts, businesses, and hackers. By 2003, the environment had changed because the inherent weaknesses of WEP became publically known and widely published in academia which hackers started to exploit for launching cyber-attacks. TJX decided against upgrading to a more secure encryption algorithm for cost reasons, and ultimately was a victim of a cyber-attack in 2005.

Further, TJX's short implementation timeframe for a major technology leap introduced additional risk. For example, it is plausible that TJX security technology team's lack or inadequate experience and/or training led to misconfiguration of AP's that allowed, hackers to join TJX Wi-Fi network without detection. Same reasoning may also explain the lack of monitoring of Wi-Fi network for data traffic load and unauthorized connections.

Lack of full compliance with PCI-DSS also contributed to the cyber-attack, because as the security technology environment changed between 2000 and 2003 with the revelation of inherent flaws in encryption algorithm, complying with PCI-DSS also became more critical. TJX was unable to adopt all twelve PCI-DSS requirements in a timely fashion and gradually moved towards a state of higher cyber security risk.

Overtime, from 2000 until the cyber-attack in 2005, the cybercrime ecosystem became increasingly sophisticated (e.g., tools for braking into systems become widely available.) As the cyber security risks increased, TJX did not have a dedicated role for managing these risks, further contributing to an already high level of exposure to a cyber-attack. This also led to an inaccurate assessment of risk posed by the use of deprecated encryption algorithm.

Further, flaws in managerial decision making process may also have been a factor with reference to migrations towards a higher risk state. Biases can contribute to flawed decisions by managers. One such bias is *ease of recall bias* that relates to decision making process where memories and recent experiences strongly influence the decision. For example, people are more likely to purchase insurance for an event that they have just experience than to purchase it before the event occurred [24]. That is, availability of information biases a decision, or formally stated, ease of recall bias emanates from availability heuristic [24]. With this context in mind, TJX was using encryption technology with vulnerabilities for more than two years before the cyber-attack[14] and continued to do so until the cyber-attack was discovered. Having no memory of a breach at TJX due to use of deprecated encryption technology and oblivious to cyber-attacks at other retailers, it is plausible that availability heuristic played a role in management's decision to not upgrade to a stronger encryption in favor of cost savings [18].

Another behavioral aspect is, a decision maker's tendency to favor/seek information that confirms his/her own beliefs and discount contradicting information when making a decision is called *confirmation trap* [24]. This bias may also have played a role in TJX's

[14] Although the cyber-attack was launched in middle of 2005, TJX was not aware and continued to use WEP encryption until fraudulent charges stared appearing on TJX customer statements – TJX was alerted by a credit card company of a possible data breach.

migration to a higher risk state. Table 4.3 depicts a message from the TJX CIO Paul Butka in November 2005 to his staff [18], with reference to security technology upgrades. In this memo, Mr. Butka is requesting agreement on his belief that cyber security risk is low. In response there were only two opposing views on record from his staff (see Table 4.2), very likely a minority and therefore majority of his staff agreed with his assessment that risk was low. This confirmation trap led to postponing upgrades, therefore migrating security technology infrastructure to higher risk of a cyber-attack.

"My understanding [is that] we can be PCI-compliant without the planned FY07 upgrade to WPA technology for encryption because most of our stores do not have WPA capability without some changes," Butka wrote. "WPA is clearly best practice and may ultimately become a requirement for PCI compliance sometime in the future. I think we have an opportunity to defer some spending from FY07's budget by removing the money for the WPA upgrade, but would want us all to agree that the risks are small or negligible."

Table 4.3: TJX CIO memo regarding security technology upgrade [18].

4.9 Step #9: Recommendations

Based on STAMP/CAST analysis following are some key recommendations, that can help TJX and other such organizations in managing cyber security risks more effectively in the future.

- A dedicated executive role with cyber security responsibilities and authority for executing cyber security risk management policies, will allow for a consistent view of TJX security technology across the organization. Further, it will also help with better coordination between System Development and System Operations, integration of compliance requirements during system design, and with communication and proper framing of security technology risks. As an analogy, in general investment firms have compliance departments with a fully staffed executive role and authority to ensure compliance with SEC rules. Compliance oversees trading transactions for any irregularities (for example, insider trading) not only within the firm, but employees are also required to submit their holdings including those of their spouses. Similarly, a dedicated role for cyber security will be more effective in managing cyber security risks, ensuring compliance with PCI-DSS.
- According to PCI Security Standards Council, compliance is a business issue requiring management attention and is an ongoing process of assessment, remediation and reporting. The risk of non-compliance affects the whole organization because of financial and goodwill costs. Therefore TJX needs to understand and communicate effectively the risks of non-compliance and importance of integrating PCI-DSS early in the system lifecycle on a voluntary basis. One approach can be to integrate PCI-DSS requirements within appropriate components in development and operations parts of the control structure. CAST is not arguing that doing so would ensure full protection against a cyber-attack, but rather it will help manage the risk more effectively. Further this approach will ensure that TJX is shielded from significant financial liability, because TJX was fined $880,000 by VISA for non-compliance with PCI-DSS, and in addition TJX settled with VISA for $41 million related to costs associated with the loss of customer information from the cyber-attack [25]. Clearly, benefits of investments in proactively managing PCI-DSS compliance by TJX outweigh the potential costs of non-compliance.
- With managements support, building a safety culture at TJX can help reduce risks of a future cyber-attack significantly. Specific steps can include:

    - Identifying safety critical systems, trends, processes, and procedures with reference to cyber security. For example, these *safety critical entities* can include encryption technology, hardware components (AP, servers, etc.), data retention/disposal/archival polices, a list of Key Threat Indicators (KTI) (KTI can be network traffic beyond an established threshold at TJX stores, number of network connections at odd hours of the day, etc.) to include in monitoring metric, and prevailing cyber security trends.
    - After safety critical entities are documented, then implement a plan to manage these entities with periodic reviews to update the list of safety critical entities.
- Understand limitations and objectives of standards and align them with cyber security and business needs of an organization. For example, if TJX was in full compliance with PCI-DSS, it would have reduced TJX liability significantly and would have been a good business decision. But from the technology perspective it will still leave TJX systems exposed to cyber security risks. For example, consider PCI-DSS data standard which states that "encrypt transmission of cardholder data across open, public networks [13]". PCI-DSS does not explicitly state that data must be encrypted when transmitted within TJX – that is over the *intranet or behind a firewall*, but only when it is sent over a public network. Clearly, after understanding the method used to launch the cyber-attack, TJX would want to encrypt sensitive data at all times as it flows through its systems over the intranet or internet. Another example is that PCI-DSS did not explicitly mandate using stronger encryption WPA until 2006, even though WPA was available in 2003 . Earlier recommendations with reference to safety culture and a dedicated cyber security role would allow addressing these gaps.
- Review and design systems architecture for Payment Card Processing System, so that customer data is dispersed across servers and databases. For example, store and process payment card number and expiration attribute on different servers.

With these recommendations analysis of TJX cyber-attack using STAMP/CAST is complete. It can be observed that CAST highlighted system-level insights that otherwise could have been overlooked if another method of analysis was used.

5 Comparing STAMP/CAST with Federal Trade Commission (FTC) and Canadian Privacy Commission (CPC) Findings

This section presents comparisons between selected STAMP/CAST recommendations, and actions proposed by the Canadian Privacy Commission (CPC) and the Federal Trade Commission (FTC.) CPC conducted its own investigation, because Canadian customers of TJX were also impacted by the cyber-attack, and suffered personal information losses. FTC believed that TJX had violated provisions of the Federal Trade Commission Act, and launched an investigation. Table 5.1 shows a list of recommendations with the source, each of which is discussed next.

Both FTC and STAMP/CAST generated recommendation #1 albeit with a difference. FTC proposed designating an *employee or employees* to be accountable for information security

No.	Recommendation	CPC	FTC	STAMP/CAST

1	Create an executive level role for managing cyber security risks.	No	*[15]	Yes
2	PCI-DSS integration with TJX processes.	No	No	Yes
3	Develop a safety culture.	No	No	Yes
4	Understand limitations of PCI-DSS and standards in general.	No	No	Yes
5	Review system architecture.	No	No	Yes
6	Upgrade encryption technology.	Yes	No	No
7	Implement vigorous monitoring of systems.	Yes	No	No
8	Implement information security program.	No	Yes	*

Table 5.1: Comparison of STAMP/CAST recommendations with FTC and Canadian Privacy Commission.

program. CAST specifically recommends an executive level role for managing cyber security risks, because of the systemic weaknesses revealed and discussed in our analysis. With reference to recommendations #2, #3, #4, and #5 in Table 5.1 all were generated by STAMP/CAST and have been discussed, but omitted by CPC and FTC.

Recommendations #6 and #7 were explicitly proposed by the CPC as noted in Table 5.1. Lack of encryption and monitoring of systems at TJX were identified as major contributors to the cyber-attack by CPC. STAMP/CAST analysis addressed the question of *why* these controls were weak or non-existent at systemic level. STAMP/CAST analysis identified causal factors and revealed non-linear issues at TJX which led to weakening or lack of these controls. Although, STAMP/CAST analysis did not explicitly provide Recommendations #6 and #7, the insights from accident analysis addressed these issues by way of Recommendations #1, #2, and #3. With reference to recommendation #8 provided by FTC it is an important point. FTC recommendations as documented in its order [22] are vague which can lead to confusion on part of TJX. For example, FTC order states that TJX "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers" [22]. TJX already had in place security measures to protect customer information, but the controls were inadequate, missing, or failed due to systemic issues revealed by STAMP/CAST analysis. STAMP/CAST analysis on the other hand covers FTC proposal in all five of its recommendations and provides specifics. For example with reference to PCI-DSS, insights based on STAMP/CAST are actionable steps.

From on this discussion it can be observed that STAMP/CAST analysis, provided insights that other investigations either did not reveal or revealed in incomplete form, therefore STAMP/CAST based analysis can be a valuable supplement for understanding cyber-attacks and specifically systemic causes leading to increased cyber security risks.

6 Contributions

Our research focused on proposing a new way of approaching and managing cyber security risks, based on Systems Thinking and Systems Theory. Our research question was to see if STAMP is effective in identifying causal factors underlying a cyber-attack. Application of STAMP to the TJX case study highlighted that STAMP *can be* effective in analyzing cyber-

[15] Indicates recommendations that are close to STAMP/CAST based analysis but also has differences.

attacks. The analysis revealed insights, which might otherwise be difficult or impossible to gain using traditional technology focused approaches.

It is worth noting that the TJX case was written using publically available sources, and court documents, meaning without any access to TJX official internal documents. Further, cyber security is a sensitive issue for businesses, and getting access to detailed cyber-attack information is very challenging with reference to public companies. But, insights derived from CAST analysis based on limited publically available information still provided valuable actionable items, supporting the research findings that CAST can be an effective model for managing cyber security risks. Main contributions of this paper include:

- Highlighted a need for System Thinking and Systems Theory based approach for managing cyber security risks.
- Introduced STAMP/CAST in the context of cyber security.
- Proposed STAMP/CAST as a new approach for managing cyber security risks
- Applied STAMP/CAST to TJX cyber-attack case providing new insights including:
    - Highlighted general limitations of standards, and specifically with reference to PCI-DSS, noted a flaw in PCI-DSS requirements that would leave a business exposed to risk, because the requirement does not mandate encryption of data over the intranet. Lesson here is that standards are good which can also help deflect financial liabilities, and in many situations are required by law. But the key is in understanding what a standard *cannot* achieve and then address those vulnerabilities.
    - Highlighted systemic causes that led to the TJX cyber-attack.
    - Highlighted behavioral aspects that contributed to the TJX cyber-attack.

References

[1] S. Savage and F. B. Schneider, Feburary 2009. [Online]. Available: http://www.cra.org/ccc/files/docs/init/Cybersecurity.pdf. [Accessed 18 September 2013].

[2] I. Wladawsky-Berger, "Complex Sociotechnical Systems: the Case for a New Field of Study," Irving Wladawsky-Berger, Cambridge, MA, 2012.

[3] P. M. Senge, The Fifth Discipline, 1st ed., New York: Doubleday/Currency, 1990, pp. 68-69.

[4] N. G. Leveson, "Accident Models," in *Safeware*, Addison-Wesley, 1995, pp. 185-224.

[5] N. G. Leveson, "Questioning the Foundations of Traditional Safety Engineering," in *Engineering a Safer World: Systems Thinking Applied to Safety*, Cambridge, MA: MIT Press, 2011, pp. 7-60.

[6] N. G. Leveson, "A New Accident Model for Engineering Safer Systems," *Safety Science*, vol. 42, no. 4, pp. 237-270, 2004.

[7] N. G. Leveson, "Fault Tree Analysis," in *Safeware*, Addison-Wesley, 1995, pp. 317-326.

[8] N. G. Leveson, "Fundamentals of System Safety," in *Safeware*, Addison-Wesley, 1995, pp. 145-168.

[9] International Organization for Standardization (ISO), "ISO/IEC 27002:2005," International Organization for Standardization (ISO), [Online]. Available: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=50297. [Accessed 8 March 2014].

[10] N. G. Leveson, "A Systems-Theoretic View of Causality," in *Engineering a Safer World: Systems Thinking Applied to Safety*, Cambridge, The MIT Press, 2011, pp. 73-102.

[11] N. G. Leveson, "Systems Theory and Its Relationship to Safety," in *Engineering a Safer World: Systems Thinking Applied to Safety*, Cambridge, MA: MIT Press, 2011, pp. 61-72.

[12] N. G. Leveson, "Analyzing Accidents and Incidents (CAST)," in *Engineering a Safer World: Systems Thinking Applied to Safety*, Cambridge, The MIT Press, 2011, pp. 350-390.

[13] PCI Security Standards Council, "Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures," PCI Security Standards Council, Wakefield, MA USA, 2013, Version 3.0.

[14] THE TJX COMPANIES, INC., "FORM 10-K," THE TJX COMPANIES, INC., Framingham, 2007.

[15] VISA, "How a Visa Transaction Works," VISA, 2014. [Online]. Available: http://usa.visa.com/merchants/become-a-merchant/how-a-visa-transaction-works.jsp. [Accessed 26 March 2014].

[16] VISA, "Card Acceptance Guidelines for VISA Merchants," 2011. [Online]. Available: https://usa.visa.com/download/merchants/card-acceptance-guidelines-for-visa-merchants.pdf. [Accessed 26 March 2014].

[17] PCI Security Standards Council, "About the PCI Security Standards Council," PCI Security Standards Council, 2014. [Online]. Available: https://www.pcisecuritystandards.org/organization_info/index.php. [Accessed 26 March 2014].

[18] Ericka Chickowski, "TJX: Anatomy of a Massive Breach," *Baseline,* pp. Issue 81, p28, 30 January 2008.

[19] TJX, "Press Release - CEO Resigns," TJX, 13 September 2005. [Online]. Available: http://investor.tjx.com/phoenix.zhtml?c=118215&p=irol-newsArticle&ID=756155&highlight=. [Accessed 15 March 2014].

[20] TJX, "Press Release - New CEO," TJX, 7 September 2006. [Online]. Available: http://investor.tjx.com/phoenix.zhtml?c=118215&p=irol-newsArticle&ID=903202&highlight=. [Accessed 16 March 2014].

[21] TJX, "Press Release - TJX Staff Reductions," TJX, 8 March 2006. [Online]. Available: http://investor.tjx.com/phoenix.zhtml?c=118215&p=irol-newsArticle&ID=829093&highlight=. [Accessed 16 March 2014].

[22] Federal Trade Commission (FTC), "Cases and Proceedings (TJX DECISION AND ORDER, DOCKET NO. C-4227)," 1 August 2008. [Online]. Available: http://www.ftc.gov/enforcement/cases-proceedings/072-3055/tjx-companies-inc-matter. [Accessed 16 April 2014].

[23] Wikipedia, "Cyber-security Regulation," Wikipedia, 7 November 2013. [Online]. Available: http://en.wikipedia.org/wiki/Cyber-security_regulation. [Accessed 20 March 2014].

[24] M. H. Bazerman and D. Moore, Judgement in Managerial Decision Making, Hoboken, NJ: John Wiley & Sons, Inc., 2009.

[25] S. Romanosky and A. Acquisti, "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives," *Berkeley Technology Law Journal,* vol. 24, no. 3, pp. 1078-1081, 2014.