Cyber Safety: A Systems Theory Approach to Managing Cyber Security Risks – Applied to TJX Cyber Attack

Hamid Salim
Stuart Madnick

Working Paper CISL# 2016-09

August 2016

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

Cyber Safety: A Systems Theory Approach to Managing Cyber Security Risks – Applied to TJX Cyber Attack

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 MIT School of Engineering
smadnick@mit.edu

Abstract
To manage security risks more effectively in today's complex and dynamic cyber environment, a new way of thinking is needed to complement traditional approaches. In this paper we propose a new approach for managing cyber security risks, based on a model for accident analysis used in the Systems Safety field, called System-Theoretic Accident Model and Processes (STAMP). We have adapted and applied STAMP to cybersecurity, which we call Cybersafety, and used it to analyze the cyber-attack on TJX, the largest at that time. Our analysis revealed insights which had been overlooked in prior investigations. The lessons learned from this analysis can be extended to address ongoing challenges to cyber security.

1 Introduction

Cybercrime is impacting a broad cross section of our society. The cyber environment is continuously evolving as world continues to become more connected contributing to increasing complexity. This also introduces more opportunities for hackers to exploit new vulnerabilities.

The insight that motivated this research was that significant efforts and progress has been made in past decades at methods for reducing industrial accidents, such as System-Theoretic Accident Model and Processes (STAMP). Although there are definite differences between cyberattacks and accidents, e.g., deliberate action versus unintentional, there are also significant similarities that can be exploited.

The idea of using safety approaches to address cyber security concerns had been mentioned previously [1], [2], [3], [4] . In [5], the authors briefly suggest that the STAMP safety methodology can be used to prevent or mitigate cyber-attacks. To the best of our knowledge, this paper is the first STAMP-inspired detailed analysis, which we call Cybersafety, of a major cyber-attack, TJX. This paper attempts to understand reasons for the limited efficacy of traditional approaches, and to evaluate the effectiveness of Cybersafety.

To apply Cybersafety, 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'." [6]. Furthermore, Cybersafety takes a top-down approach. That is, it focuses on what needs to be protected or prevented. As a simple example, imagine that your organization has 1000 doors that should be locked at night. A bottom-up approach would expend considerable energy trying to have all doors locked. A top-down approach would focus most energy on the doors that pose a hazard that could impact that which is to be protected.

2 Literature Review

There have been various approaches proposed for addressing cybersecurity, such as Chain-of-Events Model and Fault Tree Analysis (FTA). In addition, we looked at other widely used frameworks for cyber security best practices. We found all these methods limited. Existing cyber security approaches mostly focus on technical aspects, with goal of creating a secure fence around technology assets of an organization. This limits systemic thinking for three main reasons: First, it does not view cyber security holistically at an organizational level, which includes people and processes. Second, focus on security technology reinforces the perception that it is solely an Information Technology department problem. Third, within the context of the cyber ecosystem, focusing only on a technical solution ignores interactions with other systems/sub-systems operating beyond an organizational boundary.

We argue that technical approaches address only a subset of cyber security risks. Savage and Schneider [7] 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 that people and management are essential dimensions of any successful holistic cyber security strategy. That view is explicitly addressed in this paper using Cybersafety analysis, which is based on STAMP.

3 System-Theoretic Accident Model and Processes (STAMP) Framework

In STAMP, to understand causal factors leading to an accident requires understanding *why* a control was ineffective. The 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.

Safety constraints are critical, missing or lack of enforcement of relevant constraints leads to elevated safety risks, which may cause loss event(s). In the hierarchical safety control structure, a higher level imposes constraints over the level immediately below it, as depicted in Figure 3.1. If these control processes are ineffective in controlling lower level processes and safety constraints are violated, then a system can suffer an accident.

Four factors may contribute to inadequate control at each level of a hierarchical structure: missing constraints, inadequate safety control commands, commands incorrectly executed at a lower level, or inadequate communication or feedback with reference to constraint enforcement [8]. 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 3.2, the downward channel is used for providing information in order to impose constraints and the upward channel is used to measure effectiveness of constraints at the lower level.

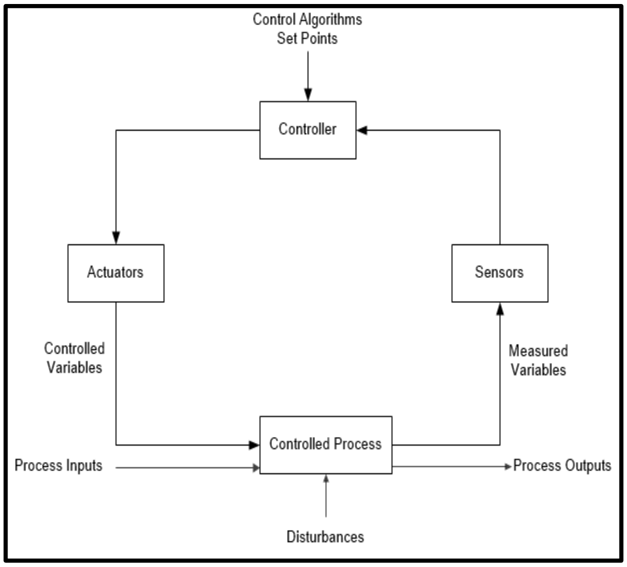

Figure 3.1: Standard control loop **[9]**.

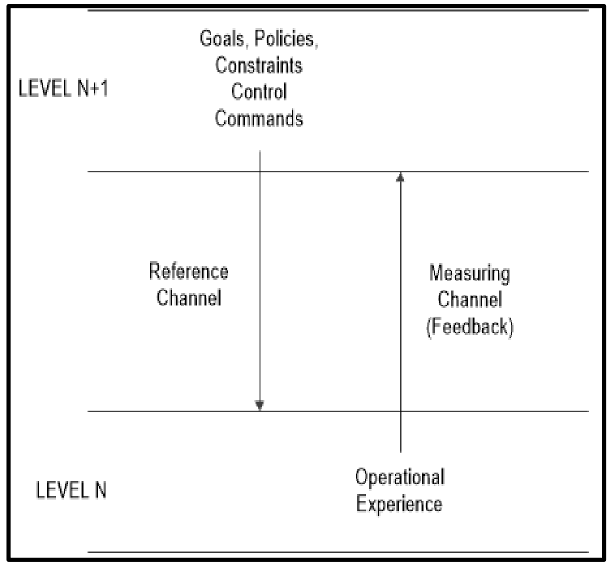

Figure 3.2: Communication channels in a hierarchical safety control structure [8].

The third concept is the process model. There are four conditions necessary to control a process as shown in Table 3.1.

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

STAMP can be used both for hazard analysis (Ex-ante) and accident analysis (Ex-post). In hazard analysis the goal is to understand scenarios and related causal factors that can lead to a loss, and implement countermeasures 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, though the ex-ante analysis is quite similar.

3.1 Causal Analysis based on STAMP (CAST)

CAST allows us to go beyond a single failure event and analyze a broader sociotechnical system, to understand systemic and non-systemic casual factors [10] and helps understand *why* loss occurred, and implement countermeasures to prevent future accidents or incidents. CAST emphasizes people's behaviors and what caused a certain behavior that led to an accident or incident [10]. CAST analysis is a nine step process, listed in Table 3.2. Analysis can be performed in any order. In the following sections, we will perform CAST analysis applied to a cyber-attack rather than an industrial accident. We will refer to this analysis method as Cybersafety.

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[1], controls for executing relevant responsibilities, and feedback channel.
2	Identify system safety constraints and system requirements associated with that hazard.	
3	Document safety control structure in place to control hazard and ensure compliance with the safety constraints.	
4	Ascertain proximate events leading to 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 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	Move up levels of the hierarchical safety control structure, establish how and why each successive higher level control allowed or contributed to inadequate control at the current level.	After deficiencies have been identified, next step is to investigate causes for those deficiencies. This requires understanding higher levels of hierarchical safety control structure, requiring consideration of overall sociotechnical system focused on *why* controls were deficient. This is in contrast to Chain of Events Model where 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 dynamics and changes in the system and the safety control structure relating to an accident or incident, and any weakening of safety control structure over time.	Most accidents/incidents occur when a system migrates towards a higher risk state *over time*. Understanding dynamics of this migration towards less safe and secure environment will help with implementing appropriate countermeasures.
9	Generate recommendations.	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 3.2: CAST steps for analyzing accidents **[10]**.

4 TJX Cyber-Attack

TJX cyber-attack was one of a series of attacks, executed as part of operation *Get Rich or Die Tryin'* and continued for five years until 2008. The ring leader, Albert Gonzalez, was even the focus of an episode of the television show *American Greed* [11].

[1] Components can be electromechanical, digital, human, or social. *Source:* [19]

As 2006 holiday season was coming to a close, TJX was working to address breach of its computer systems. On January 17, 2007, TJX announced that it was a victim of unauthorized intrusion. The breach was discovered on December 18, 2006, and payment card transaction data of approximately 46 million customers had been potentially stolen. The cyber-attack was, at the time, the largest in history, measured by number of payment card numbers stolen.

The cyber-attack highlighted operational and IT related weaknesses, which will be studied further using Cybersafety. The goal of the analysis is to understand *why* weaknesses existed and if/how they contributed to the cyber-attack.

5 Cybersafety Analysis of the TJX Cyber-Attack

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

5.1.1 System(s)

Cyber-attack resulted in loss of payment card data, and TJX suffered financial losses of over $170 million. To understand why the hackers were able to steal so much of information without detection, the system to be analyzed is ***TJX payment card processing system***.

5.1.2 Hazard(s)

The hazard to be avoided is ***TJX payment card processing system allowing unauthorized access***.

5.2 Step #2: System Safety Constraints and System Requirements

1. TJX must protect customer information from unauthorized access.
2. TJX must provide adequate training for managing technology infrastructure.
3. Measures must be in place to minimize losses from unauthorized access including:
    3.1. TJX must communicate with payment card processors to minimize losses.
    3.2. TJX must work with law enforcement and private cyber security experts.
    3.3. TJX must provide support to customers whose information may have been stolen.

5.3 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 [10].

Figure 5.1 shows the hierarchical system safety control structure. Dotted arrows and boxes indicate development part of the control structure, and solid arrows and boxes indicate operational part. Each box (dotted or solid) represents a component. Dashed rectangle labeled as *System Boundary* indicates boundary of the system to be analyzed. Numbers represent control structures with control and feedback channels forming a loop. Physical processes (discussed in forthcoming sections) are identified by dashed oval.

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). Second interaction is between Systems Management and Payment Card Processing System (loop #17), and third interaction is between Systems Management and TJX Retail Store System (loop #18).

5.4 Step #4: Proximate Event Chain

Event chain analysis is not capable of providing critical information with reference to causality of an accident, but basic events of the cyber-attack are identified for understanding physical process involved in the loss [10].

Normally in CAST proximate 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 actual loss occurred. In the TJX case, the cyber-attack started eighteen months before detection, and contributing causes were in place since 2000, five years before the cyber-attack. Proximate events are summarized below.

1. In 2005 TJX decided against upgrading to a stronger encryption algorithm from 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. Hackers exploited inherent encryption algorithm weaknesses, and decrypted key to steal employee accounts and passwords.
5. Using stolen account information, hackers accessed corporate servers in Framingham, MA.
6. In late 2005 hackers downloaded *previously stored* customer payment card data from corporate servers using Marshalls store Wi-Fi connection in Florida.
7. In 2006 hackers discovered that TJX was processing and transmitting transactions without encryption.
8. In 2006 hackers installed a script on TJX corporate servers to capture unencrypted payment card data.
9. In 2006 hackers installed 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 downloaded the files to the Latvian server.

5.5 Step #5: Analyzing the Physical Process

As shown in Figure 5.1, the key process in hierarchical control structure is the TJX Retail Store System. The goal of this step is to determine *why* controls were ineffective in preventing the system from transitioning into a hazardous state leading to the cyber-attack. Several factors will be considered, including [10]:

- How and why controls were ineffective in preventing system hazard and contributed to an accident.
- What physical failures (if any) were involved in the loss.
- Were there any communication and coordination flaws between the physical system and other interacting component(s).

5.5.1 TJX Retail Store System

TJX Retail Store System is the subject of analysis, and is a part of four control loops as shown in Figure 5.1. It is the direct touch point of TJX with its customers where Point of Sale (POS) transactions occur.

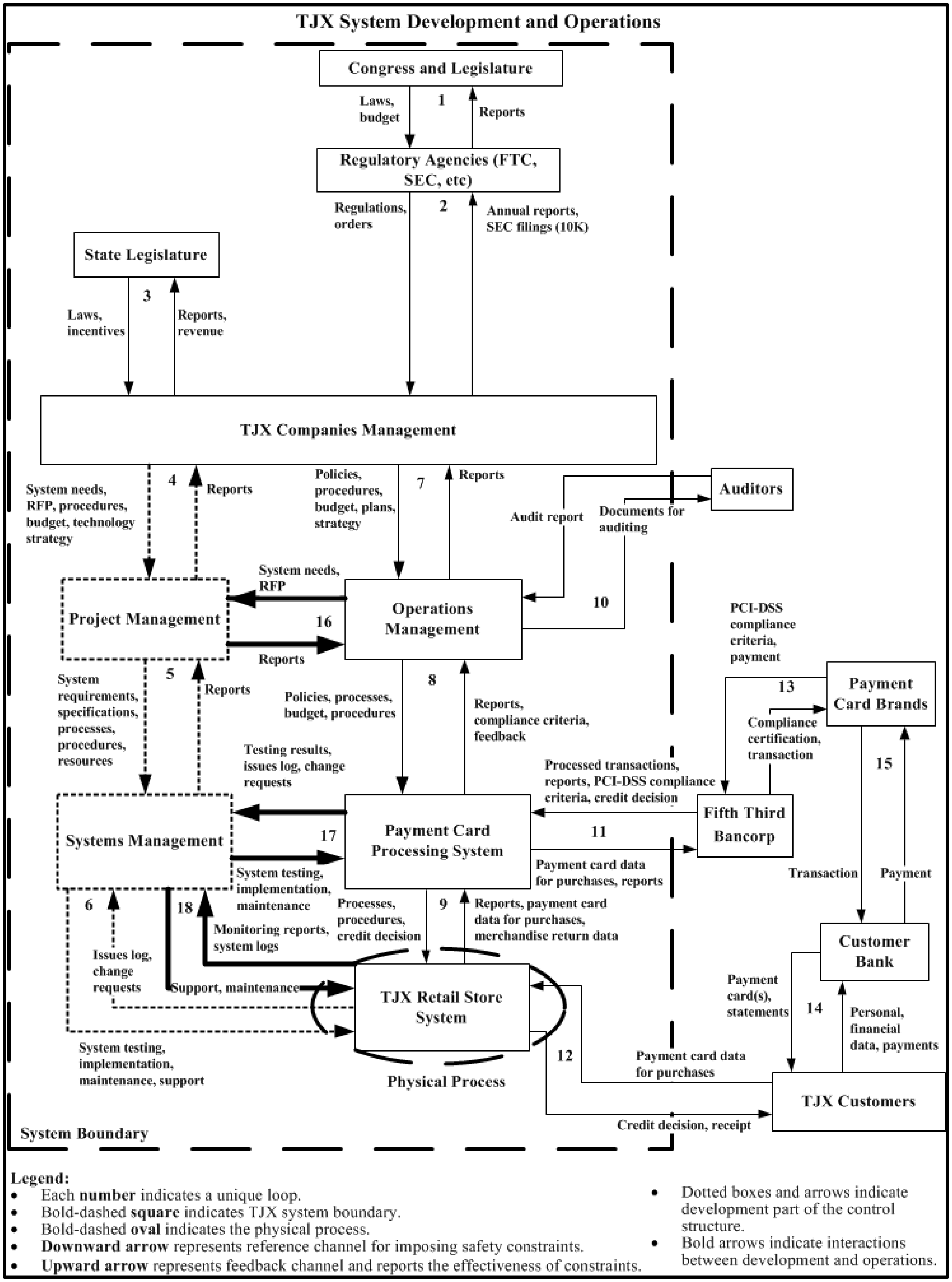

Figure 5.1: TJX system development and operations hierarchical control structure.

5.5.1.1 Inadequate control/feedback

5.5.1.1.1 Security Technology Management Capabilities

The TJX store was targeted because hackers used “war-driving,” which specifically looks for Wi-Fi networks that accept connection(s) without authentication, because the store’s Access Point (AP) was misconfigured it did not require authentication. This contributed to weakening of control by Systems Management over the process both via loop #6 and loop #18, and further, there was inadequate feedback from the process to Systems Management during support and maintenance phase (loop #18).

5.5.1.1.2 Monitoring

Hacker’s presence was never detected , despite the fact that they were downloading large amounts of data from TJX corporate server, using Wi-Fi network in Miami, FL. Loop #18 in Figure 5.1 will be analyzed further to understand causes underlying the weakened control.

5.5.1.1.3 Encryption technology

Software utilities for decrypting deprecated WEP key were freely and publically available. Hackers leveraged AP misconfiguration and inherent weaknesses of WEP encryption algorithm to steal employee account and password. To understand why Systems Management did not replace the deprecated algorithm at the physical process level, higher levels of the control structure would need to be analyzed. CAST analysis of the process is summarized in Figure 5.2.

Safety Requirements and Constraints Violated:

- Prevent unauthorized access to customer information.

Emergency and Safety Equipment (Controls):

- Security technology at the store included 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 accessing corporate servers.

Failures and Inadequate Controls:

- Access Point (AP) misconfiguration
    - The AP was misconfigured with a default setting of *open authentication* that allowed connections to anyone without authentication.
- Inadequate monitoring of 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 undetected.
- Inadequate implementation/maintenance of processes and/or procedures at the physical process level.
    - Stores were collecting customer information that was not required to make a purchase or a return (e.g. drivers license). 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.

Physical Contextual Factors:

- Wi-Fi technology became available in 1999.
- TJX was an early adopter of first generation Wi-Fi technology at over 1200 retail stores in 2000, requiring a significant learning curve, training, and new knowledge base in a short span of time.

- 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 though TJX did not suffer a cyber-attack during this time.

Figure 5.2: CAST analysis of TJX Retail Store System (Physical Process Level).

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

Step 5 highlighted three key control/feedback inadequacies at the physical process level: AP was incorrectly configured, Wi-Fi network monitoring was inadequate, and 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 hierarchical safety control structure need to be analyzed [10].

5.6.1 Payment Card Processing System

Moving one level up from the physical process in the hierarchical control structure, note that TJX Retail Store System physical process is controlled by Payment Card Processing System, as shown in Figure 5.1(loop #9)

Payment Card Processing System also interacts with Systems Management (loop #17). This link is to ensure that systems are subjected to rigorous testing, for secure processing of payment card transactions by incorporating them during system design.

5.6.1.1 Inadequate control/feedback

5.6.1.1.1 Compliance with Payment Card Industry-Data Security Standard (PCI-DSS)

At the time of cyber-attack in 2005, TJX was not PCI-DSS compliant, which is usually a requirement for accepting payment card(s). In order to be compliant a merchant must satisfy *all* twelve requirements of PCI-DSS and its sub-requirements comprising of approximately eighty pages [12], requiring a significant effort on part of the merchant. As an example, TJX was in violation of the following requirements and sub-requirements:

- *Requirement 3*: Protect Stored Card Holder Data [12]
    - *Sub-requirement 3.1*: Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes.

  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. Furthermore, TJX Operation did not have a formal data retention policy.
- *Requirement 4*: Encrypt transmission of cardholder data across open, public networks [12]. TJX was storing and transmitting customer payment card data to the Fifth Third Bancorp without encryption [13].

To understand why TJX was not in compliance, it will help to gain an understanding of the role a bank plays in credit approval process as shown in Figure 5.1 (loop #11). Payment card transactions flow through multiple entities and systems before a credit decision is made, VISA transaction flow is shown in Figure 5.3.

In 2005 Fifth Third Bancorp was TJX’s major acquirer bank and responsible party for ensuring PCI-DSS compliance by merchants. Based on our analysis, the following issues have come to light.

Figure 5.3: VISA transaction flow **[14]**.

- There is a 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, and TJX could choose another processor and since PCI-DSS was not legally required, Fifth Third Bancorp leverage is limited in requiring it.
- It is difficult for Fifth Third Bancorp to gain deep insights into TJX systems to validate and verify the degree that PCI-DSS has been implemented, because it has no regulatory role. For these reasons implementing PCI-DSS is the responsibility of TJX, which submits voluntary yearly reports regarding compliance status.
- Per PCI-DSS, Fifth Third Bancorp is not responsible for auditing TJX with reference to PCI-DSS compliance.

5.6.1.1.2 Payment Card Processing System and Systems Management Interaction
The Payment Card Processing System was sending unencrypted information to the bank for possibly several reasons: PCI-DSS requirements were not effectively communicated to system development, there was systemic lack of awareness of PCI-DSS requirements, and there was lack of clarity on roles and responsibilities with reference to PCI-DSS implementation between development and operations. The analysis of Payment Card Processing System is summarized in compressed form inFigure 5.4. Analysis of higher level components is needed to understand why these oversights occurred and for what reason.

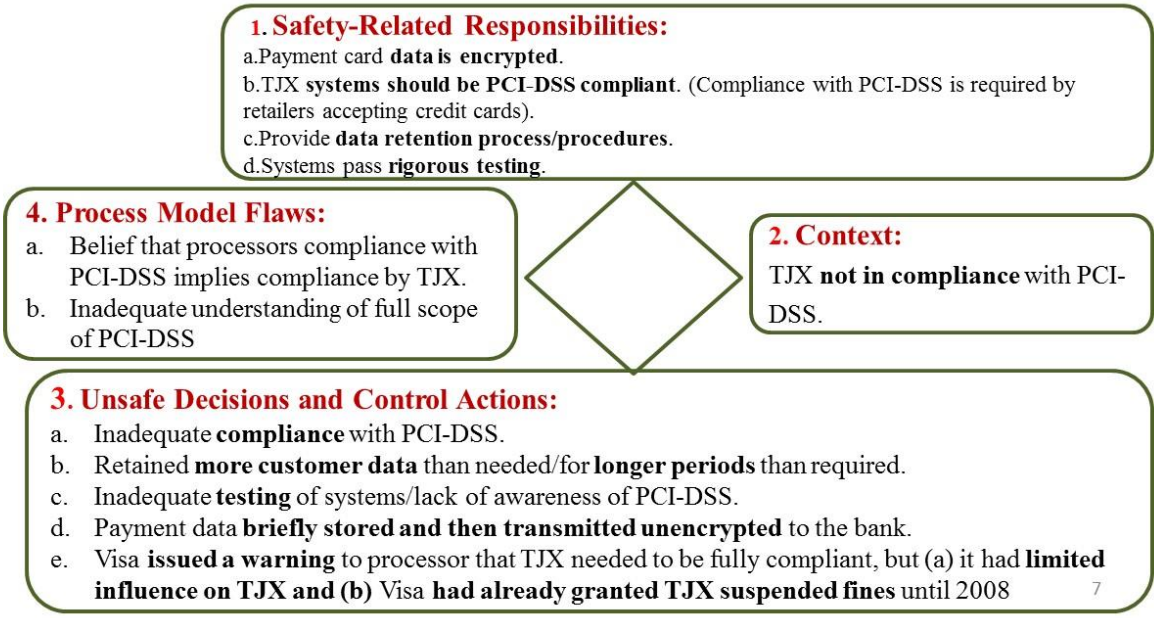

Figure 5.4: CAST analysis of Payment Card Processing System.

5.6.2 Operations Management and other upper levels

Next level up in the control structure is Operations Management, which 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.

A similar analysis was conducted for this level, and all the upper levels. A detailed description of these analyses can be found in [15]. But, to give an example of the range of factors that can contribute to such a cyber-attack, we will briefly mention one of the interesting upper levels of the control structure: The role of the State Legislature.

5.6.3 State Legislature

TJX is headquartered in Massachusetts. If its headquarters had been in Nevada, certain factors would have been different. That is because, in Nevada, all retail operations are required to be PCI-DSS compliant, which was not the case in Massachusetts at that time. Thus, the Massachusetts State Legislature also controls TJX Management by enacting laws. Although we have not investigated the reasons, we suspect that, much like VISA and Fifth Third Bancorp, Massachusetts wants to be "business-friendly" and impose as few regulations as possible. This is illustrated in the feedback shown in Figure 5.1 (loop #3).

5.7 Step #7: Coordination and Communication

The CAST analysis revealed key coordination and communication weaknesses discussed below.

- Payment Card Processing System is controlled by Operations Management (loop #8), and interacts with Fifth Third Bancorp (loop #11), which should be responsible for ensuring that TJX is compliant with PCI-DSS but was relying on TJX to satisfy all requirements of PCI-DSS. Also, at TJX the general view was that PCI-DSS compliance is a technology issue and that First Third Bancorp compliance implies TJX compliance.

- Cyber security risk posed by use of WEP was well understood within TJX [16], but because PCI-DSS was not a priority, the risks were not effectively communicated to the executive level. Further, there was no dedicated role within TJX that was responsible for managing cyber security risks companywide.
- Disconnect between system development and operations during system design.

5.8 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 [10]. This step discusses some operational and behavioral aspects revealed that contributed to the TJX cyber-attack.

A major change that contributed to the cyber-attack was TJX's early move from wired to wireless networking (Wi-Fi) in 2000, in a short span of one year. By 2003, the environment had changed because the inherent weaknesses of WEP became publically known and hackers started to exploit for launching cyber-attacks. TJX decided against upgrading to a more secure encryption algorithm for cost reasons.

TJX's short implementation timeframe for a major technology leap introduced additional risk. It is plausible that technology team's inadequate experience led to misconfiguration of AP's that allowed hackers to launch an attack. Same reasoning may also explain lack of monitoring of Wi-Fi network for data traffic and unauthorized connections.

Lack of full compliance with PCI-DSS also contributed to the cyber-attack, and TJX 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. 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 cyberattack risks.

5.8.1 Recall Bias.

Biases can contribute to flawed decisions by managers. One such bias is *ease of recall bias* that relates to decision making process where recent experiences, or lack thereof, strongly influence the decision. Having no experience of a breach at TJX and oblivious to cyber-attacks at other retailers, it is plausible that the *recall bias* heuristic played a role in management's decision to not upgrade to a stronger encryption in favor of cost savings [16].

5.8.2 Confirmation Trap

Another behavioral aspect, called *confirmation trap* [17], is a decision maker's tendency to favor/seek information that confirms his/her own beliefs and discount contradicting information. Table 5.1 depicts a message from the TJX CIO in November 2005 to his staff [16], regarding security technology upgrades. In this memo, he is requesting agreement on his belief that cyber security risk is low. The majority of his staff agreed with his assessment. 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 5.1: TJX CIO memo regarding security technology upgrade **[16]**.

5.9 Step #9: Recommendations

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 is needed with cyber security responsibilities and authority for executing cyber security risk management policies. Further, it will 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.
- Per PCI Security Standards Council, compliance is a business issue requiring management attention and is an ongoing process of assessment, remediation and reporting. TJX needs to understand and communicate effectively the risks of non-compliance and importance of integrating PCI-DSS early in the system lifecycle.
- Building a Cybersafety culture can help reduce risks of a future cyber-attack significantly. Specific steps can include:
    - Identifying critical systems, trends, processes, and procedures with reference to cyber security.
    - After critical entities are documented, implement a plan to manage these entities with periodic reviews to update the list.
- Understand limitations standards and align them with cyber security and business needs of an organization. For example, PCI-DSS data standard states that "encrypt transmission of cardholder data across open, public networks [12]". PCI-DSS does not explicitly state that data must be encrypted when transmitted within TJX – that is over the *intranet or behind a firewall*. Also PCI-DSS did not explicitly mandate using stronger encryption WPA until 2006.

With these recommendations analysis of TJX cyber-attack 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.

6 Comparing Cybersafety Findings with Federal Trade Commission (FTC) and Canadian Privacy Commission (CPC) Findings

This section presents comparisons between selected Cybersafety CAST recommendations, and actions proposed by the FTC and the CPC.

Error! Reference source not found. Comparison of Cybersafety CAST recommendations with FTC and Canadian Privacy Commission.

Both FTC and CAST generated recommendation #1 albeit with a difference. FTC proposed designating an *employee or employees* to be accountable for information security program. CAST specifically recommends an executive level role for managing cyber security risks. With reference to recommendations #2, #3, #4, and #5 in **Error! Reference source not**

found., all of these were generated by CAST and have been discussed in either this report, or the more complete analysis [15], but importantly, omitted by CPC and FTC.

Recommendations #6 and #7, regarding lack of encryption and monitoring of systems, were explicitly proposed by the CPC. CAST analysis identified causal factors and revealed non-linear issues at TJX which led to weakening or lack of these controls. Although, our CAST analysis did not explicitly provide Recommendations #6 and #7, the insights were addressed by way of Recommendations #1, #2, and #3.

Recommendation #8 provided by FTC is an important point, but vague. FTC 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" [18]. 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 our analysis.

The Cybersafety analysis covers the FTC proposal in all five of its recommendations and provides specifics, for example, with reference to PCI-DSS, we provide actionable steps. Importantly, our analysis, provided insights that other investigations either did not reveal or revealed in incomplete form, therefore it can be a valuable supplement for understanding cyber-attacks and specifically systemic and non-linear causes leading to increased cyber security risks.

7 Contributions

Our research proposed a new method, Cybersafety, of analyzing cyber security risks drawing on prior research and experience in preventing accidents, based on Systems Thinking and Systems Theory and the STAMP methodology. The analysis revealed insights, which might otherwise be difficult or impossible to gain using traditional technology focused approaches.

Main contributions of this paper include:

- Highlighted the value for a System Thinking and Systems Theory based approach for managing cyber security risks.
- Introduced Cybersafety as a new approach for managing cyber security risks
- Applied our analysis to the TJX cyber-attack case providing new insights including:
  - Highlighted general limitations of standards, specifically PCI-DSS.
  - Highlighted systemic causes that contributed to the TJX cyber-attack.
  - Highlighted behavioral aspects that contributed to the TJX cyber-attack.

References

[1] M. M. a. A. D. C. I. N. Fovino, "Integrating cyber attacks within fault trees," *Rel. Eng. Syst. Safety,* vol. 94, no. 9, p. 1394–1402, 2009.

[2] C.-C. L. a. M. G. C.-W. Ten, "Vulnerability assessment of cybersecurity for SCADA systems using attack trees," in *IEEE Power Eng. Soc. General Meeting*, 2007.

[3] T. G. P. P. a. E. S. C. Schmittner, "Security application of failure mode and effect analysis (FMEA)," in *33rd Int. Conf. Comput. Safety, Rel. Security,* Florence, Italy, 2014.

[4] M. B. F. C. Y. H. a. L. P.-C. S. Kriaa, "Safety and security interactions modeling using the bdmp formalism: Case study of a pipeline," in *33rd Int. Conf. Comput. Safety, Rel. Security*, 2014.

[5] W. Y. a. N. G. Leveson, "An integrated approach to safety and security based on systems theory," *ACM*, vol. 57, no. 2, p. 31–35, 2014.

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

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

[8] 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.

[9] 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.

[10] 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.

[11] *AMERICAN GREED EPISODE 40: HACKERS, OPERATION GET RICH OR DIE TRYIN'.* [Film]. USA: CNBC, 2011.

[12] 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.

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

[14] 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].

[15] H. M. Salim, "Cyber safety : a systems thinking and systems theory approach to managing cyber security risks," MIT, Cambridge, MA, 2014.

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

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

[18] 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].

[19] 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.