Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)^3

3 Sept 2014

CYBER SAFETY: A Systems Thinking and Systems Theory Approach to Managing Cybersecurity – Applied to TJX Case

Hamid Salim
Professor Stuart Madnick

Massachusetts
Institute of
Technology

MITSloan
MANAGEMENT

genda

. TJX (TJ Max and Marshalls stores) Case

. **S**ystem-**T**heoretic **A**ccident **M**odel and **P**rocesses (**STAMP**) and **C**ausal **A**nalysis based on **ST**AMP **(CAST**)

. STAMP/CAST Applied to TJX

. Contributions

1. **Background of the TJX** (TJ Maxx and Marshalls stores) **Case**

Mar 29, 2007

data breach: At 45.6M card numbers, it's the gest ever

ses the compromise in June 2005 at CardSystems ons

By Jaikumar Vijayan FOLLOW

Computerworld | Mar 29, 2007 1:00 PM PT

After more than two months of refusing to reveal the size and scope of its data breach, TJX Companies Inc. is finally offering more details about the extent of the compromise.

In filings with the U.S. Securities and Exchange Commission yesterday, the company said 45.6 million credit and debit card numbers were stolen from one of its systems over a period of more than 18 months by an unknown number of intruders. That number eclipses the 40 million records compromised in the mid-2005 breach at CardSystems Solutions and makes the TJX compromise the worst ever involving the loss of personal data.

MORE LIKE THIS

Theft of 45.6M Card Numbers Largest Heist Yet

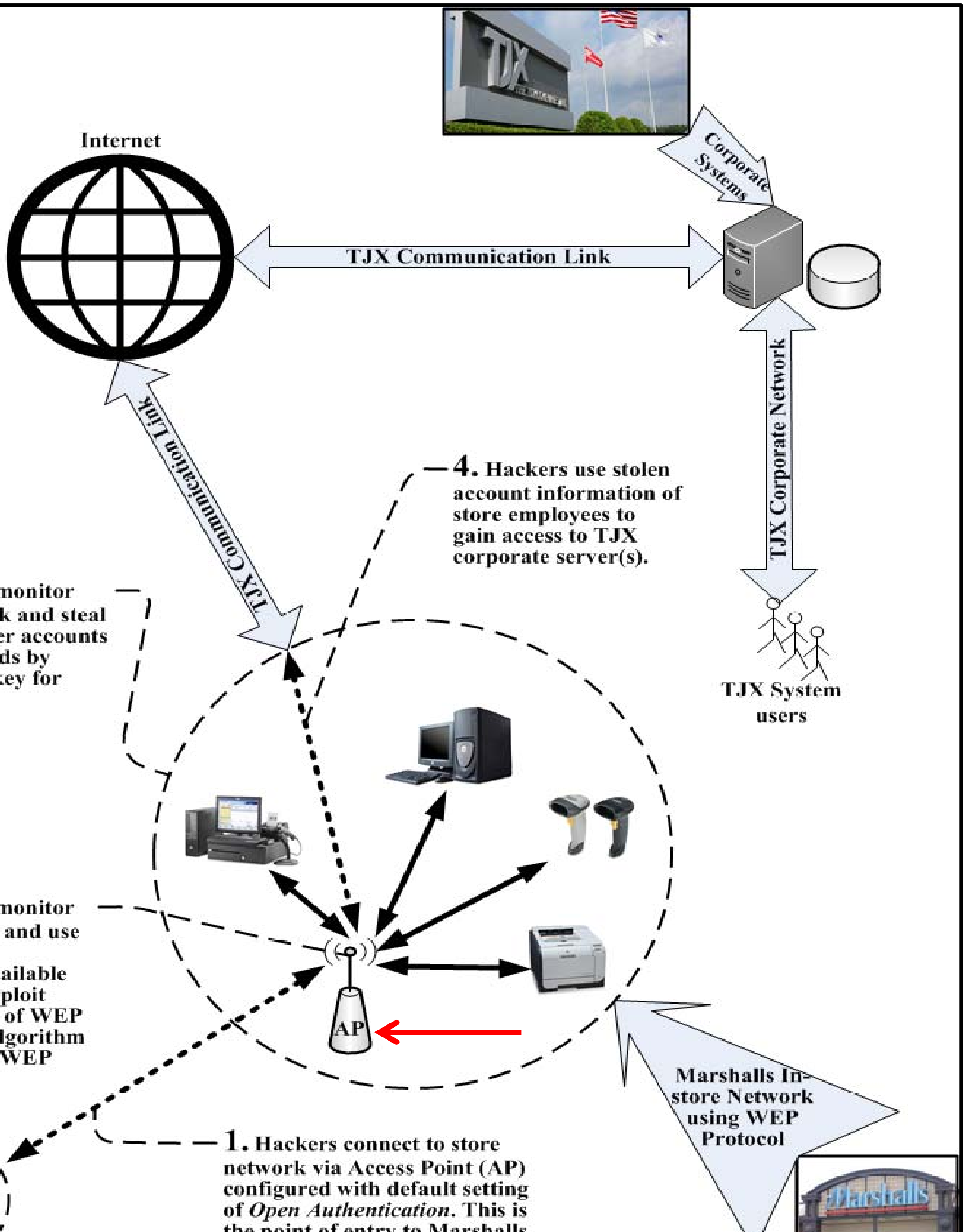
Update: Retail breach may have exposed card data in four countries

Stolen TJX data used in Florida crime spree

(TJ Maxx & Marshalls) Case Study – Some Highlights

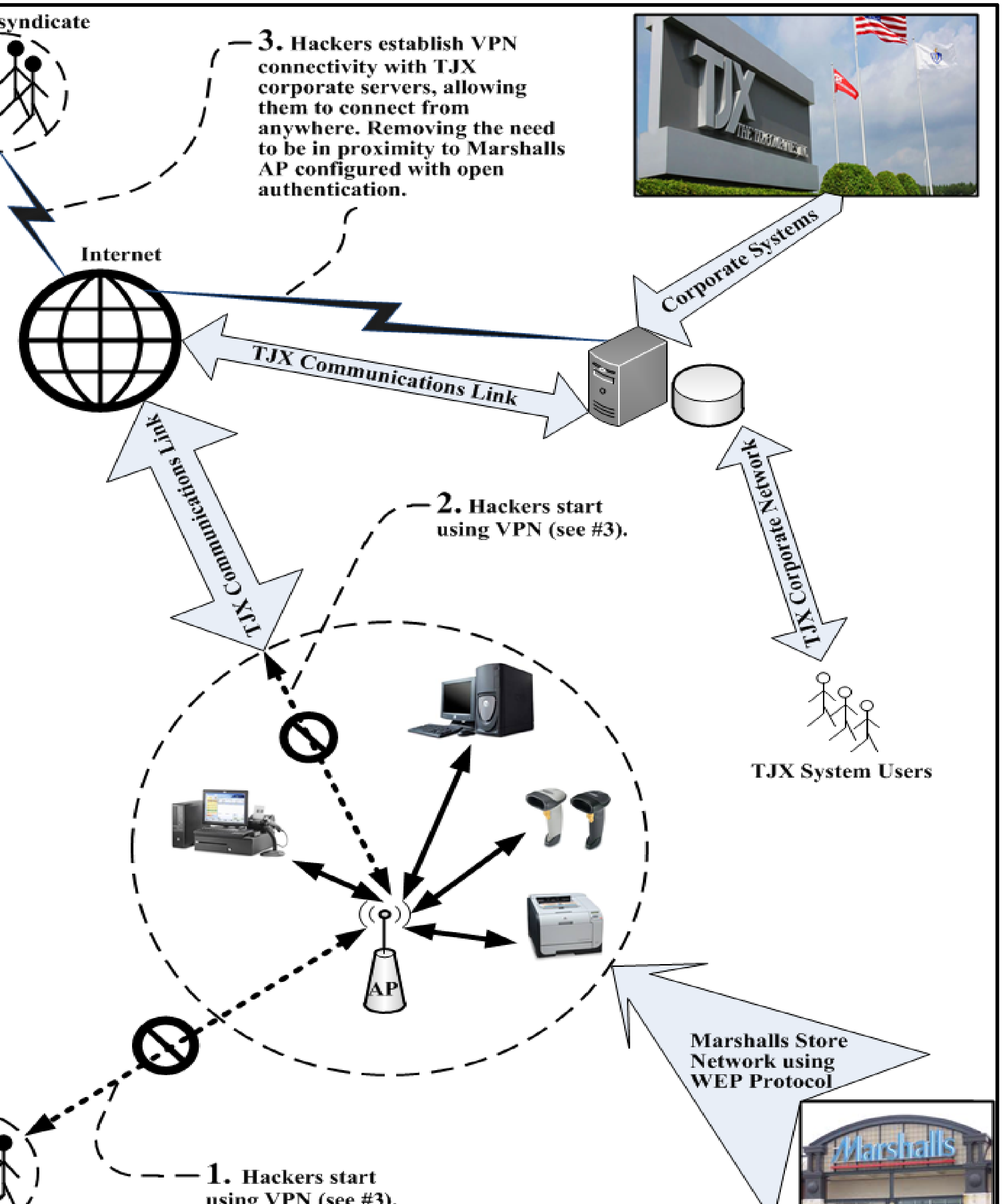
- Major off-price US based retailer, **revenues > $25 billion (FY2014)**
- Victim of **largest (by number of cards) cyber-attack** in history, when announced **in 2007**.
- Cost to **TJX > $170 million,** per SEC filings.
- Cyber-attack launched from a **store on Miami, FL** in 2005 by exploiting **Wi-Fi vulnerability.**
- Hackers ultimately reached corporate payment servers and stole **current transaction data**.
- Cyber-attack lasted for **over 1.5 years**

: Federal/State Court records **(primary)**, TJX SEC Filings, Others (NYT, WSJ, Globe, FTC, Academic Journal articles)


Internet
TJX Communication Link
Corporate Systems
TJX Corporate Network
TJX System users
TJX Communication Link
4. Hackers use stolen account information of store employees to gain access to TJX corporate server(s).
monitor
k and steal
er accounts
ds by
key for
monitor
and use
ailable
ploit
of WEP
lgorithm
WEP
AP
Marshalls In-store Network using WEP Protocol
1. Hackers connect to store network via Access Point (AP) configured with default setting of *Open Authentication*. This is the point of entry to Marshalls
Marshalls

Breaching Marshalls Store

1. **AP- Open authentication** vs Shared Key authentication.
2. **WEP** publically known **weak algorithm compromised.**
3. **Sniffers used** to monitor data packets**.**
4. Hackers steal store **employee account information** and **gain access to TJX corporate servers.**

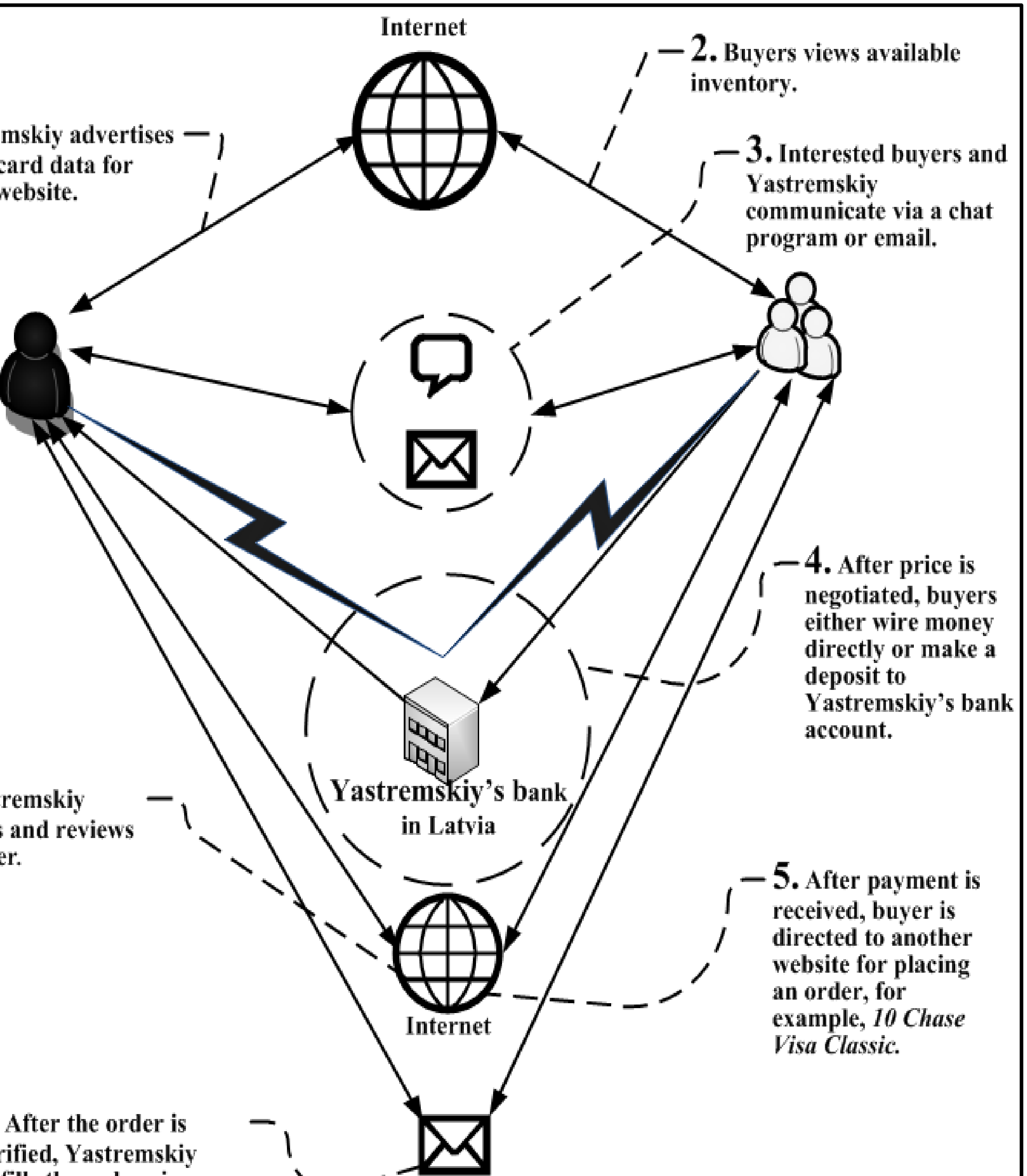

3. Hackers establish VPN connectivity with TJX corporate servers, allowing them to connect from anywhere. Removing the need to be in proximity to Marshalls AP configured with open authentication.

2. Hackers start using VPN (see #3).

1. Hackers start using VPN (see #3).

Hackers Establish VPN Connectivity

1. Hackers use **Marshalls AP to install VPN** connection.
2. VPN is between TJX **corporate server and hacker controlled servers in Latvia**.
3. Code installed on TJX **corporate payment processing server.**

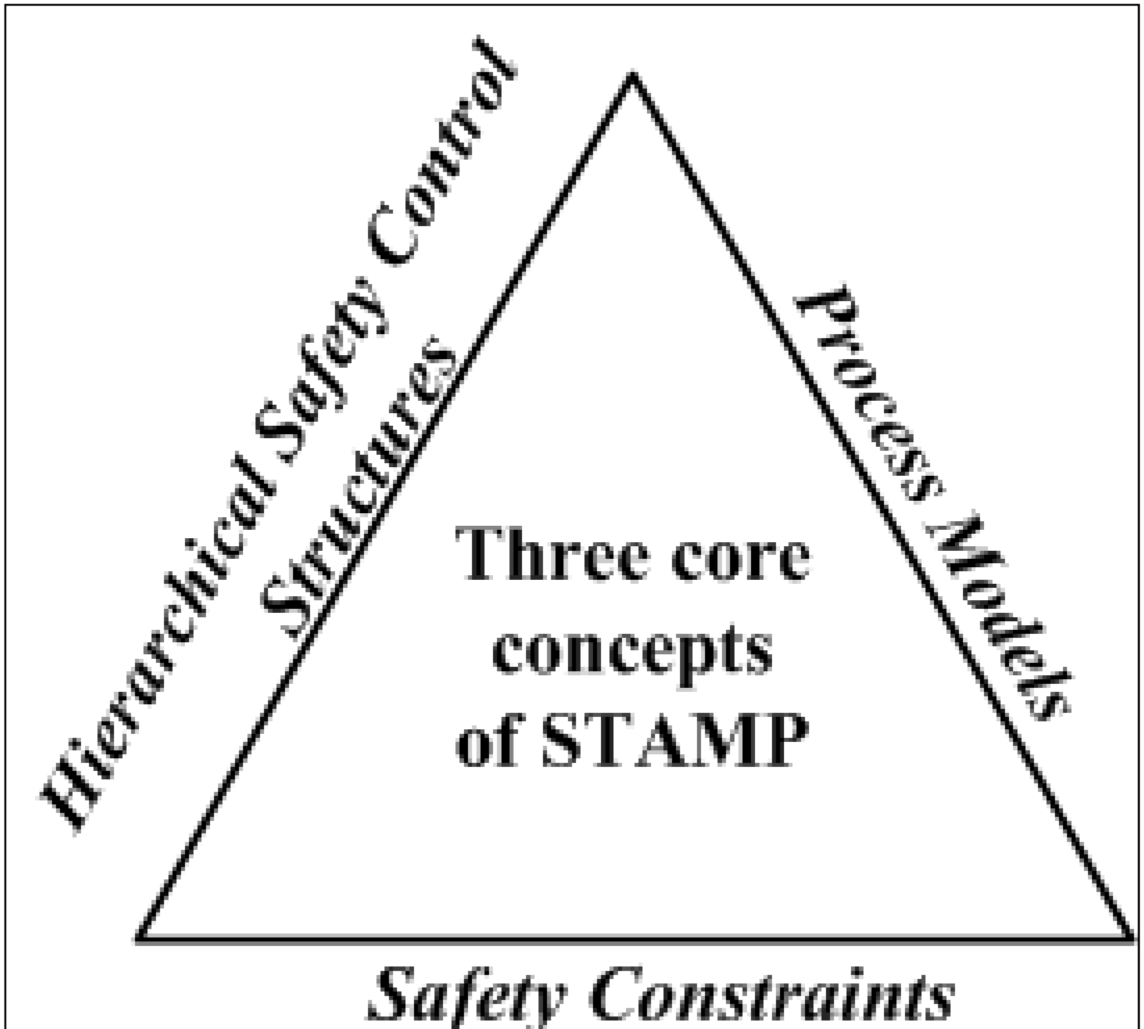

Internet
2. Buyers views available inventory.
mskiy advertises card data for website.
3. Interested buyers and Yastremskiy communicate via a chat program or email.
4. After price is negotiated, buyers either wire money directly or make a deposit to Yastremskiy's bank account.
Yastremskiy's bank in Latvia
remskiy s and reviews er.
5. After payment is received, buyer is directed to another website for placing an order, for example, *10 Chase Visa Classic.*
Internet
After the order is rified, Yastremskiy

Flow for Sales of Stolen Payment Card Information.

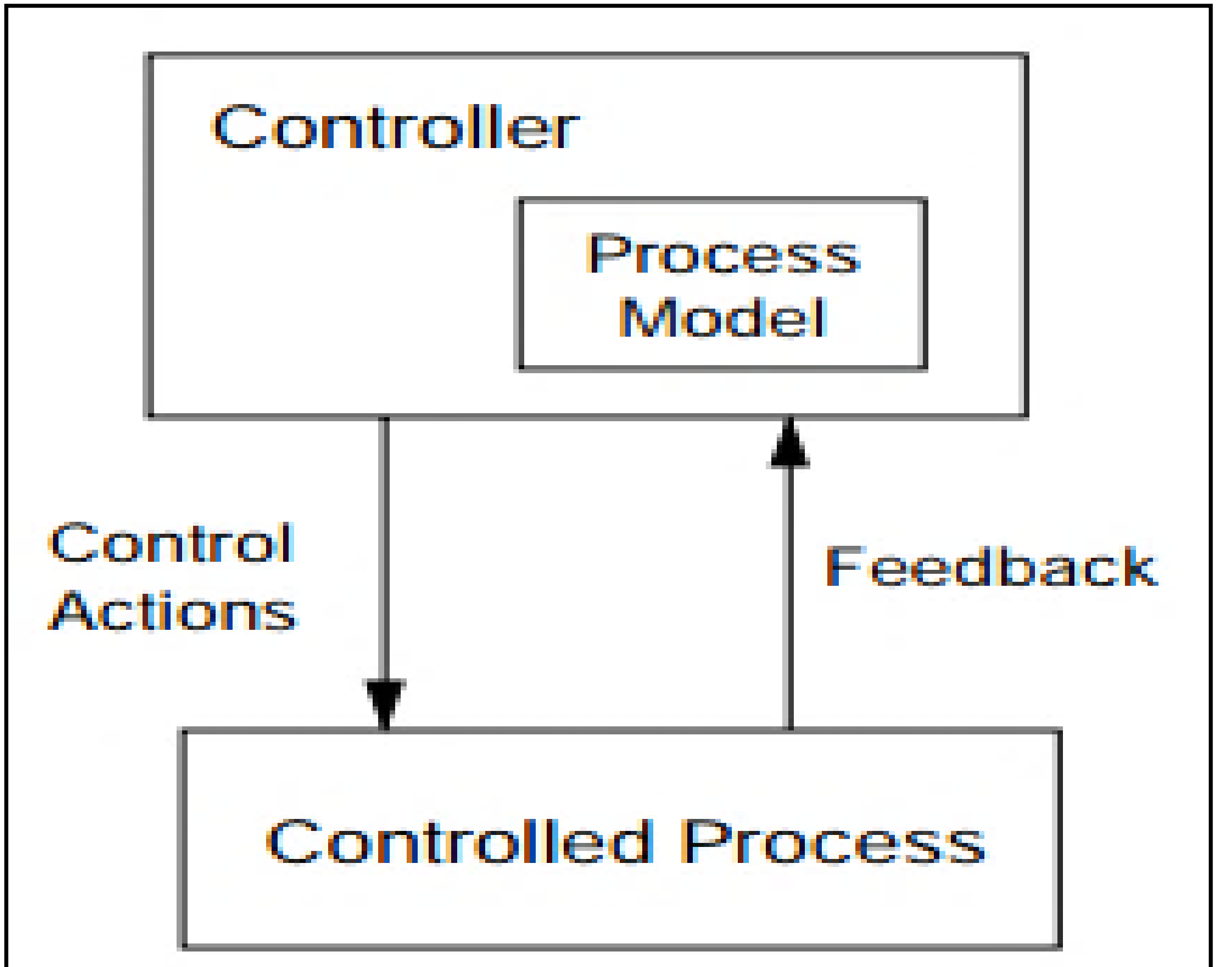
- Via Bank in Latvia

2. **S**ystem-**T**heoretic **A**ccident **M**odel and **P**rocesses (**STAMP**) and **C**ausal **A**nalysis based on **ST**AMP (**CAST**)

STAMP Model


Hierarchical Safety Control Structures
Process Models
Three core concepts of STAMP
Safety Constraints

TAMP Hierarchical Control Model



AST Steps for Analyzing Accidents or Incidents

.	**STAMP/CAST Analysis Steps**
	Identify the system(s) and hazard(s) associated with the accident or incident.
	Identify the system safety constraints and system requirements associated with that hazard.
	Document the safety control structure in place to control the hazard and ensure compliance with the safety constraints.
	Ascertain the **proximate events leading to the accident** or incident.
	Analyze the accident or incident at the **physical system level**.
	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.
	Analyze overall coordination and communication contributors to the accident or incident.
	Determine the dynamics and changes in the system and the safety control structure relating to an accident or incident, and any weakening of the safety control structure over time.
	Generate recommendations.

3. STAMP/CAST Applied to TJX

p #1: Identify System(s) and Hazard(s)

System(s)

- TJX payment card processing system

Hazard(s) – at system level

- System allows for unauthorized access

p #2 (1/2): Define System Safety Constraints and quirements

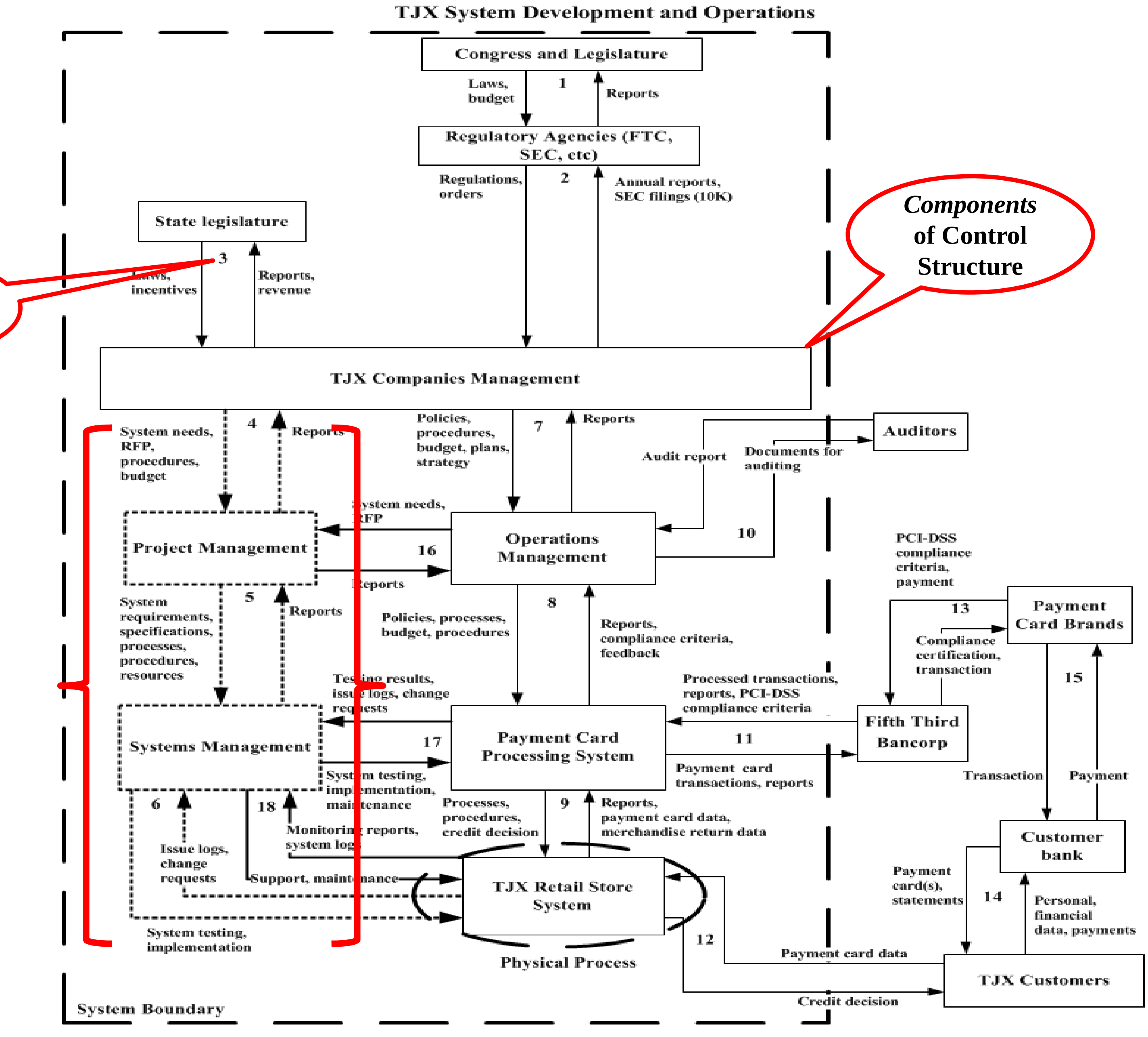
stem Safety Constraints – at system level

Protect customer information from unauthorized access.

Provide adequate **training to staff** for managing security echnology infrastructure.

Minimize losses from unauthorized access to payment system

3:
rchical
ol
ure



TJX System Development and Operations
Congress and Legislature
Laws, budget
1
Reports
Regulatory Agencies (FTC, SEC, etc)
Regulations, orders
2
Annual reports, SEC filings (10K)
State legislature
3
Laws, incentives
Reports, revenue
Loop numbers
Components of Control Structure
TJX Companies Management
System needs, RFP, procedures, budget
4
Reports
Policies, procedures, budget, plans, strategy
7
Reports
Auditors
Audit report
Documents for auditing
Project Management
System needs, RFP
16
Reports
Operations Management
10
PCI-DSS compliance criteria, payment
Payment Card Brands
13
Compliance certification, transaction
15
System requirements, specifications, processes, procedures, resources
5
Reports
Policies, processes, budget, procedures
8
Reports, compliance criteria, feedback
Processed transactions, reports, PCI-DSS compliance criteria
Testing results, issue logs, change requests
Systems Management
17
Payment Card Processing System
11
Fifth Third Bancorp
System testing, implementation, maintenance
Payment card transactions, reports
Transaction
Payment
6
18
Issue logs, change requests
Monitoring reports, system logs
Processes, procedures, credit decision
9
Reports, payment card data, merchandise return data
Customer bank
Payment card(s), statements
14
Personal, financial data, payments
Support, maintenance
TJX Retail Store System
System testing, implementation
12
Payment card data
Physical Process
TJX Customers
Credit decision
System Boundary

Legend:

#4: Proximate Event Chain, (1/2)

2005 TJX decided **not to upgrade** to a stronger encryption algorithm continued using deprecated WEP encryption.

2005, hackers use **war-driving method** to discover a **misconfigured cess Point** (AP) at a Marshalls store in Miami, FL.

ackers join the store network and start monitoring data traffic.

2005, they exploited **inherent encryption algorithm weaknesses** at store, and decrypted the key to steal employee account and password.

sing **stolen account information**, hackers accessed corporate payment d processing servers in Framingham, MA.

late 2005 hackers downloaded customer payment card data from TJX porate transaction processing servers in Framingham, MA **using rshalls store connection in Florida.**

2006 **hackers discover vulnerability**, that TJX was processing and

4: Proximate Event Chain, (2/2)

2006 hackers installed a script on TJX corporate servers to capture encrypted payment card data.

2006 hackers used TJX corporate servers **as staging area and eate files containing customer payment card data** and started wnloading files **using Marshalls store network**.

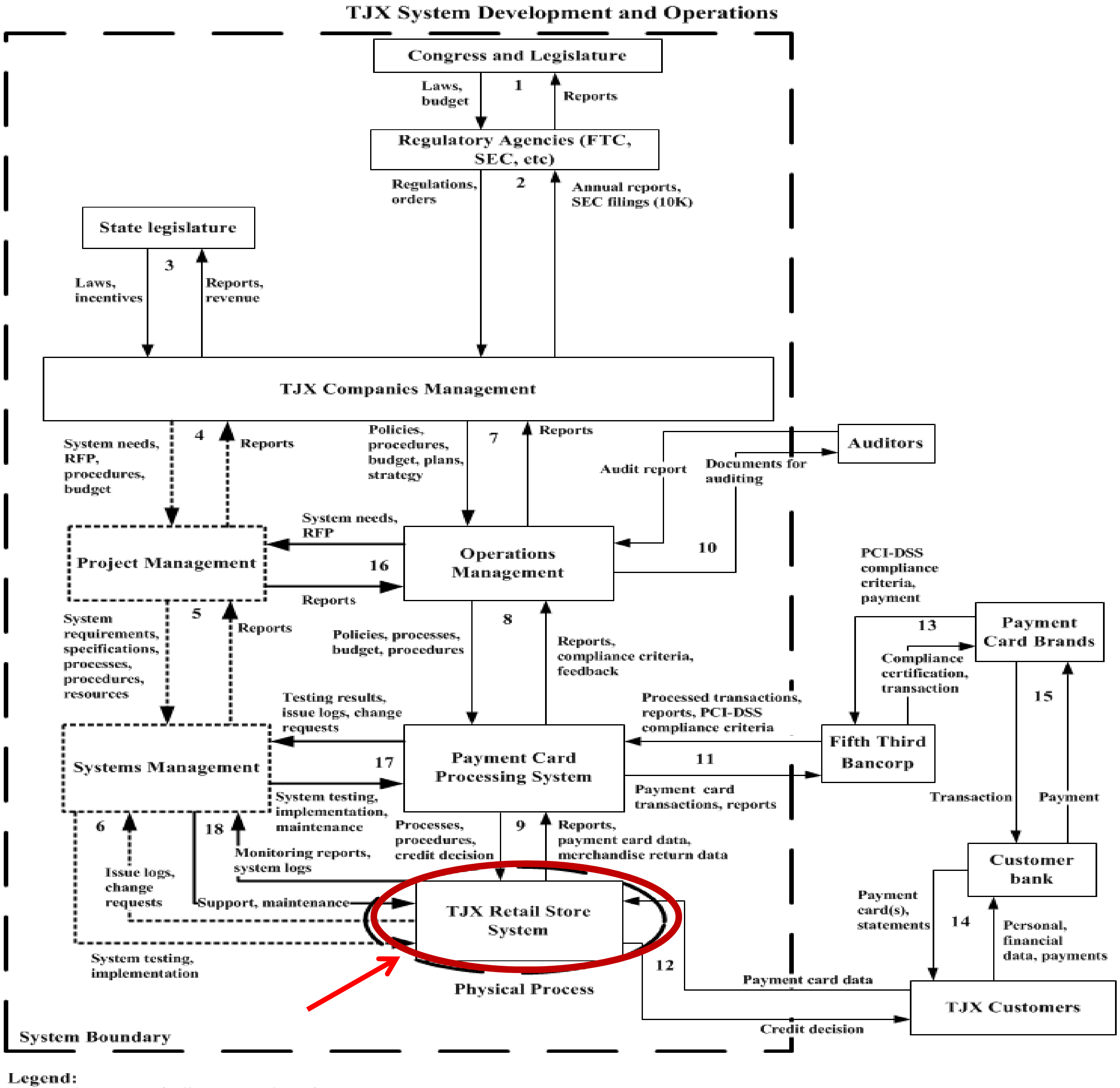
late 2006 hackers **installed a dedicated VPN connection** between X server in Framingham, MA and a server in Latvia.

2006 hackers started moving files **directly from TJX server to the tvian server**.

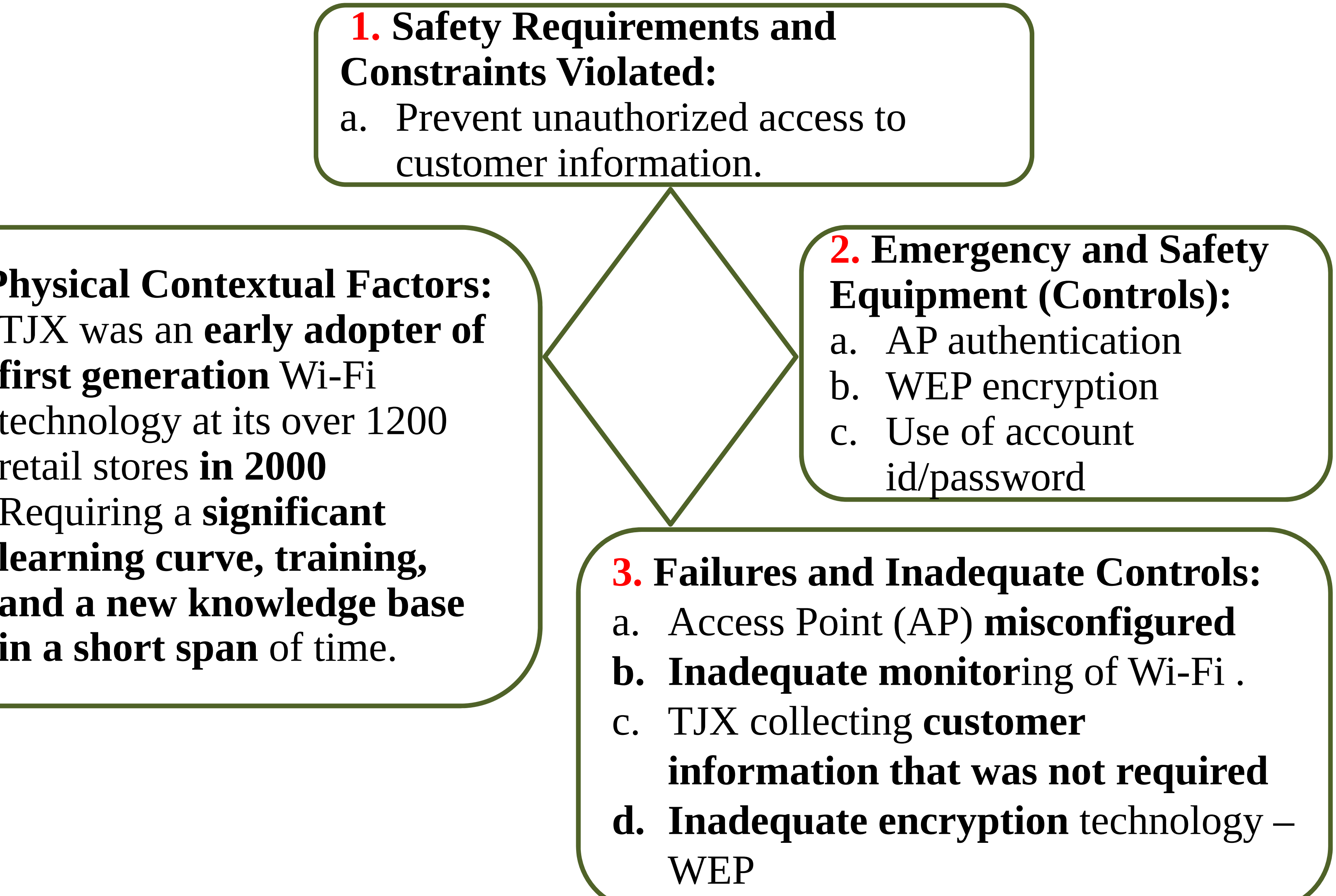
December 2006, TJX was alerted by a credit card company of ssible data breach of TJX systems, initiating an investigation.

January 2007, TJX **announced publically** that it was a victim of a ber-attack.

#5:
zing
hysical
ss (TJX
. Store
n),


TJX System Development and Operations
Congress and Legislature
Laws, budget
1
Reports
Regulatory Agencies (FTC, SEC, etc)
Regulations, orders
2
Annual reports, SEC filings (10K)
State legislature
Laws, incentives
3
Reports, revenue
TJX Companies Management
System needs, RFP, procedures, budget
4
Reports
Policies, procedures, budget, plans, strategy
7
Reports
Auditors
Audit report
Documents for auditing
10
System needs, RFP
Project Management
16
Operations Management
Reports
System requirements, specifications, processes, procedures, resources
5
Reports
Policies, processes, budget, procedures
8
Reports, compliance criteria, feedback
PCI-DSS compliance criteria, payment
13
Payment Card Brands
Compliance certification, transaction
15
Testing results, issue logs, change requests
Processed transactions, reports, PCI-DSS compliance criteria
Systems Management
17
Payment Card Processing System
11
Fifth Third Bancorp
System testing, implementation, maintenance
Payment card transactions, reports
Transaction
Payment
6
18
Processes, procedures, credit decision
9
Reports, payment card data, merchandise return data
Customer bank
Monitoring reports, system logs
Issue logs, change requests
Support, maintenance
TJX Retail Store System
Payment card(s), statements
14
Personal, financial data, payments
System testing, implementation
12
Payment card data
Physical Process
TJX Customers
Credit decision
System Boundary
Legend:

#5: Analyzing the Physical Process (TJX Retail Store System), (2/2)



1. Safety Requirements and Constraints Violated:

a. Prevent unauthorized access to customer information.

Physical Contextual Factors:

TJX was an **early adopter of first generation** Wi-Fi technology at its over 1200 retail stores **in 2000**

Requiring a **significant learning curve, training, and a new knowledge base in a short span** of time.

2. Emergency and Safety Equipment (Controls):

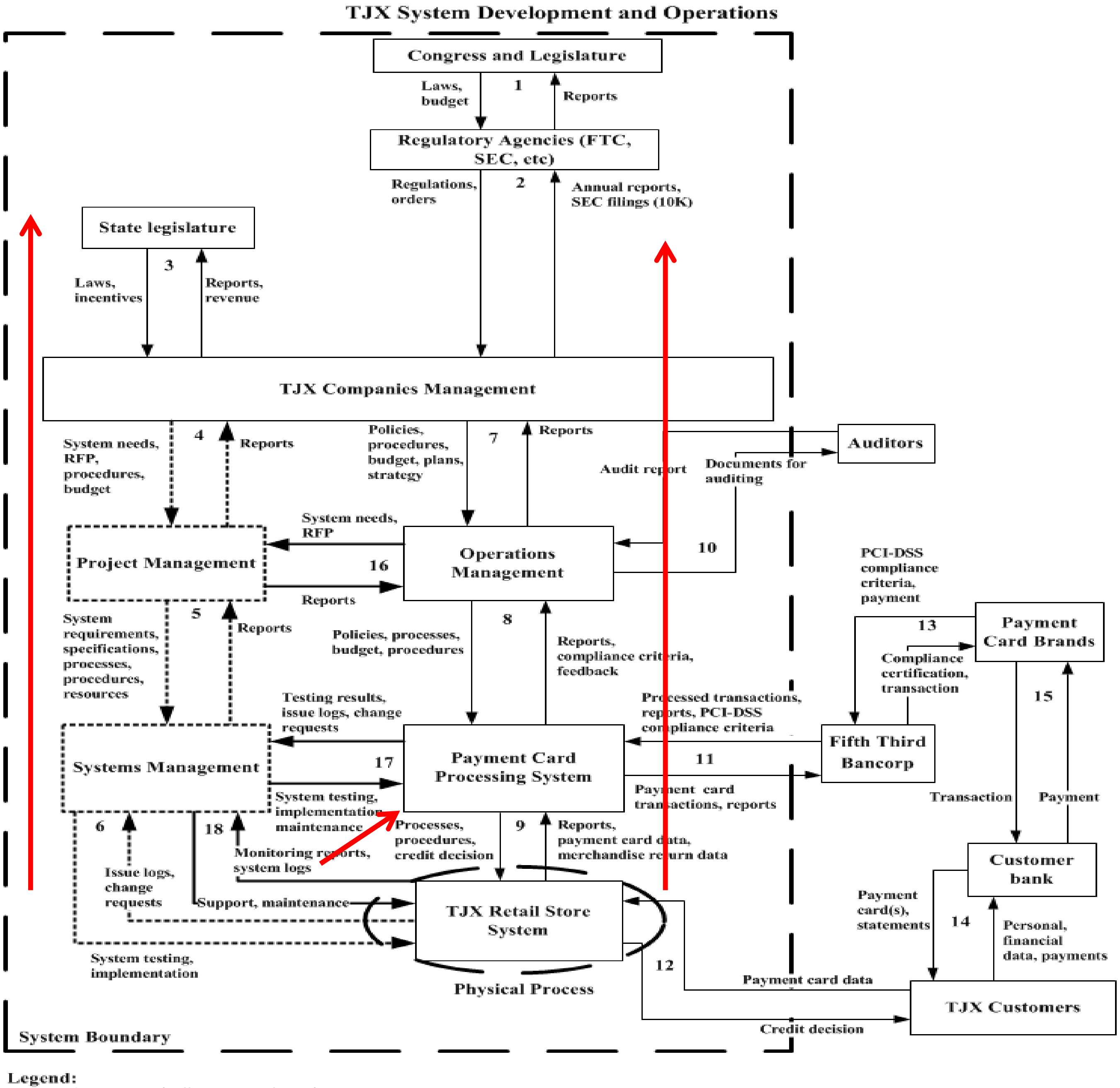
a. AP authentication
b. WEP encryption
c. Use of account id/password

3. Failures and Inadequate Controls:

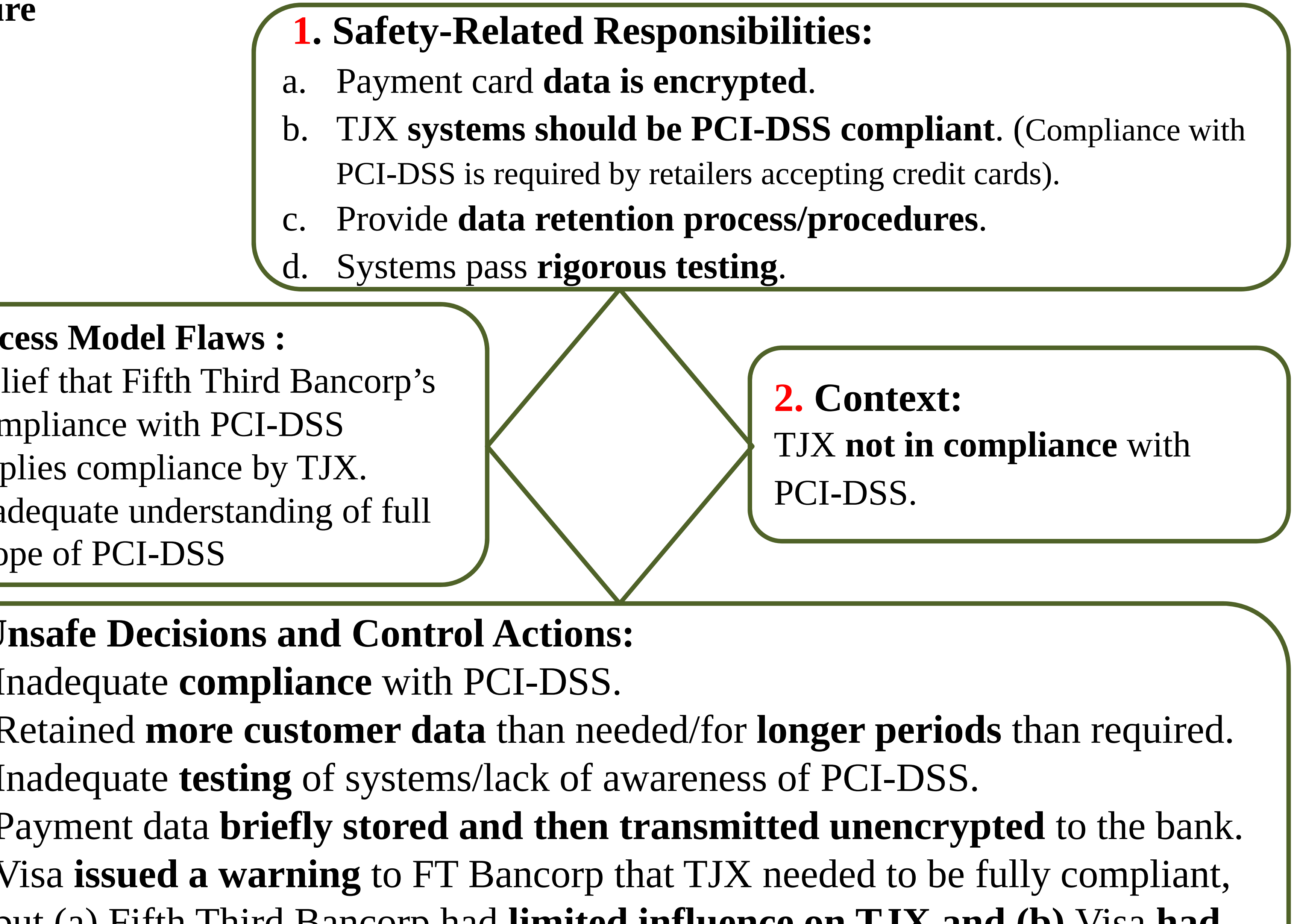
a. Access Point (AP) **misconfigured**
b. Inadequate monitoring of Wi-Fi .
c. TJX collecting **customer information that was not required**
d. Inadequate encryption technology – WEP

6:
sis of
r Levels

rchical
Control
ure


TJX System Development and Operations
Congress and Legislature
Laws, budget
1
Reports
Regulatory Agencies (FTC, SEC, etc)
Regulations, orders
2
Annual reports, SEC filings (10K)
State legislature
3
Laws, incentives
Reports, revenue
TJX Companies Management
System needs, RFP, procedures, budget
4
Reports
Policies, procedures, budget, plans, strategy
7
Reports
Audit report
Documents for auditing
Auditors
10
Project Management
System needs, RFP
16
Reports
Operations Management
5
System requirements, specifications, processes, procedures, resources
Reports
Policies, processes, budget, procedures
8
Reports, compliance criteria, feedback
PCI-DSS compliance criteria, payment
Payment Card Brands
13
Compliance certification, transaction
15
Testing results, issue logs, change requests
Processed transactions, reports, PCI-DSS compliance criteria
Systems Management
17
Payment Card Processing System
11
Fifth Third Bancorp
System testing, implementation maintenance
Payment card transactions, reports
Transaction
Payment
6
18
Processes, procedures, credit decision
9
Reports, payment card data, merchandise return data
Customer bank
Monitoring reports, system logs
Issue logs, change requests
Support, maintenance
TJX Retail Store System
Payment card(s), statements
14
Personal, financial data, payments
System testing, implementation
12
Payment card data
Physical Process
TJX Customers
Credit decision
System Boundary
Legend:

: Analysis of Higher Levels of the Hierarchical Safety Control
ure



1. Safety-Related Responsibilities:

a. Payment card **data is encrypted**.

b. TJX **systems should be PCI-DSS compliant**. (Compliance with PCI-DSS is required by retailers accepting credit cards).

c. Provide **data retention process/procedures**.

d. Systems pass **rigorous testing**.

cess Model Flaws :

lief that Fifth Third Bancorp’s mpliance with PCI-DSS plies compliance by TJX.

adequate understanding of full ope of PCI-DSS

2. Context:

TJX **not in compliance** with PCI-DSS.

Jnsafe Decisions and Control Actions:

Inadequate **compliance** with PCI-DSS.

Retained **more customer data** than needed/for **longer periods** than required.

Inadequate **testing** of systems/lack of awareness of PCI-DSS.

Payment data **briefly stored and then transmitted unencrypted** to the bank.

Visa **issued a warning** to FT Bancorp that TJX needed to be fully compliant, out (a) Fifth Third Bancorp had **limited influence on TJX and (b)** Visa **had**

ep #7: Coordination and Communication

Disconnect between the views of CIO and his staff, and executive management view cyber security as a technology issue.

a. Operations Management was **aware of the compliance criteria** but due to lack or inadequate **support from executive management** those system needs were not communicated to Project Management.

b. Payment Card Processing System is controlled by Operations Management (loop #8), and interacts with Fifth Third Bancorp (loop #11). Fifth Third Bancorp relied on TJX to satisfy requirements of PCI-DSS. But TJX had **view that PCI-DSS compliance is a technology issue and that First Third Bancorp compliance implies TJX compliance.**

c. CIO prioritized budget spending because **CIO was representing a cost center** and not revenue generating function, limited CIO influence at executive level.

#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."

major change contributing to the cyber-attack was TJX's ove from wired to wireless networking (Wi-Fi) in 2000 in a ort span of one year.

. Initially cyber security risk was low because vulnerabilities were unknown to everyone – experts, businesses, **and hackers**.

. TJX decided against upgrading to a more secure encryption algorithm for cost reasons.

laws in managerial decision making process.

. **Ease of recall bias** where recent experiences strongly influence the decision (i.e., no break-ins so far.)

#8: Dynamics and Migration to a High-Risk State, (2/2)

onfirmation trap is a decision maker's tendency to favor/seek formation that confirms his/her own beliefs and discount contradicting formation.

ly understanding is that we can be PCI-compliant without the planned 707 upgrade to WPA technology for encryption because most of our stores not have WPA capability without some changes. WPA is clearly best actice and may ultimately become a requirement for PCI compliance metime in the future. I think we have an opportunity to defer some ending from FY07's budget by removing the money for the WPA upgrade, t would want us all to agree that the risks are small or negligible."

Above is a message from CIO in November 2005 to his staff, requesting agreement on his belief that cyber security risk is low. -- there were only two opposing views, a majority of his staff agreed.

This confirmation trap led to postponing upgrades

#9: Recommendations

ccording to PCI Security Standards Council, compliance is a usiness issue requiring management attention and need to **integrate CI-DSS requirements within appropriate components on evelopment and operations parts of the control structure**.

. Doing so would not ensure full protection against a cyber-attack, but it will **help manage the risk more effectively**.

). Ensure that TJX is shielded from liability, because TJX was **fined $880,000*** by VISA for non-compliance plus another **$41 million**

U**nderstand objectives** of standards and align them with cyber ecurity and business needs, but **PCI-DSS not fully adequate**.

. Data must be encrypted when sent over a public network, **but not when transmitted within TJX**, over *intranet or behind a firewall*.

). PCI-DSS did not mandate using stronger encryption WPA until 2006, even though WPA was available in 2003.

#9: Recommendations

uilding a safety culture at TJX

ific steps can include:

. *Safety critical entities* can include encryption technology, hardware components (AP, servers, etc.), data retention/disposal/archival policies, a list of **Key Threat Indicators** (KTI)* to include in monitoring metric, and prevailing cyber security trends.

. *Implement a plan* to manage these entities with periodic reviews to update the list of safety critical entities.

. A **dedicated executive role** with cyber security responsibilities, will allow for a consistent view of TJX security technology across the organization.

KTI can be network traffic beyond an established threshold at TJX stores, umber of network connections at odd hours of the day, etc.

mparison of Results from FTC and CTC Investigations and STAMP/CAST Analysis

Recommendation	CPC	FTC	STAMP/CAST
Create an executive level role for managing cyber security risks.	No	*	Yes
PCI-DSS integration with TJX processes.	No	No	Yes
Develop a safety culture.	No	No	Yes
Understand limitations of PCI-DSS and standards in general.	No	No	Yes
Review system architecture.	No	No	Yes
Upgrade encryption technology.	Yes	No	*
Implement vigorous monitoring of systems.	Yes	No	*
Implement information security program.	No	Yes	*

Canadian Privacy Commission

4. Contributions of this Research

earch Contributions

Discussed **why** traditional approaches are ineffective for managing cyber security risks.

Highlighted **need** for system thinking and systems engineering approach to cyber security.

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 case** providing insights not discovered by other methods.

Recommendations provide a **basis for preventing similar events** in the future.

CyberSafe Systems

http://www.cybersafesystems.com/

hamid.salim@sloan.mit.edu