Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC\textsuperscript{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
Agenda

1. TJX (TJ Max and Marshalls stores) Case
2. System-Theoretic Accident Model and Processes (STAMP) and Causal Analysis based on STAMP (CAST)
3. STAMP/CAST Applied to TJX
4. Contributions
1. Background of the TJX (TJ Maxx and Marshalls stores) Case
data breach: At 45.6M card numbers, it's the biggest ever

By Jaikumar Vijayan

Stay Smart
Get the latest Android news, trends and apps and tips.

Sign up for the Greenbot newsletter

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

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.
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

(TJ Maxx & Marshalls) Case Study – Some Highlights

References: Federal/State Court records (primary), TJX SEC Filings, Others (NYT, WSJ, Globe, FTC, Academic Journal articles)
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.
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.
Flow for Sales of Stolen Payment Card Information.

- Via Bank in Latvia
2. System-Theoretic Accident Model and Processes (STAMP) and Causal Analysis based on STAMP (CAST)
STAMP Model

Hierarchical Safety Control

Structures

Three core concepts of STAMP

Safety Constraints

Process Models
TAMP Hierarchical Control Model
## STAMP/CAST Steps for Analyzing Accidents or Incidents

<table>
<thead>
<tr>
<th></th>
<th>STAMP/CAST Analysis Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Identify the system(s) and hazard(s) associated</strong> with the accident or incident.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Identify the system safety constraints and system requirements</strong> associated with that hazard.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Document the safety control structure</strong> in place to control the hazard and ensure compliance with the safety constraints.</td>
</tr>
<tr>
<td>4</td>
<td>Ascertain the <strong>proximate events leading to the accident</strong> or incident.</td>
</tr>
<tr>
<td>5</td>
<td>Analyze the accident or incident at the <strong>physical system level</strong>.</td>
</tr>
<tr>
<td>6</td>
<td><strong>Moving up the levels of the hierarchical safety control structure</strong>, establish how and why each successive higher level control allowed or contributed to the inadequate control at the current level.</td>
</tr>
<tr>
<td>7</td>
<td><strong>Analyze overall coordination and communication</strong> contributors to the accident or incident.</td>
</tr>
<tr>
<td>8</td>
<td><strong>Determine the dynamics and changes</strong> in the system and the safety control structure relating to an accident or incident, and any weakening of the safety control structure over time.</td>
</tr>
<tr>
<td>9</td>
<td><strong>Generate</strong> recommendations.</td>
</tr>
</tbody>
</table>
3. STAMP/CAST Applied to TJX
Step 1: Identify System(s) and Hazard(s)

**System(s)**
- TJX payment card processing system

**Hazard(s) – at system level**
- System allows for unauthorized access

Step 2 (1/2): Define System Safety Constraints and Requirements

**System Safety Constraints – at system level**
- **Protect** customer information from unauthorized access.
- Provide adequate **training to staff** for managing security technology infrastructure.
- **Minimize losses** from unauthorized access to payment system.
Components of Control Structure

1. Congress and Legislature
   - Laws, budget
   - Reports

2. Regulatory Agencies (FTC, SEC, etc)
   - Regulations, orders
   - Annual reports, SEC filings (10K)

3. State legislature
   - Laws, incentives
   - Reports, revenue

4. TJX Companies Management
   - System needs, RFP, procedures, budget
   - Reports

5. Project Management
   - System requirements, specifications, processes, procedures, resources
   - Testing results, issue logs, change requests

6. Systems Management
   - System testing, implementation
   - Issue logs, change requests
   - Support, maintenance

7. Operations Management
   - Policies, procedures, budget, plans, strategy
   - Reports

8. Payment Card Processing System
   - Processes, procedures, credit decision
   - Reports, payment card data, merchandise return data

9. TJX Retail Store System
   - Physical Process
   - Credit decision

10. Auditors
    - Audit report
    - Documents for auditing

11. Payment Card Brands
    - PCI-DSS compliance criteria, payment

12. Fifth Third Bancorp
    - Transaction
    - Payment

13. Customer bank
    - Payment card data, statements

14. TJX Customers
    - Personal, financial data, payments

15. Credit decision
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 Access Point (AP)** at a Marshalls store in Miami, FL.

Hackers 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.

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

Late 2005 hackers downloaded customer payment card data from TJX corporate transaction processing servers in Framingham, MA using Marshalls store connection in Florida.

2006 **hackers discover vulnerability**, that TJX was processing and submitting payment card transactions without encryption.
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 latvian 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.
TJX System Development and Operations

Congress and Legislature

Regulatory Agencies (FTC, SEC, etc)

State legislature

Laws, budget

Laws, incentives

Reports, revenue

Reports

Annual reports, SEC filings (10K)

Audit report

Documents for auditing

Auditors

TJX Companies Management

System needs, RFP, procedures, budget

System needs, RFP

Reports

Police, procedures, budget, plans, strategy

Reports

System requirements, specifications, processes, procedures, resources

Testing results, issue logs, change requests

Payment Card Processing System

Processes, procedures, credit decision

Payment card data, merchandise return data

Processed transactions, reports, PCI-DSS compliance criteria

Payment Card Brands

Fifth Third Bancorp

Transaction

Payment

Transaction, payment

Payment card data, statements

Customer bank

Personal, financial data, payments

TJX Customers

TJX Retail Store System

Physical Process

Support, maintenance

Monitoring reports, system logs

System testing, implementation

System testing, implementation, maintenance

Issue logs, change requests

Legend:
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
Levels of Technical Control
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.

2. Context:
   TJX not in compliance with PCI-DSS.

Unsafe 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, but (a) Fifth Third Bancorp had limited influence on TJX and (b) Visa had
Step #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.”

A major change contributing to the cyber-attack was TJX’s move from wired to wireless networking (Wi-Fi) in 2000 in a short span of one year.

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

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

Laws in managerial decision making process.

3. Ease of recall bias where recent experiences strongly influence the decision (i.e., no break-ins so far.)
Confirmation trap is a decision maker’s tendency to favor/seek information that confirms his/her own beliefs and discount contradicting information.

My understanding is that we can be PCI-compliant without the planned FY07 upgrade to WPA technology for encryption because most of our stores not have WPA capability without some changes. 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 ending from FY07’s budget by removing the money for the WPA upgrade, it 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

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

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

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

Understand objectives of standards and align them with cyber security and business needs, but PCI-DSS not fully adequate.

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

4. PCI-DSS did not mandate using stronger encryption WPA until 2006, even though WPA was available in 2003.
#9: Recommendations

Building a safety culture at TJX

Specific steps can include:

1. **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.

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

3. 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, number of network connections at odd hours of the day, etc.
Comparison of Results from FTC and CTC Investigations and STAMP/CAST Analysis

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

* Canadian Privacy Commission
4. Contributions of this Research
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.