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

Hamid Salim

Working Paper CISL# 2014-07

May 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

By
Hamid M. Salim

Submitted to the MIT Sloan School of Management, the School of Engineering, and the Department of Electrical Engineering & Computer Science in Partial Fulfillment of the Requirements for the Degrees of

Master of Science in Engineering and Management
and
Master of Science in Electrical Engineering and Computer Science
in conjunction with the System Design and Management Program

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2014

Signature of Author...
System Design & Management Program
May 16, 2014

Certified by...
Stuart Madnick
John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management &
Professor of Engineering Systems, MIT School of Engineering
Thesis Supervisor

Certified by...
Qi D. Van Eikema Hommes
Research Scientist, Engineering Systems Division, MIT School of Engineering
Thesis Supervisor

Accepted by...
Professor Leslie A. Kolodziejski
Chair of the Committee on Graduate Students

Accepted by...
Patrick Hale
Director
System Design & Management Program

THIS PAGE INTENTIONALLY LEFT BLANK

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

By
Hamid M. Salim

Submitted to the MIT Sloan School of Management, the School of Engineering, and the Department of Electrical Engineering & Computer Science on May 16, 2014 in partial fulfillment of the requirements for the degrees of

Master of Science in Engineering and Management
and
Master of Science in Electrical Engineering and Computer Science
in conjunction with the System Design and Management Program

Abstract

"…we must think anew, and act anew…"
- President Abraham Lincoln, December 1, 1862

If we are to manage cyber security risks more effectively in today's complex and dynamic Web 2.0 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.

The objective of this thesis was twofold. The first objective was to understand why traditional approaches for managing cyber security risks were not yielding desired results. Second, propose a new method for managing cyber security risks more effectively. The thesis investigated widely used approaches and standards, and puts forward a method based on the premise that traditional technology centric approaches have become ineffective on their own. This lack of efficacy can be attributed primarily to the fact that, Web 2.0 is a dynamic and a complex socio-technical system that is continuously evolving.

This thesis proposes a new method for managing cyber security risks 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. Based on a case study specifically written for this thesis, the largest cyber-attack reported in 2007 on a major US based retailer, is analyzed using the STAMP model.

The STAMP based analysis revealed insights both at systemic and detailed level, which otherwise would not be available, if traditional approaches were used for analysis. Further, STAMP generated specific recommendations for managing cyber security risks more effectively.

Thesis Advisor: Stuart Madnick
Title: John Norris Maguire Professor of Information Technology, MIT Sloan School of Management & Professor of Engineering Systems, MIT School of Engineering

Thesis Advisor: Qi D. Van Eikema Hommes
Title: Research Scientist, Engineering Systems Division, MIT School of Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

I was fortunate to have Professor. Stuart Madnick and Qi Hommes as my advisors, and I am profoundly grateful for their support and guidance during the process of writing my thesis. Professor Madnick believed in me and my research topic, and provided support when there was no wind to fill sails or when seas were rough. Because of his continued support and patience the ship stayed afloat. His cyber security expertise and feedback provided me with tremendous learning opportunities that helped shape my thesis and create a quality product.

Qi brought new life to my thesis, and her expertise helped set sail on the correct course with reference to STAMP/CAST analysis that generated the much needed momentum. Her questions and feedback provided me with unique opportunities to reflect, think with more depth, learn, and continuously improve the quality of my work, specifically with reference to STAMP/CAST model application to cyber security. Thank you Professor. Madnick and Qi in helping me create a robust and quality product. I appreciate your time, help, and advice.

Patrick Hale as always was available to serve as a safe harbor. As a mentor, Pat provided me with advice and support to work through challenges and set sail again towards completing my thesis. Thank you, Pat for acting as an anchor during rough seas and providing guidance. Many thanks to Jeff Shao (former SDM Finance Director), for always being approachable and eager to help me with financial matters. Thanks to System Design and Management (SDM) program staff for their administrative support.

Inspiration provided by my parents has enabled me to achieve my goals throughout life. My father, from his extremely humble beginnings taught me the value of education and hard work. My mother, despite her very limited formal education taught me to read, write, and tie a necktie. Without my parents support and advice, I would not be where I am today, thank you Daddy and Ami for your guidance, advice, inspiration, values, and a loving family. My siblings and their families are dispersed across the globe, but were never too far to provide their support and encouragement. My profound gratitude to my sisters Fauzia and Sofia, my brother Sajid, my nieces Benish, Mahwish, Sidra, Zobia, and nephew Daanyal.

"To reach a port we must sail, sometimes with the wind, and sometimes against it. But we must not drift or lie at anchor." – Oliver Wendell Holmes, Sr.

THIS PAGE INTENTIONALLY LEFT BLANK

Dedicated

To my
Dear Father – a proud Naval Officer, an Engineer, and an Entrepreneur
Captain. M. Salim Anwar T.I. (M), P.N. Retired.

And to my
Dear Mother – the foundation and the guiding light of our family
Najma Salim

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Meaning
AP	Access Point
ATM	Automatic Teller Machine
CAST	Causal Analysis based on STAMP
CDE	Cardholder Data Environment
CFAA	US Computer Fraud and Abuse Act
CIO	Chief Information Officer
CSIS	Center for Strategic and International Studies
DBIR	Data Breach Investigations Report
FTA	Fault Tree Analysis
FTC	Federal Trade Commission
IEEE	Institute of Electrical and Electronics Engineers
INCOSE	International Council on Systems Engineering
IoE	Internet of Everything
IRC	Internet Relay Chat
NASA	National Aeronautics and Space Administration
NYPD	New York Police Department
PCI-DSS	Payment Card Industry - Data Security Standard
PwC	PricewaterhouseCoopers
ROI	Return on Investment
SEC	U.S. Securities and Exchange Commission
SKU	Stock Keeping Unit
SQL	Structured Query Language
STAMP	System-Theoretic Accident Model and Processes
US-CERT	United States Computer Emergency Readiness Team
USSS	United Stated Secret Service
VERIS	Verizon Enterprise Risk and Incident Sharing
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

1 Introduction

"When the financial crisis of 2008 hit, many shocked critics asked why markets, regulators, and financial experts failed to see it coming. Today, one might ask the same question about the global economy's vulnerability to cyber-attack. Indeed, the parallels between financial crises and the threat of cyber meltdowns are striking." – July, 2012.

- Kenneth Rogoff, Professor of Economics and Public Policy at Harvard University and former chief economist of the International Monetary Fund from 2001 to 2003.

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 Web 2.0 ecosystem, where more of our personal information including financial, medical, shopping behaviors, photos, and emails are stored. With cloud computing we don't even know where our confidential information is stored or how safe and/or secure is it. Web 2.0 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. Yet major *reported* breaches that include TJX, Target, Hannaford Brothers, and Heartland Payment Systems, highlight the challenges in defending against cyber-attacks with all the investments in security technology infrastructure. This is the motivation underlying this thesis, which attempts to understand reasons contributing to limited efficacy of traditional approaches, and in light of which proposes a new method for managing cyber security risks more effectively.

1.1 Cybercrime Trend

In order to safeguard consumer and other information being created every day at a monumental scale, organizations spend significant technology resources in terms of software, hardware, fees (consulting, licensing, etc.), and person hours on creating an infrastructure that in theory should withstand cyber-attack(s). Globally, costs of managing cyber-attack risk and number of cyber-attacks are always rising owing to sophisticated methods used by cyber criminals. According to Symantec [1], in 2012, globally on average there were 116 targeted cyber-attacks (targeted cyber-attack uses customized malware and social engineering[1] to gain unauthorized access to sensitive information) per day, as compared to 82 per day in 2011 [2] – an increase of over 41%.

There are two primary factors contributing to the rising number of cyber-attacks. First, cyber criminals have the benefit of jurisdiction. A cyber-attack can originate from anywhere in the world, involving multiple perpetrators of different nationalities, and can have multiple hosting servers located in different countries. Given these jurisdictional complexities, it is easy to appreciate the limitations of prosecuting cyber criminals, even though the US Computer Fraud and Abuse Act (CFAA) apply to foreign entities. Second, cyber criminals are becoming sophisticated with support from a full-fledged underground economy [3]. An underground economy is a group of virtual marketplaces spanning transnational boundaries, where cyber criminals buy/sell stolen information (payment card data, social security numbers, drivers licenses, etc.), trade hardware/software used in cyber-attacks, and buy/sell services like web hosting and decryption of payment card Personal Identification Number (PIN) [4]. The underground economy allows cyber criminals to plan, execute, exfiltrate information, and monetize stolen information quickly and anonymously resulting in high costs to victims.

1.2 Cost of Cybercrime

Measuring monetary impact of cybercrime on businesses is in itself a challenge. Further, estimating cost of losses resulting from cyber-attacks is a complicated task – a topic of on-going research. One major contributing factor to this complexity is non-availability of data or inaccurate data on costs incurred by businesses from cyber-attacks. Security experts highlight at least four barriers to accurate reporting [5]. First, is *failure to report,* businesses that are victims of a cyber-attack do not want to report, because they perceive it as having a negative impact on their brand. Second barrier is *self-selection bias* where organizations that have not suffered losses from a cyber-attack may be more likely to respond to cybercrime surveys verses those that have incurred losses. On the flip side, organizations that have suffered highly publicized large losses

[1] In social engineering, an attacker uses human interaction (social skills) to breach organizations systems. An attacker using email or other digital method may pose as a new employee, repair person, or researcher to seek enough information to infiltrate an organization's network. [90]

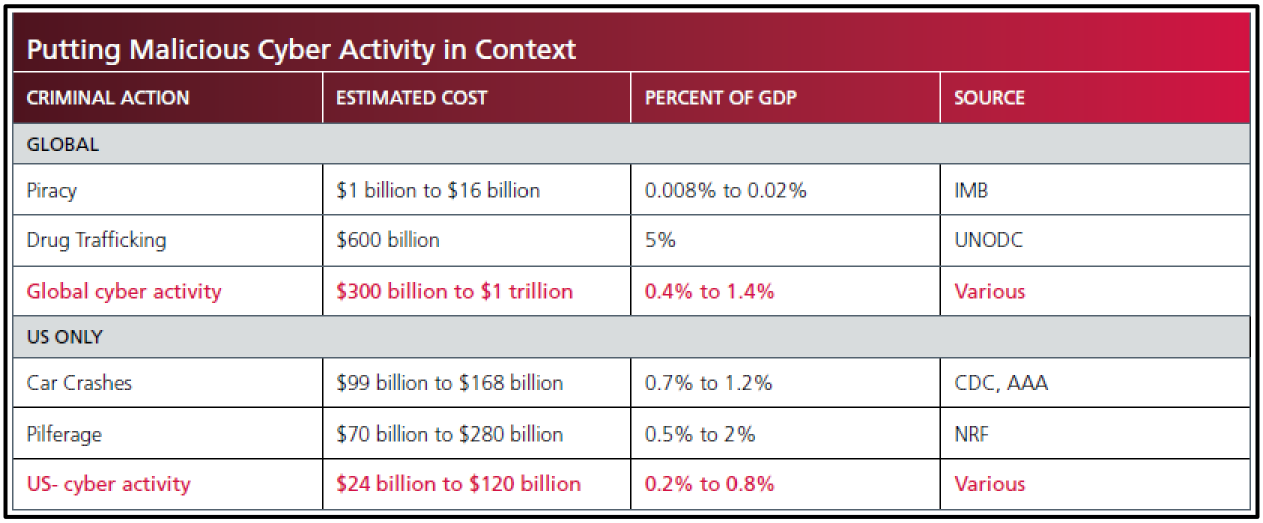
may be more willing to participate than those with moderate unreported losses. Third, there is *lack of a standard mechanism for accounting for losses*. There is not a standard set of attributes to include in calculating cost of a cyber-attack. Some attributes include system downtime, costs of purchasing new infrastructure, upgrades, security services, consulting fees, and legal fees, but there is no formal agreement on these or any other attributes. Fourth, barrier is *undetected losses* where a business is not aware that it has incurred losses from a cyber-attack. In general, when a cyber-attack is detected it is almost impossible to get an accurate estimate of losses because detailed impact of cybercrime is hard to determine, further compounding the problem is time lag between when the cyber-attack was launched until the time it was discovered.

To gain a general understanding of costs, Center for Strategic and International Studies (CSIS) in July 2013 published a report [6] sponsored by McAfee on The Economic Impact of Cybercrime and Cyber Espionage, which estimated the cost of cybercrime in the US to be $24 billion per year on the low end as shown in Table 1.1. The report used an approach of applying an analogy of already quantified and well researched events to set bounds for losses incurred from cybercrimes.

A contributing factor making cybercrime costly is that, organizations expend resources on defensive measures – ex post, and cyber criminals devote their resources to research and discovery of new offensive measures – ex ante. Managing risks of cyber security by investing in infrastructure upgrades based on past cyber-attacks is not yielding results, at a desired level. Instead, organizations globally are incurring costs that include lost information assets, human hours, lawsuits, and intangibles like goodwill and trust.

1.3 Asymmetries

Cyber criminals have a position of advantage because of asymmetries existing between them and their victims. Miller [7] points out that a technology centric cyber security strategy, creates a static and defensive posture for an organization. On the other hand, cyber criminals depict a dynamic behavior. That is, an organization must defend against all the *known* vulnerabilities, whereas cyber criminals only need to exploit *a* vulnerability – *known or unknown*, to launch a cyber-attack. Cyber criminals have the time and resources to discover vulnerabilities unknown to public, experiment, create, and execute new strategies/products for circumventing security of organizations. Savage and Schneider [8] present two additional asymmetries. First, maintaining and enhancing cyber security requires significant investments by an organization. On the other hand, launching a cyber-attack requires very little investment allowing cyber criminals to be agile. Cyber criminals can quickly adapt to a changing technological landscape at a negligible cost with support from underground economy. Second, it is difficult to quantify changes in risk achieved by new cyber security investments; therefore, security vendors are not incentivized to improve upon the technical aspects of their offerings. But cyber criminals can easily measure their Return on Investment (ROI), and therefore are incentivized to continuously innovate and improve their strategies and products for launching cyber-attacks.



Putting Malicious Cyber Activity in Context

CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global cyber activity	$300 billion to $1 trillion	0.4% to 1.4%	Various
US ONLY			
Car Crashes	$99 billion to $168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	$70 billion to $280 billion	0.5% to 2%	NRF
US- cyber activity	$24 billion to $120 billion	0.2% to 0.8%	Various

Table 1.1: Cost of cybercrime **[6]**.

1.4 Efficacy of Traditional Methods

Data gathered from around the globe by major security companies, shows that technical approaches to cyber security have limited efficacy. Symantec Corporation in its 2013 Internet Security Threat Report [1] attributed 40% of data breaches in 2012 to hackers, making them the number one source of cyber-attacks as shown in Figure 1.1. According to Symantec [9], “hacker is a term used by some to mean a clever programmer and by others, especially journalists or their editors, to mean someone who tries to break into computer systems”, Merriam-Webster defines a hacker as “a person who illegally gains access to and sometimes tampers with information in a computer system”. Symantec uses the term hacker in the context of cyber security, which means gaining illegal access to a computer system(s) with malicious intent. Behind hackers, number two source accounting for 23% of data breaches is an accidental data compromise – a problem not addressable singularly by technical solutions. Similar trend held for the year 2013 as shown in Figure 1.1, where hackers were again the primary source of data breaches, according to Symantec Corporations 2014 Internet Security Threat Report [10]. This data provides credence to limitations of technical approaches, because data breaches are on an upward trajectory.

Another source – McAfee Labs, in its first quarter 2013 McAfee Threats Report [11], highlighted perpetual growth in malware[2], see Figure 1.2. This pattern of increasing number of new malware products highlights capabilities and agility of cyber-attackers, who constantly adapt and respond to new security measures implemented by organizations. Contributing to increase in malware are vulnerabilities in security technology – that are in general exploited by malware, and therefore expose businesses to cyber security risks. McAfee Labs report attributed majority of network attacks to browser-based threats – where cyber criminals exploit vulnerabilities in popular browsers, followed by SQL injection threats – where cyber criminals exploit vulnerabilities embedded within an organizations website, see Figure 1.3. To provide context around number of known vulnerabilities in commercial technology, Symantec identified approximately six thousand new vulnerabilities for the first eleven months of 2013 [12], including vulnerabilities that were previously unknown to public or vendors and for which no patches were available, this type of vulnerability is called *zero-day* vulnerabilities. Further, in addition to browser and mobile operating system, plug-in vulnerabilities were also in the mix with Oracle Sun Java in the lead, see Figure 1.4.

This is a disturbing trend, because any medium or large organization has a website for its business, and offer e-commerce services in a Business-to-Business (B2B) or Business-to-Consumer (B2C) setting from banking to retail purchases. Therefore organizations are constantly exposed to the risk of a cyber-attack from anywhere in the world, if vulnerabilities in a browser, an application(s), or a website are detected and can be successfully exploited.

[2] Merriam-Webster defines malware as software designed to interfere with a computer's normal functioning.

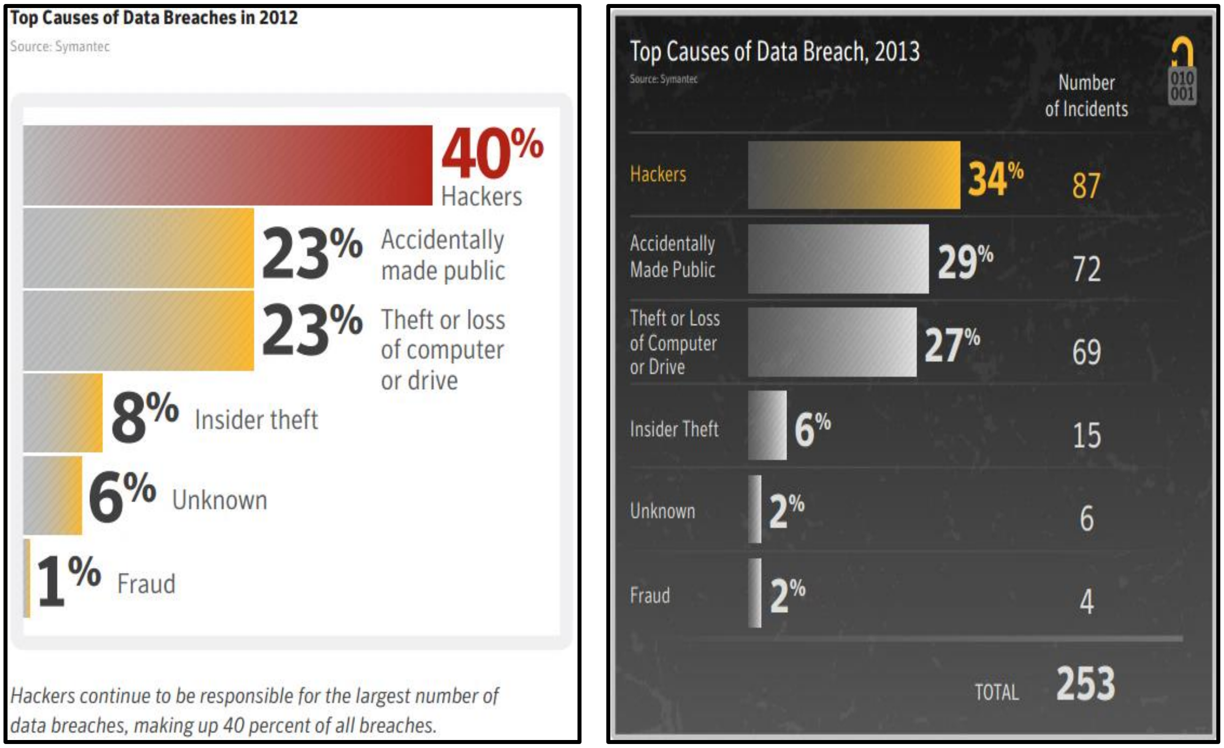


Figure 1.1: Top causes of data breaches in 2012 **[1]** and 2013 **[10]**.

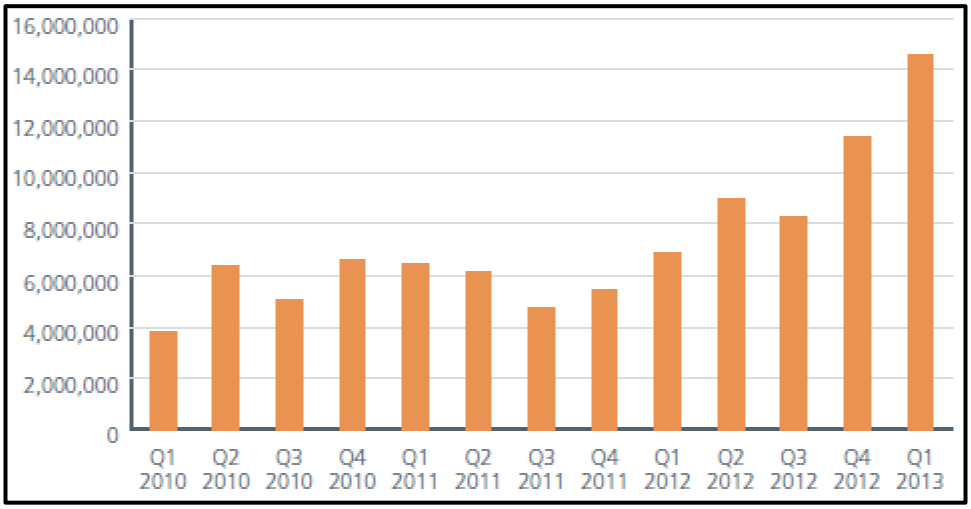


Figure 1.2: Number of new malware (2010-Q12013) **[11]**.

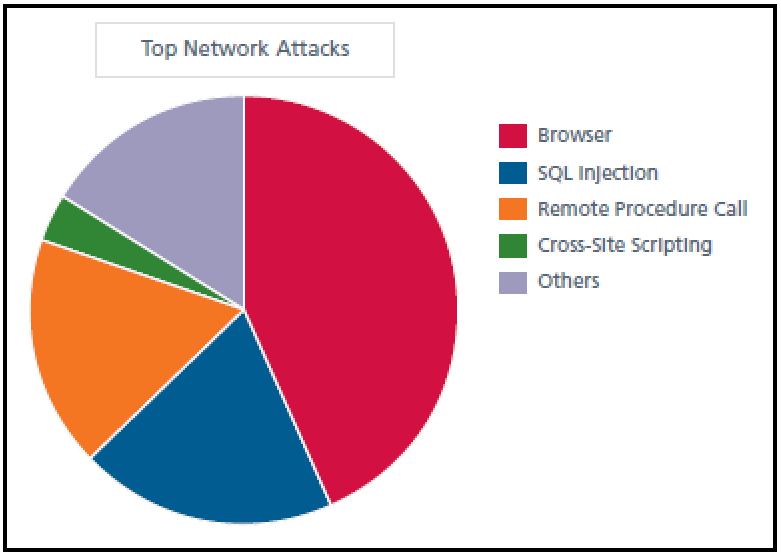


Figure 1.3: Sources of network cyber-attacks **[11]**.

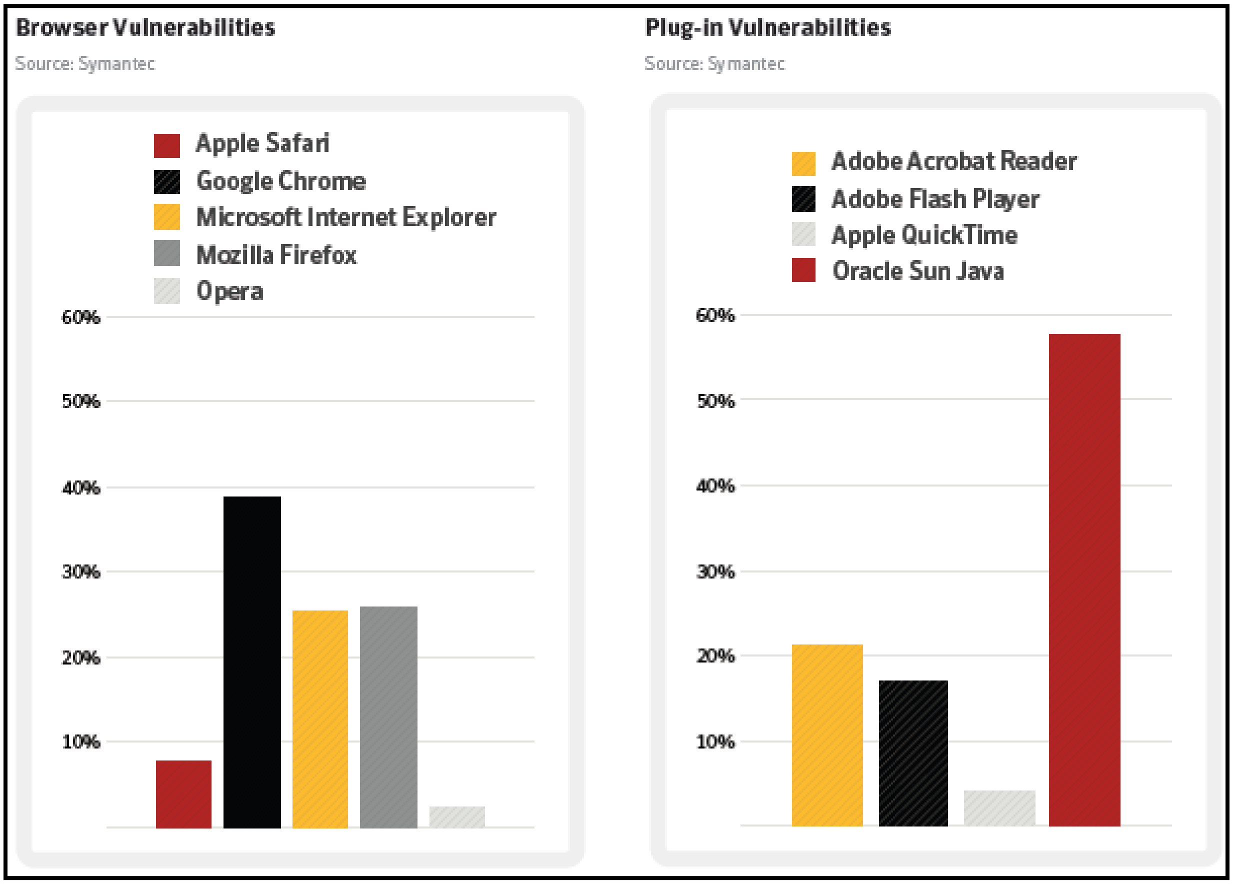


Figure 1.4: Vulnerabilities discovered during Jan-Nov, 2013 **[12]**.

1.5 Limitations of Traditional Methods

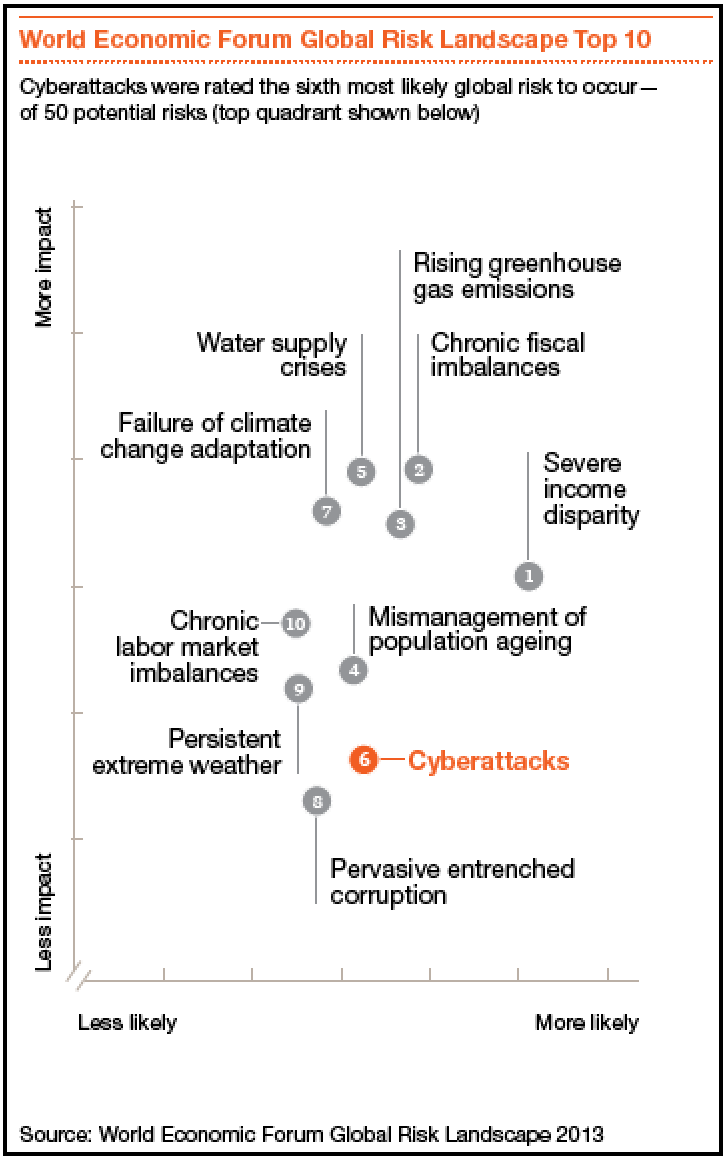
Cyber-attack risks are increasingly being recognized as a significant global threat to organizations. According to PricewaterhouseCoopers (PwC) citing 2013 World Economic Forum Global Risk Landscape report, cyber-attacks was rated sixth as a global threat out of 50 global risks covered in the World Economic Forum report [13], as shown in Figure 1.5.

Realizing that cyber-attack risks are increasing and are inevitable, organizations are starting to view cyber security as an organizational challenge rather than only as an Information Technology department issue. In the PwC 16th annual global CEO survey of 2013, 31% believed that a cyber-attack is likely to occur as indicated by red arrow in Figure 1.6 [14].

With cybercrime being viewed as a serious threat at organizational level and keeping in perspective the issues discussed above, current cyber security approaches are traditional and lack innovation. Cyber security in a business environment predominantly is addressed by making investments in hardware and software, generally amalgamated with industry standards, guidelines, and internal controls. Most efforts – specifically technical, are implemented with a central theme of creating a secure fence around 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. That is, the focus is on only part of the problem, while an organization and interactions within the organization are either not taken into account or are not a priority. Second, this narrow focus on security technology reinforces a dominant perception that cyber security is Information Technology department problem. Third, within the context of Web 2.0 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. All of these reasons highlight that technical approaches address only a subset of much larger set of cyber security problems, and are lacking a systemic view.

An important question then is why there is a lack of focus on holistic approaches to cyber security? Or in other words, why in general, technology centric solution is a dominating strategy for addressing cyber security risks? One plausible explanation is lack of awareness and/or unavailability of a comprehensive holistic model for approaching cyber security with a systemic view.


World Economic Forum Global Risk Landscape Top 10

Cyberattacks were rated the sixth most likely global risk to occur—of 50 potential risks (top quadrant shown below)

Source: World Economic Forum Global Risk Landscape 2013

Figure 1.5: Cybercrime risk in relation to top 10 global risks **[13]**.

Momentum is gaining strength in industry and academia, for a need to complement technical solutions with new approaches for addressing cyber security. John South, Chief Security Officer of Heartland Payment Systems[3] commented on cyber-attack on their systems –

[3] Heartland Payment Systems is a provider of payment card processing solutions. It processes over 11 million transactions a day and over $80 billion a year [89].

in 2008 intruders stole credit card data by exploiting a weakness in Heartland Payment Systems non-financial application, "Heartland's remediation went farther than repairing the weak

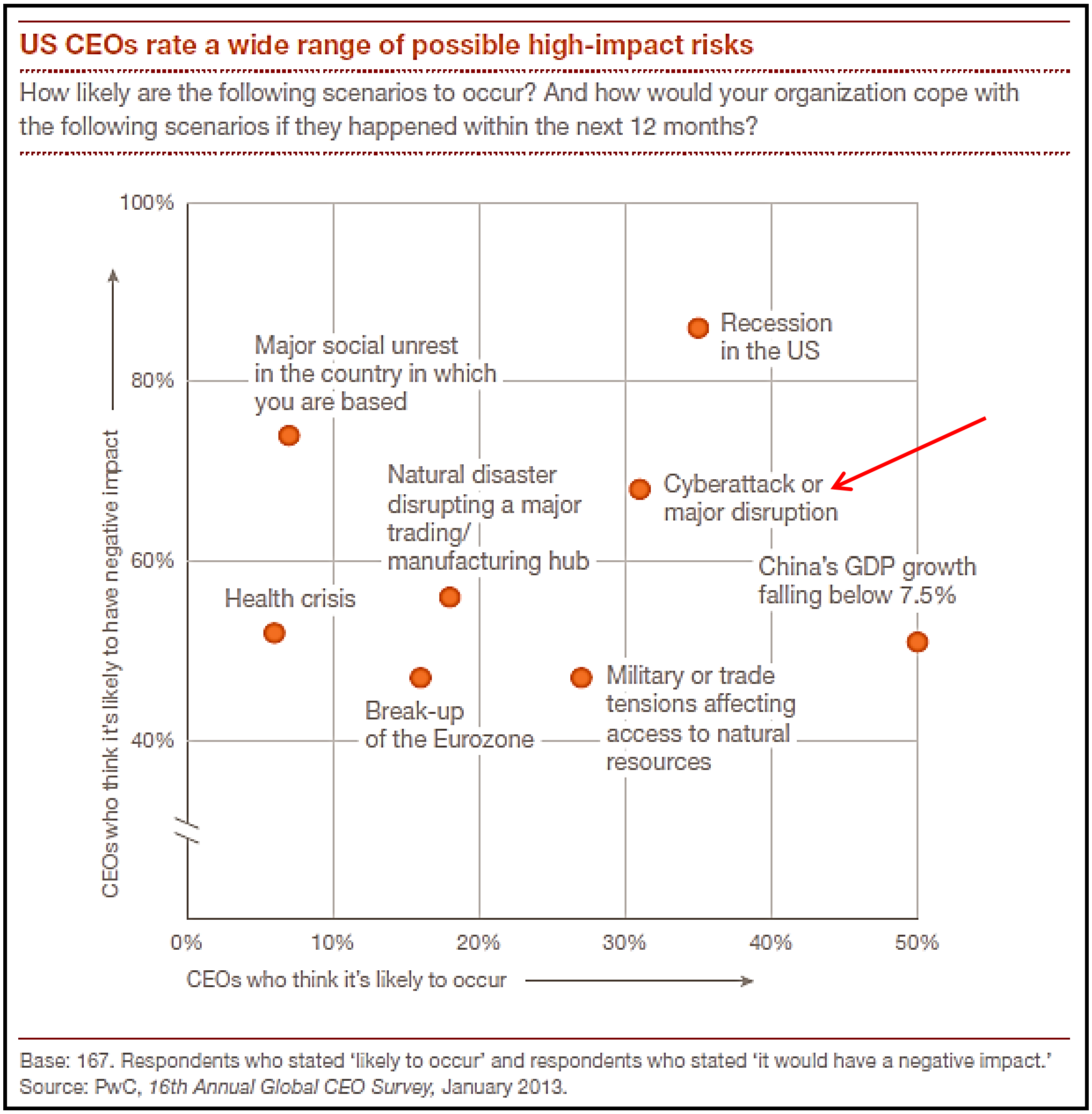


Figure 1.6: CEO view of global high impact risks **[14]**.

application. Yet the strategy of building impermeable systems, an ideal of years past, is no longer feasible, because corporations have resource and time constraints, while potential attackers have ample time, money and, in some cases, nation-state protection…" [15]. South raises two important points with this statement, first, systems have become highly complex in our Web 2.0 ecosystem requiring components and support from multiple vendors, therefore creating systems with no (or near zero) risk of a breach is no longer possible. Second, cyber criminals have a solid ecosystem of support and access to resources across national boundaries. South further states that "…traditional security strategy would be to shore up the network and apps, make sure firewalls are out there, a lot of the things you see in security standards, but the fact is he will probably try something innovative or something you're not focused on to get to the data he needs" [15]. Here South points out that even though Heartland went beyond addressing a specific vulnerability in an application, this is not a feasible approach for the future as it had been in the past, because cyber criminals are innovative and sophisticated devoting their resources to discovery of vulnerabilities. South's lack of confidence in traditional security technology that include upgrading applications/network and installing firewalls, is indicative of a gap that exists, for addressing cyber security risks beyond traditional security approaches. His comment with reference to limitations of traditional strategies highlights a need for a holistic thinking model. For example traditional cyber security strategies do not address questions like, are non-technical employees trained to spot unusual activity on a system? Is system designed to protect data by using encryption? Can human error cause a process to fail contributing to cyber security risk?

Lance James, former chief scientist at Vigilant Inc. a security services firm acquired by Deloitte[4], shared his view on technology centric approach to cyber security, "the problem with today's cyber security industry is that we throw technologies at it and don't look at the people behind the problem" [15]. James identifies a critical component of cyber security – the people, again highlighting a need for a more holistic strategy for cyber security that goes beyond technical solutions. Recall that the aforementioned Symantec report attributes 23% breaches as accidental; it is plausible to assume that people were a major contributing factor for these breaches, which reinforces James point.

International Council on Systems Engineering (INCOSE) deputy technical director William Miller agrees that only a technology focused cyber security approach puts organizations at a disadvantage. Relying on technology based methods creates a static and defensive environment because only known technical risk(s) are addressed which is only a part of the whole. The whole can include people, processes, interdependencies with other systems, and culture. Therefore organizations are left anticipating a cyber-attack even after making investments for addressing cyber-attack risks. On the other hand, cyber criminal's core business

[4] Deloitte press release: http://www.deloitte.com/view/en_US/us/press/Press-Releases/449a1510aa5fe310VgnVCM2000003356f70aRCRD.htm

is to launch cyber-attacks, and operate with agility in a dynamic environment, constantly looking for vulnerabilities in technologies or use technology to exploit human behavior. In the aforementioned statement by South, he also makes a similar point where organizations are resource constrained and cyber criminals deploy innovative methods and resources to launch cyber-attacks creating an asymmetry. According to Miller, organizations get caught in a cycle of constantly patching their hardware and software systems and not addressing the design of a system [7]. This constant patching further exposes organizations to additional cyber security risks, because new patches may in itself have unknown vulnerabilities, further timeframe for testing is generally limited in an organization, and chances are that system as a whole is not subjected to rigorous testing.

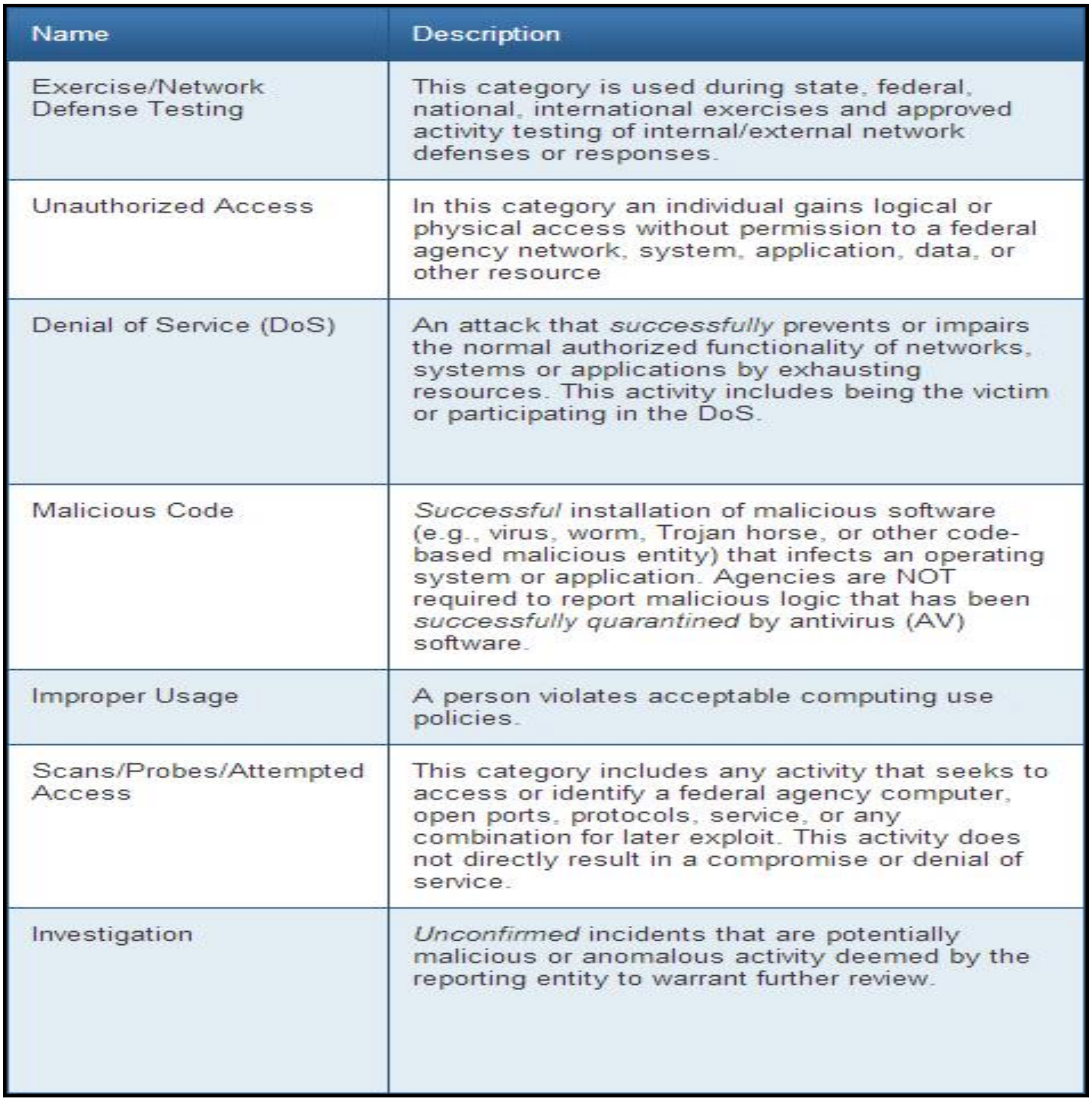
1.6 Cyber Security Risk Categories

Cyber security risks can fall into different categories, each with its own implications. United States Computer Emergency Readiness Team (US-CERT) defines six categories (excluding Exercise/Network Defense Testing category, because it is meant for federal government internal use only) for federal agencies as shown in Figure 1.7 [16], which are generally also applicable to non-government entities.

For example, *Unauthorized Access* in the context of a business implies that an individual or a group of individuals access business systems without permission, that can lead to losses including data, intellectual property, and account id/passwords. Implication of *Denial of Service (DoS)* category is when a cyber-attack renders a business website inaccessible, because the network is overwhelmed with excessive web page requests, generating high volume of traffic that cannot be handled by victim's network. Another example is when unauthorized software is installed on cyber-attack victim system(s), implications of this activity categorized as *Malicious Code* include recording of keyboard strokes, infecting systems with viruses, and stolen data. For this thesis, categories of unauthorized access and malicious code are relevant.

1.7 Holistic Approach to Cyber Security

This thesis argues 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. According to Savage and Schneider [8], cyber security itself has inherent problems, because unlike software and hardware, cyber security is not a commodity and cannot be scaled with technology add-ons. Or stated another way, in response to new threats managing cyber security risks is difficult by adding software and/or hardware. Therefore, cyber security needs a holistic approach, and to create a holistic strategy organizations need to go beyond security technology, to also understand and address non-technical risks contributing to the



Name	Description
Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.
Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource
Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.
Improper Usage	A person violates acceptable computing use policies.
Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Figure 1.7: Federal agency incident categories as defined by US-CERT **[16]**.

cyber security problem. Therefore organizations need to resist cyclical trap of traditional reactive measures, and move towards inclusion of proactive approaches to complement traditional methods for managing cyber security risks. Savage and Schneider [8] 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. An example of this is the data breach at Heartland Payment Systems, recall from earlier discussion that a flaw in Heartland Payment Systems non-financial application led to the compromise of the overall system security.

This thesis also argues that technical approaches are *a* part of a larger whole, and amalgamation with a holistic strategy will improve deterrence against a cyber-attack but not eliminate the risk completely. Thinking systemically will help focus on the whole system and its interdependencies with other sub-systems and systems.

Elaborating on complexity aspect of Web 2.0 ecosystem highlighted in previous sections, three points with reference to complexity can help in understanding, a need for a holistic approach to cyber security risk management as a complement to traditional methods. First, cyber space is a highly complex environment composed of billions [17] of connected devices running multiple complex applications. Organically adding to this complexity, is the intrinsically dynamic nature of the internet acting as a catalyst of growth, where the number of hosts increased from approximately five million in January 1995 to over 963 million in January 2013 [18]. In January 2012 there were over 888 million hosts, adding over 75 million hosts in just twelve months as shown in Figure 1.8 [18]. Second, PwC in its 17th Annual Global CEO Survey citing Cisco, indicated that number of connected devices is increasing per person and projected to grow to seven per person by the year 2020, compared to a current count of approximately three per person [19], as shown in Figure 1.9. This trend highlights increasing interaction between human and machine, providing more avenues of exposure to cyber security risks. Further, more devices implies more software and hardware contributing to a more complex Web 2.0 environment. Third, Internet of Everything (IoE) phenomenon as shown in Figure 1.10 that Cisco defines as [20], “bringing together people, process, data, and things to make networked connections more relevant and valuable …” integrates people, processes, data, and things, which historically have not operated in an interconnected manner with reference to four IoE dimensions (people, processes, data, things). IoE amalgamates all four dimensions by integrating machine-to-machine (M2M), person-to-machine (P2M), and person-to-person (P2P) connections, adding complexity to the Web 2.0 ecosystem.

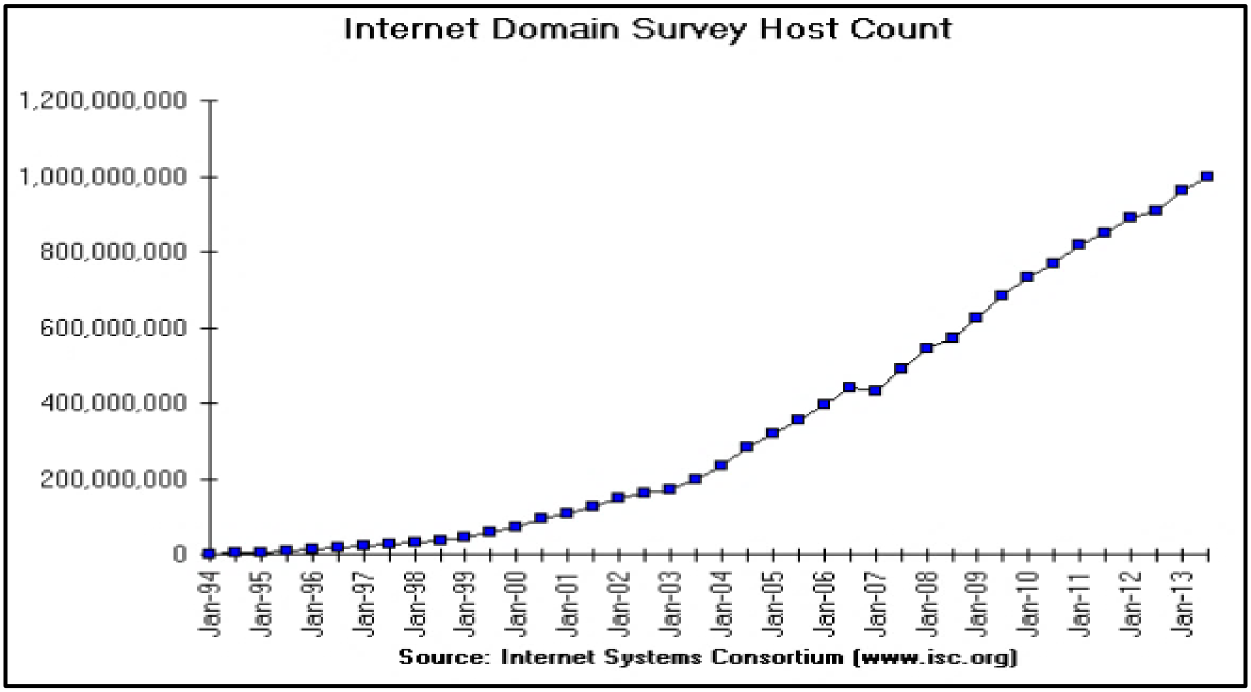


Figure 1.8: Number of internet hosts (1994-2013) **[18]**.

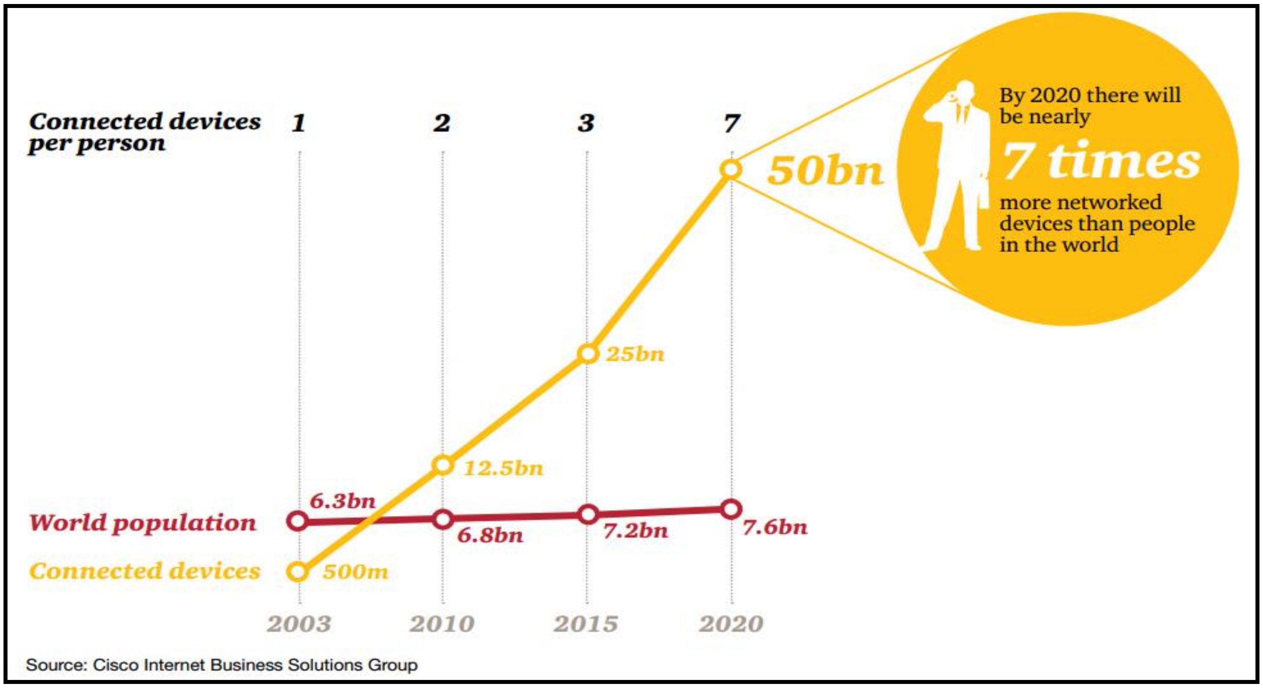


Figure 1.9: Projected growth in the number of connected devices **[19]**.

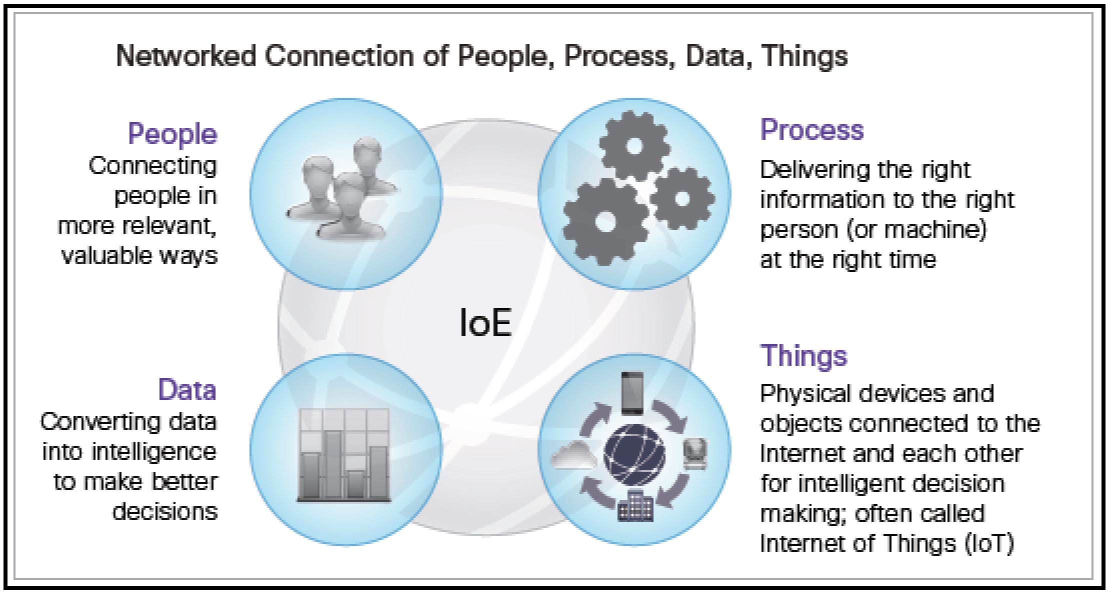

Networked Connection of People, Process, Data, Things
People
Connecting people in more relevant, valuable ways
Process
Delivering the right information to the right person (or machine) at the right time
IoE
Data
Converting data into intelligence to make better decisions
Things
Physical devices and objects connected to the Internet and each other for intelligent decision making; often called Internet of Things (IoT)

Figure 1.10: Internet of Everything (IoE) **[20]**.

The above discussion highlights the fact, that people are an essential dimension of any successful holistic cyber security strategy. In our complex Web 2.0 ecosystem, we constantly interact at a professional and personal level 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 [21]. This technical interaction with human behaviors adds to the complexity of Web 2.0 ecosystem. Further adding to this complexity are the interdependencies that exist between systems and subsystems of our global digital ecosystem.

Consequently, with an ever growing threat of sophisticated cyber-attacks, and limited efficacy of traditional approaches for safeguarding systems, organizations are exposed to costly vulnerabilities. So the question then is what is the solution for managing vulnerabilities outside of traditional security technology approaches? Hypothesis of this thesis is that traditional approaches can be complemented by incorporating additional measures guided by applying Systems Safety Model called STAMP[5] (Systems-Theoretic Accident Model and Processes) developed at MIT. STAMP is based on Systems Thinking (discussed next) and Systems Theory. The model has traditionally been applied to complex aerospace and military systems safety. This thesis applies STAMP, to cyber security to test the hypothesis.

[5] Details discussed in Chapter 2.

As a first step towards applying STAMP, cyber security needs to be viewed holistically from the lens of *systems thinking*. Peter Senge defines systems thinking as “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'…Today systems thinking is needed more than ever because we are becoming overwhelmed by complexity…Perhaps for the first time in history, humankind has the capacity to create far more information than anyone can absorb, to foster far greater interdependency than anyone can manage, and to accelerate change far faster than anyone’s ability to keep pace. Certainly the scale of complexity is without precedent.” [22]. 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. STAMP model embodies Systems Thinking in a socio-technical context.

One can now appreciate that cyber space is a complex and dynamic sociotechnical system. This is the foundation for understanding STAMP and its application to cyber security. In this thesis, I will attempt to answer the following research question by way of a case study, and to demonstrate how STAMP differs from other approaches or methods for addressing cyber security risks.

Is STAMP an effective method for identifying causal factors leading to a cyber-attack?

1.8 Thesis Structure

The objective of this thesis is to propose a Systems Safety model that may help in better managing cyber security risks and act as a complement to traditional approaches. This thesis is organized into eight chapters. Chapter 2 discusses literature review, covering Chain-of-Events Model, its derivative method Fault Tree Analysis, ISO, and COBIT. In Chapter 3, some key definitions are provided in the context of cyber security, further, some terms related to STAMP/CAST are also redefined in the cyber security context. Chapter 4 presents the TJX case study, and includes an in-depth discussion of the TJX data breach including the cyber-attack, exfiltration, operations, execution, and money laundering of proceeds from overseas. TJX was chosen as a case study because it was the first major cyber-attack that involved over $170 million in losses supported by a sophisticated underground cybercrime ecosystem. The TJX case study was specifically written for this thesis, using federal and state court documents as primary sources pertaining to the litigation, and prosecution of cybercriminals with reference to the TJX cyber-attack. Additional, sources include Wall Street Journal, The New York Times, The Boston Globe, and TJX 10K filings/annual reports. Chapter 5 analyzes the TJX cyber-attack by applying STAMP/CAST model, which consists of nine steps. In Chapter 6 recommendations from STAMP/CAST analysis are compared with a report by the Office of the Privacy Commissioner of Canada and findings of Federal Trade Commission (FTC) investigation. Chapter 7 highlights contributions that this thesis attempted to make with reference to more effectively managing cyber security risks. Finally, Chapter 8 presents some opportunities for future work with reference to STAMP in the context of cyber-security.

2 Literature Review

This chapter discusses Chain-of-Events Model and its derivative method Fault Tree Analysis (FTA) both of which are generally used for investigating cyber-attacks, and understanding causal factors leading to cyber security risks. This chapter also presents 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[6] 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[7]. Finally, a new model for analyzing accidents called System-Theoretic Accident Model and Processes (STAMP) developed at MIT [23] is introduced.

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 [24]. Second generation accident models incorporated *multiple* causal factors and associations among them for determining causes of an accident [24]. 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 [24], 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. Expanded Chain-of-Events model can also include relationships between events, which use Boolean logic for representation.

Consider an example of a salesperson travelling out of town on business, who at end of the day after making sales calls, checks into a hotel and uses work computer to access business and personal email accounts. Assume that personal email account is one of the widely used web based email services that include Gmail or Yahoo. During course of reading personal emails,

[6] http://www.isaca.org/COBIT/Pages/info-sec.aspx

[7] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533

salesperson's computer is infected by a phishing email leading to loss of personal information. An event chain for this scenario might take the form where there are three events as shown in Figure 2.1. Event 1 is described by salesperson accessing business and private email accounts from work computer, Event 2 is related to a phishing email from personal email account successfully persuading the salesperson to open an attachment, and Event 3 is described by salespersons computer being infected with malicious software leading to loss of personal information. In this situation, accessing personal emails from a work computer is a risky act. Further, Event 1 can be designated as proximate or root event in the chain, and circumstance of being away from home prompted the salesperson to depict risky behavior of using work computer for accessing personal email account with Gmail or Yahoo. In this situation, a possible solution might be to intervene between Event 1 and Event 2, to scan personal emails for malicious software. Another, option is to break the chain by eliminating Event 2, which can be achieved by restricting use of work computers for business purposes only by blocking widely used web based email services.

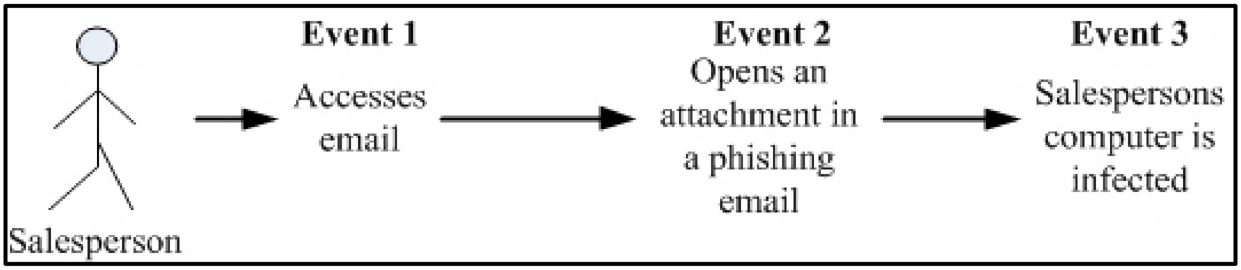

Salesperson
Event 1
Accesses email
Event 2
Opens an attachment in a phishing email
Event 3
Salespersons computer is infected

Figure 2.1: Event chain for travelling salesperson scenario.

2.1.1 Chain-of-Events Model at Verizon Business

A real world example is use of Chain-of-Events Model by Verizon Business, which every year in collaboration with United States Secret Service (USSS), Dutch National High Tech Crime Unit (NHTCU), and et al[8], conducts a study of cybercrimes from around the globe and publishes Verizon Business Data Breach Investigations Report (DBIR) [25].Verizon Business uses Verizon Enterprise Risk and Incident Sharing (VERIS) framework [26] [27] for describing security incidents. VERIS defines a security incident (or security compromise) as any event affecting any security attribute (confidentiality/possession, integrity/authenticity, and

[8] See Appendix 2 for a complete list of partners. *Source*: [25]

availability/utility) of any information asset. After the description of security incidents is complete, the framework then utilizes Chain-of-Events Model to understand the causal factors which led to a cyber-attack [28].

To illustrate the use of Chain-of-Events Model by Verizon Business, consider a hypothetical scenario discussed in 2011 DBIR report [29]. Figure 2.2 depicts the corresponding event chain illustrating a targeted phishing attack used to steal information from an organization. Each square represents events E1, E2, E3, and E4, diamond represents an error condition event CE1. VERIS defines an error as “anything done (or left undone) incorrectly or inadvertently”. This includes omissions, misconfigurations, and programming errors. According to the Verizon methodology, *‘the goal is straightforward: break the chain of events and you stop the incident from proceeding’* [29]. For example, the report points out that, security awareness training and e-mail filtering may prevent the event E1.

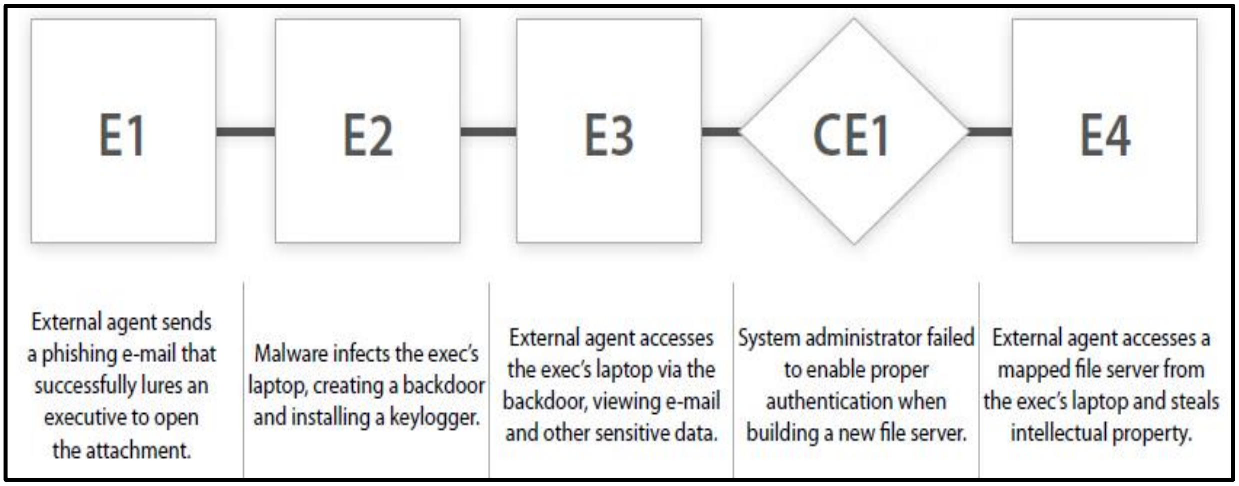

E1
E2
E3
CE1
E4
External agent sends a phishing e-mail that successfully lures an executive to open the attachment.
Malware infects the exec's laptop, creating a backdoor and installing a keylogger.
External agent accesses the exec's laptop via the backdoor, viewing e-mail and other sensitive data.
System administrator failed to enable proper authentication when building a new file server.
External agent accesses a mapped file server from the exec's laptop and steals intellectual property.

Figure 2.2: Example VERIS incident scenario **[29]**.

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. Chain-of-Events Model by design allows an analyst to consider not only risky behavior but also conditions contributing to failure events. 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 [30]. Some shortcomings of Chain-of-Events Model are discussed next within the context of cyber security.

2.1.2 Limitations of Chain-of-Events Model

Chain-of-Events Model limitations render this method ineffective for investigating causal factors in the context of cyber security. First, determination of causal factors is dependent upon the choice of events (unsafe acts or risky behavior) and related conditions[9] (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 [30]. This point is even more pronounced within the context of cyber security, because non-physical events are at the core and there are few physical events involved in a cyber-attack. For example, typically unauthorized system intrusions resulting in data loss occur by exploiting vulnerabilities in software and not by physically removing data storage device(s). With reference to subjectivity, the choice of which events to include in Chain-of-Events Model depends on how far back the events can go. This determination can be based on factors that can include organizational boundaries, expertise of an analyst, lack of information for an event, etc. Therefore, new events can always be added to an initiating or root event. With reference to conditions, the choice can depend on analysts' level of expertise or experience, introducing bias in selection of conditions. Therefore, selection of events and conditions is arbitrary leading to yielding inconsistent causal factors depending on the choice of events and conditions [30]. Issue of subjectivity is also highlighted in Verizon Business 2011 and 2012 DBIRs [29] [28].

Second, it is impossible to determine a terminal point when traversing back from an accident event [24], because there is no fixed standard to make this decision. It is also difficult to know that if a chosen terminal event or other events (in between accident and terminal events) are relevant and would provide enough information for robust counter measures to reduce cyber security risk. For example, in Figure 2.2 it is not clear that when traversing back from loss event E4, if an analyst should stop at CE1, E3, E2, or E1event because each of these events can be a candidate for further investigation into what conditions led to the loss. For example, assuming that event CE1 is chosen as terminal event and system administrator is blamed for

[9] Events have finite duration, and conditions persist until an event occurs resulting in new or different conditions [30].

misconfiguring the server. But, in this case event E1 will be ignored and questions related to the efficacy of organizations phishing email filters would not be addressed. Further, it is not possible to know what other events and conditions contributed to event E1, because it is a terminal event in the chain.

Third, in general digital forensics is widely used as a starting point for investigating a cyber-attack in a Chain-of-Events Model, which by definition is focused on technical aspects of a system under study. Chain-of-Events Model compounds its shortcomings with use of digital forensics, by narrowing the focus with reference to the choice of events and conditions. That is, limiting problem solving and investigation to technical events and conditions, leading to possibly discounting non-technical causes of a cyber-attack. Digital forensics is also facing its own challenges in today's complex Web 2.0 ecosystem limiting its efficacy, as discussed by Garfinkel [31]. Amongst several issues highlighted by Garfinkel, the three most relevant to cyber security are discussed here. First, malware can be written to reside in memory instead of a physical hard disk drive, requiring more expensive memory forensics because of the complexity involved in working with virtual memory. Second, as technology becomes more tightly coupled with daily human life, privacy laws are being tightened, limiting the ability of forensic experts to conduct investigations due to possible legal challenges. Third, Web 2.0 environment is highly complex and dynamic, requiring a forensic expert to analyze multiple software and hardware products from multiple vendors and then correlate all the data gathered. This requires expertise across software and hardware platforms, involving technology professionals from a spectrum of expertise that includes network, databases, applications, storage management, and legal to highlight a few areas. Digital forensics with its shortcomings is still a valuable tool, but its use with Chain-of-Events Model diminishes its efficacy.

Fourth, Chain-of-Events Model by design promote linear causality relationships [30] [32], making it very challenging to account for non-linear causalities that may contribute to cyber security risk. Considering the example in Figure 2.2 a non-linear causality with reference to event CE1 may be that the system administrator's negligence was due to lack of rigorous testing, because of non-availability of adequate infrastructure for a test environment attributed to organizational budget cuts. Budget constraint is a non-linear causality because it is not the direct cause of event E4 as shown in Figure 2.2. In the authors experience, IT resource constraints is a very common reason cited by management for lack of a test environment for IT projects (specifically in organizations where core business is not technology), prompting engineers to risk security and safety of technology assets contributing to an elevated cyber security risk.

Fifth, 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. Further, because of arbitrary choice of events and conditions that can lead to discovering different vulnerabilities depending on the choice, chances are that all known vulnerabilities will not be addressed. Also Chain-of-Events Model provides little or no foresight about undiscovered vulnerabilities in existing systems. This lack of foresight leaves systems exposed to cyber security risks, because future cyber-attacks are unlikely to exploit already addressed vulnerabilities, and there are thousands of phishing sites that provide opportunities to hackers for exploiting undiscovered vulnerabilities. For example, according to most recent Phishing Activity Trends Report covering 3rd quarter of 2013 [33], there were over 45,000 unique phishing sites in September, 2013 as shown in Figure 2.3, with the US as a leading[10] country by hosting over 58% of phishing sites as shown in Figure 2.4. So, an organization might improve its phishing filters following a cyber-attack, but chances are that phishing emails might still get past updated filters given the sheer number of phishing sites around the globe, that very likely generate updated versions of phishing emails[11]. Once past a phishing filter, emails can exploit a new (for which countermeasures are not implemented yet), an undiscovered (unknown to organization), or zero-day (unknown to public) vulnerability. As discussed in Chapter 1, other examples, from the perspective of an organization, with reference to a path for launching a cyber-attack with these vulnerabilities include browsers and plug-ins.

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 [30]. For example, in Figure 2.2 event CE1 could have resulted due to lack of training resulting from budget cuts over the years. This non-linearity will not be captured by Chain-of-Events Model, because generally focus is on proximate events preceding a loss, whereas a non-linear event could have been seeded years or

[10] Status of US as a top country for hosting phishing sites is primarily because, a significant number of worlds websites and domain names are also hosted in the US. [33]

[11] As discussed in Chapter 1, this is another example of asymmetry between cybercriminals and victims of cybercrimes.

months in advance. Although, Swiss Cheese Model[12] takes management and organizational issues into consideration, it is still based on Chain-of-Events Model and therefore inherits its limitations. These models also oversimplify causality and thereby countermeasures [34].

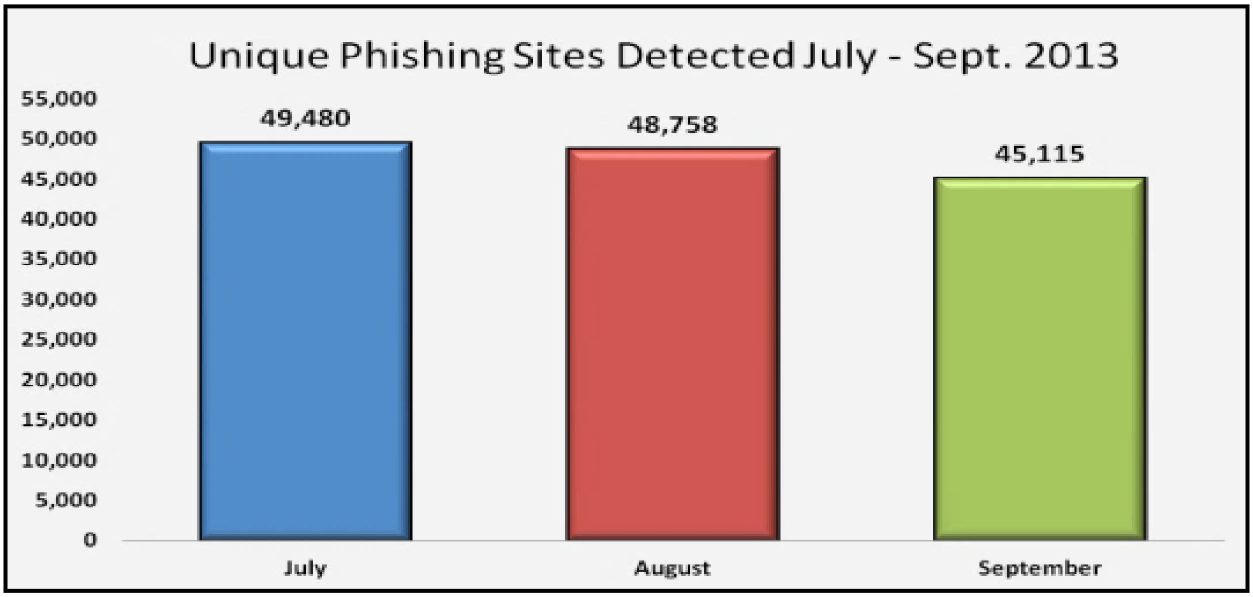
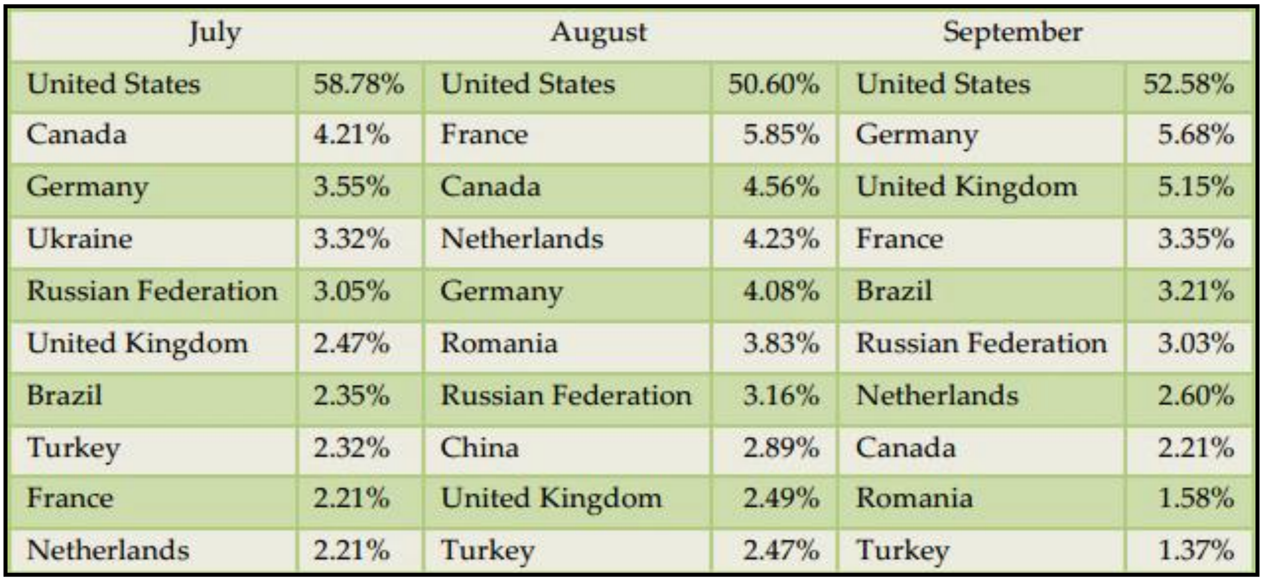


Figure 2.3: Total unique phishing sites in 3rd quarter of 2003 **[33]**.



July		August		September	
United States	58.78%	United States	50.60%	United States	52.58%
Canada	4.21%	France	5.85%	Germany	5.68%
Germany	3.55%	Canada	4.56%	United Kingdom	5.15%
Ukraine	3.32%	Netherlands	4.23%	France	3.35%
Russian Federation	3.05%	Germany	4.08%	Brazil	3.21%
United Kingdom	2.47%	Romania	3.83%	Russian Federation	3.03%
Brazil	2.35%	Russian Federation	3.16%	Netherlands	2.60%
Turkey	2.32%	China	2.89%	Canada	2.21%
France	2.21%	United Kingdom	2.49%	Romania	1.58%
Netherlands	2.21%	Turkey	2.47%	Turkey	1.37%

Figure 2.4: Top countries hosting phishing sites, as of 3rd quarter of 2013 **[33]**.

[12] In Swiss Cheese Model, organizational capabilities for addressing failures are shown as a series of roadblocks, like slices of cheese. Holes in the slices are weaknesses in parts of the system, and vary in size and position. A failure occurs when a hole in each slice momentarily aligns, and creates a condition that allows a hazard to pass through holes in all of the slices, leading to a failure [93].

2.2 Fault Tree Analysis (FTA)

FTA based on Chain-of-Events Model is a top down method for studying causes of hazards in a system [35], which uses a tree structure and Boolean logic for its construction. It is a widely adopted method for analyzing systems safety, with the idea that failures at system/sub-system level can be caused by lower level system(s)/sub-system(s) [36]. FTA comprises of four steps – system definition, fault tree construction, qualitative analysis, and quantitative analysis [35].

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 and their relationships are depicted graphically, making it easy to understand system logic and detect issues during analysis [35]. FTA has several limitations which render this method ineffective for performing causal analysis within the context of cyber security. These limitations discussed next, are in addition to the inherited shortcomings of Chain-of-Events Model.

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 [35]. In a Web 2.0 environment where systems and sub-systems are constantly being added and/or updated, using FTA for causal analysis is not an effective method for managing cyber security risks.

For software systems FTA can only be used for verification, because the software code must already have been created to generate a tree [35]. Further, systems in software and hardware intensive Web 2.0 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. In the design stage of software development lifecycle, FTA may be used for early detection of issues [35]. 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. Further, specific to software intensive systems, insights from FTA analysis would be extremely difficult to implement because changing software code is a very complex and time consuming effort once a system is in operation [35].

Intrinsically, FTA being a model is a simpler depiction of complex reality. In the context of cyber security, it is unreasonable to expect that addressing failures based on FTA will help manage cyber security risks. Because dynamic behaviors are difficult to represent with FTA [35] and cyber security risks stem from the dynamic Web 2.0 ecosystems.

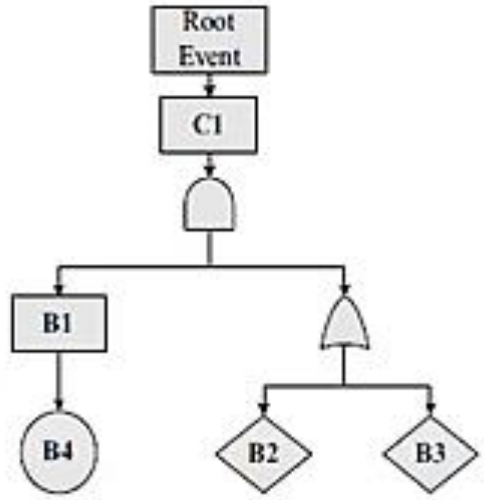
FTA is also limited to only depicting cause and effect relationships [35]. This makes it an effective method for reliability analysis, because failure[13] events are a focus in reliability analysis. But for hazard analysis additional tools would be needed in conjunction with FTA, because for hazard[14] analysis a systemic view beyond failure events is required, specifically in the context of cyber security.

To illustrate observations made above, consider Table 2.1, which shows FTA analysis of two actual accidental insider security events [36] described in row 1, fault tree for event A is shown in row 2, fault tree for event B is shown in row 3, and fault tree symbols are in row 4. Using accident in column 1 of row 1, and its corresponding fault tree in row 2 we observe that the tree represents accident well and is simple to understand. But in order to gain deeper insights and implement effective remedies detailed knowledge of system is required. For example, with reference to event B2 (B's represent basic events or root causes) for any meaningful countermeasures, it would be important to know why there was a lack of controls to monitor outbound emails, was it due to management oversight, privacy issues, lack of training, or some other reason. Similarly with reference to event B3, it is not clear if lack of technical control is due to outdated software/hardware, lack of technical expertise, or another reason. FTA either cannot or in a very limited fashion address these questions without avoiding getting too complicated, therefore additional methods would be needed to gain further understanding. Now looking at accident in column 2 of row 1 and its corresponding tree in row 3, we observe that subjectivity plays a role in FTA. For example, event C1 (C's represent secondary events requiring further investigation) is designated as employee negligence, while this is a valid reason it is also plausible that conditions around this event influenced employees actions. For example, employees may not have been clear on the scope of Freedom of Information Act, therefore to

[13] See Chapter 3 for definition.
[14] See Chapter 3 for definition.

avoid breaking any laws they delivered all of the information. So in this case employee was doing his/her job but was labeled as negligent, while systemic organizational and management issues were not taken into account.

	FTA of an Accidental Data Leakage via Outbound Email (Event A)	**FTA of an Accidental Disclosure of Sensitive Information by Insiders (Event B)**
Event Details [36]	"On September 1, 2009 one of our employees accidentally sent private information attached to an email to an incorrect email address including name, phone numbers, and related insurance policy numbers, date of birth and Social Security number. It did not include a specific address. On September 2, 2009 we recognized the error and contacted the email provider to ascertain whether or not the account was active at the time email was sent. Our firm received emails bouncing back on September 2, 2009 that the account was disabled but the original email in question did not bounce back. We are requesting from the email provider they let us know if account was active from August 31, 2009 to date"	"It accidentally handed over the data of living veterans when complying with a Freedom of Information request from Ancestry.com. The request was for data from a database of deceased veterans; however the data of 2,257 living veterans had also been identified in the database, and that the number could potentially grow to more than 4,000. The data included names, Social Security numbers, dates of birth and military assignments"

Fault Tree for Event A [36]	**Root Event:** Accidental data leakage from the outbound email **C1:** Incorrect entry of the email recipient **B1:** Failure to verify email recipient **B2:** Lack of policy & procedures to monitor outbound emails **B3:** Lack of technical controls to monitor outbound emails **B4:** Lack of due diligence  An example of a fault tree analysis of an accidental data leakage via outbound email
Fault Tree for Event B [36]	**Root Event:** Accidental data leakage **C1:** Employee negligence **C2:** Mistaken/Incorrect action **C3:** Excessive privilege or access control rights **C4:** Lack of due diligence **C5:** Non-compliance with access control procedures **C6:** Failure to maintain minimum privileges **C7:** Non-compliance of the information security policy **C8:** Ineffective implementation of audit findings **C9:** Lack of segregation of duties **B1:** Lack of concentration **B2:** Misperception **B3:** Mistaken priorities **B4:** Miscommunication **B5:** Absence/Inadequate quality control procedures/supervision **B6:** Absence of information security policy **B7:** Poor (information) management **B8:** Lack of awareness or understanding of information security policy **B9:** Disregard for the information security policy **B10:** Working around the information security policy **B11:** Insufficient business knowledge of security administrators **B12:** Permission creep

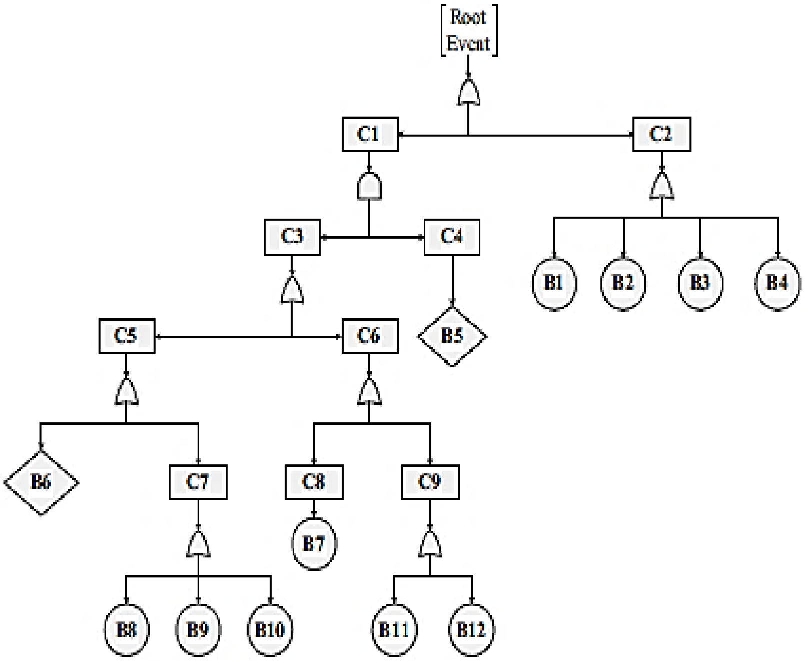
	 Root Event C1 C2 C3 C4 B1 B2 B3 B4 C5 C6 B5 B6 C7 C8 C9 B7 B8 B9 B10 B11 B12 An example of a fault tree analysis of an accidental data leakage by the Department of Veterans Affairs	
FTA Symbols [36]	▭	Rectangle represents an event to be analyzed further.
	⌓	AND gate indicates that event above happens only if all events below happen.
	△	OR gate indicates that event above happens if one or more of events below are met.
	○	Circle represents a basic fault event or event that does not have any contributory events.
	◇	Diamond represents an undeveloped event or a event that does have contributory events, but which are not shown.

Table 2.1: FTA analysis of actual events **[36]**.

2.3 Other Approaches for Managing Cyber Security Risks

It is worth to mention briefly an industry standard and a framework, because they play a role in management of cyber security risks. This section presents a framework COBIT 5 and a standard ISO/SEC 27002, typically used for managing cyber security risks.

2.3.1 COBIT[15] 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). The COBIT 5 framework provides general guidelines for information security and is based on five principles that are (1) Meeting stakeholder needs, (2) Covering enterprise end-to-end, (3) Integrated framework, (4) Enabling a holistic approach, (5) Separating governance from management. In order to manage information security, COBIT 5 uses a set of seven enablers shown in Figure 2.5 [37], which can be tailored to an organizations environment.

Developers of COBIT 5 framework recognize that many organizations primarily focus on technical dimension of information security. That is resource investments are focused towards upgrading and/or implementing new security technology. But organizational behavior, culture, policy, and approach towards managing cyber security risks does not get the needed attention [37]. The purpose of the seven enablers is to help organizations fundamentally change with reference to managing information security by also focusing on non-technical aspects of information security. COBIT 5 provides an integrated platform which organizations can use to initiate changes needed for managing cyber security risks holistically.

COBIT 5 utilizes trigger events as a catalyst for implementing information security initiatives and getting management buy-in. A trigger event can include an incident (e.g. outdated phishing email filters which do not result in a loss), an accident (e.g. misconfiguration of a server resulting in data loss), or lack of regulatory compliance. External signals such as new government regulations can also serve as a trigger for management to improve information security [37]. COBIT 5 is also designed to be an overarching framework that can integrate with other standards (e.g. ISO/IEC 27002), good practices, and frameworks [37], allowing for flexibility and broader coverage with reference to standards.

COBIT 5 also has some limitations. It is not meant for causal factor analysis, therefore additional methods or models would be needed *after* COBIT 5 has been implemented. Another issue is implementation timeframe, because successful implementation is dependent on effectively managing change within an organization [37], timeframe can be an issue in order to achieve the desired level of information security. Finally, COBIT 5 ability to integrate with other

[15] 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

standards due to its generality would require broader in-house expertise to manage an integrated framework of multiple standards.

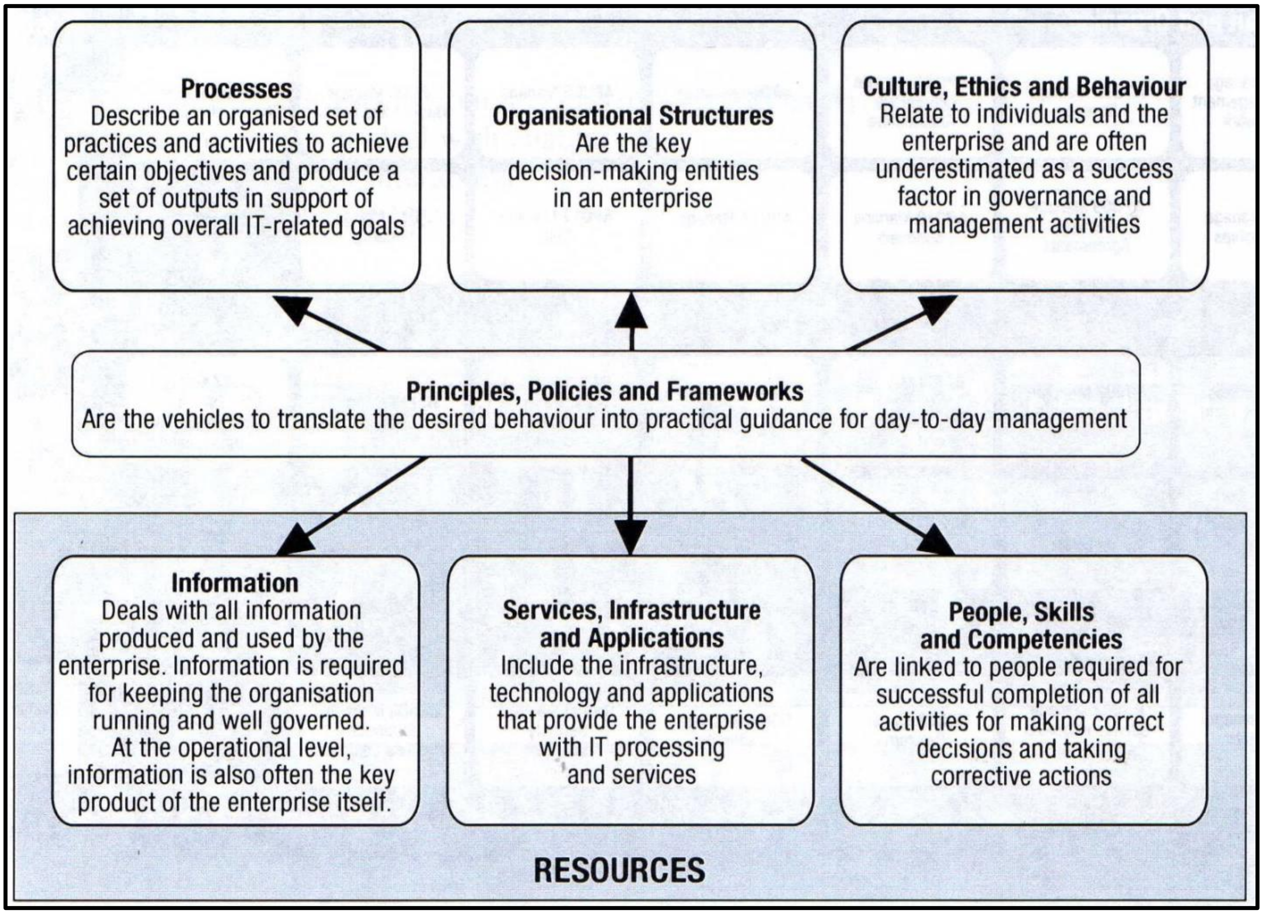

Processes
Describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals
Organisational Structures
Are the key decision-making entities in an enterprise
Culture, Ethics and Behaviour
Relate to individuals and the enterprise and are often underestimated as a success factor in governance and management activities
Principles, Policies and Frameworks
Are the vehicles to translate the desired behaviour into practical guidance for day-to-day management
Information
Deals with all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed. At the operational level, information is also often the key product of the enterprise itself.
Services, Infrastructure and Applications
Include the infrastructure, technology and applications that provide the enterprise with IT processing and services
People, Skills and Competencies
Are linked to people required for successful completion of all activities for making correct decisions and taking corrective actions
RESOURCES

Figure 2.5: COBIT 5 Enabler: Systemic model with interacting enablers **[37]**.

2.3.2 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[16] is one such product focused on information security. ISO/IEC 27002 demonstrates general principles and guidelines for information security management in an organization, but in contrast with COBIT 5, this standard provides detailed guidelines at a much lower level that is very close to implementation layer. The standard provides best practices for

[16] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533

dozens of controls[17] and control mechanisms for information security management including security policy, asset management, communications and operations management, access control and information security incident management [38]. For example, section 11.4 of ISO/IEC 27002 provides guidance for network access control, covering areas of policy on use of network services and user authentication for external connections to name a couple, Appendix 1 lists complete details for network access control.

Standards incorporate lessons from past experiences accumulated over many years [39], 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 Web 2.0 is 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 [40]. 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.

Furthermore, the standard states that new controls or guidelines not in the standard may be required and should be included. Like FTA, this introduces subjectivity and bias in deciding what controls will be effective and should be included, possibly leading to ignoring guidelines and controls that are more relevant.

2.4 System-Theoretic Accident Model and Processes (STAMP)

In this chapter, discussion of Chain-of-Events Model, FTA, COBIT 5, and ISO/IEC 27002 highlighted inherent inadequacies of these models and standards in managing cyber security risks, in a complex and dynamic Web 2.0 ecosystem comprising of over 800 million[18] hosts around the globe. Specifically, an inability to take into account organizational and social factors, human decisions/behaviors, and software design error(s) [30] contributions to cyber security risks leaves individuals, businesses, and governments exposed.

According to Leveson [30], "Accidents are complex processes involving the entire sociotechnical system. Traditional event-chain models cannot describe this process adequately".

[17] ISO/IEC 27002 defines control as "means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature".

[18] See Chapter 1.

In the context of cyber security, as discussed in Chapter 1 we observed that in general, cyber security risks stem from Web 2.0 ecosystem, which is a complex and dynamic sociotechnical system composed of many subsystems spread across the globe. In this Chapter and Chapter 1, we also observed a growing need for complementing traditional approaches for managing cyber security risks that are focused mostly on technical solutions, with alternative solutions that also address non-technical aspects of cyber security. Therefore, there is a need for a framework that can help with managing cyber security risks holistically.

Professor Nancy Leveson of MIT developed a framework called System-Theoretic Accident Model and Processes (STAMP), for understanding accidents holistically. Systems Thinking and Systems Theory is the foundation for STAMP framework, and a brief introduction to Systems Theory concepts is presented in the next section, starting with an introduction to the term *cyber safety*.

2.4.1 Safety and security in the context of cyber security

In general, when referring to data breaches or unauthorized access, terms *security* (generally prefixed with data, computer, application, etc.) and *cyber security* are used. But the term *security* is also closely related to *safety* and both share many attributes that include, addressing risks (safety addresses life/property risks and security relates to privacy/information security risks), protecting against loses, and both are governed by regulations [41]. *Safety* is a condition of being *Safe*, which is derived from the root *sol*. Other derivatives of *sol* include whole, uninjured, and solid. Security is derived from the root *s(w)e*, other derivatives include self, secret, solo, and solitude. Therefore in general safety relates to a broader scope and security is concerned with a narrower scope that includes individuals or a very small group.

Safety and security also differ in two important ways. First, security traditionally has been concerned with malicious activity, and safety *also* includes non-malicious activity [41]. In cyber security context, non-malicious activity can also lead to a loss. For example, a network engineer may upgrade software to provide higher speed for customers, but misconfiguration of new software can lead to a cyber-attack resulting in data loss. Second, security is generally related to *preventing unauthorized access to data*, verses preventing malicious activities in general [41]. With reference to cyber security, based on arguments presented so far in Chapters 1 and 2, it is clear that in today's Web 2.0 environment security also needs to assume a broader goal of preventing malicious activity. Leveson, also points out that security can be a subset of safety if loss includes “unauthorized disclosure, modification, and withholding of data” [41], this is consistent with the definition of loss (see Chapter 3) with reference to this thesis. Based on this discussion, this thesis will use both *cyber safety* and *cyber security* interchangeably. Specifically, cyber safety (or safety) will be used predominantly, which includes cyber security (or security) as its subset.

2.4.2 Systems Theory

Systems can be categorized by three dimensions depending upon the degree of randomness and complexity. *Organized Simplicity* refers to systems that can be physically decomposed into independent components and their behaviors into discrete events, *Unorganized Complexity* refers to systems which can be analyzed statistically, and *Organized Complexity* refers to systems that cannot be analyzed because of their complexity, and they cannot be analyzed statistically because they are organized enough so as not to depict a high degree of randomness in their behavior. Cyber space or Web 2.0 ecosystem falls in this category. System Theory was developed for systems demonstrating property of *organized complexity* [42]. These three categories are shown in Figure 2.6. At the core of systems theory are the concepts of *emergence and hierarchy*, and *communication and control*, which are discussed next within the context of cyber safety.

With reference to the first concept of emergence and hierarchy, systems that can be categorized as depicting organized complexity can be demonstrated by a hierarchy of levels. Each level in a hierarchy is more complex than the level directly below, and has emergent properties which only exist at higher level and are irrelevant at lower levels. For example, consider a software utility, which authenticates user access to a banking website. This utility typically will contain a few software modules which can include, reading user credentials (level 1), algorithm for processing user credentials (account id/password rules) and encryption (level 2), authentication success or failure (level 3). We can observe that the emergent property here is success or failure of authentication. We also observe that at level 1, this emergent property is irrelevant or non-existent, because level 1 module is only concerned with accepting user credentials regardless of how the information read will be used by higher levels in the hierarchy. Further, note that complexity in software also increases for each level, starting with level 1.

Expanding further on emergent property of our authentication algorithm, success or failure of user credentials also determines security of the module. That is, effectiveness of algorithms at lower levels determines how secure the module is from malicious attack. Thus safety is an emergent property.

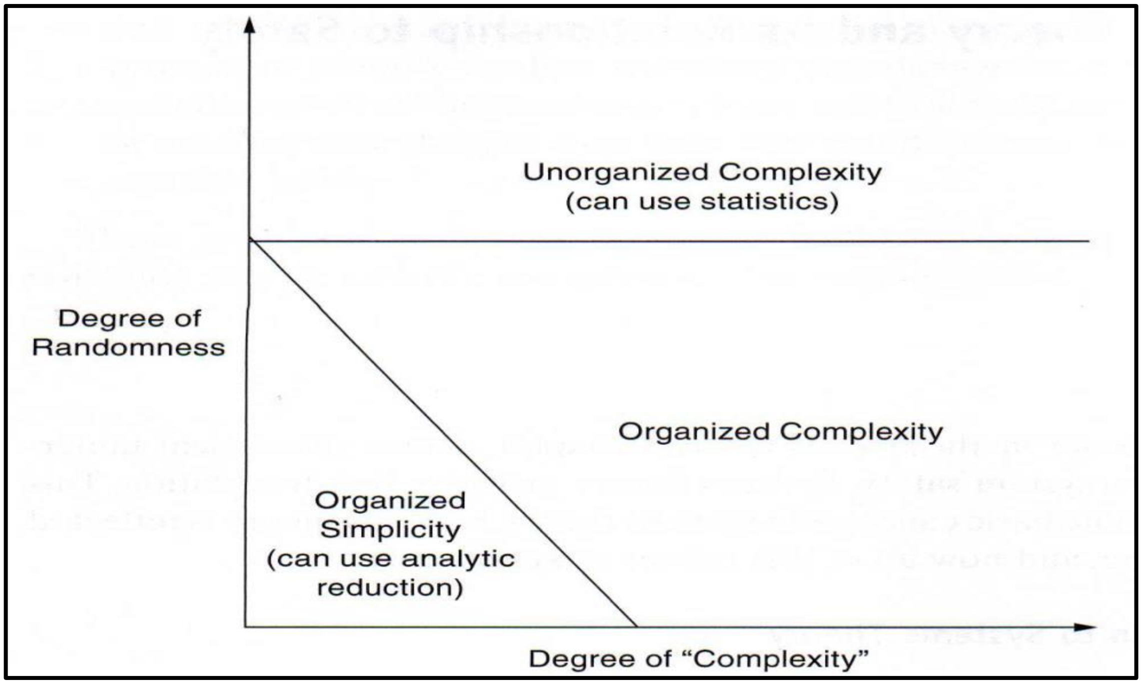


Figure 2.6: Three categories of systems **[42]**.

Second concept of communication and control can be illustrated with an example of password selection rule encountered on most websites. The selection rule is a *control* mechanism for encouraging users to choose strong passwords, and changes state of a system with reference to the level of security risk from user's perspective, because strength of a chosen password will make system more or less vulnerable to risk of a breach. The algorithm provides the requirements, which are generally stated as 'at least one numeric or at least one non-numeric/alpha character', but the user can choose more than one number or alpha/non alpha characters to make password stronger and system more secure. Further, selection rule imposes restrictions or constraints on choosing a password in order to achieve the goal of users creating strong passwords. These constraints can include minimum number of characters, mix of numeric and alphabets, use of at least one upper case letter, or disallowing use of certain characters. Controls are always associated with imposing constraints. Further in the context of cyber safety, Web 2.0 ecosystem is an *open* system, because there are inputs and outputs in this environment. For example, any internet connected device is generally listening on port 80 (default setting) per the Hypertext Transfer Protocol (HTTP) that is the protocol of data communication for the World Wide Web. Therefore, to exercise control in an open system there is a need for *communication*. Control theory dictates that open systems need feedback loops of information and control, and there are four required conditions to exercise control. First, the controller is to have goal(s), for example, a goal of authenticating users, this is called Goal Condition [42]. Second, system state must be under the influence of the controller, this is called Action Condition [42]. For example, password rules that are imposed by authentication algorithm. Third, controller must possess a model of the system, called Model Condition [42]. This condition is part of the controller and includes variables. A simple example is user authentication utility, which will have at least two variables – user's account id and password, and logic to process those variables[19]. Fourth, controller must be able to detect changes in the state of system, called Observability Condition [42]. For example, reading user provided values of authentication credentials.

Using the example of user authentication discussed earlier and viewing it in the context of Figure 2.7, which depicts a standard control loop, the goal condition of controller is to verify identity of users. Action condition is implemented via actuators, and in user authentication context it is the decision to authenticate or not to authenticate a user. Model condition resides in *Process Model* (discussed in the next section) of the controller. In our authentication example, controller's process model would have the password rules, which will be used to determine control action. Observability condition is implemented via sensors, in user authentication context it is the input provided by the user. Controlled process, which in this case is user authentication, may also receive inputs from other systems via Process Inputs. For example Captcha[20] may be used by a banking website for protection against execution of unauthorized software, also called bots. Therefore in this case, the safety of controlled process is now also exposed to inputs from other systems, which it must be able to handle because these external inputs may be inadequate or missing. The controlled process might also encounter external disturbances which it is not capable of handling. For example, consider a hypothetical flaw in a browser that may save user

[19] Model Condition will be discussed in more detail in the STAMP section.
[20] A captcha is a system that protects websites against bots by using tests that only humans can pass.

authentication credentials, and therefore permit anyone to login from the same computer, unless browser is restarted. These are the key concepts of System Theory that are the building blocks of STAMP which is discussed next.

2.4.3 STAMP Framework

In Chain-of-Events Model, an accident cause is event failure, but to include systemic or non-linear causal events leading to an accident, the definition needs to be expanded. Leveson defines an accident as, “an unplanned and undesired loss event” [34]. Losses may include death or injury, property, financial, or information. Within the context of technology assets, losses may include data and/or, unauthorized access (loss of credentials), or denial of access.

In STAMP, to understand causal factors leading to an accident requires understanding *why* a control was ineffective. Unlike Chain-of-Events Model, 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 safety constraints, hierarchical safety control structures, and process model as core concepts, which are discussed next.

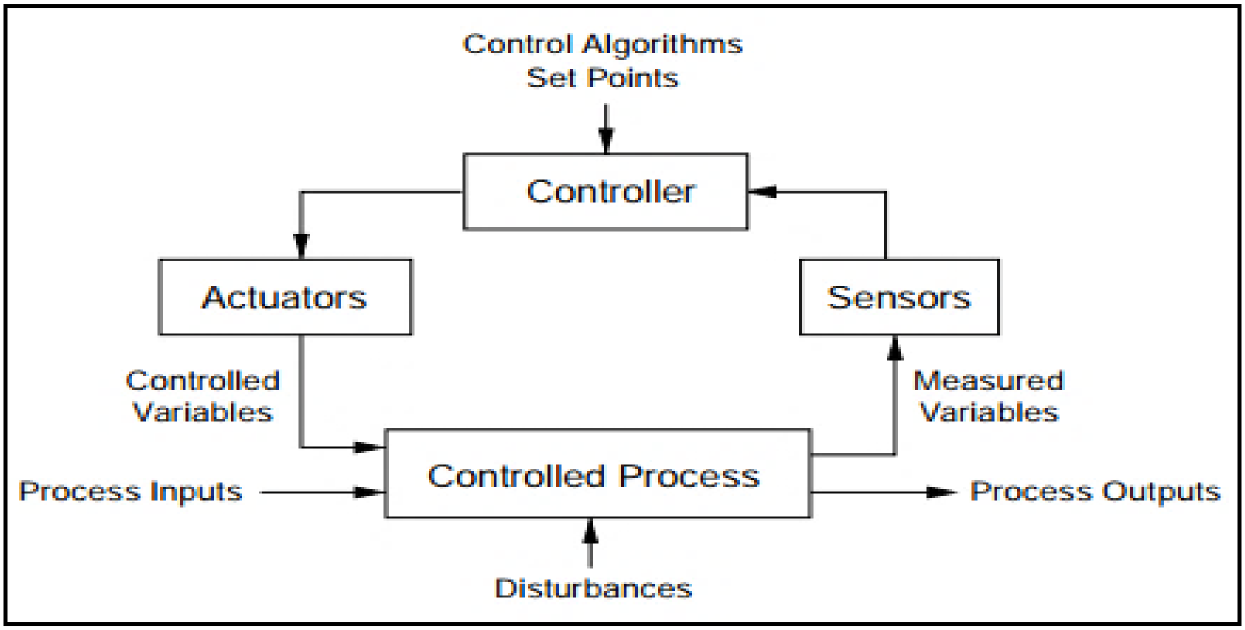


Figure 2.7: Standard control loop **[42]**.

Unlike Chain-of-Events Model where failure event is the focus, 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. As discussed in the Systems Theory section, systems are viewed as hierarchical structures where a higher level imposes constraints over the level immediately below it. 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 lower level. 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 [34]. 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 2.8, 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.

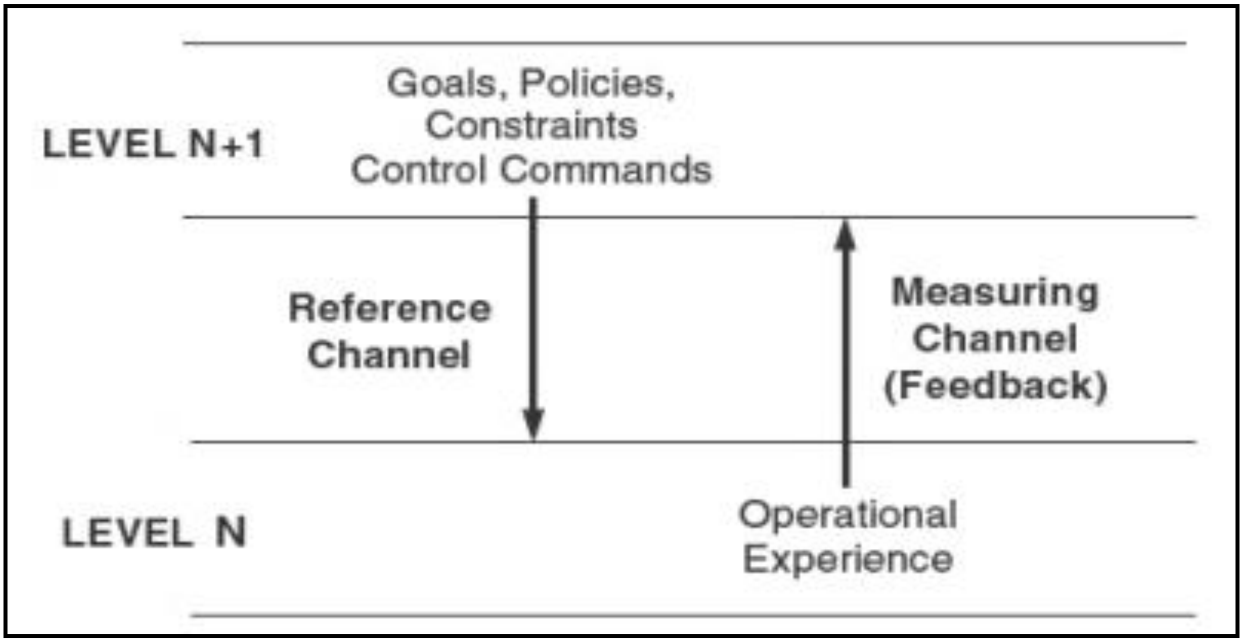


Figure 2.8: Communication channels in a hierarchical safety control structure **[34]**.

Third key concept in STAMP is process model. Recall from the discussion of Systems Theory that there are four conditions necessary to control a process. These are shown in Table 2.2, 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 2.2: 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 2.9. According to Leveson [34], "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".

This discussion has presented a basic and condensed introduction to STAMP and its foundation blocks. Following is a summary of some key points [34].

1. STAMP views systems as interrelated components kept in a state of dynamic equilibrium by feedback control loops. Systems are treated as open and dynamic that are continuously adapting to the environmental changes.

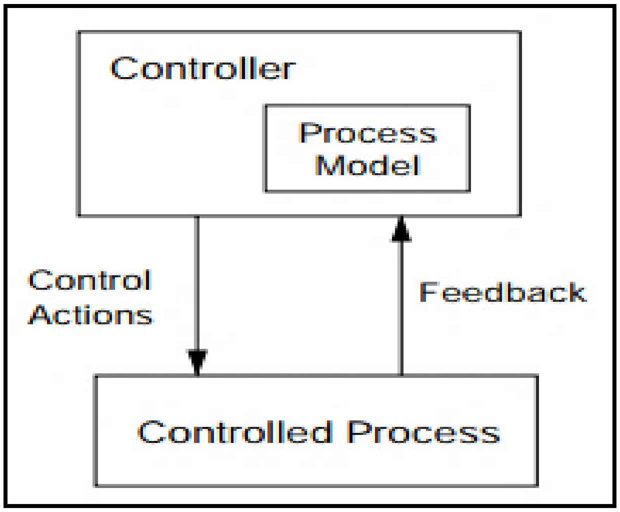


Figure 2.9: Controller with a process model **[34]**.

2. STAMP views safety as an emergent property that is achieved by imposing appropriate safety constraints.
3. STAMP helps in analyzing accidents by identifying safety constraints that were violated and understanding why the control did not impose them.
4. STAMP views safety not as a component failure problem, but rather a lack of safety constraints. Safety control structure is used to enforce safety constraints that will also ensure effectiveness as changes occur overtime.

Further STAMP can be used both for hazard analysis (Ex ante) and accident analysis (Ex post), see Figure 2.10. 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 thesis is CAST, which will be used to analyze an accident and is discussed next.

2.5 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 [43]. 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 [43]. Referring back to the example in Figure 2.2, consider event CE1, which relates to system administrators failure to properly enable authentication, in this case CAST would allow an analyst to look beyond failure event (CE1) with a systemic view and focus on *why* the system administrator failure happened rather than to stop at event CE1 and hold him/her responsible.

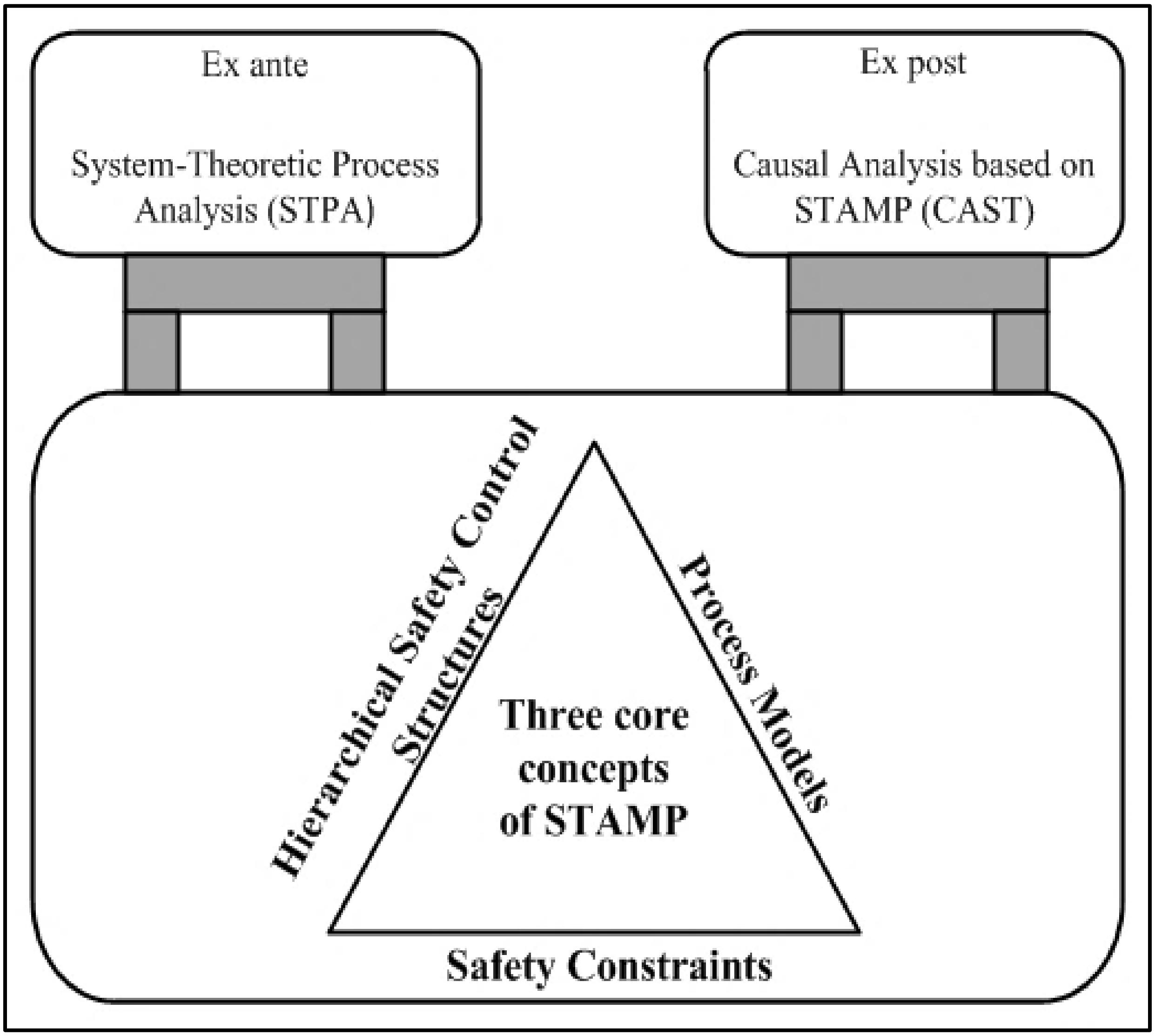

Ex ante
System-Theoretic Process Analysis (STPA)
Ex post
Causal Analysis based on STAMP (CAST)
Hierarchical Safety Control Structures
Process Models
Three core concepts of STAMP
Safety Constraints

Figure 2.10: System-Theoretic Accident Model and Processes (STAMP), and STAMP based hazard analysis (STPA) and accident analysis (CAST).

2.5.1 General Process for Analyzing Accidents using CAST

STAMP views accidents or incidents as a culmination of complex processes and not individual events. Therefore, accident/incident analysis using CAST involves understanding dynamic process underlying an accident or incident. Accident process is represented by a sociotechnical safety control structure for the system involved in an accident or incident, and relevant safety constraints that were breached at each level, along with the reasons explaining why the safety constraints were violated [43]. Leveson [43] proposes a nine step process for analyzing accidents using CAST; these steps can be carried out in any order and are listed below in Table 2.3:

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[21], 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.

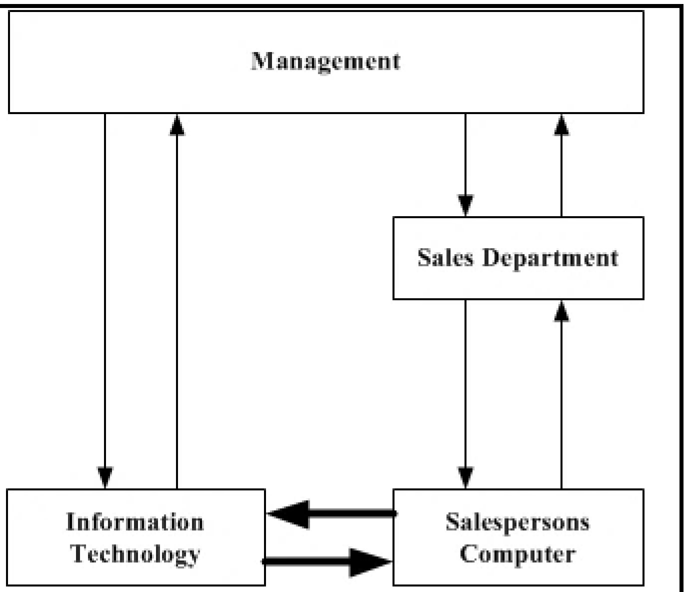
[21] Components can be electromechanical, digital, human, or social. *Source:* [30]

		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 [43], "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 incident, and any weakening of the safety control structure over time.	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 implementing appropriate countermeasures.
9	Generate recommendations.	

Table 2.3: CAST steps for analyzing accidents **[43]**.

Using the example in Figure 2.1, CAST steps are applied only for illustration purpose and not as a detailed analysis, to gain a general minimal understanding of the CAST model. The steps and their application are listed in Table 2.4. Details of CAST are discussed in Chapter 5 where the model is applied to an actual cyber-attack.

No.	CAST Step	Application to example in Figure 2.1
1	Identify the system(s) and hazard(s) associated with the accident or incident.	System: In our example this can be the *productivity software* (Microsoft Office, that also includes Microsoft Outlook email system) Hazard: Productivity software allows for phishing emails being delivered to employees.
2	Identify the system safety constraints and system requirements associated with that hazard.	System Safety Constraints: 1) Organization must protect its email system from phishing emails. 2) Organization must have measures in place to address any incident or accident resulting from a phishing email, that can include: • Isolating and disabling affected systems. System Requirements: Constraints are stated in "should not" type of sentences. Requirements are the positive statements. Our constraints are stated in positive statements, so requirements can be omitted. Comments: • Note that safety constraints and requirements (if any) are at the system level.
3	Document the safety control structure in place to control the hazard and ensure compliance with the safety constraints.	A simple safety hierarchical control structure for our example can be drawn as shown below. Each box is a component in the control structure that controls lower level components by imposing constraints. Information Technology and Salespersons Computer components also indicate interaction, as highlighted by bold arrows.

		 Management Sales Department Information Technology Salespersons Computer
4	Ascertain the proximate events leading to the accident or incident.	Proximate events can be: 1. Salesperson uses work computer while travelling to check personal emails via Gmail, Yahoo, etc. 2. Salesperson is lured by a phishing email and opens an attachment. 3. Salespersons computer is infected.
5	Analyze the accident or incident at the physical system level.	The physical system level in our example is the Salespersons Computer component, because that is the source of the accident. At this physical process level, it appears that there was nothing preventing salesperson from accessing personal emails via Gmail or other free web email service providers, using his/her business computer. To understand why this was the case analysis of components higher in the control structure, would be required.
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	Referring to the control structure in Step #3, next level up from Salespersons Computer component is Sales Department component. As mentioned in Step #5, this component (and higher components) needs to be analyzed to understand causal factors that led

	inadequate control at the current level.	to the accident. Possible causes can include lack of policy on use of business resources for personal use. Another, cause could be that the salesperson violated company policy, in which case further investigation would be needed to understand what conditions led to the unsafe behavior depicted by the salesperson.
7	Analyze overall coordination and communication contributors to the accident or incident.	Referring to the control structure in Step #3, and assuming that there was a policy on use of business computer for personal use, communication between Sales Department and Salespersons Computer components can be analyzed to understand why the policy was ineffective.
8	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.	As an example assume that the salesperson used Gmail for accessing personal emails, one plausible reason that allowed the productivity software system to migrate towards higher risk, is that the policy for using business resources for personal use was never updated to explicitly state that Gmail service cannot be accessed using business resources.
9	Generate recommendations.	1. A recommendation can be to implement periodic reviews of policy with reference to use of business resources for personal use. 2. Another recommendation can be to disable non-company provided email services on business computers.

Table 2.4: Application of CAST model steps (for illustration only).

Above example of CAST model application provided a high level overview of the process, which will be helpful in Chapter 5 when the model is applied with depth.

3 Definitions

This chapter introduces some key definitions used in TJX cyber-attack analysis using the STAMP/CAST model. Recall that STAMP/CAST is rooted in the field of System Safety, and applying it to cyber security requires redefinition of some terminology in that context. In addition, some non-STAMP/CAST related definitions are also included.

- **Definition: Accident**
  As defined in STAMP: "An undesired and unplanned event that results in a loss[22]" [44].
  As defined in SAFEWARE: According to Leveson in her book titled Safeware, accident is defined as "an undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss" [45].
  Redefined in the context of cyber security: Drawing from both definitions, an accident is an undesired (or desired) and unplanned (or planned) (but not necessarily unexpected) event that results in a loss.
  Comments: Within the context of cyber security, hackers generally desire to launch a cyber-attack and plan accordingly. On the other hand, system(s) may be compromised without a malicious intent, that is, without any desire to do harm or planning. But non-malicious intent can also result in a loss and therefore can be categorized as an accident.

- **Definition: Failure**
  Leveson defines failure as, "A failure is the nonperformance or inability of the system or component to perform its intended function for a specified time under specified environmental conditions" [45]. STAMP uses this definition in Reliability Engineering, and will also be applicable in the context of cyber security.

- **Definition: Hazard**
  As defined in STAMP: "A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss)" [44].
  Redefined in the context of cyber security: N/A.

[22] See definition of Loss.

Comments: Same definition applies in cyber security context.

- **Definition: Incident**

  As defined in STAMP: "A near miss or incident is an event that involves no loss (or only minor loss) but with a potential for loss under different circumstances" [45].

  Redefined in the context of cyber security: An incident is an event that involves no loss.

  Comments: In cyber security an incident is simply a no loss event. The reasoning being that, it would be difficult to define and measure 'only a minor loss' in the context of cyber security from both malicious and non-malicious viewpoints. Because if a system is breached it will in general involve a loss ranging from data to unavailability of system(s). Further any breach by definition involves a loss that caused the breach. In general, losses leading to a breach can include account id/password, privileges to use a system, or encryption key(s).

- **Definition: Loss in Cyber Security Context**

  Losses in cyber security generally include any hardware/software that is a victim of a cyber-attack (malicious) intent or non-malicious intent, information (including financial, private, or confidential), unauthorized (or inadvertent) disclosure, modification, or withholding of data, intellectual property, human life or injury, or customer goodwill.

- **Definition: Unauthorized Access**

  Unauthorized access can either be from the perspective of an organization or a system. From an organizations perspective, any access to information by anyone using another person's account information without their permission or knowledge is unauthorized access.

- **Definition: Web 2.0**

  Websites are categorized as Web 2.0 if they use technology that allows interaction with a website as compared to static pages. For example, an online shopping website is a Web 2.0 site. A Web 2.0 site may also allow users to collaborate with each other [46].

4 TJX Cyber-Attack: Operation Get Rich or Die Tryin'

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 a US corporation, measured by number of payment cards stolen. This chapter discusses full spectrum of this cybercrime of which TJX was only one of the victims, to set the context for the cyber-attack this chapter also provides a general overview of cybercrime ecosystem and highlights cybercrime terminologies.

4.1 About the TJX Companies

The TJX Companies, Inc. is a Framingham, MA based leading off-price retailer with an international presence, and was ranked number 125 in the Fortune 500 listings of 2012. TJX operates over 3000 stores nationally and internationally with over 179,000 associates. Its 2012 revenues were over $25 billion from its worldwide operations, which are composed of three geographic divisions in the US – The Marmaxx Group (T.J. Maxx and Marshalls) and HomeGoods, TJX Canada, TJX Europe, and a fourth online off-price retail division called Sierra Trading Post [47]. TJX value proposition offers brand, fashion, quality, price, and a treasure hunt shopping experience achieved by high inventory turnover relative to traditional retailers [48].

4.2 Mission, Vision and Values

Core to TJX operations are its, *mission* – to deliver value to its customers, *vision* – to constantly prioritize returning value to shareholders, and pursue adding value to communities, and *values* – integrity and openness in operations and valuing associates. To keep its mission and values aligned with its organizational goals, TJX has a global Corporate Social Responsibility (CSR) program known as TJX V.A.L.U.E., comprising of five tenets – Vendor Social Compliance, Attention to Governance, Leveraging Differences, United with our Communities and Environmental Initiatives, encompassing the mission, vision, and values of TJX companies [49]. These statements of mission, vision, and values support TJX's business model, which is value focused, flexible and offers brand names at off-price.

4.3 Operation Get Rich or Die Tryin' (2003 – 2008)

4.3.1 The Mastermind

The mastermind of TJX cyber-attack – the biggest in history at the time, was a 22 year old college dropout from Miami, FL who at age fourteen hacked into National Aeronautics and Space Administration (NASA) computers [50]. TJX was only one of several victims of a complex and sophisticated cyber-attack executed under an umbrella of a scheme he named *Operation Get Rich or Die Tryin'*. The scheme originated in July 2003 in Miami, FL and utilized an ecosystem of hackers, couriers, fencers[23], banks, and internet currencies across continents, causing collective financial losses of over $200 million to businesses including TJX, over its lifetime of five years ending in June 2008.

Albert Gonzalez – the mastermind, was first arrested in July 2003 by the New York Police Department (NYPD) while making withdrawals just before midnight, using multiple debit cards from an Automatic Teller Machine (ATM) in upper Manhattan [50]. Investigations revealed that Gonzalez had encoded blank cards with stolen debit card numbers and was making withdrawals just before midnight to double the cash value. Because, the daily withdrawal limit of an ATM ends at midnight, a few minutes after midnight Gonzalez would be able to make new withdrawals from the same set of encoded cards he had used a few minutes earlier. In the cybercrime lingo, this process of encoding blank cards with stolen debit card information to make withdrawals from ATM's is called *cashing-out* and the person making the withdrawals is known as a *casher*. The debit card information was presumably bought online from a criminal cyber bazaar (*Shadowcrew* was one such bazaar and is discussed next) where users are involved in trafficking of stolen payment card databases [50] or was stolen by Gonzalez himself. This was the first reported and the least sophisticated of all cybercrimes attributed to the Operation Get Rich or Die Tryin'.

[23] Fencer is someone who deals in stolen property. *Source:* http://www.merriam-webster.com/dictionary/fence

Further investigations revealed that Gonzalez was a rising star on an online hacker forum called *Shadowcrew*. Shadowcrew was a marketplace of approximately 4,000 worldwide members, which through its website *shadowcrew.com* facilitated crimes related to personal information theft, payment card fraud, and creating and selling of illegal identification documents. Shadowcrew platform provided guidance on production, sale, and use of compromised debit and credit card data, by offering databases of stolen information, tips on launching successful cyber-attacks, and sale of hardware such as magnetic stripe readers/writers.

Gonzalez's involvement with Shadowcrew motivated the US Secret Service (USSS) to seek his expertise with their ongoing investigation targeting other Shadowcrew members. The USSS used its position of leverage over Gonzalez, and offered a deal asking him to become an unpaid informer in exchange for dropped charges or face prosecution and prison for 20 years [50]. This started Gonzalez's over four year long relationship with the government beginning in 2003. His assistance with Operation Firewall, which targeted Shadowcrew including his own acquaintances, led to arrest of dozens of members in late 2003 and a year later to over a dozen indictments in the District of New Jersey [50]. Gonzalez's nexus with USSS, his intimate knowledge of global cybercrime ecosystem, and association with international cybercriminals significantly contributed to successful cyber-attacks on multiple businesses including TJX.

4.3.2 Building the Team

After the end of Operation Firewall in the fall of 2003, Gonzalez relocated to his hometown of Miami, FL from New York City at the advice of US Secret Service out of concern for his safety. Once home, Gonzalez continued to work as an unpaid informant for the government, helping with several investigations and building up a level of rapport uncommon for informants [50]. Impressed by his work, a year later the USSS hired Gonzalez as a paid informant at a salary of $75,000 per year and invited him to speak at conferences on security. Unbeknownst to the USSS, since the start of their relationship with Gonzalez in 2003, Gonzalez was also using his status as an informant to rebuild his cybercrime enterprise. By taking advantage of anonymity offered by hacker forums, he stayed connected with the cybercrime world and continued to deal in stolen payment card information after his day job. As a leader, Gonzalez started assembling a syndicate of experienced hackers based in the US and abroad. Most members of his enterprise had been active in the hacker community for years and became friends with Gonzalez in forums used by hackers during his high school days. See Figure 4.11 for an organizational chart showing main syndicate members of Operation Get Rich or Die Tryin' involved with the TJX cyber-attack.

In Miami, FL as a first step Gonzalez reconnected with an old friend Christopher Scott from EFnet, an Internet Relay Chat (IRC) protocol based chat room [50]. Scott, who opted to drop out of high school instead of being expelled for disabling all his school computers with a virus he launched from his home computer [51], had been involved in the hacker community since tenth grade. Although Scott was not the leader of the syndicate, he was Gonzalez's close friend and an eager junior partner with expertise in wireless networks [52]. Scott's skills in wireless communication technology would prove to be invaluable in launching the eighteen month long cyber-attack on TJX.

4.3.3 Wireless Technology

Gonzalez was interested in exploring and understanding vulnerabilities of a new wireless communication technology that was being rapidly adopted by businesses, specifically retailers. He understood from his previous experience at Shadowcrew that the new wireless technology would have weaknesses. He knew that businesses would be unaware of vulnerabilities or will lag in taking precautions against any weaknesses, because the technology is new and in general companies would be reluctant to make new investments, towards upgrading to second generation wireless technology so early in lifecycle. Remainder of this section presents a brief overview of wireless technology that was in use at TJX at the time of the cyber-attack, which was discovered in December, 2006.

Wi-Fi [53] (also spelled Wifi or WiFi) is a widely used technology that allows an electronic device to exchange data wirelessly (using radio waves) over a computer network, including high-speed internet connections. The Wi-Fi Alliance defines Wi-Fi as *any wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards*. A device that can use Wi-Fi (such as a personal computer, video-game console, smartphone, or a tablet) can connect to a network resource such as the Internet via a wireless network Access Point (AP). Such an access point or hotspot has a range of about 20 meters (65 feet) indoors and a greater range outdoors. AP coverage can comprise an area as small as a single room with walls that block radio waves or as large as many square miles — this is achieved by using multiple overlapping access points. Wi-Fi can be less secure than wired connections (such as Ethernet) because intruder(s) do not need a physical connection, and unencrypted internet access can easily be discovered.

The first wireless communication protocol (IEEE 802.11 standard) or IEEE encryption algorithm called Wired Equivalent Privacy (WEP) was developed in 1999, which proved to be vulnerable to hackers [54]. TJX and retail industry in general, were early adaptors of wireless technology while it was still in infancy in 2000, and relied heavily on WEP for their business operations. Keeping in view the proliferation of wireless technology – specifically amongst big retailers, security experts in 2001 issued warnings that they were able to compromise encryption systems of several major retailers [55]. By 2003 new and more secure Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) encryption algorithms were available to overcome the vulnerabilities of the previous generation. Therefore, it was a publically known fact that many large retailers' wireless communication networks were vulnerable to cyber-attacks unless they upgraded to a new generation protocol. TJX was using WEP at the time of the cyber-attack. STAMP analysis in Chapter 5 will be used to understand why TJX did not upgrade to a more secure encryption algorithm when it became available.

Further, in general WEP has two main components – authentication and encryption. Authentication is a process of establishing trust for accessing a network. For example, a customer logging on to a banking website with an account id and password is a process of authentication. Customer is identifying him/herself in order to access account information. Similarly, any device requesting connection to a wireless network via an AP needs to be authenticated. To protect information from malicious intent in a wireless network, WEP uses algorithms to encrypt cleartext[24] messages for communications.

An AP with WEP can be configured in one of two ways for authenticating new clients desiring to join a wireless network. First is *Open System* authentication, which is the default setting and any client can join a network without providing any credentials – account id and a password. Second is *Shared Key* authentication, in this case when a client requests access to a network, AP transmits a string in cleartext. The cleartext string is encrypted by the client and sent back to the host and if the host determines that the string is encrypted correctly then access is granted to the client to establish a connection to the network [56]. An AP has WEP software embedded in its hardware as shown in Figure 4.1. TJX was using the default setting of open

[24] Cleartext refers to data that is transmitted or stored unencrypted. *Source:* http://en.wikipedia.org/wiki/Clear_text

authentication, and STAMP analysis in Chapter 5 will be used in an attempt to understand why this was the case.

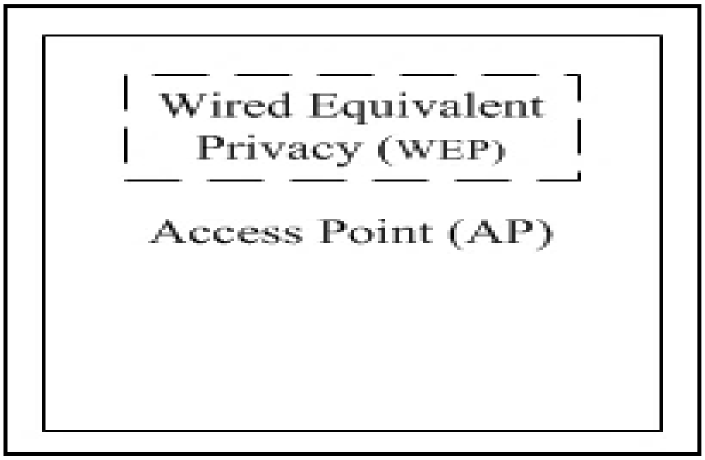


Figure 4.1: An Access Point (or Hotspot) embedded with WEP encryption.

4.3.4 War-driving

Scott, sometimes with Gonzalez began *war-driving* [57] on commercial strips in Miami FL. War-driving is when someone drives around in a vehicle with a computer and a high-power radio antennae searching for vulnerabilities in wireless networks of businesses – specifically, searching for networks using open system authentication. Scott's focus was the commercial areas along US Route 1 in Miami; BJ's Wholesale Club was his first significant target on record in 2003, a breach that lead to a loss in the range of $11-$13 million when its wireless store network was compromised, and customer payment card data stolen [57] [58] [59]. The BJ's Wholesale Club breach was reported publically in 2004 [60]. Scott, continuing with his war-driving, next worked to compromise a Miami, FL OfficeMax wireless network in 2004 and stole a payment card database that also included debit card PINs [58]. OfficeMax was a major early success for the Gonzalez enterprise. TJX was also identified as a target using war-driving approach.

4.3.5 Experts in Encoding of Blank Cards

Gonzalez reached out to his East European contacts for decryption of PINs and sales. Confident and comfortable, Gonzalez was patient in his operations, as evidenced by ICQ[25] chat log shown

[25] ICQ is the name of a communication application. *Source:* http://www.icq.com/en

in Table 4.1 [58], with one of his contacts[26] in Eastern Europe regarding stolen OfficeMax data, which he was trying to sell two years after the OfficeMax breach. In the chat conversation, Gonzalez mentions that he has eleven million cards available for sale, but many could have been expired because it has been two years since he received the data, and so far he has been able to decrypt one million payment debit card PINs. Gonzalez enterprise was very comfortable with the model of encoding blank cards with stolen debit card information and using ATM's for cashing-out, Gonzalez himself had been working with this model since at least 2003. For this reason, up until early 2006 Gonzalez enterprise was primarily focused on debt card information, and generally used international hackers for decrypting stolen PINs.

[**Gonzalez**] i have 11 million
[**Gonzalez**] i've decrypted already almost 1 million
[**Maksik**] so what happend with them ?:) why its going to be 0 soon ?:) if not a secret
[**Gonzalez**] many have expired
[**Gonzalez**] data was downloaded 2003 - 2004
[**Maksik**] so 10 millions are expired?[27]

. . . .

[**Gonzalez**] have patience please :) it took me 2 years to open pins [PIN numbers] from omx[28]
[**Maksik**] ok np ;-)
[**Gonzalez**] 2 years from the time I hack them, to download all data, the to find proper decryption method[29]

Table 4.1: Gonzalez chat log with an East European fence regarding OfficeMax breach **[58]**.

4.3.6 Sale of Stolen Payment Card Data

Gonzalez was fully focused on sales of stolen debit card data – also called *dumps* or *blocks* in hacker lingo, also enlisted Damon Patrick Toey to help with sales and cashing-out trips to ATMs, whom he first met in a chat room in 1999. Gonzalez provided protection to Toey, by exploiting his knowledge gained as a paid informant for USSS regarding ongoing government operations. He alerted Toey about undercover investigations and warned him to avoid forums and websites that were being monitored by the government.

[26] Maksik is a chat handle of Maksym Yastremskiy, who was the leader of an East European cybercrime enterprise.

[27] ICQ exchange logged by Maksym Yastremskiy April 13, 2006, 12:52 p.m. to 12:54 p.m.

[28] 'omx' is a reference to OfficeMax.

[29] ICQ exchange logged by Maksym Yastremskiy May 27, 2006, 10:16 a.m. to 10:17 a.m.

In general, Gonzalez deployed three models for monetizing the stolen payment cards. First, model was to encode blank cards with stolen data and use cashers for cashing-out trips to ATM's. But this method was risky as evident from the aforementioned arrest of Gonzalez. There are also geographical constraints, that is, there are only a limited number of ATM's a casher can cash-out from in a single run. The main benefit of this model was that cash was available in US currency instantaneously.

For the second model, Gonzalez used his own syndicate to sell dumps (or blocks) of stolen information. Gonzalez would send customers to Toey and also direct him to internet locations where the data was harvested. Toey would receive a percentage of proceeds. To monetize sales, Gonzalez asked that buyers pay in Internet Currency, which was easy to monetize at the time. Internet currency is a virtual currency which can be bought and sold using mainstream currencies like the US Dollar. Internet currency may also be used for online shopping, for example, *Amazon Coins*[30]. This model did not yield desired profit margins, because Toey did not have a network to sell domestically and internationally. This method was also risky because selling information from within the US had greater chances of scrutiny, specifically in light of the US Patriot Act.

Gonzalez third model was to use Yastremskiy's enterprise to sell stolen payment card data. TJX payment card data was primarily monetized using this model. Yastremskiy was the leader of an East European based criminal enterprise, whose primary focus was buying and selling stolen payment card information. Yastremskiy was based in Ukraine, which does not have an extradition treaty with the US [61] and was a major actor in stolen payment card data business. He was a preferred fence for Gonzalez because of his experience and connections across Eastern Europe, Asia, and the Americas. This model was preferred by Gonzalez because of higher profit margins, and information was sold overseas by someone not part of Gonzalez enterprise, therefore it was less risky. Yastremskiy and Gonzalez had agreed to split the profits evenly [58].

[30] http://www.amazon.com/gp/help/customer/display.html/ref=zeroes_subnav_help?ie=UTF8&nodeId=201181010 last accessed July 24, 2013.

4.3.7 The TJX Breach – Heyday of Operation Get Rich or Die Tryin' (July 2005 – December 2006)

Previous sections discussed some core building blocks of *Operation Get Rich or Die Tryin'* and provided a general overview of cybercrime ecosystem. This section describes the TJX cyber-attack which is the subject of STAMP analysis in Chapter 5.

Gonzalez enterprise was emboldened and experienced after successfully breaching wireless networks of several retail stores over a period of two years, and Scott increased his war-driving activities on the commercial strips of Miami, FL. He enlisted Jonathan James, who was known for being the first American juvenile to be jailed for computer crimes. At age 15 in 1999, James hacked into the computers of US Department of Defense [62].

In 2005, Marshalls store in Miami, FL was networked with first generation encryption algorithm WEP for communications within the store. WEP has two main goals, to authenticate devices wishing to join a network, and provide privacy by way of encryption.

WEP authentication serves as a first layer of protection against unauthorized access and offers open system (default setting) and shared key authentication options. Open system authentication does not require an account id or a password to join a network. A wireless network is simply discovered by an antenna of a device seeking connection to desired network, and device is granted access. Open system authentication steps are illustrated in Figure 4.2. Shared key authentication as the name suggests, requires a WEP key to be shared between a device seeking connection and AP of desired network. This shared WEP key is used to encrypt/decrypt initial challenge message between a device and AP. Both WEP keys and challenge texts are configured by network administrators. Figure 4.3 illustrates steps for shared key authentication.

WEP's second layer of protection is privacy of communication between devices within a network, by way of encryption. A key point here is that a wireless network in general may be configured with four different combinations of authentication and encryption. Each combination of authentication and encryption determines if one or both layers of WEP protection are in use. These combinations are summarized in Table 4.2, and TJX was configured with combination number two as indicated by the shaded row.

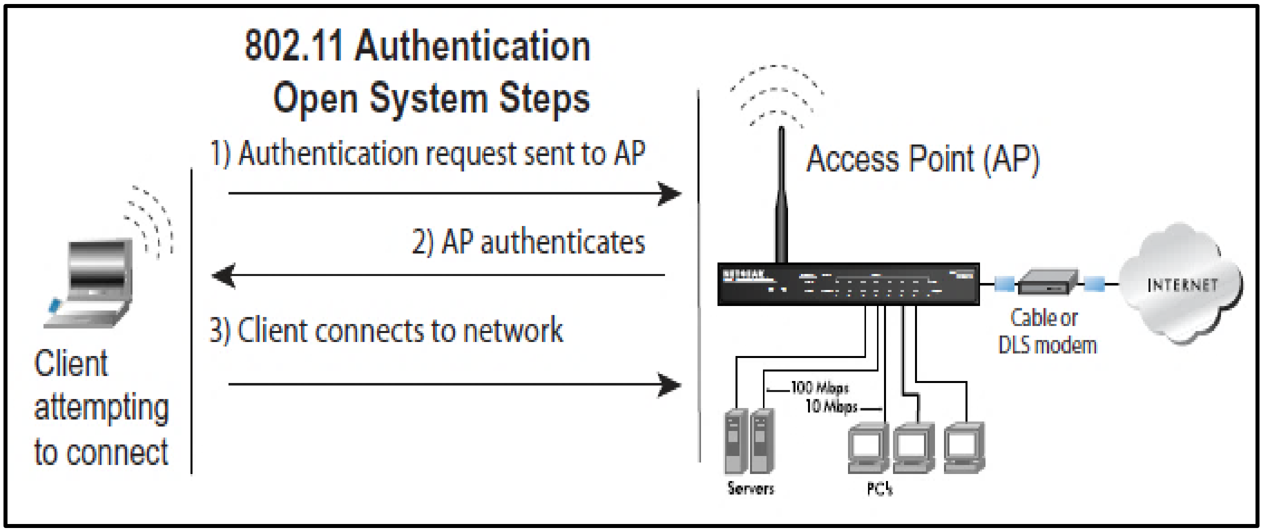


Figure 4.2: WEP (IEEE 802.11) open system authentication steps **[63]**.

For authentication of devices, the Marshalls AP was using the default setting of *open system authentication*, meaning allowing successful wireless connections to the store network to any device that was within range of AP. For encryption Marshalls was using *WEP key*. On July 12 and 18, 2005 Scott and James parked outside two TJX operated Marshall Stores in Miami, FL and authenticated their computer with the store network via AP [57]. Once on the network, the intruders started monitoring WEP encrypted network traffic by using packet sniffers.

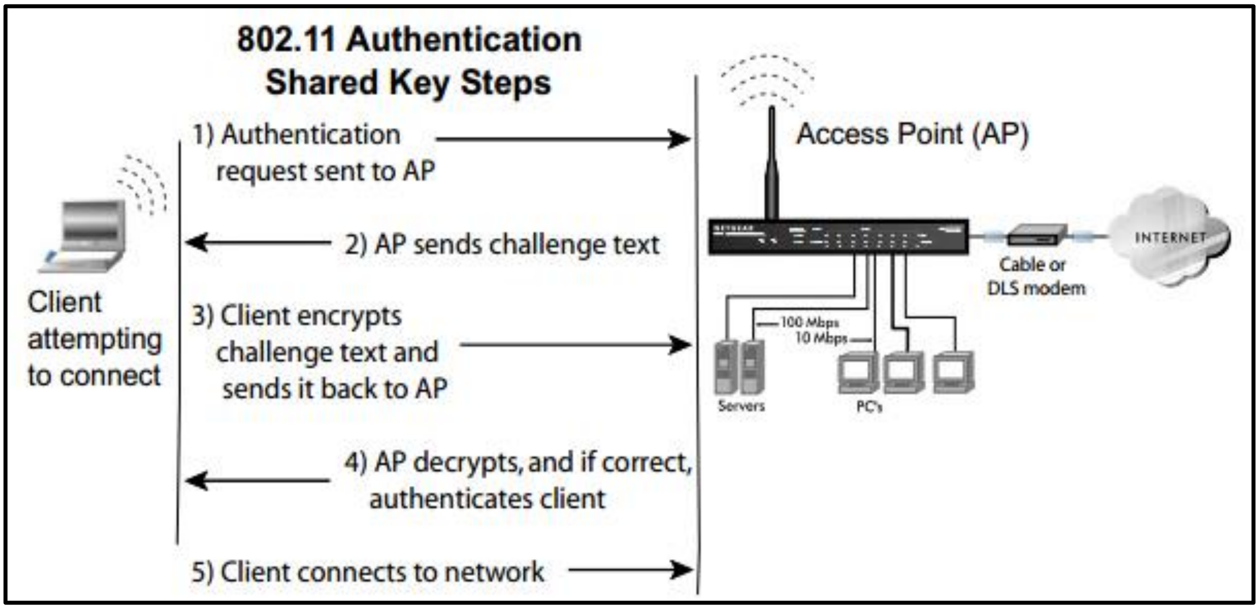

802.11 Authentication
Shared Key Steps
1) Authentication request sent to AP
2) AP sends challenge text
3) Client encrypts challenge text and sends it back to AP
4) AP decrypts, and if correct, authenticates client
5) Client connects to network
Client attempting to connect
Access Point (AP)
Cable or DLS modem
INTERNET
100 Mbps
10 Mbps
Servers
PC's

Figure 4.3: WEP (IEEE 802.11) shared key authentication steps **[63]**.

	Authentication Mode	WEP Encryption	Comments
1	Open system authentication	No encryption	• Any device can connect to a network. • Communication between devices within a network is not encrypted. • No layer of protection.
2	Open system authentication	Encryption	• Any device can connect to a network. • Communication between devices within a network is encrypted. • Only devices with correct WEP key can view decrypted contents of messages between devices. Although any device can monitor data traffic in encrypted form. • Single layer of protection. *This configuration was used by TJX at its Miami, FL stores.*
3	Shared key authentication	No encryption	• Only devices configured with a shared WEP key may connect to a network. • Communication between devices within a network is not encrypted with WEP key. • Single layer of protection in the context of WEP.
4	Shared key authentication	Encryption	• Only devices configured with a shared WEP key may connect to a network. • Communication between devices within a network is encrypted. • Dual layers of protection.

Table 4.2: Wi-Fi configuration combinations of authentication and encryption **[63]**, Author.

This type of attack is also called a *Passive Attack*[31]. Packet sniffer applications or *sniffers* are analogous to wire-tapping a phone line. Sniffers are in general used by computer network administrators to monitor network traffic and/or for troubleshooting network issues. Sniffers allow network administrators to be able to view and save contents of data packets as they travel

[31] A passive attack is when data traffic on a computer network is intercepted but not modified – that is data packet information is only read. The data traffic may be captured and saved for further analysis.

over a wireless or wired network. A powerful and popular sniffer program is *tcpdump*[32]. Sniffers are freely and publically available and are native to popular computer operating systems like UNIX, and versions are also available for other platforms like MS Windows and Linux.

WEP was publically known to have several vulnerabilities since 2000, as highlighted by Walker in his 2000 paper [64]. Relevant to a passive attack, the weakness of WEP that can be exploited is decrypting WEP key by observing and analyzing data traffic until, due to an inherent flaw WEP key information is repeated in data packets [64]. This can be achieved in a few hours depending on network traffic. Further, software utilities that compromised WEP encryption key by exploiting WEP vulnerabilities were also publically available. Scott by utilizing these WEP key decryption utilities, observing and analyzing Marshalls store network traffic, and using his prior experience was able to capture and view all communication in cleartext by decrypting network data packets in transit, using the decrypted WEP key. Further, with WEP key decrypted and more experimenting, monitoring by using sniffers, and capturing user account and password of store employees [65], Scott was able to access Marshalls parent company TJX's servers in Framingham, MA within a couple of weeks, see Figure 4.4. Once on the corporate servers he also provided store employee(s) user account and passwords to Gonzalez and James. Access to TJX corporate servers was also helped by the fact that, being successfully authenticated on a store network at Marshalls in Miami, Scott had established a trust relationship with the larger corporate wide TJX network. A trust relationship in general allows a user account to share rights and privileges across network domains, or put another way, after a successful authentication it allows a user to have access to all associated resources in a network without a need for repeating the authentication process.

[32] http://www.tcpdump.org/ last accessed July 17, 2013.

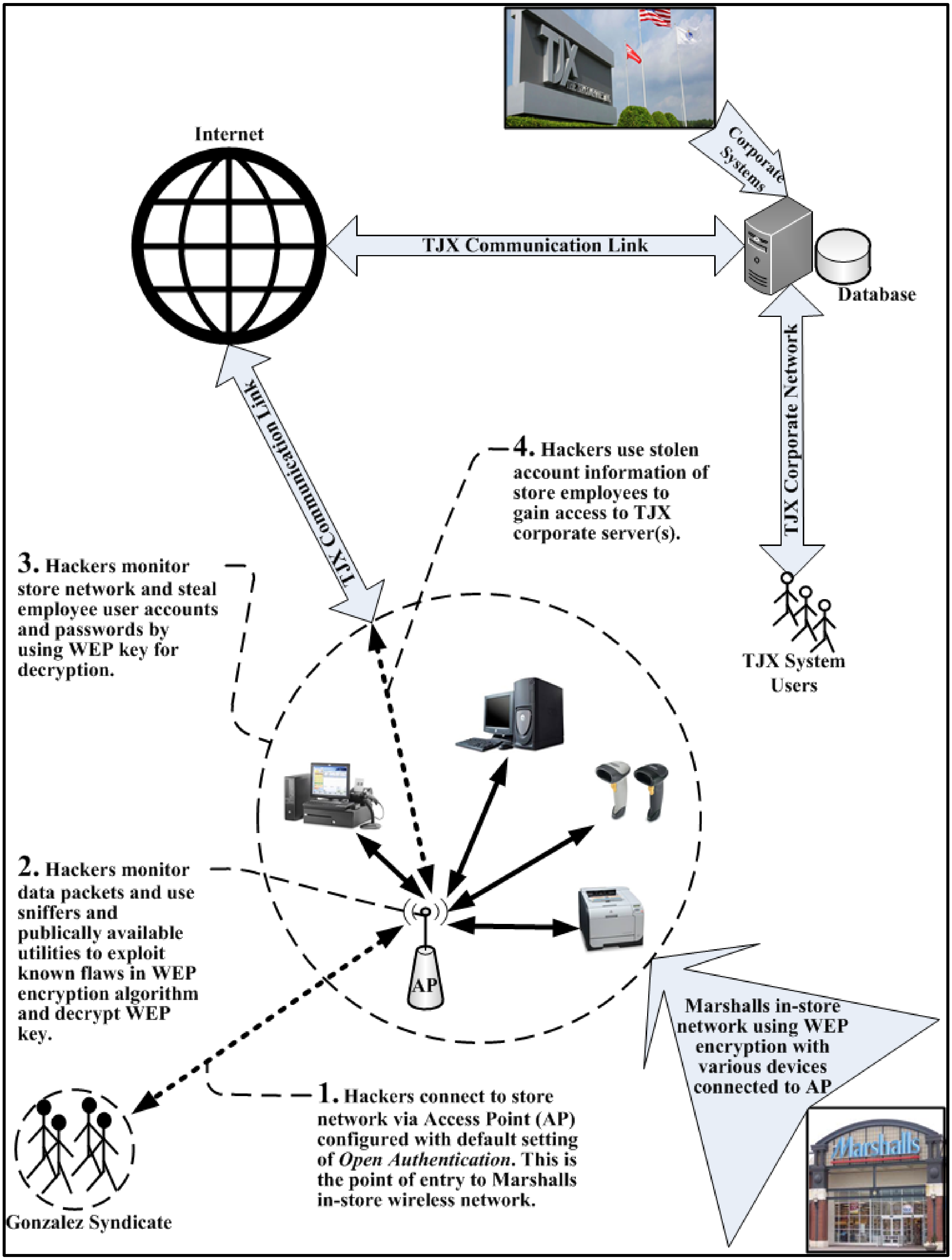

Internet
Corporate Systems
TJX Communication Link
Database
TJX Corporate Network
TJX Communication Link
4. Hackers use stolen account information of store employees to gain access to TJX corporate server(s).
3. Hackers monitor store network and steal employee user accounts and passwords by using WEP key for decryption.
TJX System Users
2. Hackers monitor data packets and use sniffers and publically available utilities to exploit known flaws in WEP encryption algorithm and decrypt WEP key.
AP
Marshalls in-store network using WEP encryption with various devices connected to AP
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 in-store wireless network.
Gonzalez Syndicate
TJX
Marshalls

Figure 4.4: TJX breach using Wi-Fi at a Miami, FL Marshalls store.

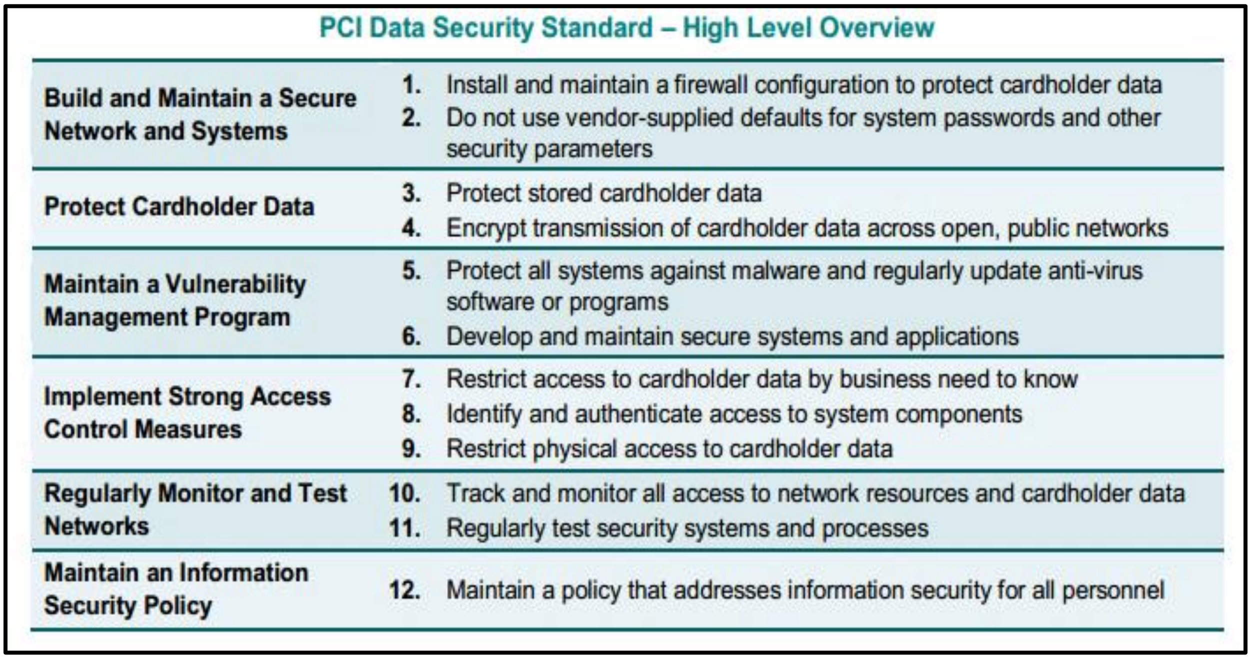
Having established the only entry point[33] to TJX corporate systems via Marshalls AP as shown in Figure 4.4, Scott continued to explore the corporate network while parked outside the Marshalls store in Miami. In order to spend more hours exploring TJX corporate servers, Scott and James rented rooms at nearby hotels and deployed more powerful six foot tall radio antenna [50] to receive radio signals from Marshalls AP. This allowed them to avoid raising suspicion by being parked for extended hours in the Marshalls parking lot. Their efforts yielded results and Scott discovered unencrypted payment card data related to transactions from 2003 or before stored on TJX corporate servers. In general, TJX had not started encrypting payment card data until beginning of 2004 [59] [66]. In September and November of 2005, Scott downloaded this unencrypted data from 2003 or before onto his computer, and forwarded the stolen information to Gonzalez for monetization via Yastremskiy – Gonzalez's East European fence. At this point, Gonzalez realized that most of the card data they had was two years old[34] from 2003 or prior transactions and many cards were expired [59].

The data was old because TJX was not in compliance with The Payment Card Industry Security Standards Council (PCISSC) standard called Data Security Standard (DSS), and agreements TJX had with credit card companies [67]. Payment Card Industry (PCI) Data Security Standard was the first generation standard known as PCI from 2004-2006. PCI was called Payment Card Industry (PCI) Data Security Standard (DSS) – PCI-DSS starting from its second version in 2006. PCI-DSS will be used through the rest of this thesis with an implicit understanding that until 2006 it was referred to as PCI. PCI-DSS is a set of requirements designed to ensure that entities processing, storing, or transmitting payment card information maintain a secure environment. The PCI DSS is administered and managed by the PCISSC, an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, and Discover.). Payment card brands and their designated banks are responsible for enforcing merchant compliance with PCI-DSS. High level PCI-DSS security requirements are shown in Figure 4.5. According to PCI-DSS a cardholder data environment (CDE) includes people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. Requirements in Figure 4.5 apply to all system components

[33] Hackers needed to be on TJX wireless network in order to access corporate server(s), because at this time the hackers had not established a direct connection to corporate server(s).

[34] The older the payment cards are the less is the market value, because the difference between the issue and expiry dates is small, thereby reducing the window of opportunity (or 'shelf life') for hackers to sell the stolen information.

that are within or connected to CDE. System components are comprised of network devices, servers, computing devices, and software applications. These agreements and standards impose limits on for how long merchants can store payment card information, what information can be collected, and security requirements. To understand why TJX was non-compliant with PCI-DSS, the issue will be analyzed using STAMP in Chapter 5.



PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	**1.**	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.**	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.**	Protect all systems against malware and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.**	Restrict access to cardholder data by business need to know
	8.	Identify and authenticate access to system components
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.**	Track and monitor all access to network resources and cardholder data
	11.	Regularly test security systems and processes
Maintain an Information Security Policy	**12.**	Maintain a policy that addresses information security for all personnel

Figure 4.5: PCI-DSS requirements **[68]**.

During the course of exploring TJX corporate servers, vulnerability related to processing of current[35] transactions was discovered by Gonzalez. He found that for an instant, payment card information for current transactions is stored unencrypted on corporate server while it is being processed. This slot was between the times when a payment card was swiped at a store checkout terminal and when information after being received was sent unencrypted for approval to credit card company network [66] [59]. Gonzalez sought help from his longtime friend from teenage years Stephan Watt, to write a custom sniffer application that could exploit this vulnerability. Watt was a genius, who graduated college at age 19. When Gonzalez contacted him, he was

[35] Current means a transaction in transit, just after a card is swiped at a checkout terminal.

working as a programmer at Morgan Stanley in New York City[36]. Watt developed the custom sniffer application within ten hours naming it '*blabla'* and on May 15, 2006 handed it over to Gonzalez, so he can install the script on the TJX corporate server using his access via Marshalls AP. The custom sniffer application exploited the aforementioned vulnerability and captured the unencrypted current payment card transactions in transit. Once a predetermined file size limit was reached, sniffer was programmed to compress and store files containing stolen data on TJX corporate server(s), for later download by Gonzalez enterprise using Marshalls AP as shown in Figure 4.6.

Until now the cybercriminals had only one way of accessing TJX corporate servers in Framingham, MA, which was via Miami, FL Marshalls AP. Because of this limitation downloading files containing hundreds of thousands of transactions, required long hours parked outside the Marshalls store. To overcome risk of detection, using Marshalls AP in May 2006 Scott installed a Virtual Private Network (VPN) connection from corporate TJX payment card processing server in Framingham, MA to a server in Latvia, and presumably elsewhere including California. A VPN is a network created by connecting two or more private computers by utilizing public infrastructure. Gonzalez had acquired and controlled servers in Latvia, Ukraine, Netherlands, Argentina, and California for his enterprise. The overseas servers allowed Gonzalez enterprise to conceal stolen data, launch cyber-attacks from locations outside of the US, and store sniffer applications and other tools used for launching cyber-attacks. The Virtual Private Network (VPN) also allowed Gonzalez syndicate members to securely access TJX corporate servers in Framingham, MA from anywhere in the world without the risk of physical or virtual detection, see Figure 4.7. With the 'blabla' software, VPN connection, and servers for harvesting stolen data installed, the infrastructure was complete for the next phase of TJX cyber-attack. In October and December of 2006, Gonzalez enterprise downloaded TJX current payment card data – real time payment card information as customer cards were swiped, by using sniffer application provided by Watt, over the VPN connection setup by Scott, directly onto a server in Latvia for harvesting and sales by Yastremskiy's enterprise worldwide.

Sales method for stolen information involved use of a website owned by Yastremskiy that advertised availability of stolen payment cards. The site listed number of cards and their

[36] At the behest of US Secret Service, Gonzalez had reached out to Watt in the past to see if he was interested in working for the government. Watt had refused government offers because of his activist tendencies, but agreed to help Gonzalez with his personal request for a custom sniffer application.

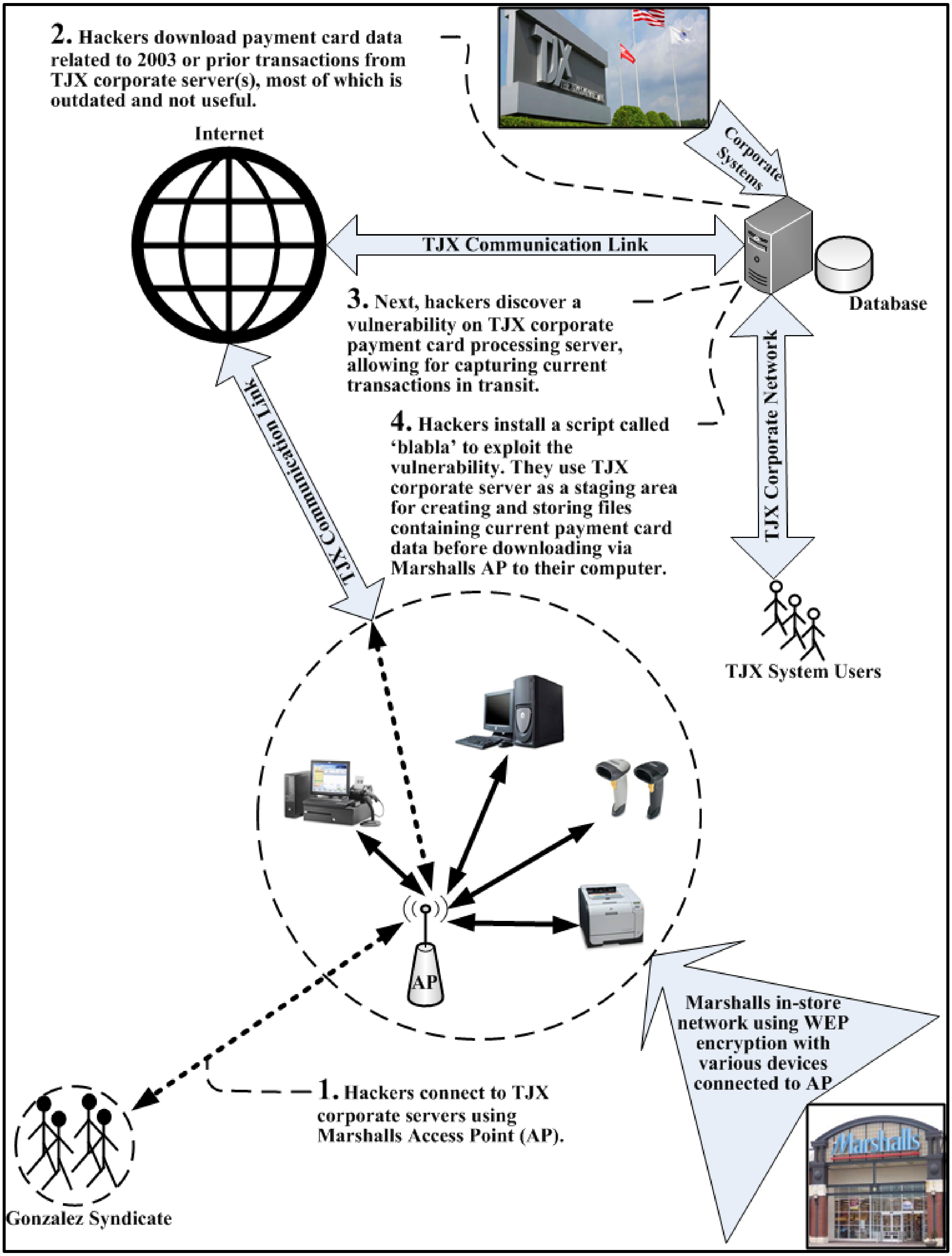

2. Hackers download payment card data related to 2003 or prior transactions from TJX corporate server(s), most of which is outdated and not useful.
Internet
Corporate Systems
TJX Communication Link
Database
3. Next, hackers discover a vulnerability on TJX corporate payment card processing server, allowing for capturing current transactions in transit.
4. Hackers install a script called 'blabla' to exploit the vulnerability. They use TJX corporate server as a staging area for creating and storing files containing current payment card data before downloading via Marshalls AP to their computer.
TJX Communication Link
TJX Corporate Network
TJX System Users
AP
Marshalls in-store network using WEP encryption with various devices connected to AP
1. Hackers connect to TJX corporate servers using Marshalls Access Point (AP).
Gonzalez Syndicate

Figure 4.6: Downloading payment card data using Marshalls AP.

prices. Price of each card was determined by the quantity ordered, the higher the quantity the lower the per unit price. The purchase process started with a potential buyer contacting Yastremskiy in a chat room or via email. Yastremskiy would then instruct the buyer to wire money using Western Union or other similar service to Yastremskiy, or to another member of his enterprise. If a buyer was known to Yastremskiy, then he would instruct the buyer to wire money directly to one of his bank accounts. After receipt of payment, Yastremskiy directed the buyer to another website to place an order. For example, a buyer's order would be in a form indicating quantity and type of card, similar to *10 Chase Visa Classic*. Once the order was placed and acknowledged, the website automatically accessed stolen card information databases controlled by Yastremskiy, retrieved the requested quantity and type of card data and forwarded the information to Yastremskiy for review. At this point in time, buyer also received an order confirmation message. After Yastremskiy reviewed the order details, he fulfilled the order by emailing the card information to the buyer [69]. This flow is shown in Figure 4.8.

But by using Yastremskiy's enterprise for sales, Gonzalez had to address the challenge of repatriating proceeds from overseas back to the US. Gonzalez used couriers and cashers for this purpose based in the US, Humza Zaman was one such courier/casher who had a day job at Barclays Bank in New York City, responsible for firewall security of Barclay's systems. As a casher, Zaman would receive ATM cards for cashing-out from Gonzalez linked to banks in Latvia, where the money had been deposited by Yastremskiy's enterprise. Zaman would then ship the cash in FedEx boxes minus his 10% commission to a drop box in Miami, FL. In his second role as a courier Zaman travelled to California to pick up cash from Yastremskiy syndicate member(s). Gonzalez repatriated between $600,000 and $800,000 through Zaman [70] [71]. General transaction flow is shown in Figure 4.9.

In December 2006 TJX was alerted to possible fraudulent transactions by a major credit card company. Immediately, TJX began working with the US Department of Justice, US Secret Service, Royal Canadian Mounted Police, and credit card companies. Following the advice of US law enforcement, the news of the cyber-attack was not made public until a month later, to avoid alerting hackers and to increase chances of tracking the cyber-attackers. TJX also engaged security vendors – General Dynamics Corporation and IBM Corporation, to investigate the cyber-attack. TJX internal investigation revealed on December 18, 2006 that TJX have suffered a serious cyber-attack. But Gonzalez enterprise was well aware that their cyber-attack had been discovered, presumably by the presence of security experts and techniques used by them to trap the hackers on TJX systems. General Dynamics even counter-attacked with a *zero-day exploit* hoping to capture information like IP address or hackers account id that could possibly lead to cybercriminals or isolate their activities on TJX corporate server(s), but were not able to trace

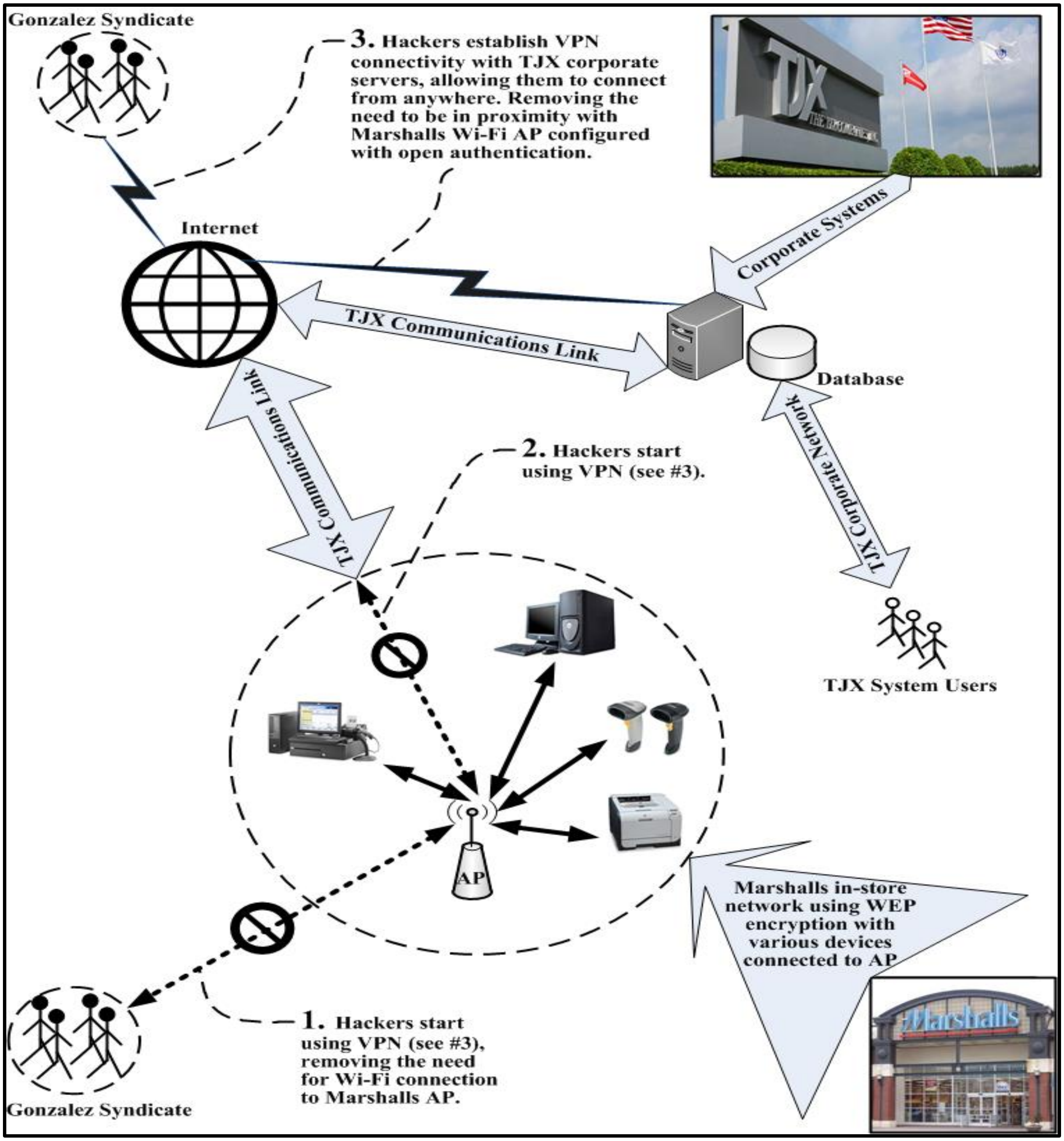

Gonzalez Syndicate
3. Hackers establish VPN connectivity with TJX corporate servers, allowing them to connect from anywhere. Removing the need to be in proximity with Marshalls Wi-Fi AP configured with open authentication.
Internet
Corporate Systems
TJX Communications Link
TJX Communications Link
Database
TJX Corporate Network
2. Hackers start using VPN (see #3).
TJX System Users
AP
Marshalls in-store network using WEP encryption with various devices connected to AP
1. Hackers start using VPN (see #3), removing the need for Wi-Fi connection to Marshalls AP.
Gonzalez Syndicate

Figure 4.7: Hackers establish VPN connectivity to TJX corporate systems.

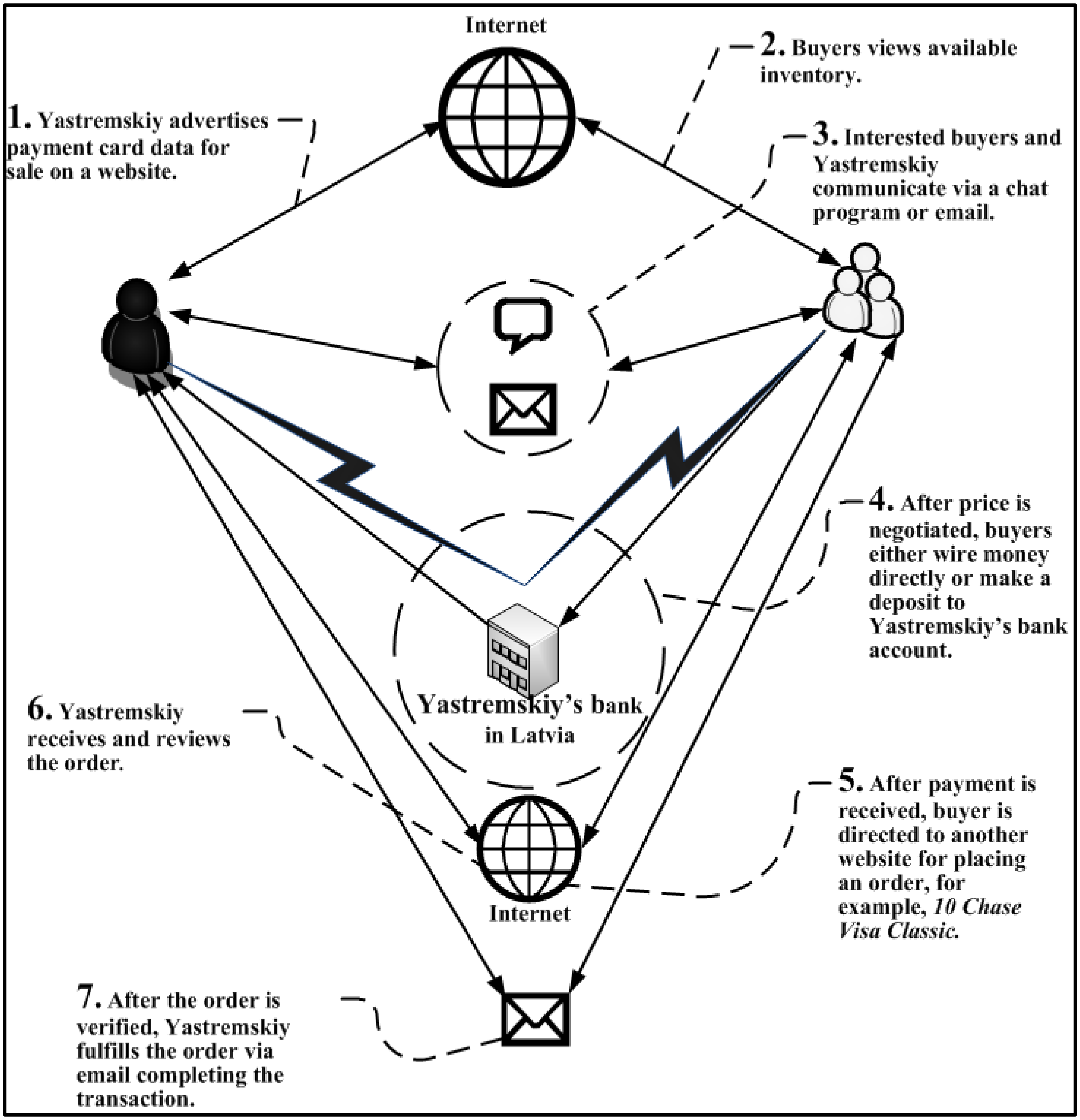

Internet
1. Yastremskiy advertises payment card data for sale on a website.
2. Buyers views available inventory.
3. Interested buyers and Yastremskiy communicate via a chat program or email.
4. After price is negotiated, buyers either wire money directly or make a deposit to Yastremskiy's bank account.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

Figure 4.8: General flow of sales for stolen payment card information.

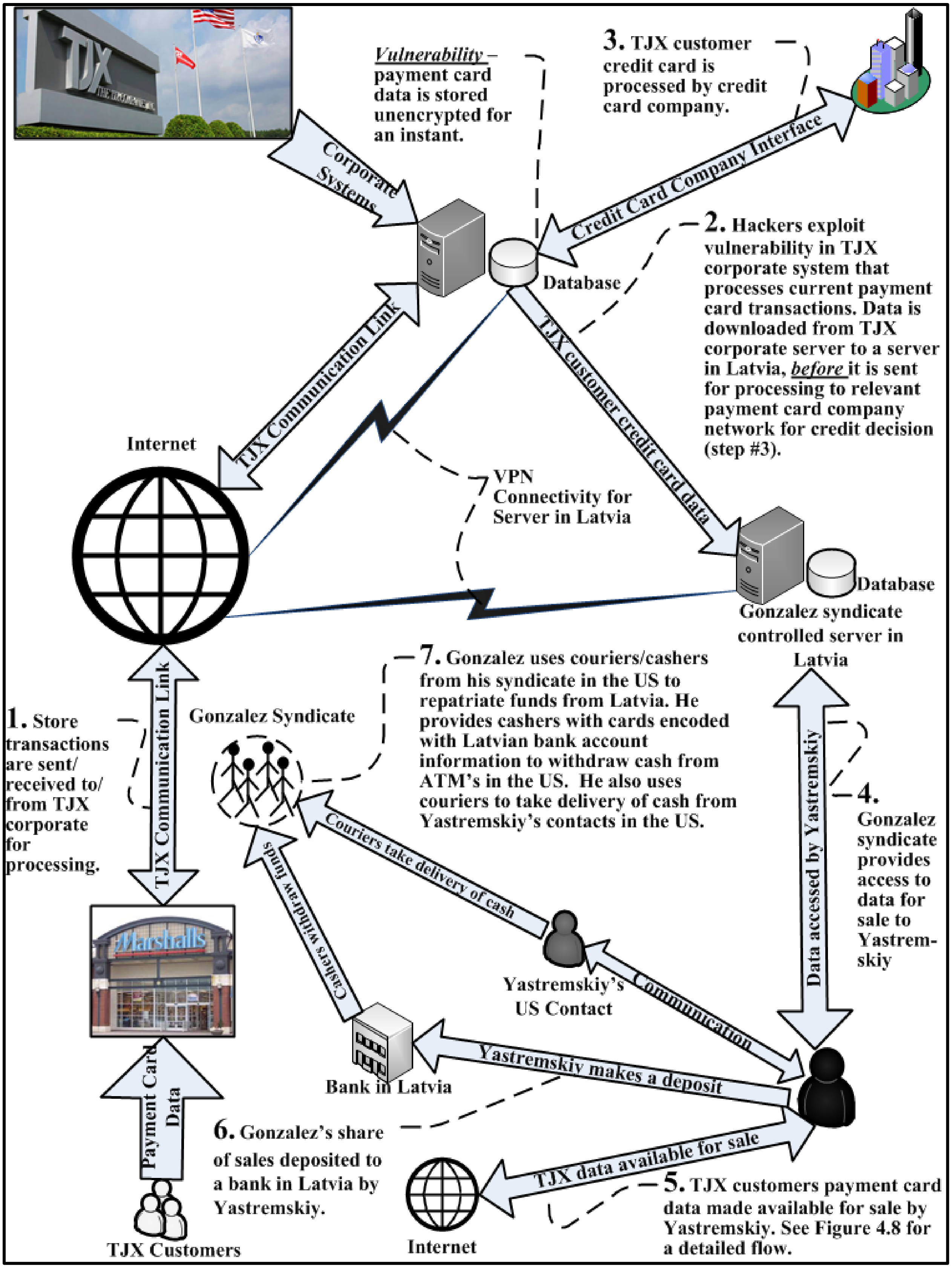
Gonzalez or other syndicate members. A zero-day attack exploits vulnerability in a computer system on the same day or before the vulnerability is publicly known [72]. Gonzalez shared this experience with Yastremskiy during a chat session as depicted in the following excerpt:

"after those faggots at general dynamics almost owned me with 0day while I was owning tjx I don't want to risk anything" [58]

At this juncture, Gonzalez evaluated risks for his enterprise and decided to abort further cyber-attacks on TJX, but according to TJX forensic investigators they could only confirm that, Gonzalez enterprise was able to steal over eleven million current unique payment card numbers [58]. Additionally, investigators found over forty million unique payment card numbers stolen from various businesses on two computer servers controlled by Gonzalez. In financial terms, according to TJX Form 10-K filing in 2009 [73] covering fiscal 2008 year, TJX had expensed $171.5 million in pre-tax dollars cumulatively towards losses incurred by the cyber-attack, out of which $146.3 million had been spent [58]. Some of the expenses were lawsuits (filed by customers, credit card companies), professional fees for investigating the cyber-attack, attorney fees, management time, and investments in upgrading security technology. In its most current Form 10-K filing in April 2014 [74] covering fiscal year 2013, TJX continues to maintain a reserve of $12.8 million for any possible future losses.

4.3.8 Post TJX Cyber-attack Evolution of Operation Get Rich or Die Tryin' (2007 – 2008)

When Gonzalez aborted TJX cyber-attack, businesses had also started making their websites more sophisticated as online shopping was becoming popular, with web pages using SQL for many features including shopping cart checkout process. Website security at the time was not at the forefront for many businesses, and Gonzalez again saw an opportunity in exploiting security vulnerabilities in browsers. Realizing that Scott's skills of hacking into wireless networks were becoming of less value to the enterprise, Gonzalez turned to Toey for help in launching Structured Query Language (SQL) injection cyber-attacks. SQL is a programming language designed for working with databases. A SQL injection cyber-attack, injects malicious SQL code via an input data field(s) in an application that can include account id, password, or address field, further in general SQL injection attack uses a web page for inserting malicious code. Poorly architected websites and/or user applications can lead to SQL injection vulnerabilities. If successful, hackers can read or modify database contents, or even shut down databases. Using this method, Gonzalez syndicate executed a cyber-attack on Hannaford Brothers in March, 2008. The attack resulted in a loss of approximately four million payment card data.


Corporate Systems
Database
Credit Card Company Interface
TJX Communication Link
Internet
TJX customer credit card data
Database
Gonzalez syndicate controlled server in Latvia
Gonzalez Syndicate
TJX Communication Link
Couriers take delivery of cash
Cashers withdraw funds
Data accessed by Yastremskiy
Yastremskiy's US Contact
Communication
Bank in Latvia
Yastremskiy makes a deposit
Payment Card Data
TJX data available for sale
TJX Customers
Internet

Vulnerability – payment card data is stored unencrypted for an instant.

1. Store transactions are sent/ received to/ from TJX corporate for processing.

2. Hackers exploit vulnerability in TJX corporate system that processes current payment card transactions. Data is downloaded from TJX corporate server to a server in Latvia, *before* it is sent for processing to relevant payment card company network for credit decision (step #3).

3. TJX customer credit card is processed by credit card company.

4. Gonzalez syndicate provides access to data for sale to Yastrem-skiy

5. TJX customers payment card data made available for sale by Yastremskiy. See Figure 4.8 for a detailed flow.

6. Gonzalez's share of sales deposited to a bank in Latvia by Yastremskiy.

7. Gonzalez uses couriers/cashers from his syndicate in the US to repatriate funds from Latvia. He provides cashers with cards encoded with Latvian bank account information to withdraw cash from ATM's in the US. He also uses couriers to take delivery of cash from Yastremskiy's contacts in the US.

VPN Connectivity for Server in Latvia

Figure 4.9: Monetization flow of stolen TJX payment cards.

4.3.9 Soup Nazi Ends Operation Get Rich or Die Tryin'

Yastremskiy, being a major buyer and seller of stolen payment card information, had been on the radar of USSS for a few years. Undercover agents would buy stolen payment card data from Yastremskiy in an effort to understand his operation and gather evidence. USSS agents met with Yastremskiy numerous times in locations like Thailand and Dubai for buying stolen data. It was in Dubai in June 14, 2006 during one of the meetings with USSS agents, that the US government with Dubai authorities conducted a sneak-and-peak search of Yastremskiy's computer in his hotel room and took an image of his computer on a thumb drive. The government discovered a stockpile of information related to Yastremskiys' operation, including detailed ICQ chat session logs and records of dealings with buyers and sellers for whom Yastremskiy acted as a fence.

Because Yastremskiy was based in Ukraine and without an extradition treaty, it would be impossible to extradite him to the US the government had to wait for Yastremskiy to leave Ukraine. Yastremskiy did leave and was arrested on July 26, 2007 by the Turkish National Police accompanied by USSS agents while vacationing in Antalya, Turkey. He was arrested on a warrant issued in the Southern District of California for distributing stolen payment card numbers.

With Yastremskiy out of business, USSS began analysis of his computer. Logs of Yastremskiy's ICQ chat sessions singled out someone, with an identification number 201679996 as a major seller of stolen payment card information to Yastremskiy. ICQ protocol uses numbers to identify members and a member can have multiple identification numbers to preserve anonymity. Further investigations led USSS agents to the registration information for 201679996, which was only an email address, and no name, physical address, or other contact information was available. But the email *soupnazi@efnet.ru* was sufficient for identification. *Soupnazi was an alias used by Gonzalez* in hacker forums dating back to his Shadowcrew days and was very well known to the government from his days as an informant when he helped with Operation Firewall targeting other Shadowcrew members.

Gonzalez was arrested on June, 2008 from a Miami hotel, and *Operation Get Rich or Die Tryin'* ended with arrests and conviction of all the other members. Later, Gonzalez led investigators to a barrel containing aired out clear plastic bags of money amounting to approximately $1.2 million buried in his parent's backyard in his Miami family home. Gonzalez was well aware that Yastremskiy was under investigation and when asked why he continued to do business with Yastremskiy, Gonzalez replied “I never thought he would leave Ukraine” [50]. All syndicate members with the exception of Jonathan James who committed suicide were arrested, pleaded guilty to all counts in government indictments, and signed plea agreements for reduced sentences that ranged between three and twenty years.

4.3.10 Operation Get Rich or Die Tryin’ ended in June 2008, but …

On July 26, 2013 Gonzalez and Toey – still in jail serving their sentence, were named as co-conspirators in a criminal indictment which named six defendants in Russia and Ukraine for launching cyber-attacks on NASDAQ, Jet Blue, and others to steal bank account and payment card information of millions of customers. The cyber-attacks took place from 2005 until 2012; see Figure 4.10 for a high level timeline. According to the indictment, conservative estimate puts the number of stolen cards at 160 million and monetary losses to businesses and banks in excess of $300 million [75] [76]. In the aforementioned discussion, Gonzalez was closely working with the East European hackers to whom he also provided sniffer programs, SQL injection code, and databases of stolen information for sale. The July 2013 indictment demonstrates the vastness and complexity of Gonzalez enterprise while it was in operation, and the impact it is having on businesses even today.

Most importantly, Operation Get Rich or Die Tryin’ illustrates general complexity underlying a cyber-attack and the difficulty of recovering losses. In Chapter 5 STAMP will be used to analyze the TJX cyber-attack, the analysis will attempt to demonstrate a need for a complementary approach that views cyber security risk beyond traditional technical lens. STAMP analysis will demonstrate that managing cyber security risks is a sociotechnical issue as well, involving human behavior and other non-linear factors such as management support and allocation of resources for addressing cyber security at an organizational level.

4.4 TJX Operations and IT

TJX cyber-attack highlighted operational and IT related strengths and weaknesses of the company, which will be studied further using STAMP in Chapter 5, key questions 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 any of the strengths of TJX played a role that resulted in increased cyber security risks.

4.4.1 Wireless Network Technology

TJX was one of the early adopters of Wi-Fi technology and had 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 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.
- 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 that 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.

4.4.2 Monitoring of networks

Hackers were able to install VPN connection on 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 will be explored using STAMP.

4.4.3 Retention of customer information

During 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 general policies regarding retention and type of information.

4.4.4 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.

4.4.5 Compliance with PCI-DSS and Credit Card Rules

TJX was out of compliance with PCI-DSS standards and credit card rules. But it is not clear 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 it is not clear which party is responsible for enforcing payment processing standards. This topic will also be analyzed using STAMP.

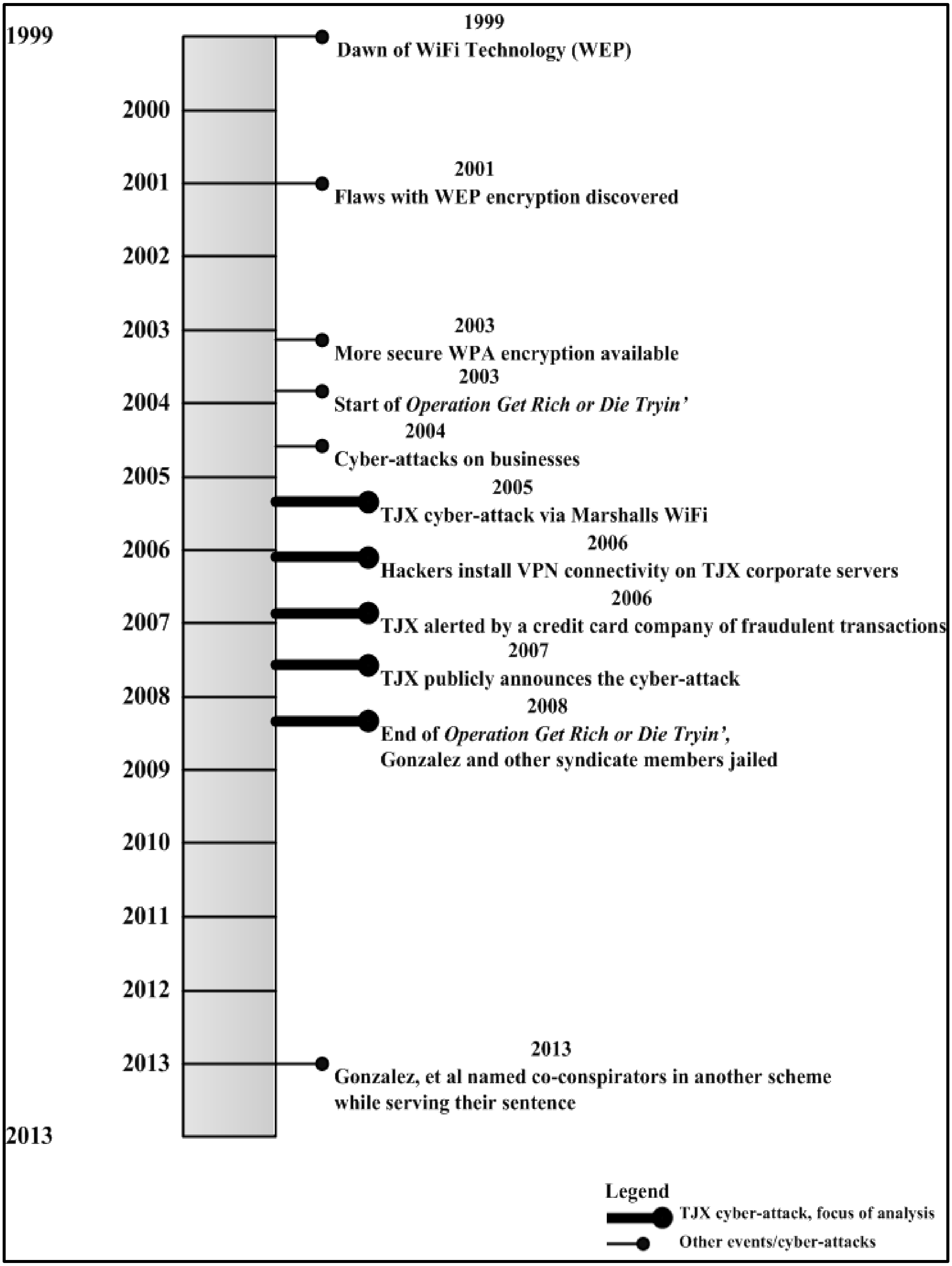

1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2013
1999
Dawn of WiFi Technology (WEP)
2001
Flaws with WEP encryption discovered
2003
More secure WPA encryption available
2003
Start of *Operation Get Rich or Die Tryin'*
2004
Cyber-attacks on businesses
2005
TJX cyber-attack via Marshalls WiFi
2006
Hackers install VPN connectivity on TJX corporate servers
2006
TJX alerted by a credit card company of fraudulent transactions
2007
TJX publicly announces the cyber-attack
2008
End of *Operation Get Rich or Die Tryin'*,
Gonzalez and other syndicate members jailed
2013
Gonzalez, et al named co-conspirators in another scheme
while serving their sentence
Legend
TJX cyber-attack, focus of analysis
Other events/cyber-attacks

Figure 4.10: High level timeline of *Operation Get Rich or Die Tryin'*.

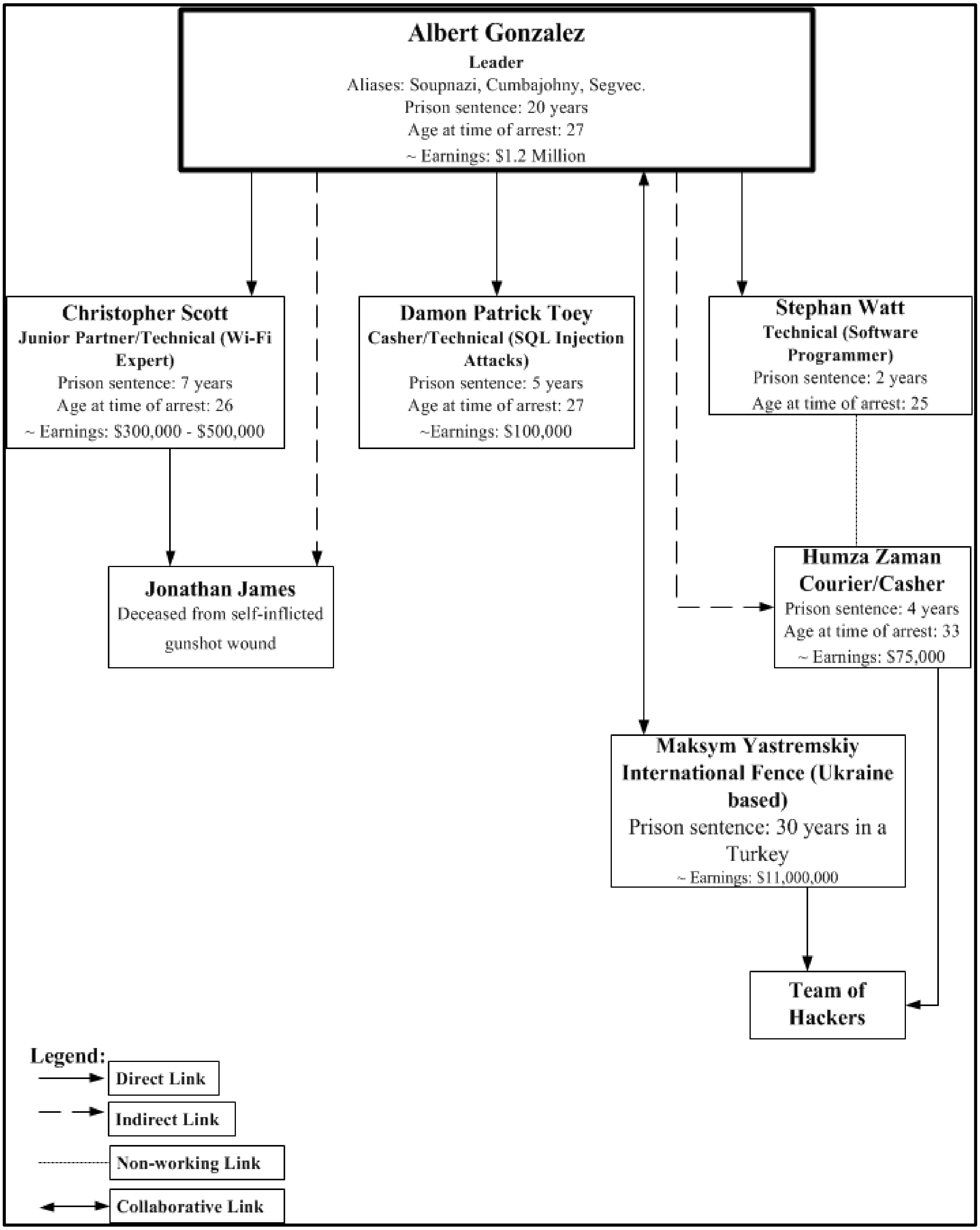

Albert Gonzalez
Leader
Aliases: Soupnazi, Cumbajohny, Segvec.
Prison sentence: 20 years
Age at time of arrest: 27
~ Earnings: $1.2 Million
Christopher Scott
Junior Partner/Technical (Wi-Fi Expert)
Prison sentence: 7 years
Age at time of arrest: 26
~ Earnings: $300,000 - $500,000
Damon Patrick Toey
Casher/Technical (SQL Injection Attacks)
Prison sentence: 5 years
Age at time of arrest: 27
~Earnings: $100,000
Stephan Watt
Technical (Software Programmer)
Prison sentence: 2 years
Age at time of arrest: 25
Jonathan James
Deceased from self-inflicted gunshot wound
Humza Zaman
Courier/Casher
Prison sentence: 4 years
Age at time of arrest: 33
~ Earnings: $75,000
Maksym Yastremskiy
International Fence (Ukraine based)
Prison sentence: 30 years in a Turkey
~ Earnings: $11,000,000
Team of Hackers
Legend:
Direct Link
Indirect Link
Non-working Link
Collaborative Link

Figure 4.11: Organizational structure of operation Get Rich or Die Tryin'.

5 STAMP/CAST Analysis of TJX Cyber-Attack

This chapter analyzes the TJX cyber-attack described in Chapter 4 using CAST. The period covered is from when the cyber-attack started in mid-2005 until it was publically announced in January 2007. The CAST steps were discussed in Chapter 2 and are outlined in Table 5.1 below for reference.

Step No.	STAMP/CAST Analysis Step Description
1	Identify the system(s) and hazard(s) associated with the accident or incident.
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.
5	Analyze the accident or incident at the physical system level.
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.
7	Analyze overall coordination and communication contributors to the accident or incident.
8	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.
9	Generate recommendations.

Table 5.1: CAST steps for analyzing accidents **[43]**.

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

5.1.1 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 (see Chapter 1). Payment card data was stolen from 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.

5.1.2 Hazard(s)

The hazard that is being 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.

5.2 Step #2: System Safety Constraints and System Requirements

5.2.1 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.

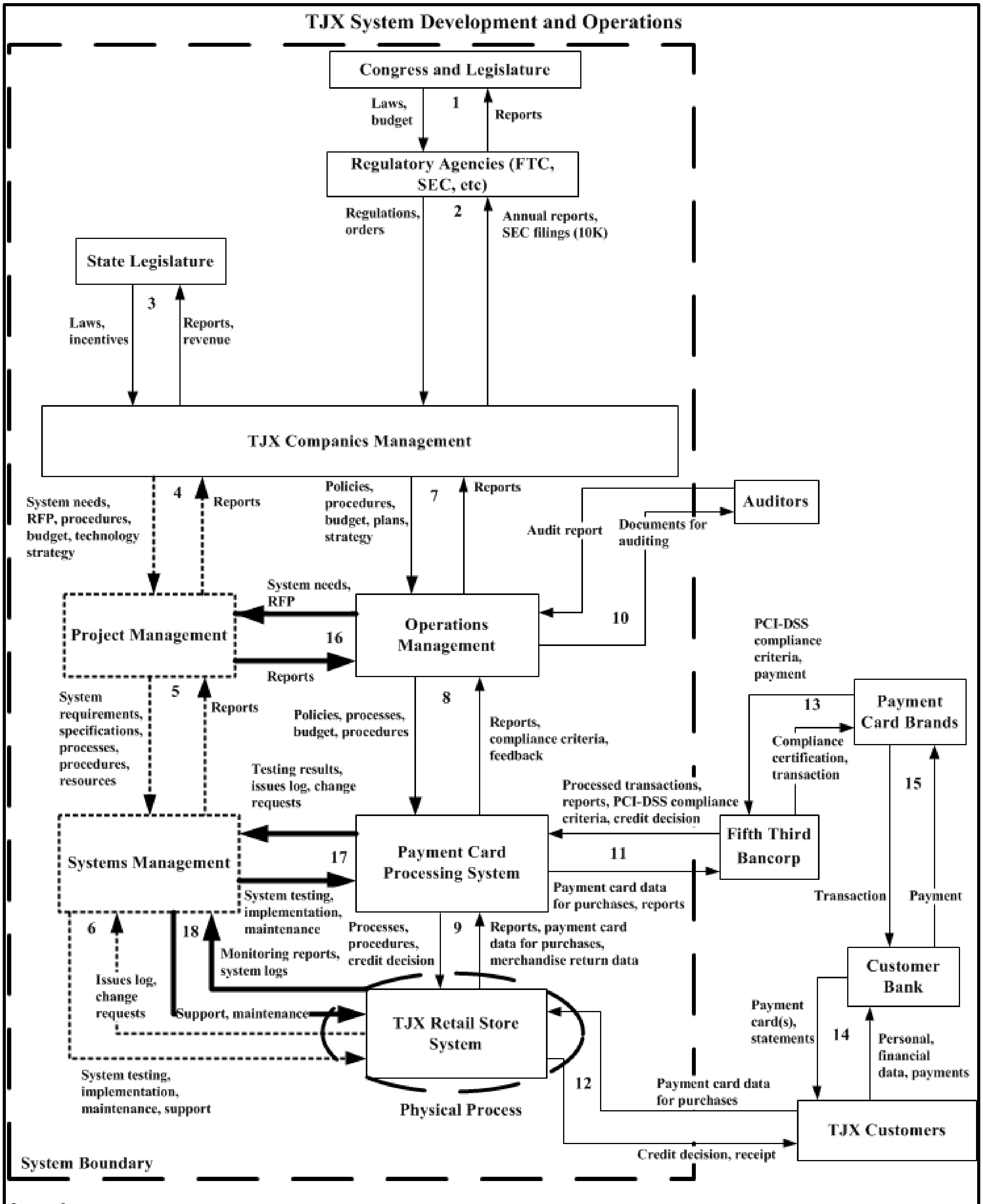
5.3 Step #3: TJX Hierarchical System Safety Control Structure

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 [43]. System Development and Operations (Figure 5.1), System development (Figure 5.2), and System Operations (Figure 5.3) control structures are discussed next.

5.3.1 Development and Operations Hierarchical Control Structure

Figure 5.1 shows combined system development and operations 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. The structure was constructed from information contained in the TJX 2007 annual report and from research conducted for writing the TJX cyber-attack case in Chapter 4.

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.


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, technology strategy
4
Reports
Policies, procedures, budget, plans, strategy
7
Reports
Auditors
Audit report
Documents for auditing
System needs, RFP
Project Management
16
Reports
Operations Management
10
PCI-DSS compliance criteria, payment
System requirements, specifications, processes, procedures, resources
5
Reports
Policies, processes, budget, procedures
8
Reports, compliance criteria, feedback
13
Payment Card Brands
Compliance certification, transaction
15
Testing results, issues log, change requests
Processed transactions, reports, PCI-DSS compliance criteria, credit decision
Systems Management
17
Payment Card Processing System
11
Fifth Third Bancorp
System testing, implementation, maintenance
Payment card data for purchases, reports
Transaction
Payment
6
18
Processes, procedures, credit decision
9
Reports, payment card data for purchases, merchandise return data
Monitoring reports, system logs
Customer Bank
Issues log, change requests
Support, maintenance
TJX Retail Store System
Payment card(s), statements
14
Personal, financial data, payments
System testing, implementation, maintenance, support
12
Payment card data for purchases
Physical Process
TJX Customers
Credit decision, receipt
System Boundary

Legend:

- Each **number** indicates a unique loop.
- Bold-dashed **square** indicates TJX system boundary.
- Bold-dashed **oval** indicates the physical process.
- **Downward arrow** represents reference channel for imposing safety constraints.
- **Upward arrow** represents feedback channel and reports the effectiveness of constraints.
- Dotted boxes and arrows indicate development part of the control structure.
- Bold arrows indicate interactions between development and operations.

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

5.3.2 System Development Hierarchical Control Structure

Hierarchical control structure for system development dimension is shown in Figure 5.2. The boundary labeled as *System Boundary* (dashed rectangle) encloses components that are the subject of analysis; numbers represent control structures with control and feedback channels forming a loop. TJX Retail Store System component of the hierarchical control structure, represented by dashed oval is the physical process where customers make purchases or return merchandise. This is also the entry point for customer payment card data that flows via TJX systems for credit decisions. The physical process is also starting point for the CAST analysis. TJX physical process will be analyzed in CAST Step #5 and rest of the components in Step #6.

Next level up is Systems Management component, which controls TJX Retail Store System (loop #6). Control is by way of implementing and maintaining technology including security technology for retail stores, and providing technical support and maintenance on an ongoing basis. Feedback from the TJX Retail Store System is received in the form of change requests and issues log for software and hardware systems, logs generated automatically by software and hardware systems for technical experts, and customized reports created by Systems Management, which can for example, include memory usage by software systems, network traffic load at the store network, and software application response times. Next level up is Project Management component that controls Systems Management (loop #5) by way of system requirements, specifications, procedures, processes, resources, and receives feedback in the form of reports. Project Management is responsible for managing technology projects across the TJX Company and works with TJX executive management to prioritize projects and accordingly allocates resources to System Management. Additionally, Project Management is responsible for processes, procedures, and training for System Management. Security technology is also the responsibility of Project Management, that is, ensuring that TJX security technology is setup according to TJX polices and industry standards.

Next level up is TJX Management (loop #4) that controls Project Management. TJX Management in addition to RFP's, provides high level system needs, procedures, technology strategy, and budget for Project Management. Feedback is in the form of reports. Next level up of the control structure is the Regulatory Agencies (loop #2), which controls TJX Management by way of regulations with reference to TJX business operations. Feedback is in the form of report filings to these agencies. At this level TJX Management is also controlled by the State

Legislature (loop #3). TJX is headquartered in Massachusetts; therefore state legislature of TJX home state has more power to exercise control via laws as compared to other states or regions. State Legislature also offers incentives to attract businesses to the state in order to stay competitive for businesses. Feedback is in terms of reports. At the highest level is US Congress and Legislature (loop #1), which exercises control over TJX by way of laws. Feedback is provided in the form of reports. Each of these components is discussed in detail as part of the CAST analysis in Step #5 and Step #6.

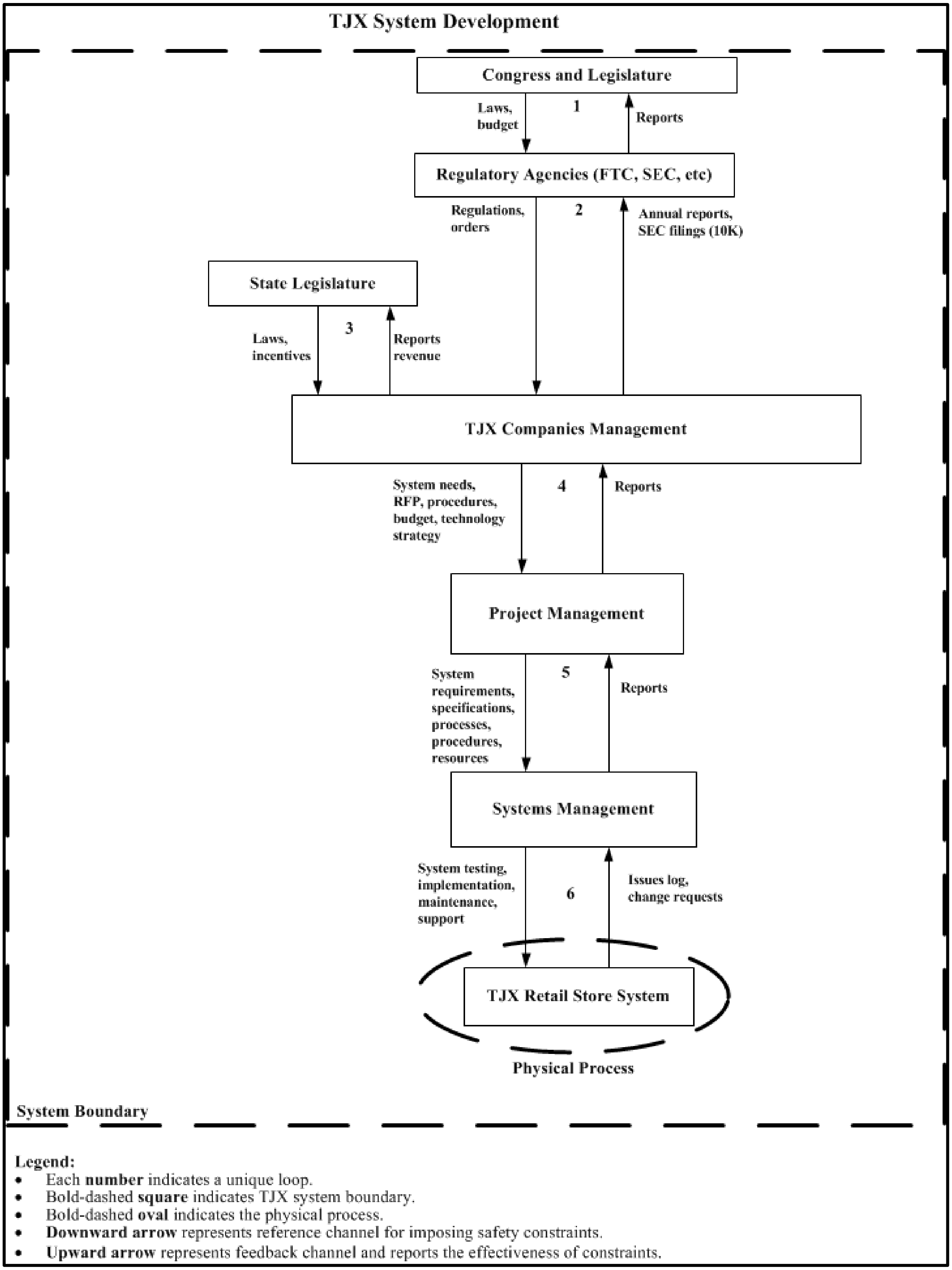

TJX System Development
Congress and Legislature
Laws, budget
1
Reports
Regulatory Agencies (FTC, SEC, etc)
Regulations, orders
2
Annual reports, SEC filings (10K)
State Legislature
Laws, incentives
3
Reports revenue
TJX Companies Management
System needs, RFP, procedures, budget, technology strategy
4
Reports
Project Management
System requirements, specifications, processes, procedures, resources
5
Reports
Systems Management
System testing, implementation, maintenance, support
6
Issues log, change requests
TJX Retail Store System
Physical Process
System Boundary
Legend:
• Each number indicates a unique loop.
• Bold-dashed square indicates TJX system boundary.
• Bold-dashed oval indicates the physical process.
• Downward arrow represents reference channel for imposing safety constraints.
• Upward arrow represents feedback channel and reports the effectiveness of constraints.

Figure 5.2: TJX system development hierarchical control structure.

5.3.3 System Operations Hierarchical Control Structure

Hierarchical control structure for system operations is shown in Figure 5.3. The boundary labeled as *System Boundary* (dashed rectangle) encloses components that are the subject of analysis; numbers represent control structures with control and feedback channels forming a loop.

According to Figure 5.3, the control structure has several components that interact with other components outside of the system boundary, those components that are external to the system boundary are not included in the analysis, but to understand the context a brief discussion is included in this section, and a detailed discussion of relevant external components is in the forthcoming analysis in CAST Step #5 and Step #6. As discussed earlier, TJX Retail Store System is the physical process. In this operational control structure moving one level up from the physical process is Payment Card Processing System (loop #9). Payment Card Processing System controls the TJX Retail Store System, by way of processes, procedures, and credit decisions for customers. Feedback is in the form of reports and payment card data from the physical system. TJX, per general industry trend had outsourced its payment card processing to Fifth Third Bancorp as reflected by interaction in Figure 5.3 (loop #11).

Next level up in the hierarchy is Operations Management that controls Payment Card Processing System (loop #8) as shown in Figure 5.3. Operations Management is responsible for setting policies, processes, budgets, and procedures for Payment Card Processing System, feedback are in the form of reports and compliance criteria. Operations Management is also responsible for auditing and interacts with TJX external auditors for yearly audits (loop #10). Next level up is TJX Management, which controls Operations Management by way of policies, procedures, budget, strategy, and plans (loop #7). Feedback is provided in the form of reports. Levels above the TJX Management have been discussed in the previous section and have similar role and responsibilities for operations dimension as development dimension.

Loop #12 represents interaction between TJX Retail Store System and TJX Customers. Any human visiting a TJX store with intent of making a purchase or only for browsing is a TJX customer. Customers interact with TJX Retail Store System by way of making a merchandise purchase or return. Customers present their payment card information for purchases or receipted merchandise returns and receive a credit decision or a credit in case of a return. For merchandise returns without a receipt, customers are asked to present additional information that includes a driver's license, address, etc.

Loop #11 represents interaction between Payment Card Processing System and Fifth Third Bancorp. As mentioned earlier, TJX had outsourced its payment card transaction processing to Fifth Third Bancorp bank. For processing the payment card transaction, Fifth Third Bancorp forwards customer information to Payment Card Brands (VISA, MasterCard, etc.) for further processing (loop #13). Payment Card Brands then interact with the Customer Bank that issued the payment card as represented by loop #15. Customer Bank then debits customer account for the amount of purchase as represented by loop #14.

Loop #10 represents interaction between Operations Management and Auditors. Operations Management provides business documentation for audit purposes and receives an audit report.

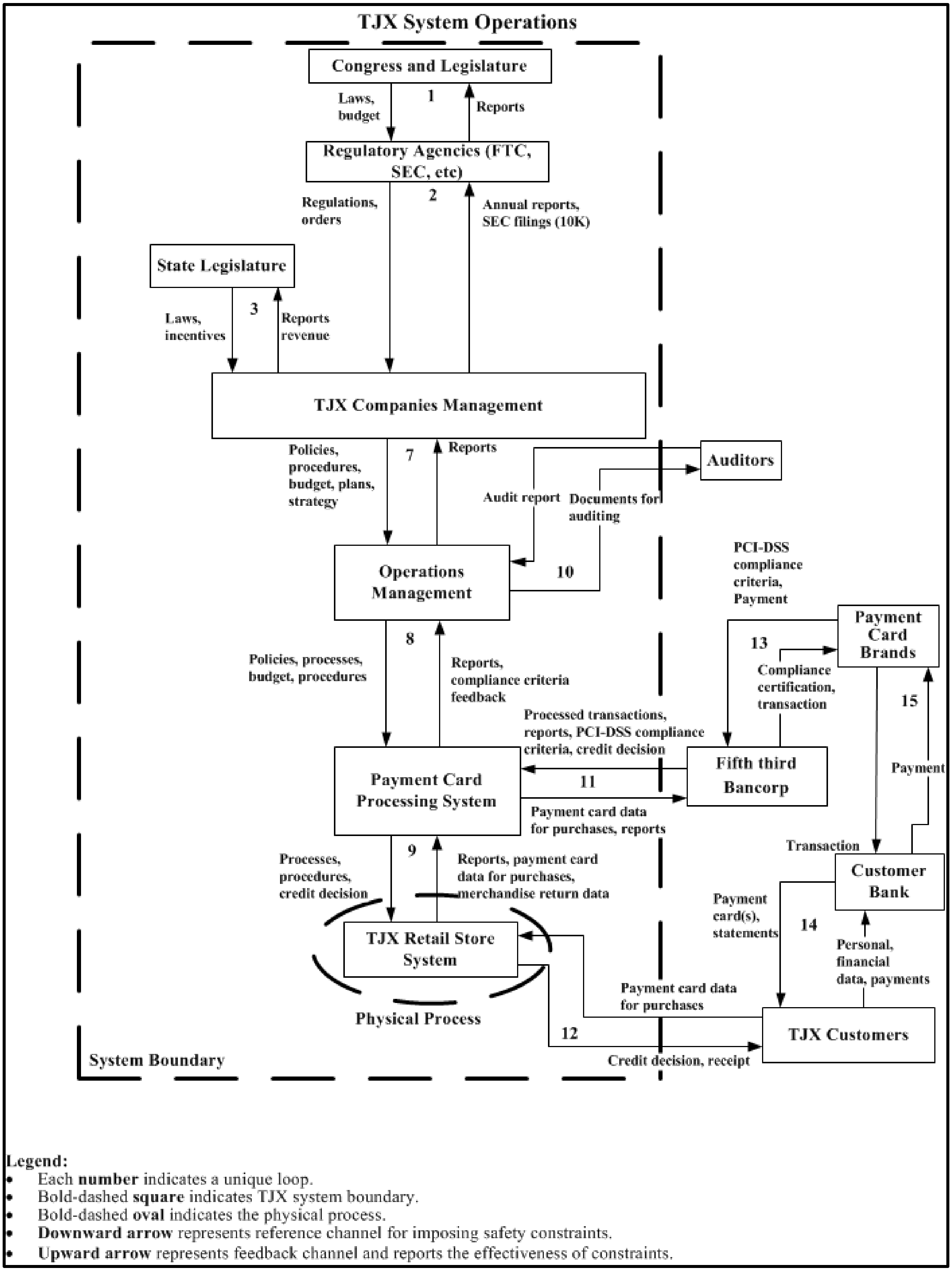

TJX System Operations
Congress and Legislature
Laws, budget
1
Reports
Regulatory Agencies (FTC, SEC, etc)
Regulations, orders
2
Annual reports, SEC filings (10K)
State Legislature
Laws, incentives
3
Reports revenue
TJX Companies Management
Policies, procedures, budget, plans, strategy
7
Reports
Auditors
Audit report
Documents for auditing
10
Operations Management
PCI-DSS compliance criteria, Payment
Payment Card Brands
13
Compliance certification, transaction
8
Policies, processes, budget, procedures
Reports, compliance criteria feedback
Processed transactions, reports, PCI-DSS compliance criteria, credit decision
15
Payment
Payment Card Processing System
11
Fifth third Bancorp
Payment card data for purchases, reports
Transaction
Customer Bank
9
Processes, procedures, credit decision
Reports, payment card data for purchases, merchandise return data
Payment card(s), statements
14
Personal, financial data, payments
TJX Retail Store System
Payment card data for purchases
Physical Process
12
TJX Customers
System Boundary
Credit decision, receipt
Legend:
Each number indicates a unique loop.
Bold-dashed square indicates TJX system boundary.
Bold-dashed oval indicates the physical process.
Downward arrow represents reference channel for imposing safety constraints.
Upward arrow represents feedback channel and reports the effectiveness of constraints.

Figure 5.3: TJX system operations hierarchical control structure.

5.4 Step #4: Proximate Event Chain

According to Leveson, event chain is not capable of providing critical information with reference to causality of an accident – in this case the 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 [43].

Further in STAMP proximate[37] 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. TJX case is specifically unique in this sense, 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, see Figure 4.10 for focus of CAST analysis with reference to time horizon. Therefore, in the context of cyber-security and specifically in this thesis *proximate* can also mean a longer time horizon generally in the range of 1-2 years. Proximate events leading to the TJX cyber-attack were discussed in Chapter 4 and are summarized below. Note that there were multiple incidents and accidents involved in the cyber-attack. Accidents are indicated by a '*'[38] 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.

[37] Merriam-Webster defines proximate as not being distant in time, space, or significance.
[38] * 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.*

5.5 Step #5: Analyzing the Physical Process

In this step, loss at the physical process level is analyzed. As shown in Figure 5.1, 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 [43]:

- 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.

5.5.1 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 5.1 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 5.1. 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.

5.5.1.1 Inadequate control/feedback

5.5.1.1.1 Security Technology Management Capabilities

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 using networks AP. TJX store network fell in this category, because its AP was incorrectly configured and opportunities for correct install during implementation (loop #6) and maintenance/support (loop #18) were missed as shown in Figure 5.1. 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.

5.5.1.1.2 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 5.1 needs to be analyzed further to understand causes underlying the weakened control, because Systems Management via loop #18 was responsible for monitoring.

5.5.1.1.3 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 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 5.4.

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 its 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 reinforcing a 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 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 5.4: CAST analysis of TJX Retail Store System (Physical Process Level).

5.6 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. According to Leveson, understanding behavior at any level of a sociotechnical safety control structure requires investigating control at the next higher level [43].

5.6.1 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 5.1 (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[39] bank (loop #11) as shown in Figure 5.1. It is also responsible for ensuring that TJX is in compliance with PCI[40]/PCI-DSS[41] requirements listed in Figure 4.5 and not in violation of any payment card brand rules[42].

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.

5.6.1.1 Inadequate control/feedback

5.6.1.1.1 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 listed in Figure 4.5 and its sub-requirements comprising of approximately eighty pages [68], 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 [68]
    - *Sub-requirement 3.1*: Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes. These include limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements…

[39] After mergers and acquisitions the name has changed to Vantiv (http://www.vantiv.com/).

[40] Payment Card Industry (PCI) Data Security Standard name was the first standard known as PCI from 2004-2006.

[41] PCI was called Payment Card Industry (PCI) Data Security Standard (DSS) – PCI-DSS starting from its second version in 2006.

[42] PCI-DSS will be used through rest of the thesis with an implicit understanding that until 2006 it was referred to as PCI.

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 [66] 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 [68]. 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 [66].

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 5.1 (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 5.5 and definition of each entity is shown in Figure 5.6. All major credit cards in general have a similar transaction flow.

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

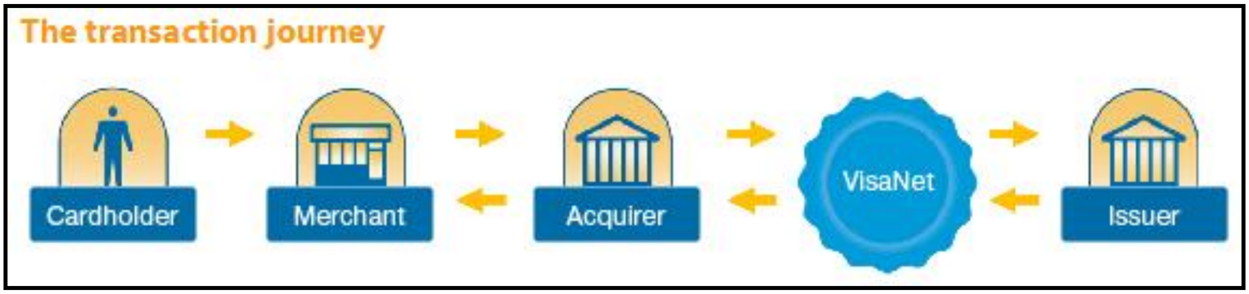
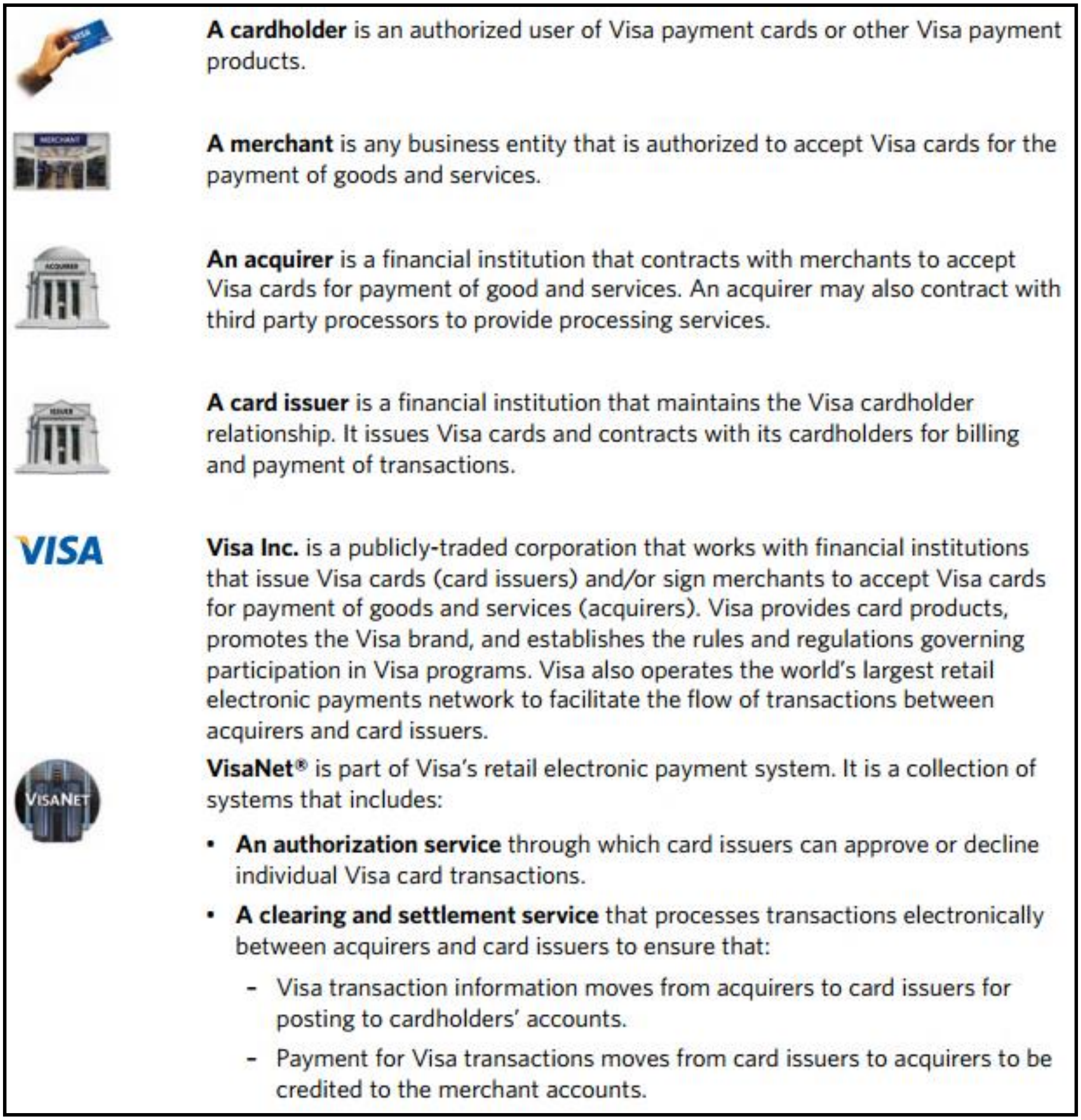


Figure 5.5: VISA transaction flow **[77]**.

- 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, and therefore Fifth Third Bancorp leverage is limited for rigorous enforcement of PCI-DSS, which is needed because of the scope and scale of PCI-DSS implementation. 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.

5.6.1.1.2 Payment Card Processing System and Systems Management Interaction

Because Payment Card Processing System was sending unencrypted customer data to the bank, it is plausible to conclude that 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 required to understand why this oversight occurred and for what reason. CAST analysis of Payment Card Processing System is summarized in Figure 5.7.



A cardholder is an authorized user of Visa payment cards or other Visa payment products.

A merchant is any business entity that is authorized to accept Visa cards for the payment of goods and services.

An acquirer is a financial institution that contracts with merchants to accept Visa cards for payment of good and services. An acquirer may also contract with third party processors to provide processing services.

A card issuer is a financial institution that maintains the Visa cardholder relationship. It issues Visa cards and contracts with its cardholders for billing and payment of transactions.

Visa Inc. is a publicly-traded corporation that works with financial institutions that issue Visa cards (card issuers) and/or sign merchants to accept Visa cards for payment of goods and services (acquirers). Visa provides card products, promotes the Visa brand, and establishes the rules and regulations governing participation in Visa programs. Visa also operates the world's largest retail electronic payments network to facilitate the flow of transactions between acquirers and card issuers.

VisaNet® is part of Visa's retail electronic payment system. It is a collection of systems that includes:

- **An authorization service** through which card issuers can approve or decline individual Visa card transactions.
- **A clearing and settlement service** that processes transactions electronically between acquirers and card issuers to ensure that:
  - Visa transaction information moves from acquirers to card issuers for posting to cardholders' accounts.
  - Payment for Visa transactions moves from card issuers to acquirers to be credited to the merchant accounts.

Figure 5.6: VISA transaction flow entity definitions **[78]**.

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 [79], 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.
    - In 2005 hackers downloaded payment card data that was at least two years old.
- 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 payment card data must be encrypted for these operations. There are three plausible explanations for this flaw, first either Systems Management was not aware of the PCI-DSS encryption requirement, second testing was inadequate, and third 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" [80]. 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 5.7: CAST analysis of Payment Card Processing System.

5.6.2 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 5.1 (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.

5.6.2.1 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 5.8.

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, therefore 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 [81].
  - 2006 – New CEO named [82].

- 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 [80].

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 5.8: CAST analysis of Operations Management.

5.6.3 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 5.9.

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 presumably may have shifted focus away from operational details.
  - 2005 – CEO resigns, new President named [81].
  - 2006 – New CEO named [82].
- 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 [83], 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 [80].

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 5.9: CAST analysis of TJX Companies Management.

5.6.4 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 5.1 (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 with reference to company’s payment card processing practices. An excerpt from the FTC decision [84] and order with reference to TJX information security policies is shown in Table 5.2; CAST analysis of Regulatory Agencies is summarized in Figure 5.10.

> *“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 5.2: Excerpt of Federal Trade Commission’s order to TJX **[84]**.

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 [85], 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 [85].

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 as discussed in Chapter 2 forensic investigations have their own limitations. As was discussed in Chapter 4, 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 5.10: CAST analysis of Regulatory Agencies.

5.6.5 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 5.1 (loop #3). CAST analysis for State Legislature is summarized in Figure 5.11.

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 MA.
  - PCI-DSS is a law in State of Nevada[43], enforced by State of Nevada Attorney General or a district attorney of any county.
- Lack of regulation with reference to collection and retention period of customer information with reference to purchases or returns.

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

Process Model Flaws:

- Unaware of PCI-DSS compliance status of TJX.

Figure 5.11: CAST analysis of State Legislature.

5.6.6 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 5.1 (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, USSS was involved in investigating the TJX cyber-attack. CAST analysis of Congress and Legislature is shown in Figure 5.12.

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 5.12: CAST analysis of Congress and Legislature.

5.6.7 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 5.1. 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 5.1 is for ongoing maintenance and support of systems at the physical process level. Feedback for loop #18 includes monitoring reports and system logs. CAST analysis of Systems Management is summarized in Figure 5.13.

5.6.7.1 Inadequate control/feedback

5.6.7.1.1 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.

5.6.7.1.2 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.

5.6.7.1.3 System maintenance

TJX was in the practice of using actual customer payment card data for resolving system issues and ongoing maintenance [66]. 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 5.13: CAST analysis of Systems Management.

5.6.8 Project Management

Next level up along the development part is Project Management that controls Systems Management as shown in Figure 5.1 (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 5.14.

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 [80].
- Lack or inadequate executive management support for implementing PCI-DSS standards, because cost was favored over critical security upgrades [80].
- 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 5.14: CAST analysis of Project Management.

5.6.9 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 5.1 (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 5.15.

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 as noted below, reduced corporate staff, and cut in senior executive salaries [83], may have contributed to additional pressure on the CIO with reference to cost containment.
  - 2005 – CEO resigns, new President named [81].
  - 2006 – New CEO named [82].
- 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 [80].
- 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 and with a focus on technology attributes only [80].

Figure 5.15: CAST analysis of TJX Companies Inc. Management.

5.7 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 did not object to the following activities that were in violation of PCI-DSS.

    - Continued use of deprecated WEP encryption (after a stronger encryption algorithm WPA became available).
    - Collection of customer information irrelevant to payment card processing.
    - Storage of customer information beyond the time period needed for payment card transaction processing.
    - Unsafe handling of customer information as it flowed through TJX systems. Specifically transmitting unencrypted customer data to the acquiring bank.

  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 [80], 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 5.1 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 [80] (see Table 5.4) 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 5.3, 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 5.3: Staff responses to the TJX CIO memo **[80]**.

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 5.1, 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.

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 [43]. 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, starting in 2000 until the cyber-attack in 2005 cyber security environment became sophisticated as discussed in this thesis. 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 [86]. That is, availability of information biases a decision, or formally stated, ease of recall bias emanates from availability heuristic [86]. With this context in mind, TJX was using encryption technology with vulnerabilities for more than two years before the cyber-attack[44] 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 [80].

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* [86]. This bias may also have played a role in TJX's migration to a higher risk state. Table 5.4 depicts a message from the TJX CIO Paul Butka in November 2005 to his staff [80], 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 5.3), 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 5.4: TJX CIO memo regarding security technology upgrade **[80]**.

[44] 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.

5.9 Step #9: Recommendations

Based on STAMP/CAST analysis following are some key recommendations, that can help TJX 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 [87]. 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, in case of TJX full compliance with PCI-DSS 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. Consider step #4 in Figure 4.5, in this step 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 (most likely because as discussed in Chapter 2, standards take time to update). 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 insights that otherwise could have been overlooked if another method of analysis was used.

6 Comparing STAMP/CAST with FTC and Canadian Privacy Commission Findings

This chapter presents comparisons between selected STAMP/CAST recommendations, and actions proposed by Canadian Privacy Commission and FTC. Canadian Privacy Commission 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 6.1 shows a list of recommendations with the source, each of which is discussed next.

No.	Recommendation	Canadian Privacy Commission	FTC	STAMP/CAST
1	Create an executive level role for managing cyber security risks.	No	*[45]	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 6.1: Comparison of STAMP/CAST recommendations with FTC and Canadian Privacy Commission.

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 program. CAST specifically recommends an executive level role for managing cyber security risks, because of the systemic weaknesses revealed and discussed in Chapter 5. With reference to recommendations #2, #3, #4, and #5 in Table 6.1 all were generated by STAMP/CAST and have

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

been discussed in Chapter 5. Recommendations #6 and #7, were proposed by the Canadian Privacy Commission as noted in Table 6.1, further, during STAMP/CAST analysis in Chapter 5 causes with reference to Recommendations #6 and #7 were discussed, that highlighted non-linear issues that would not be obvious otherwise. Based on the insights from STAMP/CAST analysis recommendations #6 and #7 have been addressed by STAMP/CAST in its recommendations #1, #2, and #3. With reference to recommendation #8 provided by FTC it is an important point. FTC recommendation as documented in its order [84] are vague that can lead to confusion on the 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" [84]. TJX already had in place security measures to protect customer information, but the controls were inadequate or failed due to systemic issues as discussed in Chapter 5. 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 and discussed in Chapter 5 are actionable steps.

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

7 Contributions

The abstract of this thesis quoted President Abraham Lincoln, accordingly the research focused on proposing a new way of approaching and managing cyber security risks, based on Systems Thinking and Systems Theory. Thesis 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-attacks. The analysis revealed insights, which might otherwise be difficult or impossible to gain using traditional technology focused approaches.

It is worth noting that TJX case was written using publically available sources, and court documents were the primary source with an outside-in view, 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 thesis 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 that PCI-DSS requirement #4 in Figure 4.5 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 cyber-attack.

8 Future Work

This thesis attempted to apply STAMP/CAST from the field of Systems Safety to cyber security. Based on the thesis research there is much room to refine STAMP/CAST and STAMP/STPA so it is more easily adaptable to cyber security risk management. Four key areas based on this thesis with reference to opportunities for future work are discussed next.

8.1 Definitions

Applying a Systems Safety model to cyber security required some redefinitions to reflect change in context with reference to application of STAMP/CAST to a virtual environment instead of a physical one. In order to facilitate CAST application to cyber security, definitions need to be created and refined. Mapping of STAMP definitions in the context of cyber security will further help in applying STAMP to cyber security. For example, with reference to CAST Step #4, proximate chain of events needs to be reviewed to incorporated spatial nature of cybercrime.

8.2 CAST Steps

Reviewing and possibly updating CAST steps in the context of cyber security is another area where opportunities for future work exist. For example, with reference to CAST Step #3, role of Congress and Legislature, Regulatory, and State Legislature components can be reviewed and possibly updated in the context of cyber security.

8.3 Architecture

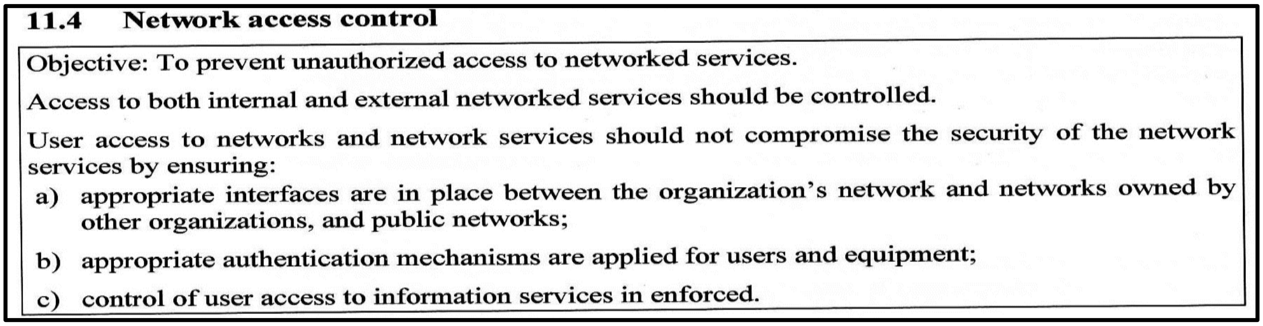
There are opportunities for investigating implementation of STAMP/CAST recommendations in system architecture. STAMP/STPA can be used to design a system for safety, which may provide guidance in implementing STAMP/CAST recommendations in the context of cyber security.

8.4 STAMP/CAST Application to Other Industries

This thesis applied STAMP/CAST to retail industry, primarily because TJX cyber-attack was the largest of its time. But STAMP/CAST can be used to analyze incidents or accidents in any industry, including finance, manufacturing, healthcare, or education. Further, lessons learned from the STAMP/CAST analysis of the TJX cyber-attack, can be applicable to other industries as well. For example, with reference to standards it is important to understand what precisely a standard will accomplish or not accomplish. As mentioned in Chapter 7, by complying with the PCI-DSS standard TJX may have avoided financial penalties imposed by VISA, but TJX would still be exposed to the risk of a cyber-attack. Another example is the discovery of systemic issues that led to the TJX cyber-attack. These same issues can cause increased level of cyber security risk in many industries.

Appendix 1

This appendix shows full details of section 11.4 of ISO/IEC 27002 that provides guidance for network access control.



11.4 Network access control

Objective: To prevent unauthorized access to networked services.

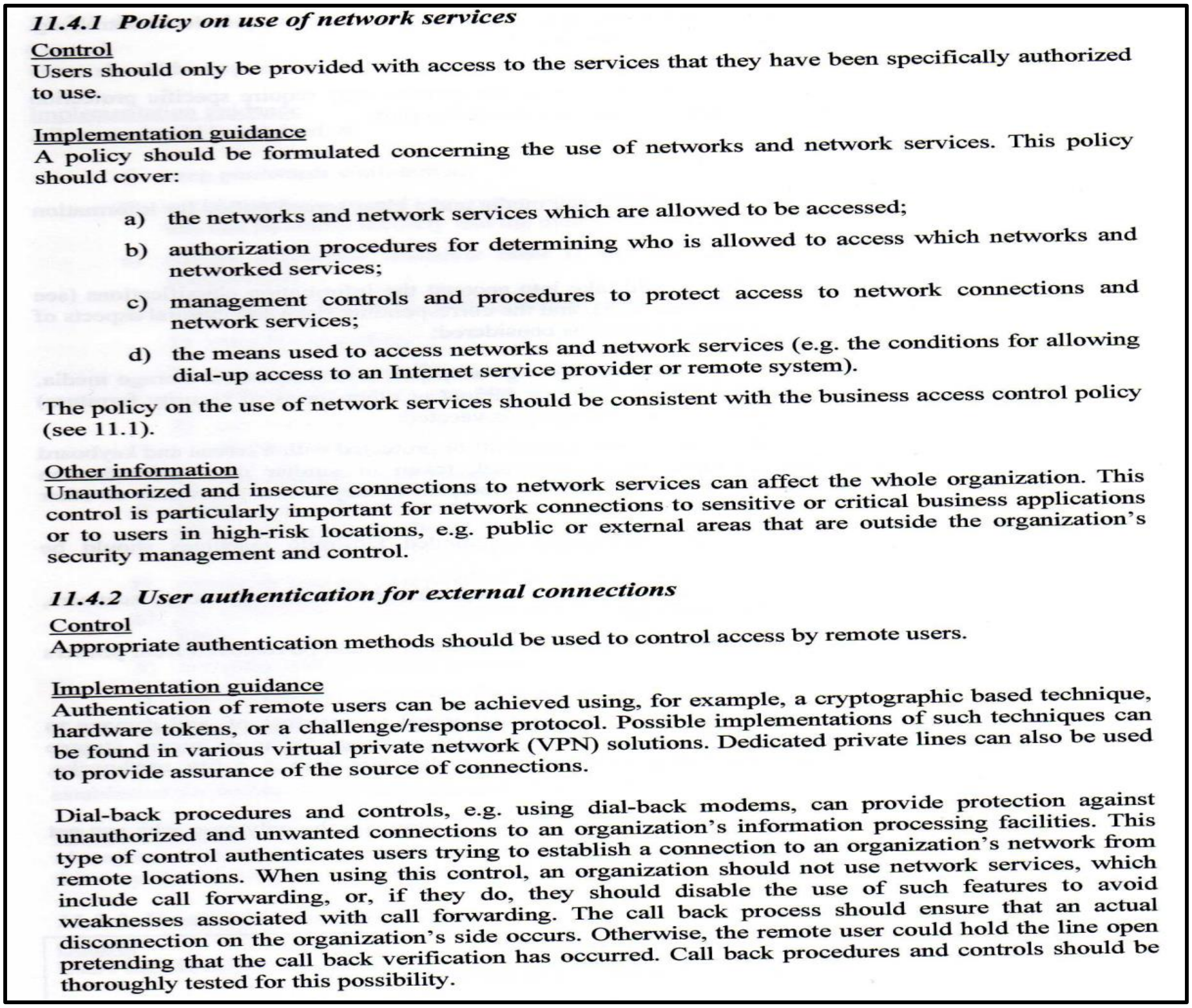
Access to both internal and external networked services should be controlled.

User access to networks and network services should not compromise the security of the network services by ensuring:

a) appropriate interfaces are in place between the organization's network and networks owned by other organizations, and public networks;

b) appropriate authentication mechanisms are applied for users and equipment;

c) control of user access to information services in enforced.



11.4.1 Policy on use of network services

Control
Users should only be provided with access to the services that they have been specifically authorized to use.

Implementation guidance
A policy should be formulated concerning the use of networks and network services. This policy should cover:

a) the networks and network services which are allowed to be accessed;

b) authorization procedures for determining who is allowed to access which networks and networked services;

c) management controls and procedures to protect access to network connections and network services;

d) the means used to access networks and network services (e.g. the conditions for allowing dial-up access to an Internet service provider or remote system).

The policy on the use of network services should be consistent with the business access control policy (see 11.1).

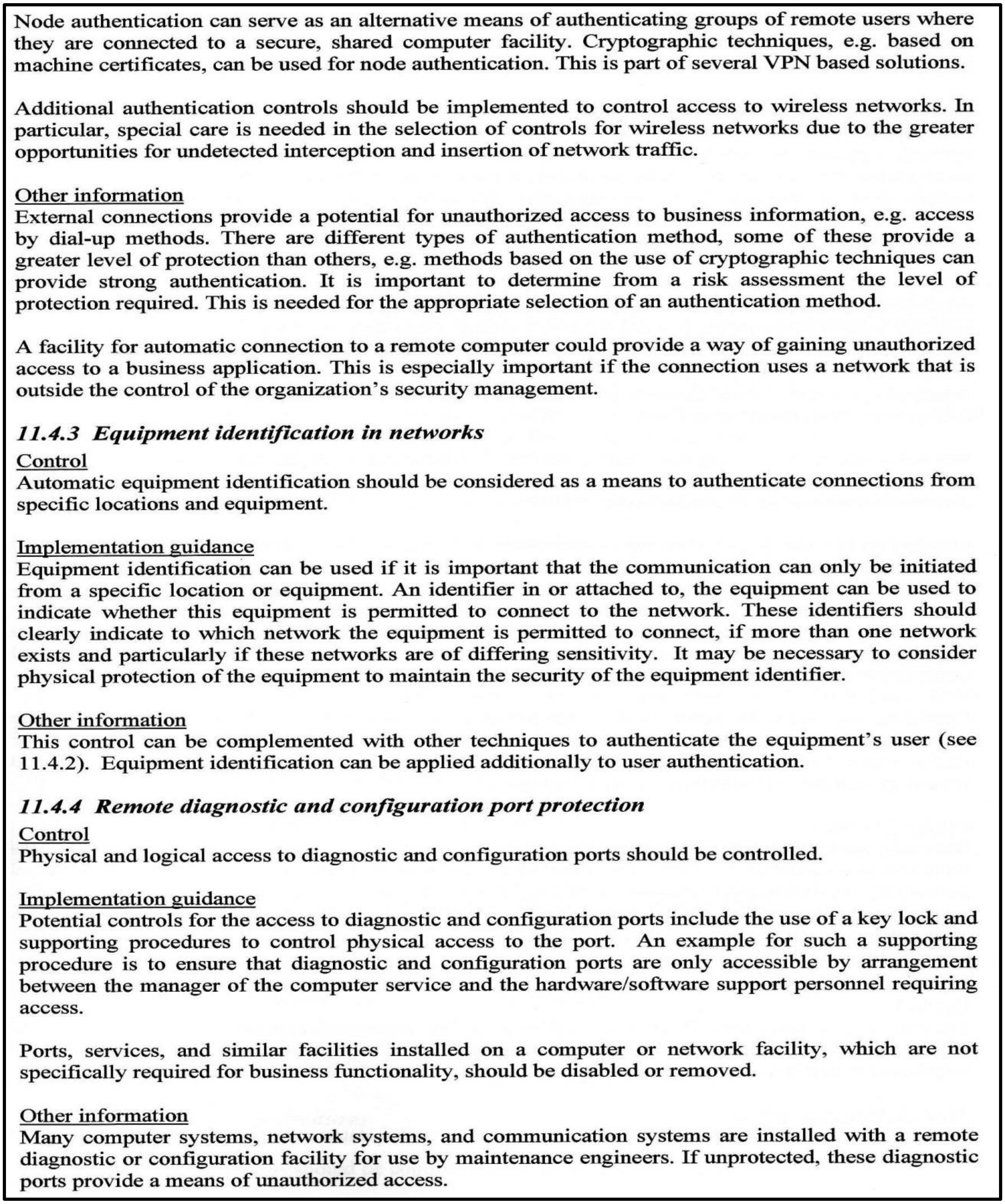
Other information
Unauthorized and insecure connections to network services can affect the whole organization. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organization's security management and control.

11.4.2 User authentication for external connections

Control
Appropriate authentication methods should be used to control access by remote users.

Implementation guidance
Authentication of remote users can be achieved using, for example, a cryptographic based technique, hardware tokens, or a challenge/response protocol. Possible implementations of such techniques can be found in various virtual private network (VPN) solutions. Dedicated private lines can also be used to provide assurance of the source of connections.

Dial-back procedures and controls, e.g. using dial-back modems, can provide protection against unauthorized and unwanted connections to an organization's information processing facilities. This type of control authenticates users trying to establish a connection to an organization's network from remote locations. When using this control, an organization should not use network services, which include call forwarding, or, if they do, they should disable the use of such features to avoid weaknesses associated with call forwarding. The call back process should ensure that an actual disconnection on the organization's side occurs. Otherwise, the remote user could hold the line open pretending that the call back verification has occurred. Call back procedures and controls should be thoroughly tested for this possibility.



Node authentication can serve as an alternative means of authenticating groups of remote users where they are connected to a secure, shared computer facility. Cryptographic techniques, e.g. based on machine certificates, can be used for node authentication. This is part of several VPN based solutions.

Additional authentication controls should be implemented to control access to wireless networks. In particular, special care is needed in the selection of controls for wireless networks due to the greater opportunities for undetected interception and insertion of network traffic.

Other information
External connections provide a potential for unauthorized access to business information, e.g. access by dial-up methods. There are different types of authentication method, some of these provide a greater level of protection than others, e.g. methods based on the use of cryptographic techniques can provide strong authentication. It is important to determine from a risk assessment the level of protection required. This is needed for the appropriate selection of an authentication method.

A facility for automatic connection to a remote computer could provide a way of gaining unauthorized access to a business application. This is especially important if the connection uses a network that is outside the control of the organization's security management.

11.4.3 Equipment identification in networks

Control
Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.

Implementation guidance
Equipment identification can be used if it is important that the communication can only be initiated from a specific location or equipment. An identifier in or attached to, the equipment can be used to indicate whether this equipment is permitted to connect to the network. These identifiers should clearly indicate to which network the equipment is permitted to connect, if more than one network exists and particularly if these networks are of differing sensitivity. It may be necessary to consider physical protection of the equipment to maintain the security of the equipment identifier.

Other information
This control can be complemented with other techniques to authenticate the equipment's user (see 11.4.2). Equipment identification can be applied additionally to user authentication.

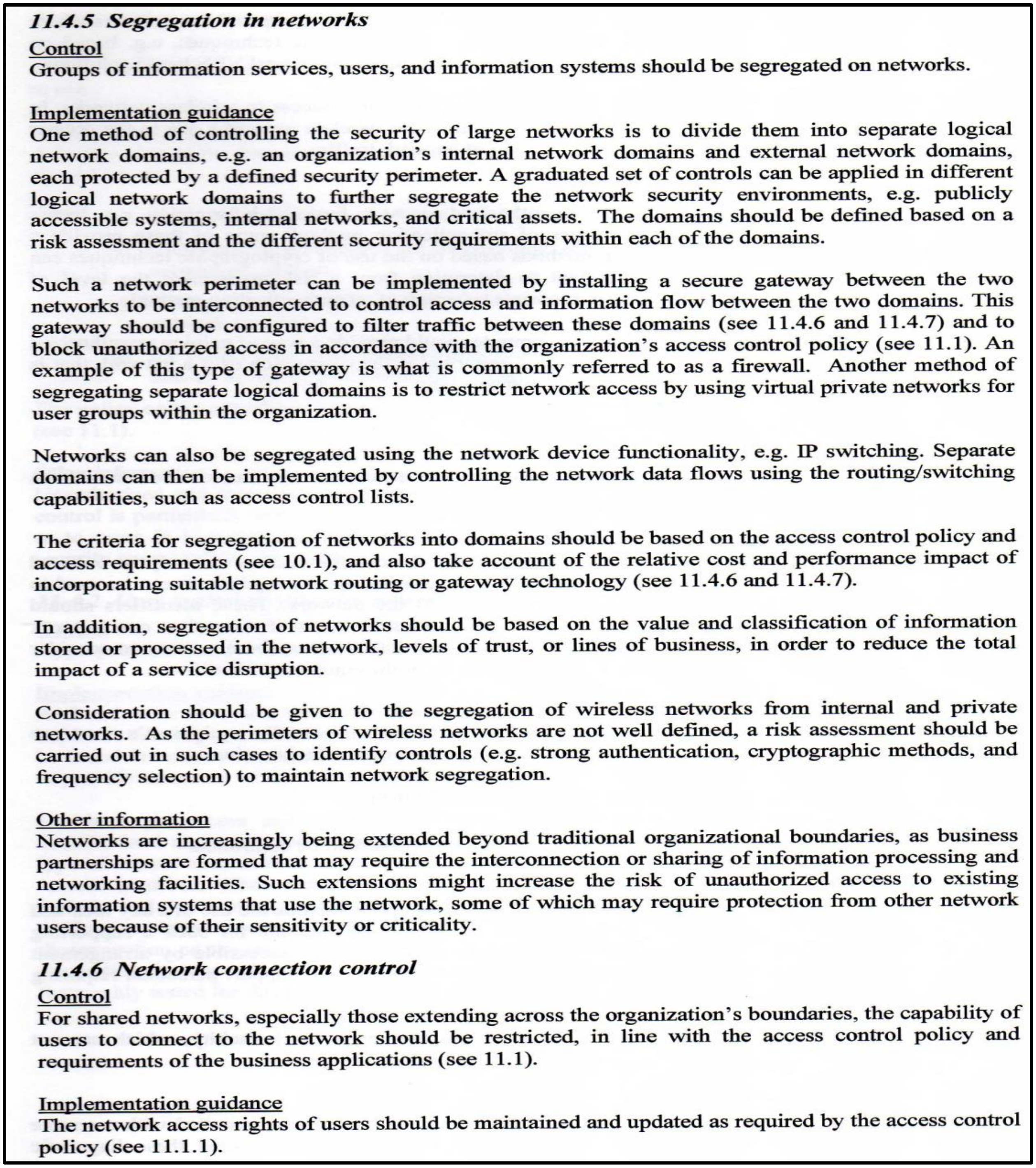
11.4.4 Remote diagnostic and configuration port protection

Control
Physical and logical access to diagnostic and configuration ports should be controlled.

Implementation guidance
Potential controls for the access to diagnostic and configuration ports include the use of a key lock and supporting procedures to control physical access to the port. An example for such a supporting procedure is to ensure that diagnostic and configuration ports are only accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access.

Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, should be disabled or removed.

Other information
Many computer systems, network systems, and communication systems are installed with a remote diagnostic or configuration facility for use by maintenance engineers. If unprotected, these diagnostic ports provide a means of unauthorized access.



11.4.5 Segregation in networks

Control
Groups of information services, users, and information systems should be segregated on networks.

Implementation guidance
One method of controlling the security of large networks is to divide them into separate logical network domains, e.g. an organization's internal network domains and external network domains, each protected by a defined security perimeter. A graduated set of controls can be applied in different logical network domains to further segregate the network security environments, e.g. publicly accessible systems, internal networks, and critical assets. The domains should be defined based on a risk assessment and the different security requirements within each of the domains.

Such a network perimeter can be implemented by installing a secure gateway between the two networks to be interconnected to control access and information flow between the two domains. This gateway should be configured to filter traffic between these domains (see 11.4.6 and 11.4.7) and to block unauthorized access in accordance with the organization's access control policy (see 11.1). An example of this type of gateway is what is commonly referred to as a firewall. Another method of segregating separate logical domains is to restrict network access by using virtual private networks for user groups within the organization.

Networks can also be segregated using the network device functionality, e.g. IP switching. Separate domains can then be implemented by controlling the network data flows using the routing/switching capabilities, such as access control lists.

The criteria for segregation of networks into domains should be based on the access control policy and access requirements (see 10.1), and also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology (see 11.4.6 and 11.4.7).

In addition, segregation of networks should be based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption.

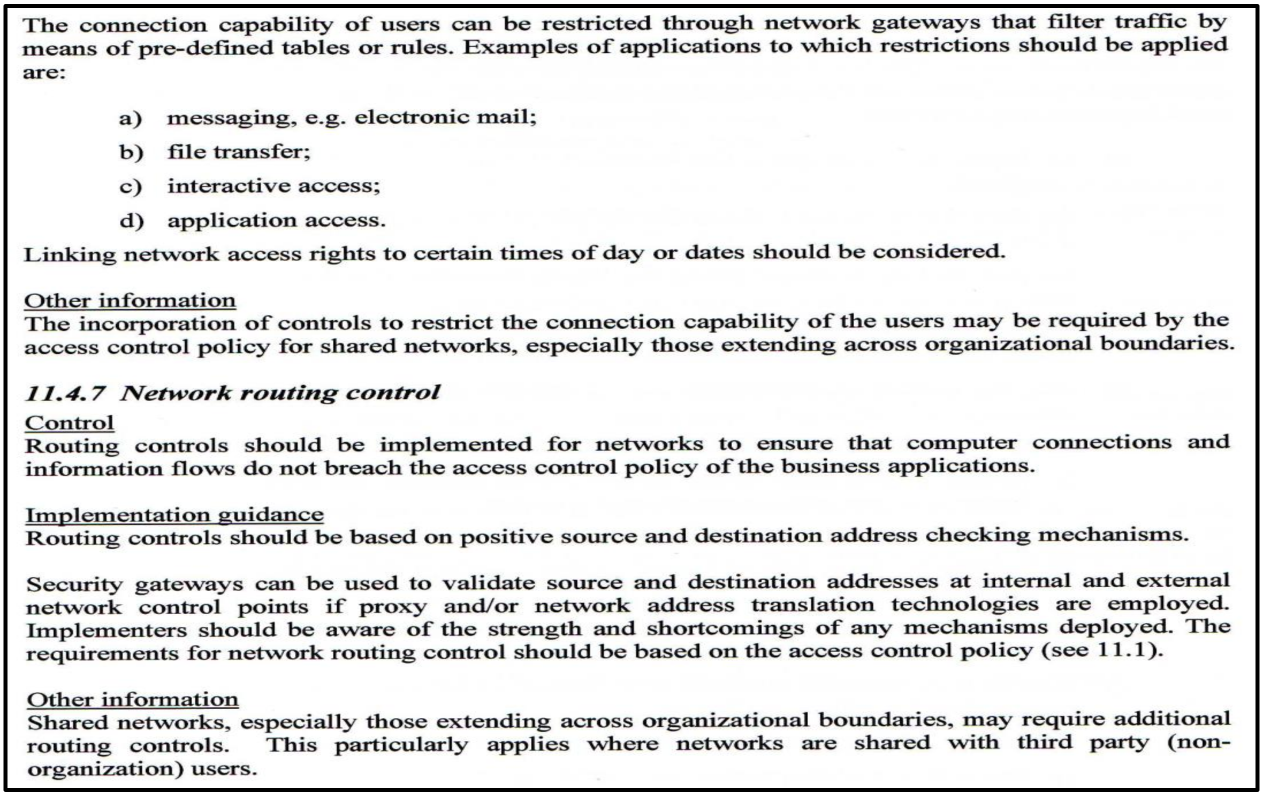
Consideration should be given to the segregation of wireless networks from internal and private networks. As the perimeters of wireless networks are not well defined, a risk assessment should be carried out in such cases to identify controls (e.g. strong authentication, cryptographic methods, and frequency selection) to maintain network segregation.

Other information
Networks are increasingly being extended beyond traditional organizational boundaries, as business partnerships are formed that may require the interconnection or sharing of information processing and networking facilities. Such extensions might increase the risk of unauthorized access to existing information systems that use the network, some of which may require protection from other network users because of their sensitivity or criticality.

11.4.6 Network connection control

Control
For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications (see 11.1).

Implementation guidance
The network access rights of users should be maintained and updated as required by the access control policy (see 11.1.1).



The connection capability of users can be restricted through network gateways that filter traffic by means of pre-defined tables or rules. Examples of applications to which restrictions should be applied are:

a) messaging, e.g. electronic mail;

b) file transfer;

c) interactive access;

d) application access.

Linking network access rights to certain times of day or dates should be considered.

<u>Other information</u>
The incorporation of controls to restrict the connection capability of the users may be required by the access control policy for shared networks, especially those extending across organizational boundaries.

11.4.7 Network routing control

<u>Control</u>
Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

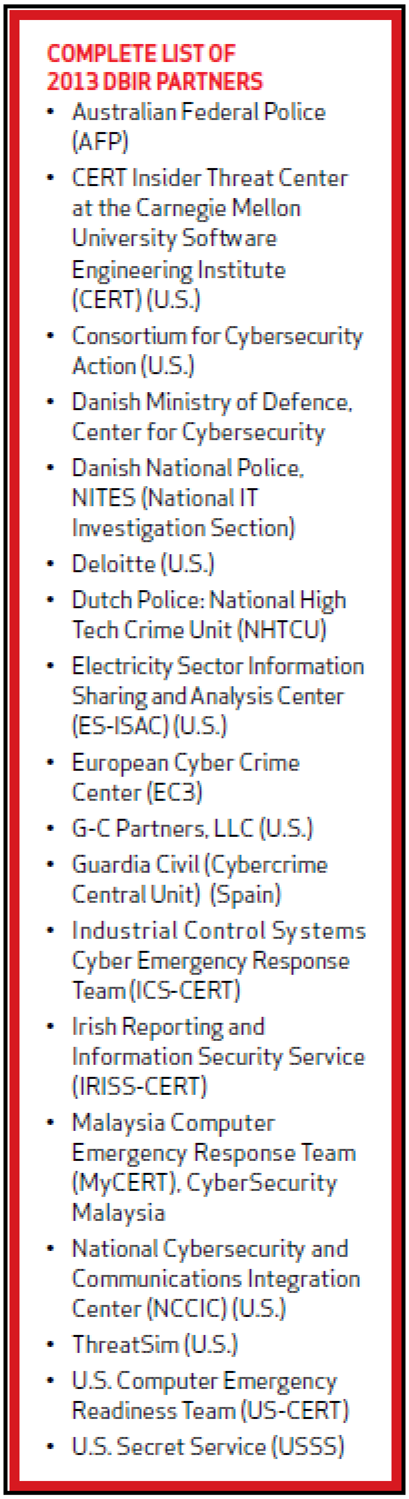
<u>Implementation guidance</u>
Routing controls should be based on positive source and destination address checking mechanisms.

Security gateways can be used to validate source and destination addresses at internal and external network control points if proxy and/or network address translation technologies are employed. Implementers should be aware of the strength and shortcomings of any mechanisms deployed. The requirements for network routing control should be based on the access control policy (see 11.1).

<u>Other information</u>
Shared networks, especially those extending across organizational boundaries, may require additional routing controls. This particularly applies where networks are shared with third party (non-organization) users.

Appendix 2

This appendix lists all the participants of Verizon's DBIR report of 2013.



COMPLETE LIST OF
2013 DBIR PARTNERS

- Australian Federal Police (AFP)
- CERT Insider Threat Center at the Carnegie Mellon University Software Engineering Institute (CERT) (U.S.)
- Consortium for Cybersecurity Action (U.S.)
- Danish Ministry of Defence, Center for Cybersecurity
- Danish National Police, NITES (National IT Investigation Section)
- Deloitte (U.S.)
- Dutch Police: National High Tech Crime Unit (NHTCU)
- Electricity Sector Information Sharing and Analysis Center (ES-ISAC) (U.S.)
- European Cyber Crime Center (EC3)
- G-C Partners, LLC (U.S.)
- Guardia Civil (Cybercrime Central Unit) (Spain)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- Irish Reporting and Information Security Service (IRISS-CERT)
- Malaysia Computer Emergency Response Team (MyCERT), CyberSecurity Malaysia
- National Cybersecurity and Communications Integration Center (NCCIC) (U.S.)
- ThreatSim (U.S.)
- U.S. Computer Emergency Readiness Team (US-CERT)
- U.S. Secret Service (USSS)

References

[1] Symantec Corporation, "Security Response Publications: Internet Security Threat Report 2013 Vol.18 (2012 Trends, Volume 18, Published April 2013)," Symantec Corporation, April 2013. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf OR http://www.symantec.com/security_response/publications/threatreport.jsp. [Accessed 12 October 2013].

[2] Symantec Corporation, "Security Response Publications: Internet Security Threat Reports (2012, April - Volume XVII)," Symantec, 2014. [Online]. Available: http://www.symantec.com/security_response/publications/archives.jsp. [Accessed 12 October 2013].

[3] Symantec Corporation, "Symantec Global Internet Security Threat Report: Trends for 2008 Volume XiV, published April 2009," Symantec Corporation, 2009. [Online]. Available: http://www.symantec.com/security_response/publications/archives.jsp OR http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf. [Accessed August 2013].

[4] G. L. Frank B. Strickland, "Articles: IBM Center for The Business of Government (The Cyber Underground Economy: Unconventional Thinking for a Fundamentally Different Problem)," 2011. [Online]. Available: http://www.businessofgovernment.org/article/cyber-underground-economy-unconventional-thinking-fundamentally-different-problem. [Accessed 18 September 2013].

[5] P. Hyman, "Cybercrime: It’s Serious, But Exactly How Serious?," *COMMUNICATIONS OF THE ACM*, vol. 56, no. 3, pp. 18-20, 2013.

[6] L. A. James and S. Baker, "The Economic Impact of Cybercrime and Cyber Espionage," Center for Strategic and International Studies (CSIS), Washington D.C., 2013.

[7] W. D. Miller, "Systems Thinking for a Secure Digital World," *CrossTalk, The Journal of Defense Software Engineering*, vol. 25, no. 5, pp. 11-14, 2012.

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

[9] Symantec Corporation, "Glossay (Hacker)," Symantec Corporation, 2014. [Online]. Available: http://www.symantec.com/security_response/glossary/define.jsp?letter=h&word=hacker. [Accessed 26 April 2014].

[10] Symantec Corporation, "Security Response Publications: Internet Security Threat Report 2014 Vol.19 (2013 Trends, Volume 19, Published April 2014)," Symantec Corporation, April 2014. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf OR http://www.symantec.com/security_response/publications/threatreport.jsp. [Accessed 19 April 2014].

[11] McAfee Labs, "Business Home," 2013. [Online]. Available: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf. [Accessed 14 October 2013].

[12] Symantec Corporation, "Security Response Publications: 2013, November - Symantec Intelligence Report," Symantic, 2014. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_11-2013.en-us.pdf. [Accessed 16 February 2014].

[13] PricewaterhouseCoopers, "Publications: PricewaterhouseCoopers," PricewaterhouseCoopers (PwC), 11 April 2013. [Online]. Available: http://www.pwc.com/en_US/us/10minutes/assets/pwc-cybersecurity-realities.pdf. [Accessed 7 August 2013].

[14] PricewaterhouseCoopers (PwC), "Global CEO Survey," PricewaterhouseCoopers (PwC), 2013. [Online]. Available: http://www.pwc.com/gx/en/ceo-survey/2013/index.jhtml. [Accessed 5 April 2014].

[15] G. J. MILLMAN, "Cyber Compliance: Defense Strategies Neglect “Know Your Enemy”

Rule," The Wall Street Journal, New York, 2013.

[16] United States Computer Emergency Readiness Team (US-CERT), "Federal Incident Reporting Guidelines (Federal Agency Incident Categories)," United States Computer Emergency Readiness Team (US-CERT), [Online]. Available: http://www.us-cert.gov/government-users/reporting-requirements. [Accessed 5 May 2014].

[17] D. Evans, "Cisco," Cisco, April 2011. [Online]. Available: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. [Accessed 15 August 2013].

[18] I. Internet Systems Consortium, "ISC Domain Survey," Internet Systems Consortium, Inc., July 2013. [Online]. Available: http://www.isc.org/services/survey/. [Accessed 18 September 2013].

[19] PricewaterhouseCoopers (PwC), "Global CEO Survey," PricewaterhouseCoopers (PwC), 2014. [Online]. Available: http://www.pwc.com/gx/en/ceo-survey/2014/download.jhtml. [Accessed 27 April 2014].

[20] Cisco, "Cisco Consulting Thought Leadership (Business Topics), At-A-Glance (Internet of Everything (IoE))," Cisco, December 2013. [Online]. Available: http://www.cisco.com/web/about/ac79/index.html#~bus OR http://www.cisco.com/web/about/ac79/docs/IoE/IoE-AAG.pdf. [Accessed 28 April 2014].

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

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

[23] N. G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, Cambridge, MA: MIT Press, 2011.

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

[25] Verizon, "The 2013 Data Breach Investigations Report," Verizon, 2014. [Online]. Available: http://www.verizonenterprise.com/DBIR/2013/. [Accessed 18 February 2014].

[26] Verizon, "VERIS Overview," Verizon, 4 August 2012. [Online]. Available: http://www.veriscommunity.net/doku.php?id=overview. [Accessed 11 August 2013].

[27] Verizon, "Verizon Enterprise Risk and Incident Sharing Metrics Framework," 2012. [Online]. Available: http://www.verizonenterprise.com/resources/whitepapers/wp_verizon-incident-sharing-metrics-framework_en_xg.pdf. [Accessed 11 August 2013].

[28] Verizon, "The 2012 Data Breach Investigations Report (DBIR)," Verizon, 2012. [Online]. Available: http://www.verizonenterprise.com/DBIR/2012/. [Accessed 12 August 2013].

[29] Verizon, "The 2011 Data Breach Investigations Report (DBIR)," Verizon, 2011. [Online]. Available: http://www.verizonenterprise.com/DBIR/2011/. [Accessed 12 August 2013].

[30] 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.

[31] N. P. S. M. U. Simson L. Garfinkel, "Digital forensics research: The next 10 years," *Digital Investigation,* vol. 7, no. Supplement, pp. S64-S73, 2010.

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

[33] Anti-Phishing Working Group, Inc. (APWG), "Resources: APWG Phishing Attack Trends Reports," Anti-Phishing Working Group, Inc. (APWG), 20 February 2014. [Online]. Available: http://docs.apwg.org/reports/apwg_trends_report_q3_2013.pdf. [Accessed 20 February 2014].

[34] 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.

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

[36] P. Patil, P. Zavarsky, D. Lindskog and R. Ruhl, "Fault Tree Analysis of Accidental Insider Security Events," in *2012 International Conference on Cyber Security*, Washington D.C., 2012.

[37] ISACA, "COBIT 5 for Information Security," in *COBIT 5 for Information Security*, Rolling Meadows, IL: ISACA, 2012, pp. 23, 55-59.

[38] International Organization for Standardization (ISO), "Store," International Organization for Standardization (ISO), [Online]. Available:

http://www.iso.org/iso/catalogue_detail?csnumber=50297. [Accessed 28 August 2013].

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

[40] 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].

[41] N. G. Leveson, "Terminology," in *Safeware*, Addison-Wesley, 1995, pp. 182-183.

[42] 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.

[43] 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.

[44] N. G. Leveson, "Definitions (Appendix A)," in *Engineering a Safer World: Systems Thinking Applied to Safety*, Cambridge, The MIT Press, 2011, pp. 467-468.

[45] N. G. Leveson, "Terminology," in *Safeware*, Addison-Wesley, 1995, pp. 171-184.

[46] Wikipedia, "Web 2.0," Wikipedia, 14 March 2014. [Online]. Available: http://en.wikipedia.org/wiki/Web_2.0. [Accessed 23 March 2014].

[47] TJX, "About Us: TJX Corporation," June 2013. [Online]. Available: http://www.tjx.com/about-tjx.asp. [Accessed 27 July 2013].

[48] TJX, "TJX '101': The TJX Companies Inc.," 2013. [Online]. Available: http://www.tjx.com/files/pdf/TJX-101-2013.pdf. [Accessed 27 July 2013].

[49] TJX, "Corporate Responsibility: A. TJX Corporation," 2013. [Online]. Available: http://www.tjx.com/corporate.asp. [Accessed 27 July 2013].

[50] J. Verini, "The Great Cyberheist," *The New York Times*, p. MM44 of Sunday Magazine, 10 November 2010.

[51] K. Zetter, "TJX Accomplice Sentenced to 7 Years in Prison," WIRED, 29 March 2010. [Online]. Available: http://www.wired.com/threatlevel/2010/03/christopher-scott-sentencing/. [Accessed June 2013].

[52] *USA v CHRISTOPHER SCOTT (US Dist. Court, Dist. of Massachusetts, Criminal No.08-CR-10224-DPW),* 2010.

[53] Wikipedia, "Wikipedia," Wikipedia, [Online]. Available: http://en.wikipedia.org/wiki/Wi-Fi. [Accessed May 2013].

[54] "Wired Equivalent Privacy (WEP)," Wikipedia, [Online]. Available: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy#cite_note-802.11-1997-0. [Accessed 15 March 2014].

[55] J. Pereira, "How Credit-Card Data Went Out Wireless Door," The Wall Street Journal, 4 May 2007. [Online]. Available: http://online.wsj.com/news/articles/SB117824446226991797. [Accessed 15 March 2014].

[56] The Institute of Electrical and Electronics Engineers, Inc. (IEEE), *IEEE Std 802.11-1997,* New York: IEEE, 1997.

[57] *USA v ALBERT GONZALEZ (US Dist. Court, Dist. of Massachusetts, Criminal No.08 CR 10223 PBS, INDICTMENT),* 2008.

[58] *USA v ALBERT GONZALEZ ((Government's Sentencing Memorandum, related cases 09-CR-10262-PBS, 09-CR-10382-DPW (Redacted version)),* 2008.

[59] *USA v ALBERT GONZALEZ (US Dist. Court, Dist. of Massachusetts, Criminal No. 08-10223-PBS, RULE 11 HEARING),* 2009.

[60] Weiss, Todd R. (Computerworld), "Credit card data breach probed at BJ's stores," Computerworld, 19 March 2004. [Online]. Available: http://www.computerworld.com/s/article/91412/Credit_card_data_breach_probed_at_BJ_s_stores. [Accessed 10 May 2014].

[61] US Government, "US Embassy in Ukraine," [Online]. Available: http://ukraine.usembassy.gov/arrested-info.html. [Accessed July 2013].

[62] K. Poulsen, "Former Teen Hacker’s Suicide Linked to TJX Probe," 2009.

[63] NETGEAR, "WEP Wireless Security," in *Wireless Networking Basics,* Santa Clara, CA: NETGEAR, 2005, pp. 2-5,2-6.

[64] Jesse R. Walker, "Unsafe at any key size; An analysis of the WEP encapsulation," *IEEE 802.11-00/362*, 27 Oct 2000.

[65] *USA v ALBERT GONZALEZ (US Dist. Court, Dist. of Massachusetts, Case No.08 CR 10223 PBS, INDICTMENT),* 2008.

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

[67] *TJX Companies Retail Security Breach Litigation (US Dist. Court, Dist. of Massachusetts, Master Docket No.07 10162 WGY),* 2007.

[68] 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.

[69] *USA v MAKSYM YASTREMSKIY (INDICTMENT,06CR1989-H),* 2007.

[70] *USA v HUMZA ZAMAN (VIOLATION(Conspiracy)),* 2009.

[71] *USA vs HUMZA ZAMAN (US Dist. Court, Dist. of Massachusetts, 09-CR-10054 (MLW), GOVERNMENT'S SENTENCING MEMORANDUM),* 2010.

[72] Symantec, "Glossary: Symantec," [Online]. Available: http://www.symantec.com/security_response/glossary/define.jsp?letter=z&word=zero-day-exploit. [Accessed 18 July 2013].

[73] TJX, "Investor Information: TJX Corporation," 31 March 2009. [Online]. Available: http://investor.tjx.com/phoenix.zhtml?c=118215&p=IROL-secToc&TOC=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9vdXRsaW5lLnhtbD9yZXBvPXRlbmsmaXBhZ2U9NjI0MTU4MCZzdWJzaWQ9NTc%3d&ListAll=1. [Accessed 27 July 2013].

[74] TJX, "Investor Information: TJX Corporation," 2 April 2014. [Online]. Available: http://investor.tjx.com/phoenix.zhtml?c=118215&p=irol-sec. [Accessed 16 May 2014].

[75] D. Bray Chad And Yadron, "Nasdaq, Others, Targeted by Hackers," *The Wall Street Journal*, 26 July 2013.

[76] Department of Justice, "Office of Public Affairs," 25 July 2013. [Online]. Available: http://www.justice.gov/opa/pr/2013/July/13-crm-842.html. [Accessed July 2013].

[77] 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].

[78] 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].

[79] 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].

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

[81] 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].

[82] 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].

[83] 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].

[84] 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].

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

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

[87] 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.

[88] N. G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, Cambridge, MA: The MIT Press, 2011, pp. 61-63.

[89] Heartland Payment Systems, "About Heartland," Heartland Payment Systems, 24 October 2013. [Online]. Available: http://www.heartlandpaymentsystems.com/About-Heartland. [Accessed 24 October 2013].

[90] US Computer Emergency Readiness Team (US-CERT), "Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks," Department of Homeland Security, 2014. [Online]. Available: http://www.us-cert.gov/ncas/tips/ST04-014. [Accessed 16 February 2014].

[91] *USA v ALBERT GONZALEZ (US Dist. Court, Dist. of Massachusetts, Criminal No. 08-CR-10223-PBS, Criminal No. 09-CR-10262-PBS, Criminal No. 09-CR-10382-DPW), GOVERNMENT'S SENTENCING MEMORANDUM,* 2010.

[92] PCI Standards Security Council, "Documents Library (PCI DSS Quick Reference Guide v2.0)," 2014. [Online]. Available: https://www.pcisecuritystandards.org/security_standards/documents.php?agreements=pcidss&association=pcidss. [Accessed 4 April 2014].

[93] Wikipedia, "Swiss Cheese Model," Wikipedia, 2014. [Online]. Available: http://en.wikipedia.org/wiki/Swiss_cheese_model. [Accessed 29 April 2014].