

Applying Systems Thinking to Healthcare Data Cybersecurity

by

Kristie Chung

Bachelors in Computer Information Systems

Florida Institute of Technology, 2013

Submitted to the System Design and Management Program
in partial fulfillment of the requirements for the Degree of
Master of Science in Engineering and Management

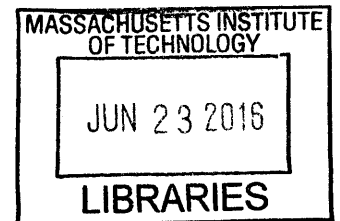
at the

Massachusetts Institute of Technology

September 2015

©2015 Kristie Chung.

All rights reserved.



ARCHIVES

The author hereby grants to MIT the permission to reproduce and distribute publicly paper and electronic copies of this thesis document in whole or in part in any medium now known or hereafter created.

Signature redacted

Signature of Author _____


Kristie Chung

Submitted to the System Design and Management Program


August 2015

Signature redacted

Certified and Accepted by _____


Patrick Hale

Senior Lecturer, Engineering Systems Division

Thesis Supervisor

Executive Director, System Design and Management Program

THIS PAGE INTENTIONALLY LEFT BLANK

Abstract

Since the HITECH Act of 2009, adoption of Electronic Health Record (EHR) systems in US healthcare organizations has increased significantly. Along with the rapid increase in usage of EHR, cybercrimes are on the rise as well. Two recent cybercrime cases from early 2015, the Anthem and Premera breaches, are examples of the alarming increase of cybercrimes in this domain. Although modern Information Technology (IT) systems have evolved to become very complex and dynamic, cybersecurity strategies have remained static. Cyber attackers are now adopting more adaptive, sophisticated tactics, yet the cybersecurity counter tactics have proven to be inadequate and ineffective. The objective of this thesis is to analyze the recent Anthem security breach to assess the vulnerabilities of Anthem's data systems using current cybersecurity frameworks and guidelines and the Systems-Theoretic Accident Model and Process (STAMP) method. The STAMP analysis revealed Anthem's cybersecurity strategy needs to be reassessed and redesigned from a systems perspective using a holistic approach. Unless our society and government understand cybersecurity from a sociotechnical perspective, we will never be equipped to protect valuable information and will always lose this battle.

Thesis Supervisor: Patrick Hale

Title: Senior Lecturer, Engineering System Division
Executive Director, System Design and Management Program

Acknowledgments

First and foremost, my deepest gratitude is extended to my advisor Mr. Patrick Hale. I have been amazingly fortunate to have his continuous support, guidance and understanding through SDM program and in writing this thesis. He has been always available to listen and to provide insightful advices throughout the process. This thesis could not have been finished without his encouragement and guidance.

I had a privilege to learn from Professor Nancy Leveson, who has introduced STAMP method and taught how to apply systems thinking in real world. In her courses I was able to apply everything I have learned from SDM curriculum. Her lectures not only transformed my view but also made me to become a better and more mature human being.

Thanks to MIT SDM cohorts who have inspired me and challenged me with different perspectives. I also want to thank the entire SDM Staffs for the amazing support to create the best learning experiences possible.

Finally, I am indebted to my mom and sister for their continuous love and patience. None of this would have been possible without their encouragement and support.

Disclaimer

The views expressed in this thesis are those of the author and do not reflect the official position of the Massachusetts Institute of Technology. Due to the recent occurrence and the ongoing investigation of the breach, the facts accepted here are based from the media coverage and the resource listed in the reference section.

Table of Contents

Abstract	3
Acknowledgments	4
Disclaimer	5
Table of Contents	6
Abbreviations	8
1. Introduction	11
1.1 Cybercrime in the Healthcare Industry	13
1.2 Financial Impact of Cybercrime.....	17
1.3 Traditional Cybersecurity Methods and Limitations.....	19
1.4 Thesis Structure.....	21
2. Literature Review.....	21
2.1 Chain of Events Model.....	21
2.2 National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (CSF).....	23
2.3 HIPAA, HITECH and Meaningful Use	27
2.4 System-Theoretic Accident Model and Processes (STAMP)	29
2.5 Causal Analysis based on STAMP (CAST).....	30
2.6 System Theoretic Process Analysis (STPA).....	32
3 Definitions.....	35
4 Anthem Breach Overview.....	36
4.1 Company Overview.....	37
4.2 Mission, Vision, and Values	38
4.3 Anthem Breach Details	39
4.3.1 Facts	39
4.3.2 Advanced Persistent Threat	39
4.3.3 Scheme.....	42
5. STAMP-CAST Analysis of Anthem Breach	47
5.1 Step 1: Defining System Accidents and Hazard	48
5.1.1 System Description	48
5.1.2 System Accident and Hazards	48

5.2 Step 2: System Safety Constraints and System Requirements	49
5.3 Step 3: Hierarchical System Safety Control Structure	50
5.3.1 System Operations Hierarchical Control Structure.....	51
5.4 Step 4: Proximate Event Chain	52
5.5 Step 5: Analyzing the Physical Process	54
5.5.1 Identifying Physical and Operational Controls.....	54
5.5.2 Security Analysis	55
5.6 Step 6: Analysis of Higher Levels of the Hierarchical Safety Control Structure.....	55
5.6.1 Information Security Management.....	55
5.6.2 Operations Management.....	59
5.6.3 Human Resources (HR).....	61
5.6.4 Anthem Executive Management	63
5.6.5 Health Insurance Industry.....	66
5.6.6 Regulatory Agencies.....	68
5.6.7 Congress	70
5.6.8 Inadequate Controls and Missing Feedback.....	71
5.7 Step 7: Coordination and Communication.....	72
5.8 Step 8: Dynamics and Migration to a High-Risk State	73
5.9 Step 9: Recommendations.....	74
6. Recommendations	75
7. Future Work	79
Conclusion.....	80
Appendix 1 Anthem Communication to members after breach.....	81
Appendix 2 HIPAA Security Standards Matrix.....	82
Bibliography.....	85

List of Tables

Table 1: Impact of cyberbreach in healthcare within last 5 years (McCan 2012)	16
Table 2: NIST Framework Tier Matrix (NIST 2014)	25
Table 3: Covered Entities under HIPAA (U.S. Department of Health & Human Services 1996)	28
Table 4: CAST analysis steps (Leveson 2011)	31
Table 5: Anthem, Inc. history (Anthem n.d).....	38
Table 6: CAST steps for analyzing accidents (Leveson 2011).....	48
Table 7: Unsafe safety control actions – Information Technology Department.....	59
Table 8: Unsafe safety control action – Anthem Operations Department	61
Table 9: Unsafe safety control action – Anthem Human Resources	63
Table 10: Unsafe safety control actions – Anthem Executive Management	65
Table 11: Unsafe safety control action – Health insurance industry	67
Table 12: Unsafe safety control action – Healthcare regulatory agencies.....	70
Table 13: Unsafe safety control action – Federal Legislation	71

List of Figures

Figure 1: Personal Health Data Flow map (Datamap.org n.d)	16
Figure 2: 2014 Data Breach Summary per Category (ITRC 2014)	17
Figure 3: Per capita cost of a data breach by industry (Ponemon 2014)	19
Figure 4: Heinrich’s Chain of Event (domino) model (Transport Canada 2007).....	23
Figure 5: Intel Use Case of applying NIST CSF (CaseyTim, etc. 2015).....	27
Figure 6: STPA Control Structure	34
Figure 7: Causal Factors in STPA	34
Figure 8: Wellpoint APT diagram.....	44
Figure 9: Domain name registration history for Wellpoint[.]com	44
Figure 10: Wellpoint[.] com IP history in 2014-2015.....	45
Figure 11: Wellpoint[.]com Registrar update history (BargerRich 2015).....	45
Figure 12: Social Engineering Search Example	46
Figure 13: Hierarchical Structure of Anthem’s Information System and Management Process.....	51
Figure 14: Anthem, Inc. Executive Leadership Organizational Chart (Anthem, 2015).....	64
Figure 15: Anthem stock price trend (January 2015- March 2015).....	74
Figure 16: Relationship between Effectiveness and Cost of three steps of loss prevention.....	76

Abbreviations

API	Application Program Interface
APT	Advanced Persistent Threat
BCBS	Blue Cross Blue Shield
CAST	Causal Analysis based on STAMP
CCS	Council on CyberSecurity
CSC	Critical Security Controls
COBIT	Control Objectives for Information and Related Technology
DHHS	US Department of Health and Human Services
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
HITECH	Health Information Technology for Economic and Clinical Health
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resources
IEC	International Electrotechnical Commission
IOC	Incident Of Compromise
ISA	International Society of Automation
ISO	International Organization for Standardization
MD5	Message Digest 5
NH-ISAC	National Health Information Sharing and Analysis Center
NIST	National Institute of Standards and Technology
OCR	Office of Civil Rights
OIG	Office of Inspector General
ONC	The Office of National Coordinator
OSI	Open Systems Interconnection
OSINT	Open Source Intelligence Techniques
PHI	Protected Health Information
PII	Personally Identifiable Information
SHA	Secure Hash Algorithm
STAMP	Systems-Theoretic Accident Model and Processes
STPA	STAMP-Based Process Analysis
VPN	Virtual Personal Network

THIS PAGE INTENTIONALLY LEFT BLANK

Introduction

Cybercrime is rapidly growing, and cyber criminals are outsmarting us. 2014 was the year of breaches; JP Morgan Chase, Good Will, UPS, Dairy Queen, and Neiman Marcus were all compromised. It seems our society has not learned many lessons from major breaches of Target, Home Depot, and TJ Maxx which occurred in the last 5 years, and we still are not well-equipped to protect against attackers. There have been many efforts to protect personal data and other confidential information, yet these efforts seem to be inadequate and failing, often leading to disastrous outcomes. Each time there is a breach, the number of victims grows and people start to become desensitized from one breach to the next. We are only halfway through 2015, but there have already been two major breaches in the healthcare industry, which impacted more than a quarter of the entire U.S. population. The FBI warned in 2014 that the healthcare industry is vulnerable and there is a rising trend of cybercrime in this domain. Although there was a clear warning and previous cases of major breaches, it was not enough to prepare organizations to stop future incidents.

Why is it so difficult to prevent cybercrime when public awareness is so high? Massachusetts Institute of Technology (MIT) Professor Nancy Leveson, who created the STAMP model for accident and hazard analysis, has defined the risk as a “combination of severity and likelihood.” In an accident, risk is hard to calculate, as the probability is hard to estimate. However, with cybercrime, the likelihood of an attack is very high, especially when the protected information is so valuable. We should first understand cybercrime is a socio-technical problem initiated by humans using technology with malicious intent. Companies try to protect themselves by investing in cybersecurity and creating security policies, but fail to understand this is a systemic problem which requires a holistic solution.

The motivation underlying this thesis is to assess cybercrime with a more holistic view

and shed light on how to understand these cybercrimes at a deeper level, manage cybersecurity risks, and mitigate the societal impact using systems thinking. This thesis focuses on data security within the Healthcare industry because patients' personal data is the most critical asset we need to secure.

1.1 Cybercrime in the Healthcare Industry

The number of people affected by cybercrime in the healthcare industry has significantly increased within the last 5 years. Anthem Inc., the second largest health insurance company in the US, reported in February 2015 that they had a security breach exposing the personal and confidential data of 78.8 million people, approximately 25% of the US population. The Anthem breach was followed by the Premera breach in March 2015, which involved 11 million people. Symantec's 2014 Internet Security Report [1] reported that 552 million identity breaches occurred during 2013, and among them healthcare had the largest disclosed breach, which accounted for 37 percent of the total. The report pointed out that although healthcare is the heaviest regulated sector, it is the source of the highest share of known breaches. This trend continued in 2014 and 2015.

Due to the nature of the healthcare industry, many key personal identifiers need to be stored. This industry practice makes it a highly attractive target for attackers because they know they can use industry systems to obtain valuable personally identifiable information. Two recent major security breaches in the healthcare industry – Anthem and Premera Blue Cross Blue Shield in Washington State - signal the alarming increase of cybercrimes within the industry. Health Insurance Company Anthem reported in February 2015 there was a cybersecurity breach affecting 78.8 million individuals. This massive breach was followed by a cyberattack on Premera, which compromised the personal information of approximately 11

million customers. Table 1 shows the largest breaches in the healthcare industry within the last 5 years. Many of these breaches affected at least a half million people and the number of affected individuals is growing. The insurance, healthcare, and government sectors have been the major targets of attackers.

There are two major reasons why the healthcare industry in general, and large health insurance companies in particular, is being targeted by attackers. First, the healthcare industry has more access or entry points to data than any other industry due to the number of large stakeholders. Figure 1 illustrates how personal information travels from a patient to other organizations. As shown in this figure, the information travels like a web, from a patient to multiple points, including hospital and payer. The collection of patients' data are sent to the payer (the insurance company) for medical claims processing and often stored anywhere from 6 years up to 10 years in average. Unlike other industries where the dataflow is close to linear, the healthcare industry has very unique data structures and flows. Different types of patient data may be sent to many stakeholders, and there are multiple access points to those data. This is due to patients not owning, storing, and managing their data, but delegating these functions to various healthcare providers. Subsequently, data migrates to a few central places where a very large dataset is formed. From a cybersecurity perspective, this is important because although many stakeholders do their best to guard the data, if one stakeholder, especially an organization such as a hospital, insurance company, or government agency, loses the data, many people are exposed to the risk.

The second major reason the healthcare industry is targeted by cyberattackers is the nature of health data makes them very attractive to attackers. Instead of stealing credit card information, which will become useless once the card numbers are changed or blocked,

stealing health data gives the attacker all personally identifiable information including social security number, date of birth, address, and even medical history. Having access to all of this information makes it easy to impersonate the owners of the stolen data. For this reason, health data is worth a lot more than simple financial data in the black market. A Pricewaterhouse Coopers (PwC) report released in 2014 on managing cyber risks states stolen health insurance personal information can be worth \$20 per person on the black market, compared to financial information such as credit card data, which is worth only \$1. Often health insurance records contain personal identifiable information and medical history, so there is an added risk of these records being used for insurance fraud. Growth in the black market exchange of stolen information promotes hacking activity and makes these healthcare insurance records very attractive (Ablon, Libicki and Golay 2014).

There is a rising trend of stolen health data being used for medical identity theft and insurance fraud due to high medical expenses. The 2014 Fifth Annual Study on Medical Identity Theft conducted by Ponemon Institute estimated 2.3 million people are affected by medical ID theft crimes, including 481,657 new cases. Stolen medical IDs are used to receive treatments and fill prescriptions, and each individual had to pay \$13,500 on average to resolve the incident (Ponemon Institute, LLC 2015). Medical fraud is concerning as it may delay access to proper, timely treatment by its victims.

Company	Year	Number of People Affected
Anthem, Inc. (CA)	2015	80 million
Premera Blue Cross Blue Shield, Inc.(CA)	2015	11 million
Community Health System (TN)	2014	4.5 million
Advocate Medical Group (IL)	2013	4 million
AHMC Healthcare (CA)	2013	0.7 million
Utah Department of Health (UT)	2012	0.78 million
TRICARE management facility (VA)	2011	4.9 million
Nemours Foundation (DE)	2011	1 million

Table 1: Impact of cyber breach in healthcare within last 5 years (McCan 2012)

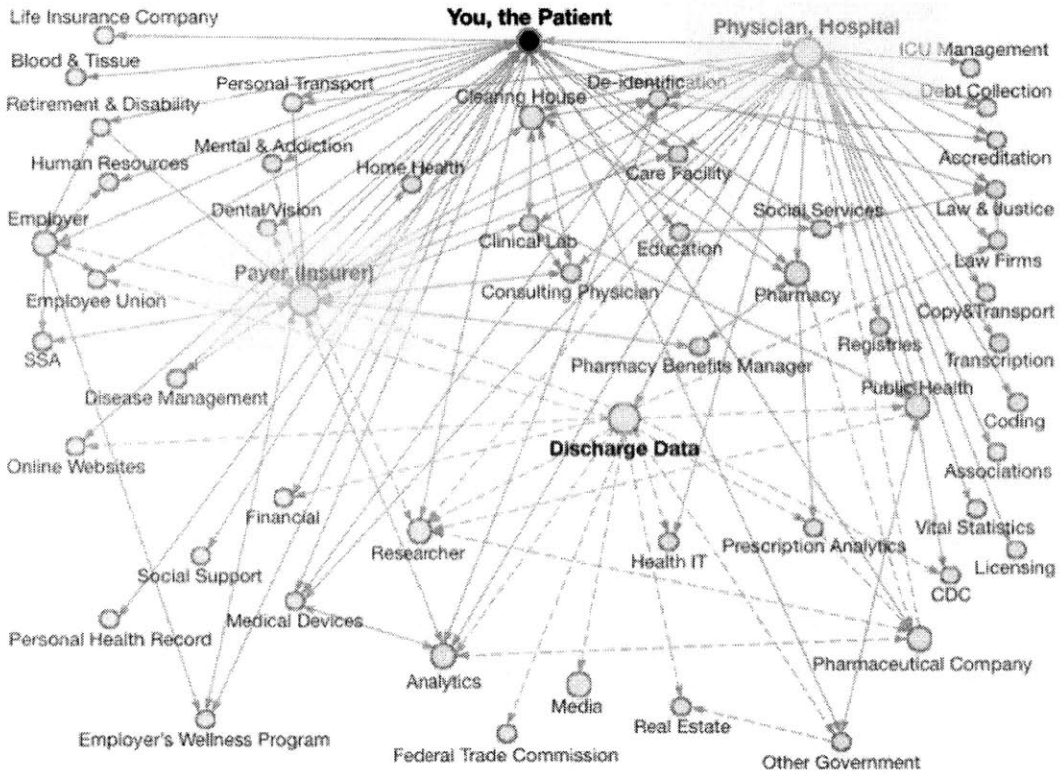



Figure 1: Personal Health Data Flow map (Datamap.org n.d)



Totals for Category: Banking/Credit/Financial	# of Breaches: 43 % of Breaches: 5.5%	# of Records: 1,198,492 %of Records: 1.4%
Totals for Category: Business	# of Breaches: 258 % of Breaches: 33.0	# of Records: 68,237,914 %of Records: 79.7%
Totals for Category: Educational	# of Breaches: 57 % of Breaches: 7.3%	# of Records: 1,247,812 %of Records: 1.5%
Totals for Category: Government/Military	# of Breaches: 92 % of Breaches: 11.7	# of Records: 6,649,319 %of Records: 7.8%
 Totals for Category: Medical/Healthcare	# of Breaches: 333 % of Breaches: 42.5	# of Records: 8,277,991 %of Records: 9.7%
Totals for All Categories:	# of Breaches: 783 % of Breaches: 100.0	# of Records: 85,611,528 %of Records: 100.0%

2014 Breaches Identified by the ITRC as of:	1/5/2015	Total Breaches: 783
		Records Exposed: 85,611,528

Figure 2: 2014 Data Breach Summary per Category (ITRC 2014)

1.2 Financial Impact of Cybercrime

Calculating the financial impact of cybercrime is not a simple task. It is not easy to estimate the loss from cybercrime for a number of reasons. First, many cybercrimes remain unreported and data are often incomplete (Mcafee Center for Strategic and International Studies 2014). Second, it is difficult to quantify the loss of information. Many people lose their personally identifiable information (PII), but any harm done due to stolen data may not be immediately apparent. Many customers whose identities are stolen will need to monitor their credit for the rest of their lives. There is no quantifiable way of measuring the inconvenience to these clients or the true value of the loss of protected information.

On the other hand, estimating the cost of mitigating data breaches is feasible to a certain degree. There could be associated administrative costs, such as public relations for damage control, customer service to answer questions from the victims, and mailing costs to send

notifications to affected customers (Stapleton 2012). A subscription to a credit monitoring and protection service is one of the most common services offered to affected customers as part of a recovery plan. One of the highest mitigation expenses are legal costs incurred as companies defend themselves from potential claims and fund possible settlements. In 2009, for example, the Department of Veterans Affairs settled a class action lawsuit for \$20 million as a result of an employee's unencrypted laptop being stolen from his personal residence. In case there are violations of any government regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), the company must pay fines. For example, New York Presbyterian Hospital had to pay \$3.3 million as a result of a HIPAA violation in a 2010 data breach.

According to a 2014 Data Breach Study published by Ponemon Institute, the total value of losses attributed to data breaches averaged \$3.5 million per incident (Ponemon 2014). Often organizations have a notion that spending on cybersecurity is costly, but considering the amount they may have to pay for the consequences of a successful attack, investing in cybersecurity often provides a great return.

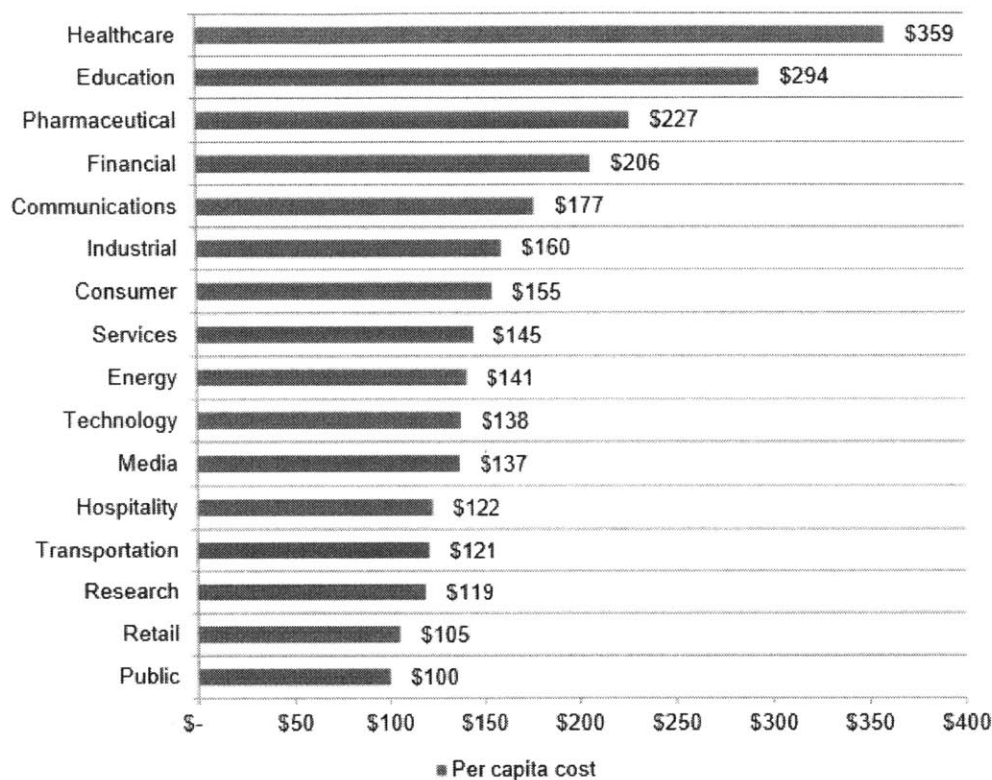


Figure 3: Per capita cost¹ of a data breach by industry (Ponemon 2014)

1.3 Traditional Cybersecurity Methods and Limitations

There has been longstanding general criticism of the lack of standards for cybersecurity methods. Although institutions desire to improve their cybersecurity posture, responsibility for it has traditionally been delegated to the IT department, and there have not been formal control guidelines or implementation standards (Martin 2014). There are few industry regulations and standards currently used by Information Security teams. Guidelines such as Control Objectives for Information and Related Technology (COBIT) 5 Framework and the National Institute of Standards and Technology (NIST) Special Publication, ISA99/IEC 62443 standard are available, but each Information security struggles with establishing effective information security strategies and risk management. Within the healthcare industry, the Health Insurance

¹ Per capita cost is defined as the total cost of data breach divided by the size of the data breach in terms of the number of lost or stolen records (Ponemon 2014)

Portability and Accountability Act (HIPAA) requires each covered entity to be in compliance with its guidelines. However, HIPAA often makes organizations focus strictly on compliance rather than security. Unless the regulation has a very high information security standard, an organization may implement only enough security to meet the requirement and nothing more. If the cost of the fine for not meeting the information security standard is less than what an organization needs to pay to increase cybersecurity, most companies will not invest in cybersecurity.

Many organizations use an old cybersecurity practice called “harden the shell,” which entails taking measures such as implementing a demilitarized zone (DMZ) and a strong firewall. This approach is often used to protect a sensitive system from any external attacks. In addition, hypertext transfer protocol secure (HTTPS) is often used for web security and is considered to offer minimal protection. Many healthcare organizations have their own security policies, yet they are not developed in coordination with all business areas since IT security is an independent, silo department. Lack of security enforcement throughout the lifecycle of an application is another concern. Security is an independent process that does not extend beyond each cycle of application deployment.

Enterprise cybersecurity strategies often focus on the live application and data. Many IT security architects struggle to create more effective cybersecurity programs, especially at the early stage of application development. This is due to the lack of a method which helps these analysts to identify vulnerabilities and how to address them. Often getting clear direction from senior management is a challenge because the value and criticality of cybersecurity is not recognized until a breach happens. It is very typical for an enterprise to implement a level of security comparable to that of other companies within the same industry. As a result,

cybersecurity has been long criticized as ineffective.

1.4 Thesis Structure

The goal of this thesis is to do a case study of the Anthem breach using the STAMP model to gain a better understanding of its underlying causes. Through this case analysis we intend to help healthcare organizations better manage their vulnerabilities and suggest how they may improve their current approaches to managing cybersecurity risks. The Anthem case was carefully chosen because it was the largest breach in the healthcare industry, affecting close to 25% of the U.S. population. Chapter 2 includes a literature review covering Chain-of-Events, Fault Tree Analysis, and the NIST cybersecurity framework. Chapter 3 provides key definitions of important terminology. In Chapter 4, an overview of the Anthem breach is provided, including details and a timeline of the incident. Chapter 5 further presents a case study using the Causal Analysis based on STAMP (CAST) method. Chapter 6 includes recommendations based on the STAMP analysis, conclusions, and opportunities for future work.

2. Literature Review

Chapter 2 is dedicated to literature reviews discussing the most commonly used traditional safety analysis models, such as Chain of Events and the new NIST framework, which was announced in February 2014. The System-Theoretic Accident Model and Process (STAMP) will also be introduced.

2.1 Chain of Events Model

The Chain of Events Model has been used for accident analysis since the 1930s. This model is based on Herbert William Heinrich's domino theory of industrial accidents and views accidents as resulting from a sequence of events rather than from a single act. A series of

events will lead to a final event, an accident, similar to a domino block falling over and causing the next block to fall (GriffinThomas, YoungMark, StantonNeville 2015). In this approach, there is typically an underlying inherent behavior or social environmental factor that may lead to a person being at fault. For instance, a person's innate tendency toward alcohol abuse or inherently violent nature may lead to undesirable behaviors such as recklessness or addictions. Later, this bad behavior will culminate in unsafe actions or the creation of unsafe conditions. An accident is one possible result of unsafe actions which causes an injury or property damage. Since each factor in this chain of events is dependent on the previous one, Heinrich believed if the chain reaction was stopped or a key factor removed from the chain, an accident could be prevented.

The major criticism of this model is that an accident is a result of a human mistake or mechanical failure and happens in a linear sequence. Often an accident occurring in a complex system involves multiple factors, and an accident can still happen even when every component and operator performs safely and correctly. It is more than the linear chain reactions and often involves dynamic processes among different parts, controls, and interactions. This model is inadequate for explaining the emergent nature of a complex system and views an accident only in terms of a linear sequence unfolding in a certain order. In addition, a human's unsafe behavior is triggered not only by the human's inherent nature, but also by an interaction between the human operator and the system. Poor architecture or design of a system also may increase human errors or unsafe actions, but this model does not consider such a possibility.

From a cybersecurity perspective, the chain of events model is inadequate for explaining most cybercrimes. Since it involves malevolent intentions and persistent acts of the attacker, the course of attacks is well orchestrated and carefully planned. Often attackers change their

tactics to penetrate into a system and modify their attacks along the way. Thus, the chain of events model will not be able to address the dynamic nature of these attacks and techniques.

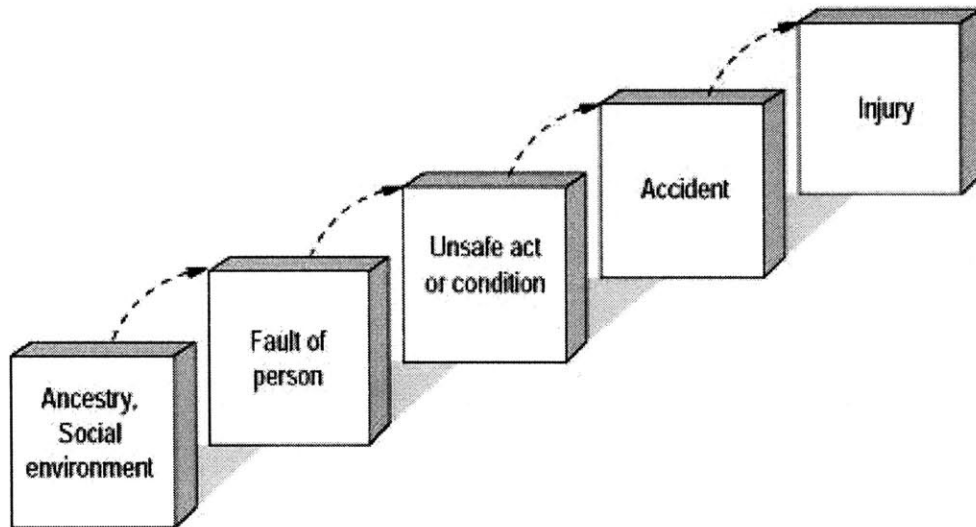


Figure 4: Heinrich’s Chain of Event (domino) model (Transport Canada 2007)

2.2 National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (CSF)

In response to the increase of alarming cybersecurity breaches in recent years, the President’s Executive Order 13636, “Improving Critical Infrastructure Cybersecurity” (CSF), was issued on February 12, 2013. The goal of this executive order was to increase the cybersecurity and resilience of critical infrastructure by developing cybersecurity standards and best practices. This is a voluntary effort designed to help organizations better manage security risks instead of enacting additional regulatory requirements. The outcome of implementing this framework would be increased protection on privacy and civil liberties. This framework is not industry or technology specific and is complementary to the existing information security

policies in organizations.

There are three parts to this framework: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is composed of five continued functions: Identify, Protect, Detect, Respond, and Recover. These functions are the basic security activities of the organizations and performing these functions would result in gaining a high level strategic overview of the organization's cybersecurity readiness. The five functions are categorized, then further sub-categorized, and then finally divided into informative references. Each subcategory is referenced to current industry standards around cybersecurity such as Critical Security Controls (CCS), Control Objective for Information and Related Technology (COBIT), and ISO Standards so the organization can refer to the standards documents for more guidance.

Framework profiles set the context of the cybersecurity risk level of each organization. NIST recommends that each organization progress to a targeted level and further, as doing so will help reduce the overall cybersecurity risk and related costs. It should be understood that the framework level is different from the maturity level, and it is determined by the outcome and not by the targeted tier level. Through a risk management review process, organizations will determine their current tier, from Tier 1 to Tier 4, and the desired tier among the four tiers defined in the Framework: Partial, Risk Informed, Repeatable, and Adaptive. Achieving a higher tier assessment indicates more sophisticated and increased cybersecurity activities within the organization (Table 2).

	Risk Management Process	Integrated Risk Management Program	External Participation
Tier 1 : Partial	No formal process	Limited organizational level awareness	No coordinated process
Tier 2: Risk Informed	No organizational wide policy	Awareness and informally shared cybersecurity info	Understands the role in the ecosystem but no formal capability
Tier 3: Repeatable	Formally approved policy, Regular update	Organization wide approach	Collaboration and risk based management
Tier 4: Adaptive	Continuous improvement	Part of Organization culture	Actively share information with partners

Table 2: NIST Framework Tier Matrix (NIST 2014)

Application of NIST CSF is done using the core framework and the tier system. For each framework category, the tier system is used to score the enterprise’s readiness and current process. Once all categories are scored, the organization will identify the areas in need of improvement. It is clearly stated that NIST’s framework will not replace the current cybersecurity policy within an organization, nor is it a regulation, rather it helps to identify what is missing. Implementation of the cybersecurity framework involves all levels of an organization: Executive, Business/Process, and Implementation/Operation. Each level communicates and collaborates with the higher level to maintain awareness of the efforts of each level and the associated impact.

Since NIST CSF has not been finalized and is still under development, there are few known applications. Intel Corporation has published their use case as shown below (Figure 5). Although Intel found the Framework to be valuable in helping to identify Intel’s strengths and opportunities for improvement, it leaves some concerns unaddressed. First, since it is

structured as a list to assess each area, it does not reflect the organizational structure and business workflow within the organization. Often vulnerabilities underlie the process of work and interactions between users, components, and systems. Since the components within the system change all the time and the NIST framework looks at one area and component at a time, the organization using the framework will miss finding vulnerabilities that may arise from the interactions between components, between a controller and a component, or between controllers.

Second, the NIST framework is based on self-assessment, and an internal review may not be objective, thus failing to see the vulnerabilities. The biggest challenge Information Security faces is the process of finding these vulnerabilities. From the inside, these vulnerabilities are not easy to identify and often arise from the changing nature of the Information Technology area. Constant upgrading and patching of software, implementing and retiring of applications, and changing personnel and vendors make it extremely difficult to assess weaknesses and vulnerabilities.

On the other hand, the scoring system itself may give the organization misconceptions. In the areas where it scored high, the organization may have the false assumption it is safe and well prepared against attacks. It is possible that the company may be physically well protected, but if the penetration comes from access that could override physical security or penetrate into the data network, then strong physical security will become meaningless.

Lastly, NIST CSF does not provide multiple scenarios or mitigation plans. Although industry standards and guidelines can be referenced, it does not guide the organization on how to handle incidents in case a breach occurs. NIST CSF merely references many external organizations' documentation, such as guidelines issued by ISO/IEC and ISA. Companies need guidance and examples of well-defined information security management systems rather than

document references that are abstract and not very practical. NIST CSF may be a good document library referencing existing useful cybersecurity guidelines, but it does not provide added value beyond that.

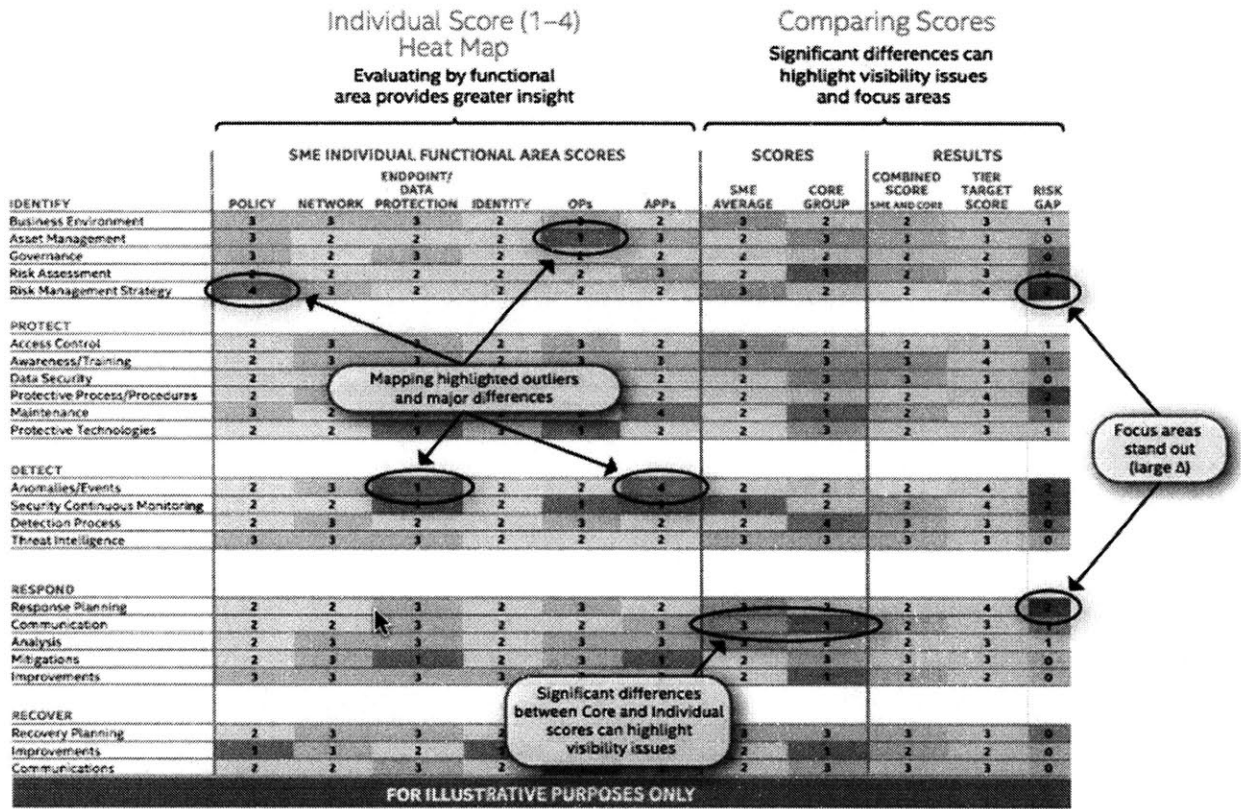


Figure 5: Intel Use Case of applying NIST CSF (CaseyTim, etc. 2015)

2.3 HIPAA, HITECH and Meaningful Use

The Health Insurance Portability and Accountability Act (HIPAA) is the mandatory standard across the healthcare industry passed by Congress in 1996. The Act was established to provide health insurance coverage portability and to protect privacy and security around sensitive health data (US Department of Health & Human Services 1996). HIPAA regulations apply to covered entities and business associates, and these covered entities are required to comply with HIPAA rules. A covered entity will fall into one of the categories defined in Table 3:

A Healthcare Provider	A Health Plan	A Healthcare Clearing House
<p>Includes:</p> <p>Doctors</p> <p>Clinics</p> <p>Psychologists</p> <p>Dentists</p> <p>Chiropractors</p> <p>Nursing Homes</p> <p>Pharmacies</p> <p>Only if the entity is involved in transmitting electronic form of health information</p>	<p>Includes:</p> <p>Health Insurance Companies</p> <p>HMOs</p> <p>Company Health Plans</p> <p>Government Programs (i.e. Medicare, Medicaid, Military, Veterans Health Program)</p>	<p>Includes:</p> <p>Entities process non-standard health information they receive from another entity into an account.</p>

Table 3: Covered Entities under HIPAA (U.S. Department of Health & Human Services 1996)

Although HIPAA is not a security policy, it provides guidelines on how to prepare against cyber risks by providing standards in three categories: Administrative Safeguards, Physical Safeguards, and Technical Safeguards. Under each category, implementation specifications are listed, including some mandatory specifications and some recommended. Administrative safeguards are the administrative functions recommended to be in place to increase safety, such as setting up risk management policy, disposal procedure, and log in activity monitoring. Physical safeguards are the measures placed in the physical structure to protect the system against cyberattacks, including facility access control and disposal of sensitive records. Technical safeguards refer to an automated security procedure implemented to protect data. Examples are data encryption, authentication process, automatic log off, integrity control, etc. In addition to these safeguards, HIPAA lists Organizational requirements. This standard requires covered entities to have contracts with business associates having access to electronic Protected Health Information (PHI). The last guideline, Policies, Procedures, and

Documentation Requirements, mandates covered entities to implement policies and procedures within their organizations and document such practice.

In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act was established under the American Recovery and Reinvestment Act of 2009 and went into effect. The goal of the HITECH Act was to enforce the HIPAA standards. The core of the HITECH Act is to adopt Healthcare Information Technology using an electronic health records (EHR) exchange with the goal of improving healthcare quality, efficiency, and safety (Office of National Health Coordinator for Health Information Technology 2009). Meaningful Use is an incentive program offered by the Center for Medicare and Medicaid Services and used to motivate organizations to adopt EHR technology. Each healthcare organization adopting and certifying EHR usage receives financial incentives. However, the program has been criticized for being not attractive enough to encourage organizations to implement security beyond what is required under HIPAA.

2.4 System-Theoretic Accident Model and Processes (STAMP)

System-Theoretic Accident Model and Process is a new accident analysis model based on systems theory and developed by Professor Nancy Leveson at MIT. A key concept of STAMP is that an accident is the result of inadequate controls, rather than a component failure or unreliable part(s). Different from the traditional accident analysis method, STAMP focuses on constraints rather than the event. It has a significant difference from reliability theory as it examines hierarchical safety control structures and process models to understand the constraints and hazards. An accident can still happen when every component in the system is reliable and worked as it was supposed to. A reliability theory fails to explain such an accident. There are more than unreliable components that could create hazards, such as unsafe interactions between

components, complex human behavior, incomplete requirements, and design errors. The STAMP model is designed to discover the causes of accidents beyond unreliable components and help users to understand the complex behaviors of the system by examining the control structure and hierarchy.

There are two processes based on the STAMP model – Causal Analysis based on STAMP (CAST) and System-Theoretic Process Analysis (STPA). CAST is used to review past accidents and find answers to the question of what has happened, thus helping the organization understand the accident by providing a more comprehensive view. STPA presents possible scenarios that may create hazardous states or directly leads to losses. By identifying these scenarios, the potential hazards can be eliminated, monitored, or controlled before the loss occurs (Leveson 2011).

2.5 Causal Analysis based on STAMP (CAST)

CAST is an ex-post analysis of an accident or incident and is completed by approaching the accident scenario from the top-down with a systematic view. Unlike traditional accident analysis methods, CAST does not attempt to find a single “root cause,” but rather helps the accident analyst understand systemic causal factors by examining the entire system design and hierarchical structure. It helps to identify the vulnerabilities of the system that could create unsafe states and control the actions and feedback involved. The objective of CAST analysis is not to blame a human or point out human mistakes, but rather to identify the system factors that lead to human mistakes. Instead of viewing a human mistake as a root cause, it must be understood as a symptom of inadequate system design or missing requirements. The nine steps involved in performing a CAST analysis are listed in the Table 4, below.

In CAST analysis, understanding the role of each component within the control structure is important. This includes: safety requirements and constraints; control of the system by the operator; the context arising from roles, responsibilities, and environmental factors; control actions caused by dysfunctional interactions; and failures or inadequate decisions. There could be multiple reasons why such interactions or failures occur, such as incorrect process or interface, inaccurate algorithm, or flawed feedback. CAST analysis will be performed and discussed further in Chapter 5.

1. Identify the system(s) and hazard(s) linked 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 and identify how the following contributed to the accidents: 1) physical and operational controls 2) physical failures 3) Dysfunctional interactions or communications 4) 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. These include 1) responsibility not assigned or components assigned for safety constraint was not performing its responsibility 2) any human decision or flawed control due to unavailable information required for safety control, underlying value structure or flawed process models.
7. Examine 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 4: CAST analysis steps (Leveson 2011)

2.6 System Theoretic Process Analysis (STPA)

As mentioned earlier, STPA is an ex-ante analysis of an accident or incident based on Systems Theory. It looks for causal scenarios by examining each safe control action and feedback loop, whereas typical analysis often finds the root cause from a component failure or a human error. The typical analysis fails to improve the safety measures of the system and often adds redundant safety features or patchwork fixes. On the other hand, STPA identifies missing constraints, insufficient feedback, inadequate safety controls, and vulnerable areas within the system so improvements can be made. STPA consists of two main steps:

- 1) Identifying potential inadequate controls of the system that may lead to one or more hazardous conditions caused by inadequate controls or safety constraints enforcement.
- 2) Determining how an unsafe control action may occur by providing possible failure scenarios.

For the first step, Leveson identified four conditions that may create a hazardous situation. First, a required control action is missing or not allowed. Second, providing a control action creates an unsafe state. Third, a safe control action is provided with incorrect timing (too early, too late, or in the wrong sequence). Last, a required safety control action is applied for too long or too short a duration (Leveson 2011).

When examining these steps, each action in the control loop must be reviewed. Mitigation and monitoring actions are as important as the control loop, especially in cybersecurity. Any changes in control action design over time should be considered, including change procedure management, performance audits, and accident analysis. Figure 6 shows a simple control structure that involves a controller, an actuator(s), a controlled process, and a sensor. In each process, an unsafe action could occur during any step. By examining how an

unsafe control action may occur in each step, the engineers will be able to design or improve safe control steps or create a mitigation process. Figure 7 illustrates causal factors to be considered in creating scenarios for analysis.

STPA analysis is an excellent method for identifying hazardous situations before an accident occurs. NIST cybersecurity frameworks, HIPAA, and ISO may provide comprehensive lists of areas within IT for assessments, but they do not reveal where the vulnerabilities lie. Identifying areas of vulnerability is the most critical step in cybersecurity because attackers will attempt to penetrate the system at its most vulnerable spots. External auditing often fails to identify vulnerabilities that come from operational or managerial levels because most security audits focus on technology selection and information technology work flow. An organization's IT Security department may have a risk assessment checklist, but often the requirements outlined on those checklists do not identify specific areas for focus, monitoring, and protection.

STPA analysis could help organizations assess the control actions required for securing protected data and identifying possible hazards stemming from missing security measures. STPA will also shed light on previously unforeseen potential problems arising from coordination or communication issues. This will help organizations create good, well-defined mitigation plans and could be used as an analysis technique to discover vulnerabilities. STPA analysis is a powerful tool that excels at comprehensively understanding a system's control structure not only from a technological perspective, but also with consideration to the organizational work flow.

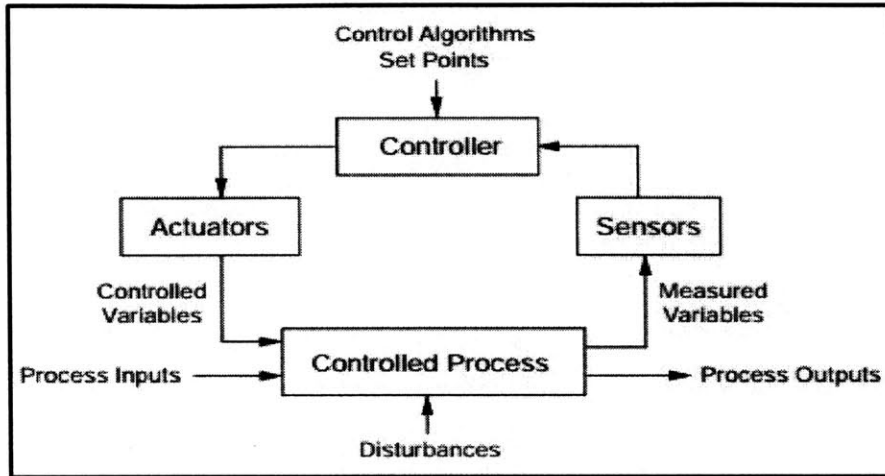


Figure 6: STPA Control Structure (Leveson 2011)

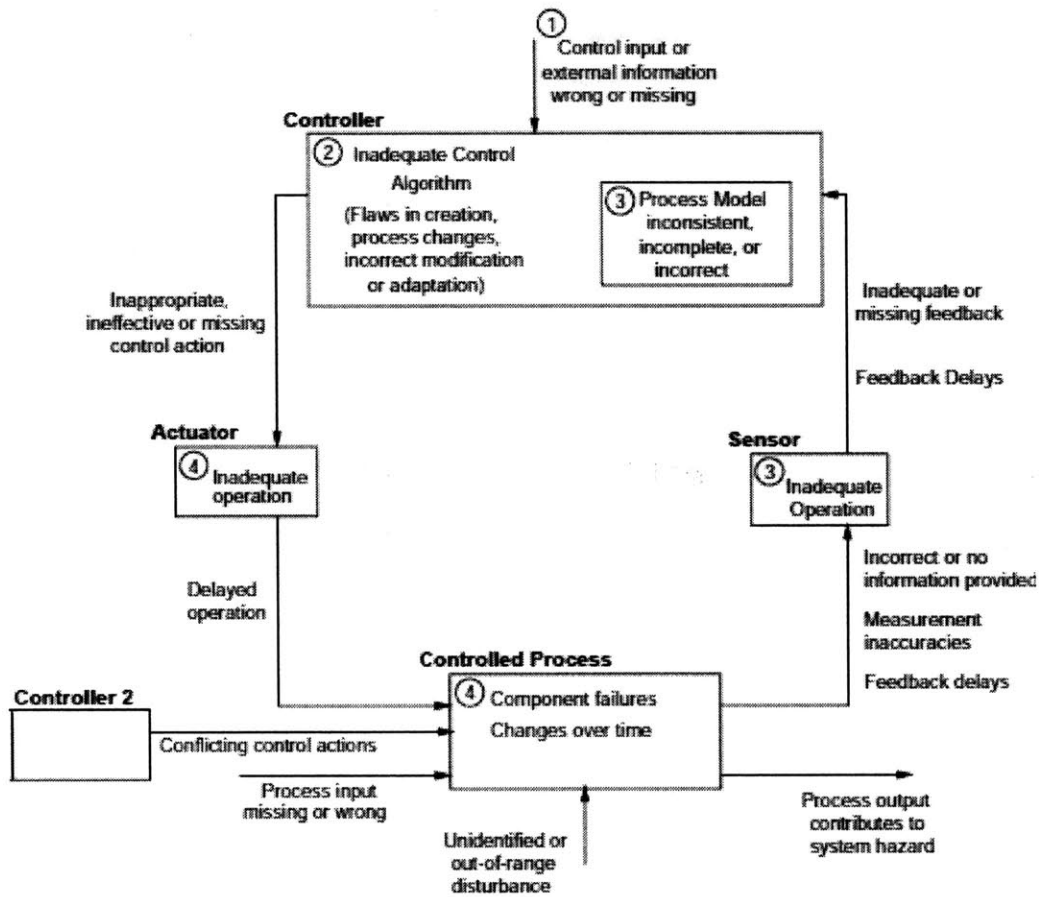


Figure 7: Causal Factors in STPA (Leveson 2011)

3 Definitions

This chapter is dedicated to providing key definitions in accident analysis using the STAMP-CAST method. HIPAA and NIST Framework will also be reviewed for relevant terms. Definition of key terms is needed to increase understanding and minimize confusion since different organizations use the same terms differently.

First, the term **“breach”** must be defined. In “Incident Response Procedures for Data Breaches Guidelines,” the U.S Department of Justice defines “breach” as “loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to a situation where persons other than authorized users and for an other than authorized purpose have access or potential access to information, whether physical or electronic.” (U.S. Department of Justice 2013) A breach is a type of accident caused by malevolent acts. Leveson defines an accident as “an undesired and unplanned event that results in a loss.” (Leveson 2011) How that loss is defined is important in healthcare since in HIPAA, a patient’s privacy is violated by unauthorized access or acquisition of the patient’s personal and confidential health records. Therefore, we must first define what needs to be protected against harm.

In HIPAA, a breach is more narrowly defined in the context of health data transactions within the covered entities as “an impermissible use or disclosure under the Privacy Rule that compromises the security or the privacy of the protected health information.” (Department of Health and Human Services 2009) It should be noted that HIPAA lists three exceptions in its definition of a breach: first, unintentional acquisition, access or use of protected health information by an authorized member; second, inadvertent disclosure of protected health information (PHI); and, finally, a failed attempt at unauthorized access, where the

information is not retained by the unauthorized party. In this thesis, only unauthorized access with malevolent intent will be discussed, since the goal is to apply systems thinking to addressing the cybersecurity problem.

Since the goal of STPA analysis is to identify hazards and vulnerabilities that may lead to a failure situation, clear definitions of the terms “hazard” and “vulnerability” are needed. Leveson defines a hazard as “a system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).” HIPAA does not define hazard in its security requirements, but it does adopt a definition of vulnerability from NIST Special Publication 800-53 Rev.4, “Security and Privacy Control for Federal Information Systems and Organization” as follows: “a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.”

In this thesis, the more specific definition of breach suggested by HIPAA will be used. Unless noted otherwise, definitions of accident, hazard, and vulnerability will be adopted from STAMP analysis.

4 Anthem Breach Overview

On February 4, 2015, major U.S. health insurer Anthem Inc., reported its IT system had been compromised by an unidentified attacker(s), and approximately 80 million people, including both current and former customers, some affiliated plan members, and employees had been affected. According to the letter from Anthem CEO Joseph R. Swedish (Appendix 1), personal information, including social security numbers, date of birth, street address, email address, employment information, and income data, were stolen, but medical and credit card

information were not compromised. Anthem immediately hired Mandiant, a company with expertise in cybercrime investigation, and offered two years of free credit monitoring services to victims affected by the security breach (Mathews and Yadron 2015). It was announced that the FBI is conducting its own investigation of the breach and closely monitoring the black market for a possible sale of the stolen information.

4.1 Company Overview

Anthem Inc. is an Indianapolis, IN based insurance company providing healthcare plans to 69 million members. The predecessor company, Blue Cross California, formed WellPoint Health Networks in 1992 as a for-profit corporate entity. In 1996, WellPoint Health Networks acquired Massachusetts Mutual Life Insurance and expanded its services to all 50 states. Blue Cross California merged and continued its expansion (Anthem, Inc. 2015). Anthem, Inc. and WellPoint HealthNetworks merged into WellPoint, Inc. and became the largest health insurance company (KazelRobert 2004). According to a 2004 SEC report, the implication behind this merger is a significant opportunity for corporate cost reduction, creating \$250 million in annual pre-tax synergies (cost reductions).

At the time, Anthem's strength was its experience with national accounts, and WellPoint's expertise was in individual and small group plans (SEC 2004). Between 2004 and 2009, WellPoint, Inc. continued its expansion through the acquisition of dental plan, data analytics, and benefits management companies. In 2014, WellPoint changed its corporate name back to Anthem, Inc. The motive behind this name change was to "create better alignment between its corporate and product brands and better reflect its purpose and strategy to help transform healthcare," according to the Blue Cross Blue Shield (BCBS) announcement (Blue Cross Blue Shield 2014). Currently, Anthem is a part of the Blue Cross Blue Shield

National Network, running BCBS health plans across 14 different states (Aaron and Rod 2014)² (ReardonStephanie 2015). According to the financial report released in the fourth quarter of 2014, the company’s 2014 net income was \$2.6 billion.

Year	Milestones
1992	Blue Cross California creates for-profit WellPoint Health Networks, inc.
1996	WellPoint Health Networks and Blue Cross California merge
2004	Anthem, Inc. and WellPoint Health Networks merge to become WellPoint, Inc.
2014	WellPoint changed its name to Anthem, Inc.

Table 5: Anthem, Inc. history (Anthem n.d)

4.2 Mission, Vision, and Values

According to Anthem’s corporate website, its mission is “to improve the health of the people we serve.” Anthem’s goal is not only to provide basic health coverage, but also to promote members’ health by accomplishing the following:

- Offering large networks of some of the region’s best physicians, specialists, and hospitals
- Reminding members to have important preventative screenings
- Providing programs and information to help manage chronic health conditions
- Offering related services, including dental coverage, life insurance, and pharmacy benefits management

From its business strategy and growth, we could see that Anthem’s focus was on expansion, which correlates to the first bullet point of ‘offering large networks.’ Anthem has expanded in Ohio and purchased a group life and disability company. In 1999, Anthem expanded into the

² California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia and Wisconsin

West by acquiring Rocky Mountain Life Company. Now it is doing business as a life and health insurance company in 47 states, packaged with its life, dental, vision, and prescription services. Anthem's business strategy has been very aggressive and focused on expansion, which is in alignment with its organizational goal of offering large networks.

4.3 Anthem Breach Details

4.3.1 Facts

The Anthem breach was first discovered on January 27, 2015 by an Anthem Database Administrator (DBA) who found a data query running using his/her credentials, but not initiated by the DBA. Upon the discovery, the DBA stopped the query immediately and notified Anthem's Information Security department. Anthem's internal investigation revealed the query started running on December 10, 2014 and ran sporadically until discovered on January 27th. Anthem reissued the IDs and passwords of their employees and notified federal law enforcement and HITRUST Cyber Threat Intelligence and Incident Coordination Center (C3). They also hired Mandiant, a leading cybercrime response firm, to conduct further investigation. Anthem CEO Joseph Swedish announced the breach to public on February 4th, 2015, stating their database containing 80 million records had been compromised by the sophisticated cyberattack. As of late February, there was no indication of exfiltrated data or data that had been commoditized (Barger 2015).

4.3.2 Advanced Persistent Threat

Based on initial discovery and investigation, the Anthem breach was a form of Advanced Persistent Threat (APT). The term APT was first used by United States Air Force back in 2006 in reference to attacks that are advanced and persistent. Advanced means the techniques used for the attacks are highly sophisticated and capable of penetrating existing

defense techniques, and persistent means the attackers have one specific target and engage in repeated attempts to accomplish the goal using various tactics until a successful penetration is achieved (Binde, McRee and O'Connor 2011). Advanced Persistent Threat is difficult to handle because the attacks are very sophisticated and highly advanced with no pre-defined pattern (Sood), thus an attack may go undetected for a long time. The attack often involves the use of malware to attack system vulnerabilities.

APT goes through this chain process in seven stages: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Action on Objectives (Hutchins, Cloppert and Amin 2012). Reconnaissance is the stage where the attackers gather information before launching attacks. Attackers would identify the organizations to attack and find individuals they want to go after (De Decker and Zuquete 2014). They often use techniques such as Social Engineering or Open Source Intelligence Techniques (OSINT). SANS Institute defines Social Engineering as “the art of utilizing human behavior to breach security without the participant even realizing they have been manipulated” (Watson, Mason and Ackroyd, Social Engineering Penetration Testing 2014). One of the social engineering techniques often used is collecting information from social media sites such as LinkedIn, Monster and Facebook.

Weaponization is the stage during which attackers prepare their tactics. Based on the information they have gathered from the Reconnaissance steps, they would identify what type of attacks will be most effective and their contingency plans if initial attempts fail.

Delivery step is the process attackers use to deliver their exploits to their intended target. This step may take a long time as they prepare for the exploitation. Recently, cyber criminals started using exploitation techniques called ‘spear phishing’ or ‘whaling’, which target a

specific individual, often a high-level corporate management person or a person with access to sensitive information, including financial and personal data (HowardRick 2009). Spear phishing is a lot more sophisticated than generic spam emails. The attack can be very well-crafted because it is designed to attack a specific individual. The sender may disguise himself/herself as someone the individual may know, such as the human resources department of the company, coworkers, the target's manager, or someone in the upper hierarchy of the company. According to a report released by Centre for the Protection of National Infrastructure (2013), spear phishing emails are remarkably effective since they are designed to trick specific users, and most targeted attacks toward a specific organization almost always start with a phishing email. Spear phishing emails contain either a file with malware codes, or a link to a scam website mirrored to a legitimate website. Links contained in the email are often shortened to look like a legitimate website.

Exploitation refers to unauthorized access by attackers. Usually, the attackers execute malicious codes using the credentials or authorized access they have obtained from the previous step. Common routes they use for executing these codes include PDF, Word, or Excel files, which are commonly used in businesses. Once exploitation occurs through a back door, the attackers will try to command and control the computer or application they used to acquire the unauthorized access. The key to this step is the attackers' ability to remain undetected while they are accessing valuable assets. Attackers often use remote access tools such as a Virtual Personal Network (VPN) or Anonymity network. Once connection is established, they will initiate data exfiltration, the process of transferring valuable data from the corporate network to a remote location under the attacker's control.

Traditional cybersecurity methods have not been very effective because attackers are

determined to obtain the goal and use various highly sophisticated attacks to do so. A traditional security method which focuses on a certain virus, layer, or physical system is inadequate to protect the system against these types of attacks and may not be capable of securing the system. Many organizations spend significant amounts of time and effort to ensure member training and network protection to isolate the breach in a limited area, but what's missing is the feedback loop to the privileged account user and security personnel. ISACA³'s study on Advanced Persistent Threat (APT) Awareness shows 65% of IT security professionals do not think APT is much different than the traditional threats, which may lead to a false assumption that they are ready for APT attacks and taking no additional measures to prevent APT attacks. The significance of this study's result is not about creating general awareness of the APT threat, but rather it highlights the need for awareness of the trend towards cybersecurity attacks on the target company's key IT security personnel.

4.3.3 Scheme

Since the Anthem breach happened fairly recently and the investigation is still ongoing, only limited information about the breach is publicly available at this time. More information and details will become available over time, and the full scope of this attack will be discovered. This section is written based on public information currently available from the media and cybercrime experts.

Although Anthem confirmed hard evidence that the attack began on December 10, 2014, it is widely suspected that the attack scheme started long before then. Dave Damato, the Managing Director at Mandiant, the leading investigation firm, confirmed that attackers accessed the Anthem system via "backdoors," not public routes (WalkerDanielle 2015).

³ An independent, nonprofit organization provides guidance to Enterprise Information Security on system governance and information security. Previously known as Information System Audit and Control Association but now goes by its acronym only (ISACA n.d.)

InformationWeek reported Anthem has shared with HITRUST keymarkers used in the cyberattacks, including the MD5 malware hash tag, the IP address, and the email address used by the hackers. Message Digest algorithm is a standard cryptographic technology used to protect data by taking an arbitrary length message and producing 128-bit hash values (FurhtBorko 2008).

According to the Wall Street Journal, security experts suspect that a state sponsored Chinese attacker group called “Deep Panda” was behind the Anthem breach. Security firm Crowdstrike, who named the group Deep Panda, has published a snapshot of the ScanBox framework that might have been used to attack Anthem, as shown in Figure 8. ScanBox is a framework in javascript format, which collects information from a web site’s visitors, but does not infect the system. The information collected includes the site from which the visitor originated, including operating system and language setting, the details of the screen image, and the credential information the visitor used (Infosec Institute 2015). It was discovered that Deep Panda’s ScanBox was packaged with the Trojan horse program Derubsi, which can steal user credentials, and connected with the IP address 198[.]200[.]45[.]112 at the end. The passive DNS record indicated this specific IP address was a home of the domain name Wellpoint[.]com, in which the 3rd and the 4th characters are replaced with the numeric character 1, instead of the letter “L.” This is to disguise the domain name as the legitimate site Wellpoint.com, which is the official site of Anthem. This domain could have deceived a person accessing this domain into thinking it is the legitimate Anthem website.

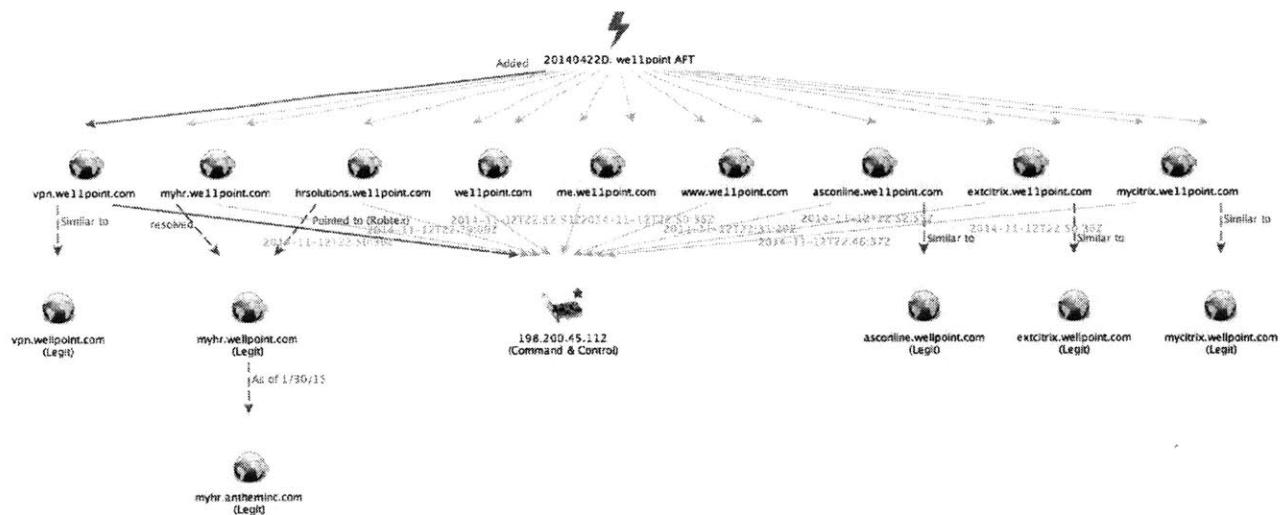


Figure 8: We11point APT diagram (Threatconnect 2015)

The security firm Threatconnect has discovered by looking into passive DNS records that the domain was registered as early as April 21, 2014. The domain used an IP address associated with the hacking group Deep Panda until it was changed to 198[.]199[.]105[.]129. During this investigation, it was also discovered the subdomains extcitrix[.]we11point[.]com, myhr[.]we11point[.]com, and hrsolutions[dot]we11point[dot]com were created in May 2014. Extcitrix is the subdomain that Athem employees use to connect via Virtual Private Network (VPN). Also the myhr subdomain indicates that the motive behind this deception was to make this site look as similar to the legitimate HR internal site as possible.

```

Domain Name: WE11POINT.COM
Registrar: GODADDY.COM, LLC
Sponsoring Registrar IANA ID: 146
Whois Server: whois.godaddy.com
Referral URL: http://registrar.godaddy.com
Name Server: NS0.HAIYAO.INFO
Name Server: NS1.HAIYAO.INFO
Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Updated Date: 22-jan-2015
Creation Date: 21-apr-2014
Expiration Date: 21-apr-2015

>>> Last update of whois database: Tue, 21 Apr 2015 23:30:38 GMT <<<

```

Figure 9: Domain name registration history for We11point[.]com (viewDNS.info search result)

IP history results for wellpoint.com.

IP Address	Location	IP Address Owner	Last seen on this IP
198.199.105.129	San Francisco - United States	Digital Ocean, Inc.	2015-01-26
198.200.45.112	Walnut Creek - United States	PEG TECH INC	2014-11-17

Figure 10: We11point[.]com IP history in 2014-2015 (viewDNS.info search result)

1 Domain Name: TOPSEC2014.COM	1 Domain Name: TOPSEC2014.COM
2 Registry Domain ID: 1857525015_DOMAIN_COM-VRSN	2 Registry Domain ID: 1857525015_DOMAIN_COM-VRSN
3 Registrar WHOIS Server: whois.godaddy.com	3 Registrar WHOIS Server: whois.godaddy.com
4 Registrar URL: http://www.godaddy.com	4 Registrar URL: http://www.godaddy.com
5 Update Date:	5 Update Date: 2014-05-06 04:52:21
6 Creation Date: 2014-05-06 04:48:49	6 Creation Date: 2014-05-06 04:48:49
7 Registrar Registration Expiration Date: 2015-05-06 04:48:49	7 Registrar Registration Expiration Date: 2015-05-06 04:48:49
8 Registrar: GoDaddy.com, LLC	8 Registrar: GoDaddy.com, LLC
9 Registrar IANA ID: 146	9 Registrar IANA ID: 146
10 Registrar Abuse Contact Email: abuse@godaddy.com	10 Registrar Abuse Contact Email: abuse@godaddy.com
11 Registrar Abuse Contact Phone: +1.480-624-2505	11 Registrar Abuse Contact Phone: +1.480-624-2505
12 Domain Status: ok	12 Domain Status: clientTransferProhibited
	13 Domain Status: clientUpdateProhibited
	14 Domain Status: clientRenewProhibited
	15 Domain Status: clientDeleteProhibited
13 Registry Registrant ID:	16 Registry Registrant ID:
14 Registrant Name: li ning	17 Registrant Name: Top Sec
15 Registrant Organization:	18 Registrant Organization: TopSec
16 Registrant Street: guangdongsheng	19 Registrant Street: china
17 Registrant City: guangzhoushi	20 Registrant City: china
18 Registrant State/Province: Alabama	21 Registrant State/Province: china
19 Registrant Postal Code: 54152	22 Registrant Postal Code: 100008
20 Registrant Country: United States	23 Registrant Country: China
21 Registrant Phone: +1.4805428751	24 Registrant Phone: +1.82776666
22 Registrant Phone Ext:	25 Registrant Phone Ext:
23 Registrant Fax:	26 Registrant Fax:
24 Registrant Fax Ext:	27 Registrant Fax Ext:
25 Registrant Email: li2384626402@yahoo.com	28 Registrant Email: TopSec.2014@163.com

Figure 11: We11point[.]com Registrar update history (BargerRich 2015)

Anthem reported these incidents to HITRUST and shared indicators, including the IP and email addresses used for the attack. There was also a statement that a MD5 malware hash was used, which gives us a clue that the attackers generated cryptographic tokens or credentials, which appeared to be authentic and were able to penetrate into the Anthem system. It was confirmed that the breach started with phishing e-mails sent to employees, most likely targeting those with administrative privileges (Schwartz 2015).

Phishing is a tool used frequently in Advanced Persistent Threat attacks. Attackers first gather information about their targets using methods like a social engineering. When the phrase ‘Database System Administrator at Anthem LinkedIn’ is entered into a search engine, it

returns with at least 8 DBA profiles with full names, tools they use, and work locations. For example, if you search Anthem DBA with the word “linkedin” in a search engine, anyone can display the 22 professionals’ profiles, including each professional’s full name, location, and job description as shown in Figure 12. Then if you search each person’s name and the keyword ‘email’, the search engine often provides results with contact information, including company email address or a phone number. Once the full name of the personnel is obtained, associated information, such as personal or company email address, can be tracked down using search engines. Some companies uniformly use a common email address format, such as first initial_lastname@company name, which makes it very easy to guess the email address of any specific person once you know the person’s full name.

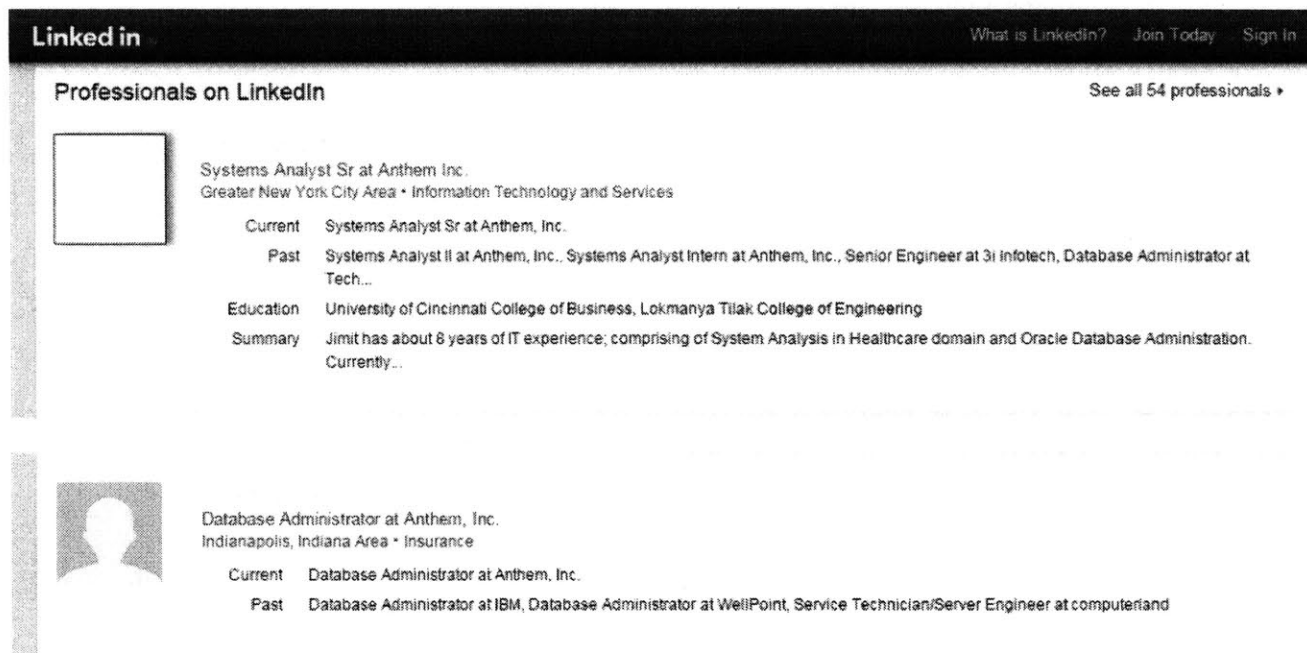


Figure 12: Social Engineering Search Example (LinkedIn search result)

The investigation by the Threatconnect group indicates China may have either been behind this attack or had a possible linkage. It was confirmed that “Sakula” malware (a variation of Derusbi backdoor malware designed to steal information from the Windows platform by

communicating with a malicious server) was created in connection with the spoof sites extrix[.]we11point[.]com and www[.]we11point[.]com in November 2014 (Figure 8). Derusbi backdoor malware was first spotted in September 2014, with a digital signature by a Korean company DTOPTOOLZ Co. It was confirmed later that the Chinese Deep Panda APT group is associated with this particular malware (Threatconnect, Inc. 2015). It is assumed that the attackers sent phishing emails to a handful of people at Anthem with a link that appeared to be Anthem's HR department. When the link was clicked, it may have looked like a legitimate site, but indeed been a spoof site. Using the scanbox tool to capture the user's credential information, the attackers would have gotten hold of the System Administrator's or Database Administrator's credentials used to log onto the spoof site. It is very possible that the Excitrix spoof site was also used to gain access to the VPN. Once they had obtained the credential, it was only the matter of time before they penetrated into the system and explored the structure of Anthem's database to determine where the targeted information resided. Although the attackers were using the credentials of users with privileged access, they may not have been noticed unless the user log was actively monitored and the query was running during non-working hours. Anthem has denied the data in question was successfully exfiltrated out of the system.

5. STAMP-CAST Analysis of Anthem Breach

In this chapter, CAST analysis will be used for the Anthem breach investigation. As discussed in an earlier chapter, the goal of applying CAST analysis is to examine the dynamics of the accident by understanding the hierarchy of the control structure and the sociotechnical aspects of the system. To apply the CAST model, the following general process will be applied to the Anthem Breach:

Steps	General Process of Applying CAST for Accident Analysis
1	Identify the system(s) and hazard(s) involved in the loss.
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 enforce the safety constraints.
4	Determine the proximate events leading to the loss.
5	Analyze the loss at the physical system level.
6	Moving up the levels of the safety control structure, determine how and why each successive higher level allowed or contributed to the inadequate control at the current level.
7	Examine overall coordination and communication contributors to the loss.
8	Determine the dynamics and changes in the system and the safety control structure relating to the loss and any weakening of the safety control structure over time.
9	Generate recommendations.

Table 6: CAST steps for analyzing accidents (Leveson 2011)

5.1 Step 1: Defining System Accidents and Hazard

5.1.1 System Description

There are many physical and virtual systems to support business workflow within Anthem, Inc., but the system analyzed here is defined as an information system that collects, processes, stores, and reports customers' health insurance claims to support Anthem's mission. The information system includes, but is not limited to, any information system components that exist internal and external to Anthem's site.

5.1.2 System Accident and Hazards

The accident and hazard affecting the Health Insurance Information System can be

characterized as one or more of the following types:

- Accident:**
- A1. Loss of protected information
 - A2. Unauthorized disclosure of protected information
 - A3. Loss of data integrity
 - A4. Disruption in business workflow
 - A5. Financial Loss
- Hazards:**
- H1. Unauthorized access to IT system or data storage containing patient information
 - H2. Malfunction of security function
 - H3. Inadequate, lack of cybersecurity measures

Since the goal of this thesis is to analyze the effectiveness of cybersecurity at protecting data against malevolent acts, the focus will be on the first three definitions of the accident: loss of protected information, unauthorized disclosure of such information, and loss of data integrity. Unauthorized access and disclosure may imply an authorized person's access to areas of the system where the person is not allowed, due to incorrect access set up or system vulnerability. The difference between loss of protected information and unauthorized disclosure is that if protected data became owned by the unauthorized person or not. For instance, exfiltration of the information will be categorized as loss of protected information, but if the information was viewed and disclosed by an unauthorized person, although the information was still within the system, the patient's privacy was still violated. Loss of data integrity can be explained as the data being corrupted, unusable, or rendered inaccurate by malicious acts.

5.2 Step 2: System Safety Constraints and System Requirements

- R1. Anthem must protect customers' personally identifiable information from unauthorized access and disclosure.
- R2. Anthem must have adequate cybersecurity in place to prevent, monitor, and detect any cybersecurity accident or incident.
- R3. Anthem must have proper security policies and procedures established and provide proper training to Information System staff members and all employees.
- R4. Anthem must have proper measures in place to minimize any losses, including:
 - 4.1 Mitigation plan - Anthem must be able to assess the damage caused by an incident and have steps in place to control the damage.
 - 4.2 Communication plan - Anthem must report all cybersecurity incidents to a government agency as required (Office of General Inspector, FBI).

5.3 Step 3: Hierarchical System Safety Control Structure

In Step 3, a hierarchical system structure, including Anthem's operation and development structure, health insurance regulatory agencies, government, and legislatures, will be identified. As a covered entity, Anthem is required to be in compliance with HIPAA regulations. The Center for Medicare and Medicaid is the office within the Department of Health and Human Services (HHS) establishing HIPAA regulations, and the Office of Civil Rights enforces regulatory compliance with audit support from the Office of Inspector General. Each State is responsible for overseeing the business operations of insurance companies within its borders and investigating consumer complaints. When there is a concern about security, the Insurance Commissioner can investigate any violation or breach.

5.3.1 System Operations Hierarchical Control Structure

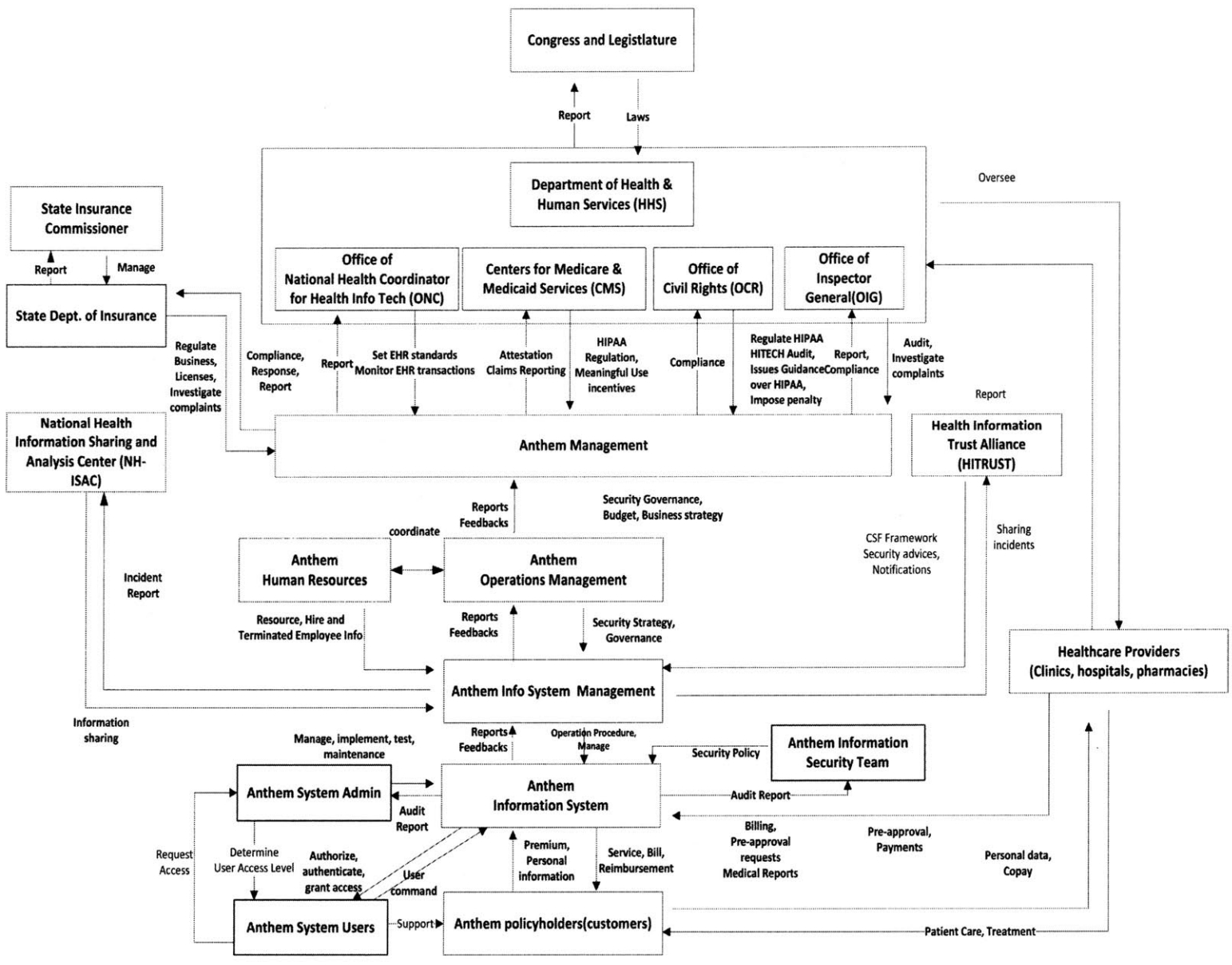


Figure 13: Hierarchical Structure of Anthem's Information System and Management Process

Figure 13 illustrates the hierarchical control structure around Anthem's information system. Each arrow indicates either a control process or a feedback loop. At the top level, Congress approves new laws and budgets for the government agency overseeing the healthcare industry, which is the Department of Health and Human Services. There are multiple offices within HHS overseeing healthcare IT security: the Office of National Health Coordinator (ONC), the Center for Medicare and Medicaid Services (CMS), the Office of Civil Rights (OCR), and the Office of Inspector General (OIG). The role of each office will be discussed in detail in section 5.6.6.

5.4 Step 4: Proximate Event Chain

Tracking the chain of events preceding the loss is often the first step in any accident investigation. However, looking exclusively at event chains will lead us to arrive at the premature conclusion of blaming a human operator or one 'cause' that will not prevent the same accident from happening again. With the STAMP analysis method, we will lay out the proximate events and examine them beyond the immediate timeline since often cyberattackers plan or the causal factors may have started well before the accident.

1. On April 21, 2014, a possible attacker(s) purchased the domain name wellpoint[.]com that was linked with IP 198[.]199[.]105[.]129. The domain registrant's contact information was changed within a few minutes to a group name TopSec China.
2. In May 2014, the subdomains extcitrix[.]wellpoint[.]com, myhr[.]wellpoint[.]com, and hrsolutions[.]wellpoint[.]com were created by the attackers.
3. It is assumed that sometime between May 2014 and December 2014, phishing emails were sent targeting specific people within Anthem with access privileges to the

database server, and the credentials were compromised.

4. Derusbi APT Malware was discovered in September 2014 and was believed to be associated with the IP address linked to the We11point.com spoof site, (198[.]199[.]105[.]129).
5. In November 2014, Sakula malware was created and planted in the spoof site.
6. On December 10, 2014, the initial breach occurred.
7. On January 27, 2015, an Anthem database administrator discovered a data query was running using his/her login, which he/she did not initiate. The administrator stopped the query immediately and notified the Information Security Department (Ragan 2015)
8. Between January 27 and January 29, 2015, Anthem conducted an internal investigation and determined the database administrator and other DBAs' credentials had been compromised. Anthem concluded it was the victim of a cyberattack. The query started on December 10, 2014 and ran sporadically between December 10, 2014 and January 27, 2015.
9. On January 29, 2015, Anthem notified federal law enforcement and HITRUST C3 (Cyber Threat Intelligence and Incident Coordination Center). Anthem reissued user credentials and secured its compromised database warehouse.
10. On February 4, 2015, Anthem CEO Joseph Swedish announced to members and the media that Anthem's database, containing 80 million records, had been compromised. A website (anthemfacts.com) was set up with information about the data breach, including frequent questions and answers, and a free credit monitoring program was established for affected parties.
11. On February 10, 2015, the Connecticut State Attorney General sent a letter on behalf of

9 other State Attorneys General (Arkansas, Illinois, Kentucky, Maine, Mississippi, Nebraska, Nevada, Pennsylvania, and Rhode Island) to Anthem expressing concern over the delay in notifying Anthem's customers about the breach (Roman 2015).

5.5 Step 5: Analyzing the Physical Process

The CAST analysis starts with analyzing the physical process. Prior to analysis, the physical and operational controls must be identified.

5.5.1 Identifying Physical and Operational Controls

The information system structure of a company is not usually open to the public, but an Audit of Information Systems General and Application Controls performed in September 2013 on Anthem's systems has been published by U.S. Office of Personnel Management Office of the Inspector General. Not all, but at least part, of Anthem's information system structure was revealed, especially concerning its security control system, as follows:

- Data centers are located in at least two separate locations: St. Louis, Missouri and Roanoke, Virginia.
- Mainframe is Unix and Intel environment
- Using Blade Logic Tool, but transitioning to Tivoli Endpoint Manager for data storage management
- IBM's Security Intelligence Portfolio QRadar was being used for Security control

Based on the report, it is also known that Anthem had policies and procedures for security such as:

- Physical and logical access control procedures, including badge readers, security guards, camera, and escort procedures
- Change Management procedures
- Annual employee training procedure, including certification
- Technical Configuration Standards in place with outsourced IT partners

5.5.2 Security Analysis

As Anthem has confirmed, the attackers used phishing emails to steal credential information and MD5 malware hashes. MD5 is a cryptographic technology with an algorithm that generates a 128-bit “message digest” output when any length of message is entered (TurnerSean, ChenLily 2011). The technology has been used since 1992, but four years later a problem where two different messages generate the same hash value, which is called “collision,” was reported. In 2004, a collision attack manipulating input blocks using this vulnerability was discovered and followed by another attack called a chosen prefix collision in 2007 (MosesTim 2009). Due to the vulnerabilities and exploitations, security experts have warned against the use of MD5 technology. Back in 2008, there was a Vulnerability Note issued by the US Homeland Security Department about the weakness in the MD5 algorithm allowing for collisions in the hash value output. They have warned that attackers could generate cryptographic tokens or data appearing to be authentic to penetrate into a system (US Homeland Security Department 2008).

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

The strength of the CAST method comes from understanding the entire hierarchical control structure in addition to the physical control system. The analyst can gain valuable insights from studying beyond the physical and human operator levels of control and looking into what roles the government, industry, and company hierarchical control structures played in the accident. In this step, we will start with Anthem’s internal structure and expand from there to cover the health insurance industry, regulatory agencies, and, finally, congress.

5.6.1 Information Security Management

The 2015 breach was not the first time Anthem was breached. In 2013, Wellpoint, Inc.

was fined \$1.7 million by HHS for a possible HIPAA violation for leaving 612,402 protected health information records unprotected over the Internet between October 23, 2009 and March 7, 2010 (Business Wire 2013). According to the Resolution agreement between Wellpoint, Inc. and HHS, the company failed to “adequately implement technology to verify that a person or entity seeking access to ePHI maintained in its web-based application database is the one claimed” (U.S. Department of Human and Health Services 2013).

The day after the Anthem breach was announced, the Wall Street Journal reported Anthem did not encrypt their data (YadronDanny, BeckMelinda 2015). This was confirmed by Anthem spokesperson Kristin Binns, stating that data at rest was not encrypted although the data traversing in or out of the database was encrypted. Currently, HIPAA regulation does not mandate that an organization encrypt its data, yet guides that any organization which believes the effort to encrypt data is considered to be a “reasonable and appropriate safeguard” after internal review must implement such protection. There has been much debate on the value of encrypting data, including the argument from Ken Westin featured in MIT Tech Review (2015). Encryption of data may discourage attackers by making data unusable when exfiltrated outside the system, but once attackers acquire an administrative privilege and get into the system, encryption does not protect stop them from seeing PHI information within the system.

Anthem CEO Joseph Swedish has stated in his apology letter to the affected customers that the system breach occurred in spite of the ‘state-of-the-art’ information security systems Anthem had in place. Although this could have been an accurate statement of Anthem’s self-assessment, according to the Audit Report of Information Systems General and Application Controls performed by the Office of Personnel Management (OPM) at WellPoint and dated

September 10, 2013, WellPoints' servers housing Federal data have never been subject to a total vulnerability scan, and WellPoint avoided full scanning by claiming that their desktop devices were being retired. In addition, when the audit team requested to conduct configuration compliance auditing, WellPoint refused, stating, "a corporate policy prohibited external entities from connecting to the WellPoint network." In the report, the OPM audit team concluded that "[they] were unable to independently attest that Anthem's computer servers maintain a secure configuration." After the Anthem breach, the Office of Inspector General released a statement that Anthem refused to schedule an IT audit, including total vulnerability scan on their servers and configuration compliance testing this summer, once again citing corporate policy (McGee 2015). In the same statement from the OIG, it was expressed they do not understand the reason why Anthem refused such audit. Although OPM's audit on Information Systems is not mandated by law, most major insurance companies choose to be voluntarily audited since the goal of the audit is to help identify vulnerabilities in their Information Systems.

As shown in the Proximate Event timeline in Section 5.4, the attack most likely started as early as April 2014. Even though Anthem could not possibly have known the attackers were preparing the attack, there were 48 days of delay between the initial breach on December 10, 2014 and the discovery of the breach made on January 27, 2015. According to Mandiant's 2014 Threat report, the median number of days to discover a breach was 229 days, so compared to this median number, Anthem's discovery was must faster than the norm. However, the time between the discovery and notification of the affected customers exceeded 14 days, which could have been more than enough time for the attackers to do significant financial damage to those whose data records were compromised. When Connecticut State Attorney General George Jepsen sent

a letter to Anthem expressing his concern, he stated, “the delay in notifying those impacted is unreasonable and is causing unnecessary added worry to an already concerned population of Anthem customers” (Roman 2015).

At least 62 days elapsed between the date of the breach discovery and notification of affected customers. Although HIPAA regulation states the communication must be made no later than 60 days from the discovery, there is no doubt this is longer than the desired timeframe to protect patients’ data. It is unclear if the delay stemmed from the time required for Anthem’s Information Security team to conduct their forensic analysis or a decision made on the timing of communications by corporate executives. 60 days is more than enough time for attackers to use the stolen data or sell them on the black market. It is concerning that the affected customers did not know about the breach during this time period. With more timely notification, customers could have taken appropriate protective measures to mitigate any long-term consequences from the theft of their personal data records.

Anthem Information Security System

Safety Requirements :

- Allocate the budget needed for security within IT and other organizations
- Define safety and security and increase security awareness within company
- Design IT security architecture and implement it
- Establish Information System security policy
- Ensure compliance with all regulations, including HIPAA
- Risk Monitoring, assessment, and communication
- Plan Mitigation in case of breach

Unsafe Decisions and Control Actions:

- Inadequate routine review process of elevated user security
- Inadequate or lack of security policy provided with reference to protection and use of

customer information

- No document on policy or procedure around roles, creating a conflict if granted to the same individual
- Used old security cryptography method MD5 regardless of the warning from security experts and prior case of hack
- Did not utilize security monitoring tool in full capacity and did not perform active, on time monitoring, thus delaying discovery of breach

Context:

- Anthem IT department was in the process of implementing an automated monitoring process for elevated user security
- Anthem IT was focused on expanding its business in multiple states, and thus needed to find ways of saving operating costs to fund expansion costs
- Anthem did not want to be transparent about their security flaws or inadequate security measures
- Anthem IT did not have any employees fully dedicated for active security monitoring as their daily work process

Process Model Flaws:

- Anthem IS Department believed physical security would be sufficient to protect data
- Belief that meeting the minimum HIPAA security requirements will suffice
- Belief that the associated risk is adequately migrated upon authentication process and controlled access to network
- Belief that spending budget on security is not a good investment; putting more priority on expanding business will be a better investment.

Table 7: Unsafe safety control actions – Information Technology Department

5.6.2 Operations Management

Looking at the history of Anthem, Inc, it is clear the company has been highly engaged in mergers and acquisitions and used that as the basis of company growth and expansion. As of December 2014, the company had 15.2 billion dollars of debt. The debt-to-

capital ratio of Anthem was 38.5% and significantly higher than the industry average, which was between 25% and 35% at the time. Prior to September 2014, Anthem had been undergoing financial declines due to losses from its commercial segment (Zacks Investment Research 2014). Anthem's commercial segment represented 53.7% of total revenue in 2014, so it had to diversify its market and expand into government and the public sector. (Market Realist 2015). To strengthen its position in the healthcare market and compensate for its losses in the commercial segment, Anthem acquired CareMore in 2011, Amerigroup in 2012, and Simply Healthcare Holdings in 2015. These acquisitions opened up the opportunity of winning Medicare and Medicaid memberships in 12 states. With its aggressive M&A strategy, Anthem was financially burdened with 'significant financial leverage' as the debt-to-capital ratio had been getting worse. The first two quarters in 2014 did not improve the debt-to-capital ratio, and the concerns of investors and management were growing. This must have forced the company to cut operational costs as much as possible during 2014.

Anthem identified the burden that high operational costs places on its customers in its 2009 report. In its statement, Anthem acknowledged, "For a healthcare company in particular, high operating costs lead to greater costs for customers, lower reimbursements to providers, and less competitiveness in the industry" (Graves and Vickers 2009). Anthem's efforts to lower its operating costs would not have been easy because frequently mergers and acquisitions increase operating costs significantly. From an operational perspective, when operating budgets are cut, many areas that are not in the top priority will be forced to make do with reduced budgets. These cost reductions might have forced Anthem into a position of not being able to follow up on the findings from the OCR audit recommending areas for information security improvements.

Anthem Operation Department

Safety Requirements:

- Coordinate with various departments such as Information Security, Facilities and HR to enforce security policies
- Plan employee training on cybersecurity
- Ensure compliance with all regulations, including HIPAA

Unsafe Decisions and Control Actions:

- Refused the OCR's request to access their systems; also refused the audit offered in 2014 and immediately after the breach
- Inadequate or lack of security policies provided in reference to the protection and use of customer information

Context:

- Anthem was focused on expanding its business in multiple states, and thus needed to reduce operating costs so that it could apply the savings to funding expansion costs
- Anthem did not want to be transparent about its security flaws or inadequate security measures.

Process Model Flaws:

- Belief that meeting the minimum necessary security requirements will suffice.
- Belief that spending on security is not a good investment, and that placing more priority on expanding the business would be a better investment.

Table 8: Unsafe safety control action – Anthem Operations Department

5.6.3 Human Resources (HR)

In prior years, Anthem suffered a high turnover rate of employees. Back in 2003, the turnover rate of first-year associates was 39.7 percent, which was much higher than the industry average. The employee satisfaction rate was 62 percent, 7 percent below the then average of 69 percent. This was obviously hurting the organization as it takes at least a year for a new

employee to become fully productive, and it also forced Anthem to incur the costs associated with recruiting, hiring, and training new employees.

Anthem identified key areas of improvement as being job competency training and career development opportunities. For over two years, it developed an e-learning training program for job training. It also established the Associate Career Development program to empower associates and promote them for their good performance. As a result, the turnover rate dropped to 28.2 percent in a two year span (Skillsoft 2010). However, the turnover rate was still considered high for WellPoint, so they started focusing more on the HR process using predictive analytics tools. In a 2009 interview, HR director David Ibarra noted that the HR department had to work closely with the finance department to increase the effectiveness of the hiring and onboarding processes (Graves and Vickers 2009). Anthem also used a business simulation program so that candidates could experience what it is like to work in a call center and the customer service department. Management believed people who do not like what they experience in the simulation will likely leave the company within one year (Hagerty and Light 2010).

Anthem Human Resources (HR)

Safety Requirements:

- Ensure employees being hired are safe personnel without criminal histories
- Ensure active employees are up-to-date with compliance and cybersecurity training
- Coordinate with the Information Security team on access provisioning upon hiring and termination

Unsafe Decisions and Control Actions:

- Did not follow up on the OCR's audit report recommendation pertaining to the HR-IS coordination process

Context:

- Anthem HR does not have authority over the coordination process
- After multiple mergers and acquisitions, having up-to-date HR information provided is not easy; even an automated process takes time to integrate when a new organization is acquired

Process Model Flaws:

- Belief that the HR processes will follow expansion and acquisition, although it may take time to do so.
- HR department's belief that information security is handled by IT department and they have a little role in Information Security.

Table 9: Unsafe safety control action – Anthem Human Resources

5.6.4 Anthem Executive Management

Looking at Anthem's current Executive Leadership organizational chart (Figure 14), it currently does not have a Chief Information Officer (CIO) or Chief Information Security Officer (CISO) dedicated to information security. (Hasib 2015) According to the job descriptions on the organizational chart on Anthem's website, Executive Vice President and Chief Administrative Officer Gloria McCarthy is responsible for Information Technology along with oversight of cross-organizational execution of their strategies. Although CAO Gloria McCarthy has profound experience in Enterprise execution and operations and has served in the healthcare industry well over 15 years, her specialty is not Information Security or Information Technology. Despite CEO Joseph Swedish's statement that 'Safeguarding clients' information is Anthem's top priority' in the letter he sent to clients after the breach, the absence of a designated CISO shows that strategic decisions on information security are not made independently, but as a part of the company's general operations and execution.

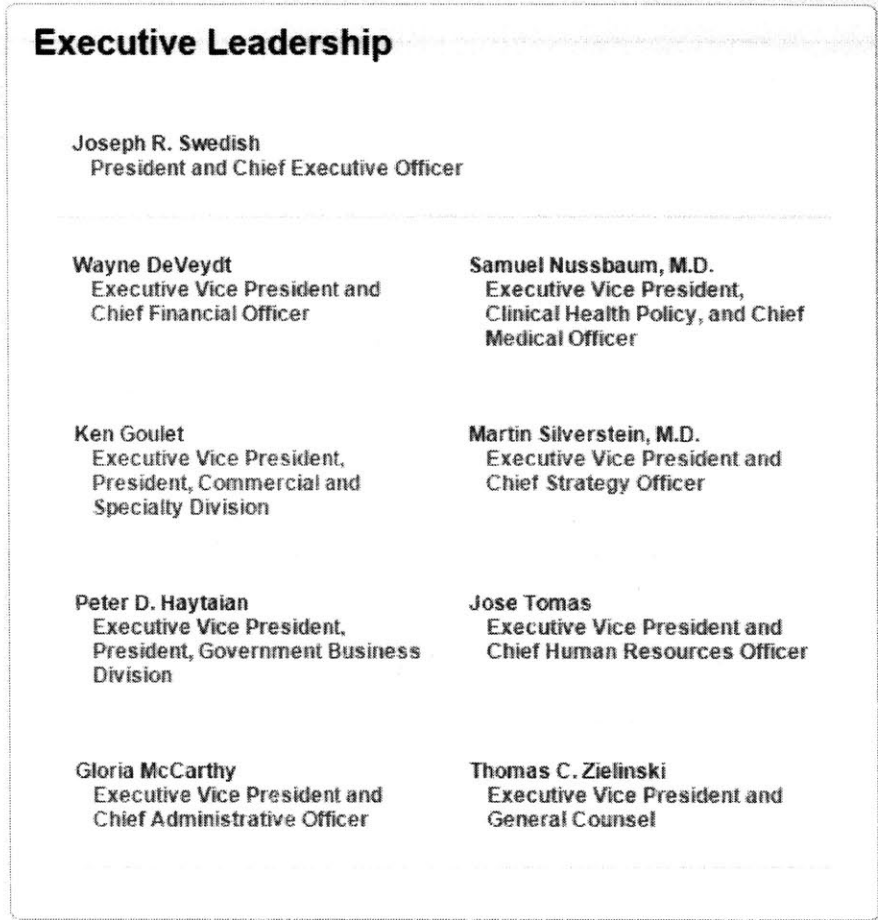


Figure 14: Anthem, Inc. Executive Leadership Organizational Chart (Anthem, 2015)

Since 2004, Anthem (formerly WellPoint) has been suffering a high turnover rate in its executive ranks. Between 2004 and 2014, more than 15 executives left the company, including three CEO changes in 2009, 2012, and 2013 (Wall 2007). This is not unusual in the healthcare industry, which is known to have the highest executive turnover rate due to mergers and acquisitions. On average, the CEO turnover rate in the healthcare industry is 50 percent higher than it is in other industries (Challenger, Gray & Christmas 2013). Such frequent changes and high turnover impact the organization on many levels. Often the key to the long-term success of cybersecurity management programs is support and alignment from the executive level. Frequent changes make maintaining focus and continuation of management programs very

difficult to achieve, since new executives often bring shifts in strategy and vision. A study done by Marblehead Group shows technical initiatives can be disrupted by executive changes, as company strategies and policies are reviewed by new company leaders (Saita 2003).

Anthem Executive Management

Safety Requirements :

- Align security policy with the organization’s mission and objectives
- Set roles and responsibilities for departments and teams on security
- Monitor regulatory compliance and communicate with regulatory organizations
- Oversight of information security compliance

Unsafe Decisions and Control Actions:

- Refused the OCR’s request to access their systems; also refused the audit offered in 2014 and immediately after the breach
- No dedicated Chief Information Security Officer within the organization
- Inadequate or lack of security policy provided in reference to protection and use of customer information

Context:

- Anthem focused on expanding its business in multiple states, thus needed to find ways of reducing operating costs so that it could apply the savings to funding its costs
- Anthem did not want to be transparent about its security flaws or inadequate security measures

Process Model Flaws:

- Belief that meeting the minimum necessary security requirements would suffice
- Belief that spending on security is not a good investment and that placing a higher priority on expanding the business would be a better investment
- Belief that being transparent about everything may raise concerns and may drive investors away

Table 10: Unsafe safety control actions – Anthem Executive Management

5.6.5 Health Insurance Industry

The health insurance industry is one of the heaviest regulated industries, and many consumers believed that there would be adequate protections in place to guard their sensitive information. When consumers shop for their health insurance, they may not be given many choices because health insurance plans are offered by their employers with intentionally constrained alternatives. Because of the limited selections available, even if an incident like this happens, it is not easy for consumers to change their insurance carrier. It is not same as choosing a retailer where there are many competitors and the cost of switching is low. The nature of having less competition in the health insurance industry leads companies to put fewer efforts and investments into earning the trust of their customers (YaraghiNiam, BleibergJoshua 2015). This viewpoint is confirmed by the Wall Street Journal reported the Anthem's comment "it [Anthem] does not expect the incident to affect 2015 financial outlook, primarily as a result of normal contingency planning and preparation."

Bitsight's 2014 study on the security ratings of companies across four different sectors showed healthcare scored the lowest. The study also noted that the duration of cybersecurity incidents in the healthcare industry was the longest, showing how inadequately the industry is prepared to mitigate damages resulting from cyberattacks. (BurtChris 2014) One of the indicators of the healthcare industry's low investment in cybersecurity is the ranking of the compensation of healthcare industry Information Security professionals as the lowest in all industry, according to Ponemon's "2013 Cybersecurity Salary Benchmark Report". Low compensation makes it difficult to attract highly qualified Information Security professionals to the healthcare industry. The annual security report released by the Health Information Management System Society (HIMSS) shows healthcare companies spend less than 3 percent

of their IT budgets on cybersecurity, and only 54 percent of Information Security professionals have experience with testing data breach response plans. Without retaining knowledgeable and experienced Information Security personnel, the healthcare industry will continue to lag other security sensitive industries in the information security area.

Health Insurance Industry

Safety Requirements:

- Build a secure, safe industry culture that does not tolerate breaches
- Build accountability that helps foster teamwork to strengthen security
- Invest in adopting the best security technology and tactics that will help protect the public's PII and PHI

Unsafe Decisions and Control Actions:

- Meeting only the minimum requirements rather than choosing the highest security possible
- Unless required by law or regulations, the best security practices will not be implemented
- Have lower pay scale and market standard for security professionals

Context:

- Healthcare industry should be conservative in adopting new technology.
- Consumers' cost of switching health insurance providers is high
- Healthcare industry is non-profit or not-for-profit and should not be paying employees higher than industry average

Process Model Flaws:

- Healthcare is a very unique industry, and the security policies and technologies from other sectors cannot be applied
- There is limited competition in the health insurance market
- High quality information security has little impact on overall cybersecurity

Table 11: Unsafe safety control action – Health insurance industry

5.6.6 Regulatory Agencies

Any health insurance company conducting business within the U.S. must follow HIPAA regulations. As a result, health insurance companies choose to implement only the minimum required information security procedures so they are not in violation of HIPAA regulations. There are two offices under HHS that play an important role in monitoring industry compliance with HIPAA regulations: the Office of the National Coordinators (ONC) and the Office for Civil Rights (OCR). ONC has responsibility for developing the health information technology infrastructure for Electronic Health Records (EHR) and sets EHR standards. ONC also monitors all EHR transactions within the industry. OCR, on the other hand, regulates and enforces HIPAA compliance and issues guidance on regulations (HealthIT.Gov unknown). OCR is also the branch that performs the HITECH audit.

Under the HIPAA Breach Notification Rule (45 CFR §§ 164.400-414) any covered entities and associated businesses are required to notify OCR of any data breach resulting in loss of PHI. The notification process differs based on the number of individuals affected. Notice to affected individuals should go out to all individuals regardless of the size of the affected group and should be reported to OCR. If there are more than 500 individuals affected, the notification should also be given to the media present in the local area of the 500 or more affected people and to the Secretary of the Department of Health and Human Services. If the number of impacted individuals is unknown at the time of breach, the organization must estimate the number for initial reporting and file an addendum later on when the impact is fully known (Department of Health and Human Services, 2009).

ONC has recently released an improved guideline, in an effort to help healthcare organizations with risk analysis and compliance (The Office of the National Coordinator for

Health Information Technology 2015). Healthcare organizations have been struggling to meet different sets of requirements between the HIPAA regulation and Meaningful Use and, more importantly, to find a better way to assess information security vulnerabilities (Department of Health and Human Services 2015). As a result, the companies have been committed to meet the minimum requirement only.

Healthcare Regulatory Agencies

Safety Requirements:

- Create effective security governing regulations pertaining to the specific industry
- Govern the information security audit process
- Enforce safety related regulation policies (HIPAA)
- Communicate any security incidents with industry partners and organizations

Unsafe Decisions and Control Actions:

- Absence of clear communication process for sharing incidents with outside of the organization; reliance on third-party organizations for communication
- Audit process exists, but not heavily enforced (company may refuse the audit)
- No public training or formal process on cyber warfare

Context:

- Audit is voluntary but not mandatory
- Communication throughout the industry on the breach is not the regulating agency's expert area
- Oversight for cybersecurity is divided among three offices within DHHS

Process Model Flaws:

- Audits may help uncover problematic areas, but should not be mandated as there is already a process for imposing fines in the event a breach occurs
- Idea that DHHS is a healthcare regulatory organization and not the IT governing organization.

- Each organization has the right not to share information with the government
- Stockholders would not like any discoveries from the audit process

Table 12: Unsafe safety control action – Healthcare regulatory agencies

5.6.7 Congress

Early in 2015, President Barack Obama urged Congress to establish new, tougher legislation to enforce and govern cybersecurity, including bigger penalties for cyber criminals. Until now, attempts in Congress to strengthen cybersecurity legislation has not been successful, mainly due to the concern of companies about sharing their internal information with the government and also to privacy concerns (PalettaDamian 2015).

Immediately after the Anthem breach, U.S. Rep. Michael McCaul, Chairman of the House Committee on Homeland Security, released the statement that the Anthem attack reminds us of “the need for Congress to take aggressive action to remove legal barriers for sharing cyber threat information. [...] and cybersecurity legislation as soon as possible” (Committee on Homeland Security 2015). In addition to the legal challenge, there have been debates between government officials who have yet to come to a consensus on the best approach to handle cyberattacks. Many large-scale cyberattacks originate outside the U.S., and there is a growing concern about these attacks because they are often easily deniable and difficult to prove (AlexanderKeith 2015).

Congress and Legislation

Safety Requirements:

- Establish effective legislation governing cybersecurity
- Ensure government and private sector coordination to improve cybersecurity strategies
- Create a foreign policy to enforce defense against cyberattacks around the globe

- Prepare mitigation of cyber warfare and large scale cyberattacks for public safety and security

Unsafe Decisions and Control Actions:

- Absence of foreign policy handling cybercrimes originated outside U.S.
- Absence of policy governing and coordinating with private sector entities in handling cyberattacks
- No formal government procedure for sharing and alerting companies of cyberattack information
- No public training or formal process on cyber warfare

Context:

- Congress has tried implementing tougher legislation but has failed
- Big concerns in the private sector about sharing information with the government due to shareholder opposition and possible lawsuits on privacy grounds
- Overall absence of international laws regarding cybersecurity
- Cyberattack scenarios are not easily identified.

Process Model Flaws:

- Idea that establishing foreign policy on cybersecurity is a sensitive issue and difficult task
- No precedent in international law for handling cyberattacks
- Belief that government cannot force private sector companies to share their private information

Table 13: Unsafe safety control action – Federal Legislation

5.6.8 Inadequate Controls and Missing Feedback

In section 5.6.1, the importance of monitoring cyberattacks was discussed. In Anthem’s case, it was not the absence of monitoring tools or processes that caused the breach, but rather the process was not effectively utilized. Many enterprises know how critical it is to have such monitoring systems in place, but once implemented, they are not actively used. Many companies believe their systems will monitor suspicious activities for

them, or staff members may feel the monitoring process is monotonous and staying vigilant can be difficult. It is also possible that the enterprise may not have enough resources to review all of the logs and activities in the system.

There is no central feedback mechanism between government and the private sector for sharing information about cyberattacks. Current HIPAA regulation has a security incident reporting procedure, but it does not include any incident that does not result in a confirmed security or privacy violation. In Anthem's case, they refused the government agency's offer of an external audit, which might have helped them identify vulnerable areas before the breach occurred. There is no formal policy or requirement by the government regarding external information security audits.

5.7 Step 7: Coordination and Communication

There are three components in the communication strategy for notification of any breach incident. First, a covered healthcare entity is required by HIPAA regulation to notify the HHS Secretary of any breach of any 'unsecured' health information within 60 calendar days from the discovery of the breach.

There are two organizations involved in the breach communication process: the National Health Information Sharing and Analysis Center (NH-ISAC) and the Health Information Trust Alliance (HITRUST). Recognized by the Department of Health and Human Services, the National Institute of Standards & Technology (NIST), and the US Department of Homeland Security (DHS), the role of NH-ISAC is to raise awareness by running the cybersecurity first responder program and issuing communication bulletins to its members. It also provides cybersecurity consulting services and recommendations for addressing information security vulnerabilities.

HITRUST is an organization established by Common Security Frameworks (CSF), which could be used as a source of guidelines for the proper handling of sensitive data. Upon receiving notification of an information security incident from a subscribed member, it issues a security alert (C3) to warn the industry of the cyber threat.

After the attack, Anthem reached out to both NH-ISAC and HITRUST about the attack and submitted an Indicator of Compromise (IOC), including the IP and email addresses the attackers used. Upon receiving the IOC, NH-ISAC shared the information with participating members and the external ISACs within 12 hours. HITRUST also shared the information immediately within its community, but decided it was not necessary to issue an industry wide warning as there were no other incidents reported (Higgins 2015). These notifications are sent out exclusively to the organization's members unless it is an emergency notification that requires industry-wide attention. Since this is a voluntary subscription based service, companies which have not joined either organization have limited access to information about these breaches. Membership in such a group is a good practice because it could give organizations a good indication on how often breaches occur or if any specific types of breaches are increasing.

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

After experiencing repeated breaches throughout the industry, people quickly forget these incidents and move on. As seen in Figure 15 (Stock Price charting between January – March 2015), Anthem's stock price dipped (highlighted area) briefly right after the announcement of the breach, but quickly recovered its value. Overall, the trend of Anthem's stock price has been steadily increasing regardless of the breach. This shows that stockholders and the public in general do not believe the breach will damage Anthem's reputation or disrupt its business. The market thinks Anthem's stock is still worth buying with

positive business prospects. Anthem may be paying fines and legal settlements, but the breach is not causing a negative outlook on its business or discouraging investors. The stock trend is a good indication of how the public and society perceive cybercrimes, even when 25 percent of the US population has been affected. Due to the frequency of breaches and the unseen consequences, the public is becoming more forgiving about these breaches. Such trends make companies less likely to focus on cybersecurity issues when making business decisions and formulating long-term strategies.

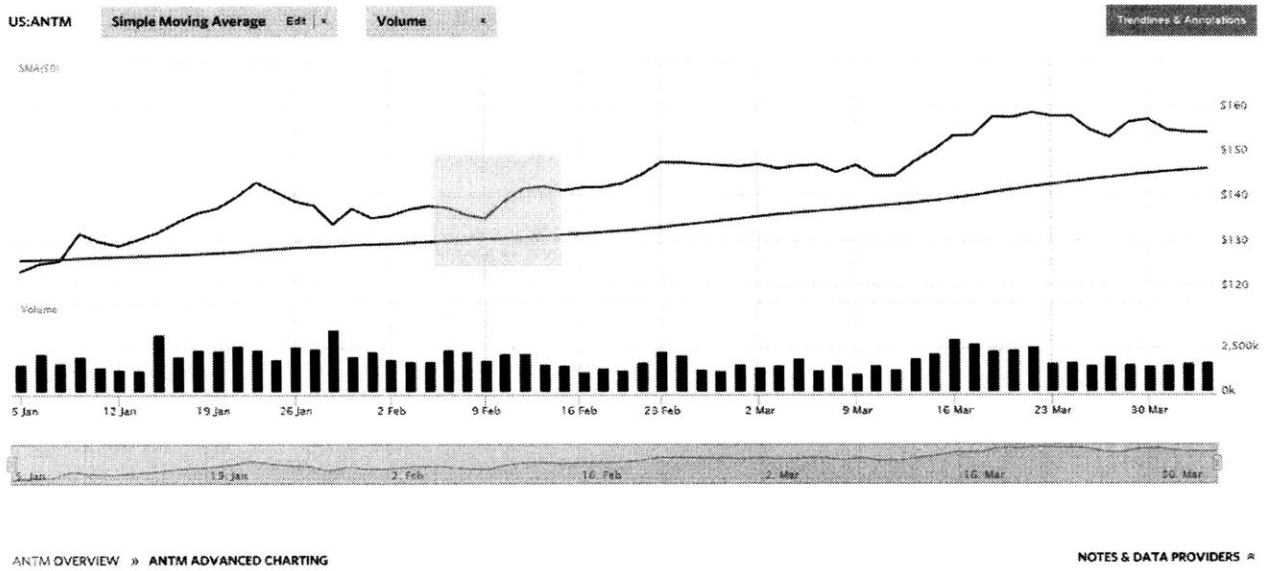


Figure 15: Anthem stock price trend :January 2015- March 2015 (NASDAQ)

5.9 Step 9: Recommendations

The last step of CAST analysis is to produce recommendations based on the results from the previous analysis steps. The recommendations from the CAST analysis are applicable not only to Anthem, but to all levels of the hierarchical control structure. This discussion will be further expanded in Chapter 6.

6. Recommendations

Would it have been possible to stop the breach if Anthem had encrypted its data? Could the damaging outcome from the breach have been prevented? These are the questions that lingered in many people's minds after the attack. Living in a dynamic, fast changing world, attackers seeking an opportunity to get into the system are adept at using dynamic, fast changing techniques. By contrast, many organizations' approaches to Information Technology systems and cybersecurity are about making the system stable, optimized, and available. Moreover, many organizations opt to spend budget only to meet the minimum security required by regulations. As Westin (2015) put it, "Cybercriminals are fully aware of the constant trade-offs that organizations make to balance security with operational efficiency, and they have repeatedly demonstrated that they are fully capable of exploiting even tiny security weaknesses." This approach often hinders organizations from adopting effective cybersecurity tactics that could defend against fast changing global cyber threats. Advanced Persistent Threat is a great example of how difficult it is for an organization to prevent cyberattacks. Attackers will quickly change their tactics if one method does not work until they are able to penetrate the system.

There are three steps in loss prevention: Protect, Mitigate, and Eliminate. Eliminate is the most effective way of handling loss. If the hazard can be completely eliminated, the accident will not happen. However, it is not practical to eliminate cyberattackers entirely in this world. The next most effective methods are mitigation and risk management. The least effective and most expensive way of handling loss is to protect. Unfortunately, the majority of companies are focused on protecting their assets, but their current strategies are not effective and are failing. It is important that our strategy move from protecting to mitigating.

The first step of managing and mitigating is to understand where the risks are. Mitigation can be effective as a loss prevention strategy only when we understand where the biggest risks are and how the greatest damage may occur. Timely response and rapid mitigation are essential to reducing the damage, and this is where monitoring plays a critical role. Without actively monitoring the system, companies will not even know when damage is occurring. Many organizations have monitoring tools, but do not fully utilize them. Continuous monitoring and defense will increase corporate awareness of cyberattacks and position companies to mitigate the damage as soon as an attack occurs.

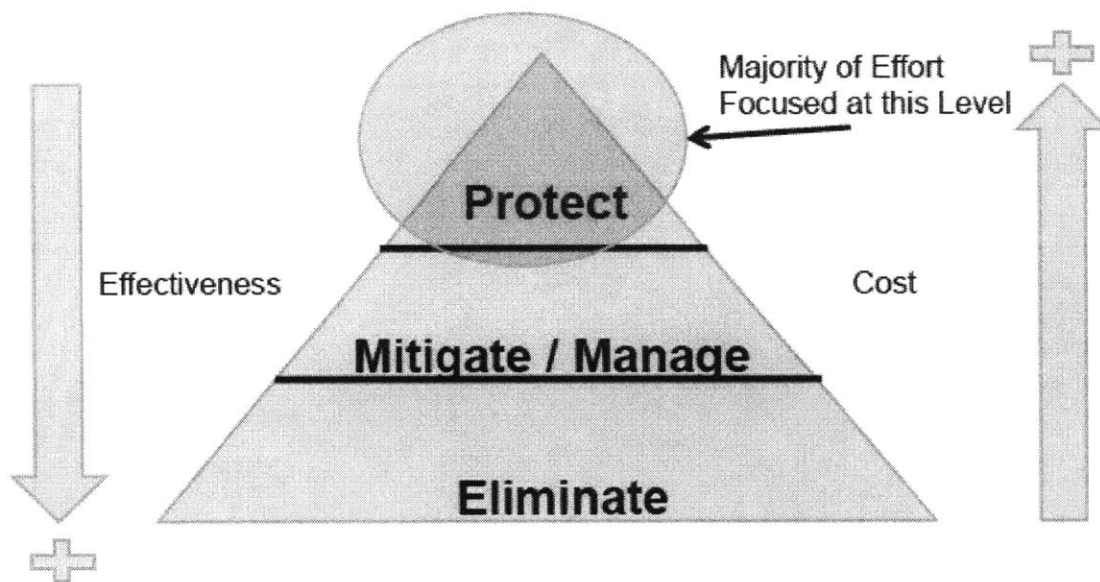


Figure 16: Relationship between Effectiveness and Cost of loss prevention (Young 2015)

CAST analysis showed that Management's and the Information System Department's lack of understanding of operational roles and responsibilities could lead to granting unnecessary access and privileges to people who may not need it. Separation of access privileges is important, in case there is a breach. For instance, a System or Database Administrator rarely needs to run a query of patients' information. The credential of privileged

accounts, including a system administrator or a super user who has full access to the application or has at least partial access to data containing personally identifiable information, is believed to be a key target of the attackers. Once the account with privileged access is compromised, it is only a matter of time before the attackers are able to gain access to the target data files and export them. Thus, separating administrative access with elevated rights to the system or physical infrastructure from privileged access to patients' protected information may prevent attackers from getting into the system, having full control, and being able to obtain PII data.

Understanding of cybersecurity risk and its importance by management, including key executives and board members, is crucial to the success of security management. As pointed out by the Chief Legal Officer of Rewards Network, Alice Geene, cybersecurity is beyond an IT and legal issue; it is an organizational priority (Reisinger 2015). An effective security program involves the education and support of the CEO and board members, which is much more than simply a policy written in a paper (Warren 2015). Although a company may undergo changes and experience turnover in top management, the organization must maintain a consistent focus on the security of the data. Information security can be reinforced by board members' clear understanding of its importance.

Information security culture within a company that owns PII data and the healthcare industry is extremely important in cultivating compliance and effectiveness. When a company's objective is to grow, information security may not be perceived as the top priority since the return on investment is not obvious. The lack of competition in the health insurance industry does not encourage health insurers to exert the highest information security in their systems. To change this environment, all health insurance companies need to share the burden of information security. Sharing information on cybersecurity and breaches in a timely manner can be critical

and helpful to protect the industry against these crimes. Initiating an industry-wide watch program and campaigns on information security will increase awareness and cybersecurity knowledge.

FBI director Robert Mueller stated, "There are only two types of companies: Those that have been hacked, and those that will be" (Mueller 2012). There is no one technology or framework that will protect our systems 100%. We should always assume attackers will find a way to breach the system, and cybersecurity is an ongoing effort to manage the risk, not a formula that we implement and hope it is going to protect. Merely building a stronger firewall, encrypting every laptop, or using biometric passwords will not stop the attackers. The more we try to protect, the attackers' methods will get smarter and more sophisticated.

As the information within the system gets stronger, the attack will be pointed toward the weakest link in the system: a human. As discovered in the STAMP analysis, the focus should be more on the controller and the feedback given back to controller; how do we better detect and mitigate attacks? The better information security strategy when we cannot protect our system completely is to be prepared with the best detection and mitigation plan so that the damage could be discovered at the earliest possible point, and its impact could be minimized.

Building a cybersecurity aware climate throughout the industry and taking a collective approach against cyberattacks is necessary. There is precedent in the finance industry that a collective approach can be successful. Back in early 2000, major credit card companies came together and established the Payment Card Industry (PCI) standards to protect cardholder data. Although it has not been a failproof standard, it has tremendously increased the data security in the finance industry.

Not only the formulation of better cybersecurity standards to fit the health insurance

industry, but also a coordinated response to these threat events would be helpful. The coordinated response should be based on sharing information and collaborating to develop proper response procedures. Working together as an industry, the awareness and protective measures against cyber threats will be heightened, and no longer will companies be meeting the bare minimum of information security requirements.

7. Future Work

A key discovery from applying the STAMP/CAST method to the Anthem breach is that a crucial point is being missed in the defense of health data. Future research in this area can be focused on establishing more adaptive, dynamic strategies, which could the industry help defend against advanced persistent threats. Current cybersecurity methods put a lot of weight on securing physical layers without putting much emphasis on human controllers and feedback loops. Such future research could help management prepare for better handling and mitigating cyberattacks. Second, more focus on cybersecurity regulations around health data is required. Current policy, regulations, and guidelines issued by government agencies fall short in offering sufficient guidance to companies. Current regulations and compliance incentives must be reviewed to raise the minimum requirements for information system security.

Conclusion

Although current regulations and frameworks provide some guidelines for enterprises on building basic cybersecurity structures, they fall short on discovering the vulnerabilities and socio-technical layers of the problem. Securing a large, complex database structure like Anthem's is challenging work, and it requires more than simple physical security or antivirus software. Instead, it requires constant monitoring and awareness.

More importantly, a company should be aware of the value and importance of securing its critical data systems against cyberattacks and come up with a strategy that will prepare the company to mitigate potential data breach losses. Top management must invest in cybersecurity with the clear understanding that it is not only about short-term return on investment, but it is also about protecting people's most valuable data and earning their trust. It is most important that as an industry, we create a security culture that promotes industry-wide coordination and vigilance. Regulators and government agencies also need to step in and lead efforts to create this cybersecurity culture by engaging all companies and establishing regulations enforcing the standards. The STAMP method is an excellent tool which can help organizations assess their vulnerabilities and understand the impact of controls on their entire systems so they can better protect important data.

Appendix 1: Anthem Communication to members after breach

This appendix includes a full letter from Anthem CEO Joseph Swedish on the website proving information and FAQ ([www.anthemfacts\[.\]com](http://www.anthemfacts[.]com)).



To Our Members:

Safeguarding your personal, financial and medical information is one of our top priorities, and because of that, we have state-of-the-art information security systems to protect your data. However, despite our efforts, Anthem Blue Cross Blue Shield was the target of a very sophisticated external cyber attack. These attackers gained unauthorized access to Anthem's IT system and have obtained personal information from our current and former members such as their names, birthdays, medical IDs/social security numbers, street addresses, email addresses and employment information, including income data. Based on what we know now, there is no evidence that credit card or medical information (such as claims, test results or diagnostic codes) were targeted or compromised.

Once the attack was discovered, Anthem immediately made every effort to close the security vulnerability, contacted the FBI and began fully cooperating with their investigation. Anthem has also retained Mandiant, one of the world's leading cybersecurity firms, to evaluate our systems and identify solutions based on the evolving landscape.

Anthem's own associates' personal information – including my own – was accessed during this security breach. We join you in your concern and frustration, and I assure you that we are working around the clock to do everything we can to further secure your data.

Anthem will individually notify current and former members whose information has been accessed. We will provide credit monitoring and identity protection services free of charge so that those who have been affected can have peace of mind. We have created a dedicated website - AnthemFacts.com - where members can access information such as frequent questions and answers. As we learn more, we will continually update this website and share that information with you. We have also established a dedicated toll-free number that both current and former members can call if they have questions related to this incident. That number is: 1-877-263-7995.

I want to personally apologize to each of you for what has happened, as I know you expect us to protect your information. We will continue to do everything in our power to make our systems and security processes better and more secure, and hope that we can earn back your trust and confidence in Anthem.

Sincerely,

Joseph Swedish
President and CEO
Anthem, Inc.

Appendix 2: HIPAA Security Standards Matrix

(U.S. Department of Health & Human Services 2007)

Appendix 2 is the HIPAA security standards a covered entity uses as a information security guideline.

ADMINISTRATIVE SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Security Management Process	§ 164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity	(R)
Assigned Security Responsibility	§ 164.308(a)(2)		
Workforce Security	§ 164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	§ 164.308(a)(4)	Isolating Health Care Clearinghouse Functions	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	§ 164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident	§ 164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	§ 164.308(a)(7)	Data Backup Plan	(R)

Contingency Plan		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedures	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	§ 164.308(a)(8)		
Business Associate Contracts and Other Arrangements	§ 164.308(b)(1)	Written Contract or Other Arrangement	(R)
PHYSICAL SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Facility Access Controls	§ 164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	§ 164.310(b)		
Workstation Security	§ 164.310(c)		
Device and Media Controls	§ 164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)
TECHNICAL SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Access Control	§ 164.312(a)(1)	Unique User Identification	(R)

		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	§ 164.312(b)		
Integrity	§ 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	§ 164.312(d)		
Transmission Security	§ 164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)
ORGANIZATIONAL REQUIREMENTS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Business associate contracts or other arrangements	§ 164.314(a)(1)	Business Associate Contracts	(R)
		Other Arrangements	(R)
Requirements for Group Health Plans	§ 164.314(b)(1)	Implementation Specifications	(R)
POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Policies and Procedures	§ 164.316(a)		
Documentation	§ 164.316(b)(1)	Time Limit	(R)
		Availability	(R)
		Updates	(R)

Bibliography

- Aaron, Greg, and Rasmussen Rod. "Global Phishing Survey: Trends and Domain Name Use in 1H 2014." *APWG*. September 25, 2014.
http://docs.apwg.org/reports/APWG_Global_Phishing_Report_1H_2014.pdf (accessed March 20, 2015).
- Ablon, Lillian, Martin Libicki, and Andrea Golay. "Markets for Cybercrime Tools and Stolen Data." *RAND*. 2014.
http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf (accessed March 20, 2015).
- Alexander, Keith. *Stopping the Next Cyber-Attack*. January 13, 2015.
<http://www.bloombergview.com/articles/2015-01-13/how-we-can-prevent-the-next-sonystyle-attack> (accessed May 15, 2015).
- Anthem, Inc.* 2015. <http://www.antheminc.com/AboutAntheminc/CompanyHistory/index.htm> (accessed March 15, 2015).
- Bailey, Brandon. "Anthem: Hackers Tried to Breach System as Early as Dec. 10." *U.S. News*. February 6, 2015. <http://www.usnews.com/news/business/articles/2015/02/06/anthem-hacker-tried-to-breach-system-as-early-as-dec-10> (accessed March 28, 2015).
- Barger, Rich. "The Anthem Hack: All Roads Lead to China." *ThreatConnect, Inc.* February 27, 2015. <http://www.threatconnect.com/news/the-anthem-hack-all-roads-lead-to-china/> (accessed March 28, 2015).
- Bellovin, Steven. "Why even strong crypto wouldn't protect SSNs exposed in Anthem breach." *arstechnica*. February 5, 2015. <http://arstechnica.com/security/2015/02/why-even-strong-crypto-wouldnt-protect-ssns-exposed-in-anthem-breach/> (accessed March 18, 2015).
- Binde, Beth, Russ McRee, and Terrence O'Connor. "Assessing Outbound Traffic to Uncover Advanced Persistent Threat." *SANS Institute*. May 22, 2011.
<https://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf> (accessed March 27, 2015).
- Blue Cross Blue Shield. "WellPoint Announces Intent To Change Corporate Name To Anthem, Inc." *Blue Cross Blue Shield*. August 13, 2014. <http://www.bcbs.com/healthcare-news/plans/wellpoint-announces-intent-to-change-corporate-name-to-anthem-inc.html> (accessed March 15, 2015).
- Burt, Chris. "Healthcare Sector More Vulnerable than Retail to Cybersecurity Risks: Study." *WHIR Hosting Cloud*. Mary 30, 2014. <http://www.thewhir.com/web-hosting-news/healthcare-sector-vulnerable-cybersecurity-risks-retail-study> (accessed March 27, 2015).
- Business Wire. "WellPoint pays HHS \$1.7 million for leaving information accessible over Internet." *Business Wire*. July 11, 2013.
<http://www.businesswire.com/news/home/20130711006294/en/WellPoint-pays-HHS-1.7-million-leaving-information#.VTEXqxPF-V8> (accessed April 16, 2015).
- Casey, Tim, Kevin Fiftal, John Miller, Dennis Morgan, and Bryan Willis. "The Cyber Security in

- Action: An Intel Use Case." *Intel, Corp.* 2015.
<https://supplier.intel.com/static/governance/documents/The-cybersecurity-framework-in-action-an-intel-use-case-brief.pdf> (accessed March 5, 2015).
- Challenger, Gray & Christmas. "Report: Healthcare has more CEO turnover than any other industry." *Advisory.com*. October 17, 2013. <http://www.advisory.com/daily-briefing/2013/10/17/health-care-has-more-ceo-turnover-than-any-other-industry> (accessed March 28, 2015).
- Cole, Eric. *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*. Syngress Publishing, 2013.
- Committee on Homeland Security. *McCaul Statement on Cyber Attack on Anthem, Inc.* February 4, 2015. <http://homeland.house.gov/press-release/mccaul-statement-cyber-attack-anthem-inc> (accessed March 16, 2015).
- De Decker, Bart, and Andre Zuquete. *Communications and Multimedia Security*. Springer, 2014.
- Department of Health and Human Services. "HIPAA Administrative Simplification Statute and Rules." *Department of Health and Human Services*. August 24, 2009. <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/> (accessed April 7, 2015).
- . "Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 3 ." *Centers for Medicare and Medicaid Services*. March 30, 2015. https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Stage3_Rule.pdf (accessed April 21, 2015).
- Furht, Borko. *Encyclopedia of Multimedia*. Springer Science & Business Media, 2008.
- Graves, Alice, and Mark Vickers. "TrendWatcher: The Quest for Better Human Capital Metrics ." *HR World*. April 6, 2009. <http://www.hrworld.com/features/trendwatcher-quest-better-hcm-040609/> (accessed March 28, 2015).
- Griffin, Thomas, Mark Young, and Neville Stanton. *Human Factors Models for Aviation Accident Analysis and Prevention*. Ashgate Publishing, Ltd., 2015.
- Hagerty, James, and Joe Light. "Job Offers Rising as Economy Warms Up." *The Wall Street Journal*. December 24, 2010. <http://www.wsj.com/articles/SB10001424052748703548604576037612752480904> (accessed April 10, 2015).
- Hasib, Mansur. *To Improve Cybersecurity, Fire Some CEOs*. June 15, 2015. <http://www.enterprisetech.com/2015/06/15/to-improve-cybersecurity-fire-some-ceos/> (accessed June 23, 2015).
- HealthIT.Gov. "What are respective roles of ONC and OCR regarding privacy and security?" *Health IT. gov*. unknown. <http://www.healthit.gov/policy-researchers-implementers/faqs/what-are-respective-roles-onc-and-ocr-regarding-privacy-and-sec> (accessed May 2, 2015).
- Higgins, Kelly Jackson. "How Anthem Shared Key Markers Of Its Cyberattack."

- InformationWeek*. February 12, 2015. <http://www.darkreading.com/analytics/threat-intelligence/how-anthem-shared-key-markers-of-its-cyberattack/d/d-id/1319083> (accessed March 28, 2015).
- Howard, Rick. *Cyber Fraud: Tactics, Techniques and Procedures*. Auerbach Publication, 2009.
- Hutchins, Eric, Michael Cloppert, and Rohan Amin. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." *Lockheed Martin Corporation*. July 31, 2012. <http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf> (accessed March 15, 2015).
- Infosec Institute . "Scanbox Framework." *Infosec Institute*. n.d. <http://resources.infosecinstitute.com/scanbox-framework/> (accessed March 28, 2015).
- Infosec Institute. "Scanbox Framework." *Infosec Institute*. February 27, 2015. <http://resources.infosecinstitute.com/scanbox-framework/> (accessed March 28, 2015).
- ISACA. *About ISACA*. n.d. <http://www.isaca.org/about-isaca/Pages/default.aspx> (accessed March 20, 2015).
- ITRC. "Identity Theft Resource Center Breach Report Hits Record High in 2014." *Identity Theft Resource Center* . n.d. <http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html> (accessed March 27, 2015).
- Kazel, Robert. *American Medical News*. December 20, 2004. <http://www.amednews.com/article/20041220/business/312209996/2/> (accessed March 15, 2015).
- Krebs, Brian. "Anthem Breach May Have Started in April." *Krebson Security*. February 9, 2015. <http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/> (accessed March 28, 2015).
- Leveson, Nancy. *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge: MIT Press, 2011.
- Mandiant. "M-Trends 2015: A View from Frontlines." *Fireeye*. 2015. <https://www2.fireeye.com/rs/fireeye/images/rpt-m-trends-2015.pdf> (accessed March 15, 2015).
- Market Realist. "Anthem-Health Insurer: An Investment Primer." *Market Realist*. April 2015. <http://marketrealist.com/2015/04/anthems-key-business-segments/> (accessed May 3, 2015).
- Martin, David. "Building a More Effective Cybersecurity Defense." *Institutional Investor*. September 18, 2014. <http://www.institutionalinvestor.com/blogarticle/3381726/blog/building-a-more-effective-cybersecurity-defense.html#.VV0AA5ON1BQ>.
- Mathews, Anna Wilde, and Danny Yadron. *The Wall Street Journal*. February 4, 2015. <http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720> (accessed March 17, 2015).
- Mcafee Center for Strategic and International Studies. "Net Losses: Estimating the Global Cost

- of Cybercrime." *Mcafee*. June 2014. <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf> (accessed May 14, 2015).
- McCan, Erin. "10 biggest HIPAA data breaches in the U.S." *Healthcare IT News*. September 10, 2012. <http://www.healthcareitnews.com/slideshow/slideshow-top-10-biggest-hipaa-breaches-united-states> (accessed March 27, 2015).
- McGee, Marianne. "Anthem Refuses Full IT Security Audit." *GovInfo Security*. March 4, 2015. <http://www.govinfosecurity.com/anthem-refuses-full-security-audit-a-7980/op-1> (accessed March 15, 2015).
- Moses, Tim. "Exploiting weaknesses in the MD5 hash algorithm to subvert security on the web." *Entrust, Inc.* January 2009. https://www.entrust.com/wp-content/uploads/2013/05/WP_MD5_Jan09.pdf (accessed April 28, 2015).
- Mueller, Robert. *FBI speeches*. March 01, 2012. https://docs.google.com/spreadsheets/d/1sOP-XOw2CqCeGZ_AsOQaX-lW0xhwiSaLxepW8My5VAs/edit#gid=571759394 (accessed March 15, 2015).
- NDAQ. Anthem, Inc. Stock chart. <http://www.nasdaq.com/symbol/antm/stock-chart> (accessed March 15, 2015).
- Office of National Health Coordinator for Health Information Technology. *Health IT Legislation and Regulations*. February 19, 2009. <http://healthit.gov/policy-researchers-implementers/health-it-legislation> (accessed March 19, 2015).
- Paletta, Damian. *Obama Calls for Tough Legislation to Combat Cyber-Attacks*. January 20, 2015. <http://www.wsj.com/articles/obama-calls-for-tough-legislation-to-combat-cyber-attacks-1421810320> (accessed May 14, 2015).
- Ponemon Institute. "2013 Cybersecurity Salary Benchmarking Report." *Ponemon Institute*. November 19, 2013. <http://www.ponemon.org/library/2013-cybersecurity-salary-benchmarking-report?s=salary> (accessed March 27, 2015).
- Ponemon Institute, LLC. "Fifth Annual Study on Medical Identity Theft." *Medical Identity Fraud Alliance*. February 2015. <http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/> (accessed March 20, 2015).
- Ragan, Steven. *Anthem confirms data breach, but full extent remains unknown*. February 4, 2015. <http://www.csoonline.com/article/2880352/disaster-recovery/anthem-confirms-data-breach-but-full-extent-remains-unknown.html> (accessed March 18, 2015).
- Reardon, Stephanie. "Anthem Data Breach May Impact 8.8 to 18.8 M Non-Customers." *Health IT Security*. February 25, 2015. <http://healthitsecurity.com/2015/02/25/anthem-data-breach-may-impact-8-8-to-18-8-m-non-customers/> (accessed March 15, 2015).
- Redhead, C. Stephen. "CRS Insights. Anthem Data Breach: How Safe Is Health Information Under HIPAA?" *Federation of American Scientists*. February 24, 2015. <http://fas.org/sgp/crs/misc/IN10235.pdf> (accessed March 5, 2015).
- Reisinger, Sue. *Beyond Hacktivism*. July 1, 2015. <http://www.corpcounsel.com/id=1202729633741/Beyond-Hacktivism>
- Roman, Jeffrey. *AGs: Anthem Breach Notification Too Slow*. February 11, 2015.

- <http://www.bankinfosecurity.com/ags-anthem-breach-notification-too-slow-a-7907/op-1> (accessed March 21, 2015).
- Saita, Anne. "Keeping security initiatives on track through executive, management turnover." *TechTarget*. June 2003. <http://searchsecurity.techtarget.com/feature/Keeping-security-initiatives-on-track-through-executive-management-turnover> (accessed March 28, 2015).
- Schwartz, Mathew. "Anthem Breach: Phishing Attack Cited." *Bankinfo Security*. February 9, 2015. <http://www.bankinfosecurity.com/anthem-breach-phishing-attack-cited-a-7895/op-1> (accessed March 28, 2015).
- Skillsoft. "Case Study: WellPoint health insurance provider increases employee satisfaction, retention through e-learning." *Skillsoft.com*. 2010. https://www.skillsoft.com/assets/case-studies/wellpoint_casestudy.pdf (accessed March 28, 2015).
- Stapleton, Tim. "Data Breach Cost." *Zurichna*. 2012. [http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/products/securityandprivacy/data%20breach%20costs%20wp%20part%201%20\(risks,%20costs%20and%20mitigation%20strategies\).pdf](http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/products/securityandprivacy/data%20breach%20costs%20wp%20part%201%20(risks,%20costs%20and%20mitigation%20strategies).pdf) (accessed May 3, 2105).
- The Office of the National Coordinator for Health Information Technology. "Guide to Privacy and Security of Electronic Health Information." *HealthIT.Gov*. April 2015. <http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf> (accessed April 22, 2015).
- Threatconnect, Inc. "The Anthem Hack: All Roads Lead to China." *Threatconnect.com*. February 27, 2015. <http://www.threatconnect.com/news/the-anthem-hack-all-roads-lead-to-china/> (accessed March 8, 2015).
- Transport Canada. *Safety Study on Risk Profiling Air Taxi Sector in Canada*. September 2007. <http://data.tc.gc.ca/archive/eng/civilaviation/regserv/safetyintelligence-airtaxistudy-menu-496.htm> (accessed May 11, 2015).
- Turner, Sean, and Lily Chen. "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms." 2011.
- U.S. Department of Health & Human Services. "For Covered Entities and Business Associates." *US Department of Health & Human Services*. 1996. <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html> (accessed March 25, 2015).
- . "Security Rule Guidance Material." *U.S. Department of Health & Human Services*. March 2007. <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf> (accessed April 10, 2015).
- . "Resolution Agreement between Wellpoint, Inc. and U.S. Department of Human and Health Services." *U.S. Department of Human and Health Services*. July 2013. <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/wellpoint-agreement.pdf> (accessed April 15, 2015).
- . "Health Information Privacy." *US Department of Health & Human Services*. 1996. <http://www.hhs.gov/ocr/privacy/> (accessed April 11, 2015).

- U.S. Department of Justice. "Incident Response Procedure for Data Breaches." *U.S. Department of Justice*. August 6, 2013. <http://www.justice.gov/sites/default/files/opcl/docs/breach-procedures.pdf> (accessed April 11, 2015).
- U.S. Homeland Security Department. "Vulnerability Note VU#836068." *CERT Software Engineering Institute*. December 31, 2008. <http://www.kb.cert.org/vuls/id/836068> (accessed April 10, 2015).
- U.S. Securities and Exchange Commission. "Anthem, Inc. 425 Filing ." *U.S. Securities and Exchange Commission*. January 12, 2004. <http://www.sec.gov/Archives/edgar/data/1156039/000119312504003533/d425.htm> (accessed March 15, 2015).
- Walker, Danielle. "Exclusive: Mandiant Speaks on Anthem Attack, Custom Backdoors Used." *SC Magazine*. February 5, 2015. <http://www.scmagazine.com/anthem-brings-in-mandiant-to-investigate-resolve-breach/article/396749/> (accessed March 10, 2015).
- Wall, J.K. "WellPoint adjust to executive exodus ." *Indianapolis Business Journal*. October 22, 2007. <http://www.ibj.com/articles/print/13440-wellpoint-adjusts-to-executive-exodus> (accessed March 28, 2015).
- Warren, Zach. "Cybersecurity isn't easy, but a strict security focus is necessary." *Inside Counsel*. May 12, 2015. <http://www.insidecounsel.com/2015/05/12/cybersecurity-isnt-easy-but-a-strict-security-focu> (accessed May 15, 2015).
- Watson, Gavin, Andrew Mason, and Richard Ackroyd. *Social Engineering Penetration Testing*. Syngress, 2014.
- . *Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense*. Syngress, 2014.
- Westin, Ken. "Encryption Wouldn't Have Stopped Anthem's Data Breach." *MIT Technology Review*. February 15, 2015. <http://www.technologyreview.com/view/535111/encryption-wouldnt-have-stopped-anthems-data-breach/> (accessed March 20, 2015).
- Williams, Pete. *Anthem, Major Health Insurer, Suffers Hack Attack*. February 4, 2015. <http://www.nbcnews.com/news/us-news/anthem-major-health-insurer-suffers-hack-attack-n300511> (accessed March 16, 2015).
- Yadron, Danny, and Melinda Beck. "Health Insurer Anthem Didn't Encrypt Data in Theft." *The Wall Street Journal* . February 5, 2015. <http://www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560> (accessed April 12, 2015).
- Yaraghi, Niam, and Joshua Bleiberg. "The Anthem hack shows there is no such thing as privacy in the health care industry." *Brookings*. February 12, 2015. <http://www.brookings.edu/blogs/techtank/posts/2015/02/12-anthem-hack-health-privacy> (accessed March 15, 2015).
- Young, Jr., William. "2015 STAMP Workshop STPA-Sec Introduction." Cambridge, 2015.
- Zacks Investment Research. "WellPoint(WLP) Increased Membership Raises Optimism." *Zacks*. September 17, 2014. <http://www.zacks.com/stock/news/147594/wellpoints-wlp-increased-membership-raises-optimism> (accessed March 28, 2015).