Healthcare Management System and Cybersecurity

Ali J. Askar

Abstract: ***The using of Electronic Health Record systems in healthcare organizations has increased in the 21st century to improve the medical services. This leads us to force a rapid increase in cyber-attacks all over the world. In the early 2015, Anthem breach was one of the biggest cyber-attack happened in the healthcare system. In nowadays IT systems have used to be dynamic and complex, the strategies of the cyber security against attacks are still static and ineffective. This paper will analyze the breach of Anthem security to evaluate the weakness of its system by using the guidelines of current cyber security in addition to the Systems-Theoretic Accident Model and Process (STAMP) method.***

Index Terms: Cryptography, Cyber security, Management System, STAMP, Healthcare Management

I. INTRODUCTION

Cybercrime is rapidly growing, and cyber criminals are outsmarting us. In 2014; JP Morgan Chase, Good Will, UPS, Dairy Queen, and Neiman Marcus were all occurred. It seems our society has not learned many lessons from major breaches of Target, Home Depot, and TJ Maxx which occurred in the last 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.

The motivation underlying this paper is to assess cybercrime with a more holistic view and shed light on how to understand these cybercrimes at a deeper level, manage cyber security risks, and mitigate the societal impact using systems thinking. This paper focuses on data security within the Healthcare industry because patients' personal data is the most critical asset we need to secure.

II. LITERATURE REVIEW

This Section is dedicated to literature reviews discussing the most commonly used traditional safety analysis models, such as Chain of Events and the new NIST (National Institute of Standards and Technology) framework. In addition, the System-Theoretic Accident Model and Process (STAMP) will also be introduced.

A. 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 [1]. 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 cyber security 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.

Revised Manuscript Received on June 8, 2019.
Ali J. Askar, College of Engineering, Al-Iraqia University, Baghdad, Iraq. aliasker2@yahoo.com.

B. NIST Framework for Improving Critical

In response to the increase of alarming cyber security breaches in recent years, the President's Executive Order 13636, "Improving Critical Infrastructure Cyber security" (CSF), was issued on February 12, 2013. The goal of this executive order was to increase the cyber security and resilience of critical infrastructure by developing cyber security 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 cyber security 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 cyber security 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 cyber security 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 cyber security 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 cyber security activities within the organization (Table I)

Table 1: NIST Framework Tier Matrix

	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 cyber security 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

(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 cyber security policy within an organization, nor is it a regulation, rather it helps to identify what is missing. Implementation of the cyber security 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.

C. HIPAA, HITECH and Meaningful Use

The Health Insurance Portability and Accountability Act (HIPAA) is the mandatory standard across the healthcare industry passed by the US 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 II:

Table 2: Covered Entities under HIPAA

A. Healthcare Provider	**A Health Plan**	**A Healthcare Clearing House**

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

(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 cyber-attacks, 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.

D. STAMP

System-Theoretic Accident Model and Process (STAMP) is a new accident analysis model based on systems theory and developed by Professor Nancy Leveson at MIT [2]. 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 [2].

E. CAST

Causal Analysis based on STAMP (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 below: -

- Identify the system(s) and hazard(s) linked with the accident or incident.
- Identify the system safety constraints and system requirements associated with that hazard.
- Document the safety control structure in place to control the hazard and ensure compliance with the safety constraints.
- Ascertain the proximate events leading to the accident or incident.
- Analyze the accident or incident at the physical system level 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.
- 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.

- Examine overall coordination and communication contributors to the accident or incident.
- Determine the dynamics and changes in the system and the safety control structure relating to an accident or incident and any weakening of the safety control structure over time.
- Generate recommendations [2].

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.

F. STPA

System Theoretic Process Analysis (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:

- Identifying potential inadequate controls of the system that may lead to one or more hazardous conditions caused by inadequate controls or safety constraints enforcement.
- 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 [2].

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 cyber security. Any changes in control action design over time should be considered, including change procedure management, performance audits, and accident analysis. Figure 1 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 2 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 cyber security 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 cyber security 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.

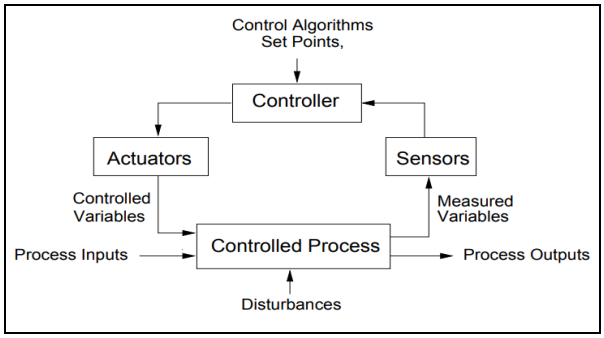

Fig. 1. STPA Control Structure[2]

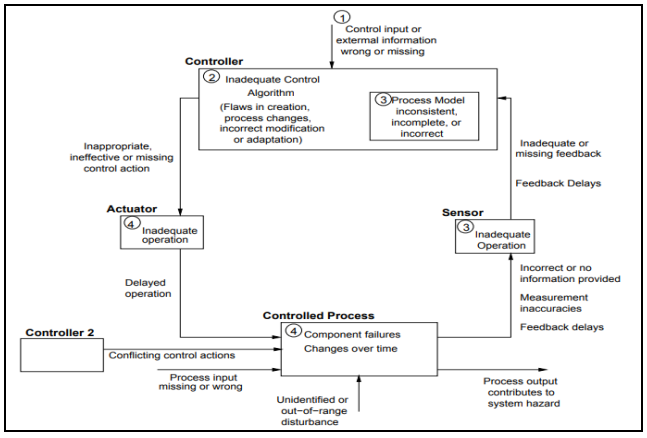

Fig. 2. Causal Factors in STPA [2]

III. ANTHEM BREACH

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 Anthem CEO Joseph R. Swedish [3], 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 [4]. 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.

A. 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 4 the, 2015, stating their database containing 80 million records had been compromised by the sophisticated cyber-attack. As of late February, there was no indication of exfiltrated data or data that had been commoditized [5].

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 [6].

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 [7]. 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 [8]. 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" [9]. 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 [10]. 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 cyber security 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. ISACA'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 cyber security attacks on the target company's key IT security personnel.

B. 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 [11]. InformationWeek reported Anthem has shared with HITRUST keymarkers used in the cyber-attacks, 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 [12]. 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. 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 [13].

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.

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 sub-domains extcitrix[.]wellpoint[.]com, myhr[.]wellpoint[.]com, and hrsolutions[dot]wellpoint[dot]com was created in May 2014. Extcitrix is the subdomain that Athem employees use to connect via Virtual Private Network (VPN). Also, the myhr sub-domain indicates that the motive behind this deception was to make this site look as similar to the legitimate HR internal site as possible.

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 [14].

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. 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.

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. 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 [15].

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.

IV. STAMP-CAST ANALYSIS OF ANTHEM BREACH

In this section, CAST analysis will be used for the Anthem breach investigation. As discussed earlier, 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:

- Identify the system(s) and hazard(s) involved in the loss.
- Identify the system safety constraints and system requirements associated with that hazard.
- Document the safety control structure in place to control the hazard and enforce the safety constraints.
- Determine the proximate events leading to the loss.
- Analyze the loss at the physical system level.
- 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.
- Examine overall coordination and communication contributors to the loss.
- 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.
- Generate recommendations.

A. Defining System Accidents and Hazard

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.

The accident and hazard affecting the Health Insurance Information System can be characterized as one or more of the following types:

Accident: Al. 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 cyber security measures

Since the goal of this thesis is to analyze the effectiveness of cyber security 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.

B. System Safety Constraints and System Requirements

R1. Anthem must protect customers' personally identifiable information from unauthorized access and disclosure.

R2. Anthem must have adequate cyber security in place to prevent, monitor, and detect any cyber security 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:

R4.1 Mitigation plan - Anthem must be able to assess the damage caused by an incident and have steps in place to control the damage.

R4.2 Communication plan - Anthem must report all cybersecurity incidents to a government agency as required (Office of General Inspector, FBI).

C. Hierarchical System Safety Control Structure

It includes a hierarchical system structure, including Anthem's operation and development structure, health insurance regulatory agencies, government, and legislatures. 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.

D. 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 cyber attackers plan or the causal factors may have started well before the accident.

E. Analyzing the Physical Process

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

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.

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 [16].

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 [17]. 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 [18].

F. 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.

1) Information Security Management (Anthem)

a) 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

b) 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

c) 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

d) 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.

2) Operations Management (Anthem)

a) Safety Requirements:

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

b) 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

c) 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.

d) 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.

3) Human Resources (Anthem)

a) 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

b) Unsafe Decisions and Control Actions:

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

c) 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

d) 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

4) Executive Management (Anthem)

a) 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

b) 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

c) 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

d) 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.

5) Health Insurance Industry

a) 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

b) 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

c) 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

d) 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 cyber security

6) Healthcare Regulatory Agencies

a) 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

b) 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

c) Context:

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

d) 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

7) Legislation

a) Safety Requirements:

- Establish effective legislation governing cyber security
- Ensure government and private sector coordination to improve cyber security strategies
- Create a foreign policy to enforce defense against cyber-attacks around the globe
- Prepare mitigation of cyber warfare and large-scale cyber-attacks for public safety and security

b) 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 cyber attacks
- No formal government procedure for sharing and alerting companies of cyber-attack information
- No public training or formal process on cyber warfare

c) Context:

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

d) Process Model Flaws:

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

8) Inadequate Controls and Missing Feedback

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 cyber security first responder program and issuing communication bulletins to its members. It also provides cyber security 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.

9) Dynamics and Migration to a High-Risk State

After experiencing repeated breaches throughout the industry, people quickly forget these incidents and move on. Anthem's stock price dipped briefly right after the announcement of the breach, but quickly recovered its value [19]. Overall, the trend of Anthem's stock price has been steadily increasingly 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.

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 cyber security 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" [20]. This approach often hinders organizations from adopting effective cyber security 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 cyber-attacks. Attackers will quickly change their tactics if one method does not work until they are able to penetrate the system.

V. 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 cyber security 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 cyber-attacks. Second, more focus on cyber security 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.

VI. CONCLUSION

Although current regulations and frameworks provide some guidelines for enterprises on building basic cyber security 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 cyber-attacks and come up with a strategy that will prepare the company to mitigate potential data breach losses. Top management must invest in cyber security 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 cyber security 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.

ACKNOWLEDGMENT

I am indebted to my mother, my late father, and my wife for their continuous love and patience. None of this would have been possible without their encouragement and support.

REFERENCES

[1] Griffin, Thomas, Mark Young, and Neville Stanton. Human Factors Modelsfor Aviation Accident Analysis and Prevention. Ashgate Publishing, Ltd., 2015.

[2] Leveson, Nancy. Engineering a Safer World: Systems Thinking Applied to Safety. Cambridge: MIT PRess, 2011.

[3] Swedish,Joseph. https://www.anthemfacts.com/cyber-attack

[4] https://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html

[5] Barger, Rich. "The Anthem Hack: All Roads Lead to China." ThreatConnect, Inc. February 27, 2015.

[6] http://www.threatconnect.com/news/the-anthem-hack-all-roads-lead-to-china.

[7] Binde, Beth, Russ McRee, and Terrence O'Connor. "Assessing Outbound Traffic to Uncover Advanced Persistent Threat." SANS Institute. May 22, 2011.

[8] https://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf

[9] Hutchins, Eric, Michael Cloppert, and Rohan Amin. "Intelligence-Driven Computer Network DefenseInformed by Analysis of Adversary Campaigns and Intrusion Kill Chains." Lockheed

Martin Corporation. July 31, 2012.

[10] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LMWhite-Paper-Intel-Driven-Defense.pdf

[11] De Decker, Bart, and Andre Zuquete. Communications and Multimedia Security. Springer, 2014.

[12] Watson, Gavin, Andrew Mason, and Richard Ackroyd. Social Engineering Penetration Testing. Syngress, 2014.

[13] Howard, Rick. Cyber Fraud.: Tactics, Techniques and Procedures. Auerbach Publication, 2009.

[14] Walker, Danielle. "Exclusive: Mandiant Speaks on Anthem Attack, Custom Backdoors Used." SC Magazine. February 5, 2015. http://www.scmagazine.com/anthem-brings-inmandiant-to-investigate-resolve-breach/article/396749.

[15] Furht, Borko. Encyclopedia ofMultimedia. Springer Science & Business Media, 2008.

[16] Infosec Insitute . "Scanbox Framework." Infosec Institute. n.d.

[17] http://resources.infosecinstitute.com/scanbox-framework.

[18] 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.

[19] 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.

[20] Turner, Sean, and Lily Chen. "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms." 2011.

[21] Moses, Tim. "Exploiting weaknesses in the MD5 hash algorithm to subvert security on the web." Entrust, Inc. January 2009. https://www.entrust.com/wpcontent/uploads/2013/05/WPMD5_JanO9.pdf.

[22] U.S. Homeland Security Department. "Vulnerability Note VU#836068." CERT Softwaer Engineering Institute. December 31, 2008. http://www.kb.cert.org/vuls/id/836068

[23] NADAQ. Anthem, Inc. Stock chart. http://www.nasdaq.com/symbol/antm/stock-chart.

[24] Westin, Ken. "Encryption Wouldn't Have Stopped Anthem's Data Breach." MIT Technology Review. February 15, 2015. http://www.technologyreview.com/view/535111/encryptionwouldnt-have-stopped-anthems-data-breach

Authors Profile

Ali J. Askar Al-Khafaji is currently working at College of Engineering/Al-Iraqia University, as a Lecturer as well as Head of Registration Office. Experienced in Data Mining, Cyber Security & Web Development from 2008 until now. Currently holds a degree of Master of Computer Science from Pune University, India. Research interest includes Cloud Computing, Data Mining and Cyber Security. Having three Publications in Several Journals. Completed more than sixteen projects and has a vast experience in the field of Computer Programming.