Running head: AN ANALYSIS OF THE ETHICS BEHIND CYBER SECURITY

AN ANALYSIS OF THE ETHICS BEHIND CYBERSECURITY MANAGEMENT

By

ADRIANA BEATRIZ GARZA

_____

A Thesis Submitted To The Honors College

In Partial Fulfillment of the Bachelors degree
With Honors in

Business Administration

THE UNIVERSITY OF ARIZONA

MAY 2016

Approved by:

_____

Dr. Paul Melendez
Department of Management and Organizations

Abstract

This paper will explore cyber breaches, and the ethics behind a company's decision-making when it comes to cyber security. At a time when cyber attacks and breaches against well-known, and reputable companies were at an all-time high, an interest to study different cyber breaches and a company's reaction to the cyber breach began to develop. In order to analyze the various cyber attacks that had taken place in recent years, a case study was completed, examining three different companies in North America that had gone through a cyber attack – Target, Ashley Madison, and Liverpool. Additionally, research of the different types of cyber attacks and the various tactics companies utilize to avoid a cyber attack was conducted. The research was guided by the question of whether Target, Ashley Madison, and Liverpool were ethical in their response that followed their respective cyber breaches. Thus, this paper will discuss the many facets of cyber security most relevant to companies, in addition to an ethical analysis of each company's actions following their respective cyber breach.

Table of Contents

Introduction 4
Question 4
Cyber Attacks Defined 7
Types of Hackers 7
Social Engineering 8
Malware 9
Historical Overview of Cyber Attacks 10
Worms 11
Viruses 11
Credit Card Cyber Attacks 12
Present Day Cyber Attacks 12
Tactics Companies Use to Combat Cyber Attacks 13
Companies in the Cyber Security Industry 16
Methods 18
Questions of Analysis 19
Theoretical Framework 20
Findings 21
Target Cyber Breach 21
Lessons Learned from Target Breach 23
Ashley Madison Cyber Breach 23
Lessons Learned from Ashley Madison 24
Liverpool Breach 25
Lessons Learned from Liverpool Data Breach 25
Ethics of Post-Cyber Breach Actions 27
Discussion 29
Conclusion 31
References 33

Introduction

> *Companies need to make major changes in the way they use computer networks to avoid further damage to national security and the economy. Too many companies, from major multinationals to small start-ups, fail to recognize the financial and legal risks they are taking – or the costs they may have already suffered unknowingly – by operating vulnerable networks.* – Shawn Henry ("Ethical Hacking Defined Against Cyber Attacks")

Organizations across the globe today must contend with the dark side of the cyber world such as cyber breaches, computer viruses and worms, and malicious behavior from employees or outsiders looking to cause destruction on the organization's computer network. While most would agree that technology has improved businesses to create more organization and increase efficiency, it has also come with many challenges. First, companies have to hire technical specialists who can find vulnerabilities in the company's network and fix them; otherwise, the company can lose the consumers' personal data and customers at the hand of a malicious attacker. A popular statement that has been circulating around in recent years is that companies spend millions of dollars on cyber security annually ("Global State of Information Security®"). The landscape of the business industry has changed dramatically, and businesses are ultimately responsible for keeping up with modern technology, especially when it comes to cyber security.

Question

The past few years have been littered with story after story premising a cyber attack against some organization. Cyber attacks are not a new phenomenon; they have existed for about thirty years, and have advanced to frightening new heights in the past decade. Businesses and organizations face different threats than what existed before the digital age, and must be cognizant of the legitimate cyber threats that can occur at any given moment. Target, Ashley

Madison, and Liverpool are some of the companies in North America that know this reality all too well. Many companies recognize the menace that cyber attacks play, and take initiatives to ensure tight cyber security networks, while other organizations tend to gloss over this subject – providing minimal protection. Therefore, the question must be asked – as the occurrence of cyber attacks continues to rise exponentially, are companies, specifically in North America, responding ethically to these breaches by implementing appropriate cyber security measures? By the same token, do companies have a swift and effective response when malicious hackers target them?

The unprecedented number of cyber breaches taking place today is shocking. By and large, businesses believe that implementing the basic forms of cyber security such as passwords, firewalls, and the like are enough to evade cyber attacks. Utilizing these types of cyber security methods, however, essentially allows the hacker with open access to the company's information and data once they can break the passwords or hack their way through the firewalls. (Levine) This notion may be the underlying reason that companies and organizations are the targets of malicious cyber attacks (Levine), and one that is worth looking at in further detail.

Cyber attacks can be costly; companies risk receiving a less-favorable reputation, plenty of negative press, and can expect a host of financial costs. An article published by CNBC, *Here's Why Companies are Still Getting Hacked*, stated that the average cost of each piece of data that is misappropriated varies from $0.58 to $174. The numbers do not include other related expenses such as settlement payments or punitive costs. Following cyber attacks, companies oftentimes take the same route – hire more IT specialists, and increase expenditure on cyber security (Levine). While this strategy appears to be a logical one, "this cycle is reactionary at best and routinely fails to protect an organization's most precious asset – its data" (Levine). In other words, while it is wise to increase cyber security after an attack, a company must proactively find

ways to protect consumer data from rapidly changing cyber threats, not simply the cyber threat that caused the breach. Detailed explanations of stronger cyber security practices that are encouraged are discussed later in this paper. One question that arises from the aforementioned information is: with technology advancing each year and the number of attacks increasing, why are businesses maintaining the same forms of cyber security?

Through this query also comes a discussion of ethics. If businesses realize that the conventional cyber security practices are simply not working as a result of a cyber breach, but do not seek out other methods, does that make their behavior unethical? Companies like Target, Ashley Madison, and Liverpool were all victims of cyber attacks that garnered a significant amount of attention and controversy. Target's attack has been said to be one of the largest data breaches that affected millions of customers. Ashley Madison, an online dating website primarily aimed at those who are married but wish to meet other people, also suffered a cyber attack in the form of a data breach in which the names of its many website users were exposed. Liverpool – one of the most prominent retail companies in Mexico – experienced a data breach as well, though not at the same magnitude as Target and Ashley Madison. The fact that all three companies experienced some type of data breach prompts a question of whether they have adjusted and altered their cyber security practices.

This paper will analyze the various cyber security methods currently employed by most companies, and the lack thereof, along with an ethical analysis from two views – Utilitarianism, and Kantian ethics. Through a case study of Target, Ashley Madison, and Liverpool, coupled with a juxtaposition of the ethical beliefs, this thesis will focus on the steps taken by each company after their respective cyber attack.

Literature Review

Cyber Attacks Defined

In order to fully understand a company's cyber security and their response to a cyber attack, a basic grasp of what a cyber attack is, and the different forms it can take is needed. First, a cyber attack is defined as any infiltration in a computer system or network, and those who carry out cyber attacks are typically called "hackers" (Harris 8). Hackers can use different technical and computer hacking methods to achieve their goal. A few of the primary ways, however, that hackers obtain information or break into a network is by using social engineering and implanting malware on a computer system; how it is used depends on the type of hacker and their motive ("Common Attacks – Security Through Education").

Types of Hackers

For the purpose of this paper, four types of hackers will be defined; they are white hat, black hat, grey hat, and hacktivist hackers. White hat hackers are essentially ethical hackers; their sole purpose for hacking is to provide an organization with relevant and valuable information that can be used to enhance their cyber security. For instance, a white hat hacker will typically find a backdoor to a software program and immediately alert the company that owns the software that there is vulnerability in the program. The company can then use this information to fix the backdoor to prevent future cyber breaches. Black hat hackers, on the other hand, infiltrate into computer systems with malicious intent. The motives behind these hackers are to steal information for their own personal gain or to simply damage the computer network or system. A black hat hacker, then, is someone who finds the vulnerability in the software program, but instead of informing the weakness to the company, might use it for extortion. Grey hat hackers are a little more difficult to identify, hence their name. These types of hackers practice both white hat hacking and black hat hacking tactics. Typically, grey hat hackers will not disclose the information they find like a black hat; however, the grey hat will also not go out

of its way to inform the organization of the vulnerability in the network. Continuing off the previous examples, the grey hat hacker may find the vulnerability in the software, but it will neither inform the company nor use the information for blackmail. In essence, the grey hat hacker does not help the company nor does it try to harm the company. The fourth type of hacker that will be looked at is called a hackitivist. A hacktivitst is a type of hacker who breaches a network to obtain information in order to express a political, religious, or particular social stance. The main motive behind a hacktivist is that he or she wishes to make a statement with the information they find. An example of a hacktivist can be a person who does not agree with an organization's practices, hacks into the organization's network to expose the company in some way, and then bring attention to the issues that the hacktivist is concerned with. As was touched on earlier, hackers tend to use similar tactics to carry out a cyber attack, one of the most common ways hackers do this is through the use of social engineering. ("The thin gray line-CNET")

Social Engineering

According to, *Social Engineering: The Art of Human Hacking* by Christopher Hadnagy, social engineering can be defined as "the act of manipulating a person to take an action that may or may not be in the 'target's' best interest. This may include obtaining information, gaining access, or getting the target to take certain action." Basically, someone uses a combination of psychology and predictions of human behavior to achieve his or her own goals. Social engineering can be used in a variety of careers – business, healthcare, and Information and Technology (IT). Social engineering is especially useful and widely implemented when it comes to sales, and even in the medical field. Doctors use social engineering to persuade patients to take on healthier lifestyles by presenting compelling reasons as to why they should – risk of diabetes, heart disease, and so forth. In the world of IT, social engineering is most often associated with

black hat hackers since it is typically used to extort everyday individuals – a characteristic of a black hat hacker. As the threat of cyber attacks become more frequent, cyber security is becoming much stronger. Therefore, black hat hackers have had to depend more on social engineering to collect sensitive and valuable information. (10**)**

At this point, one could think of a number of scenarios where social engineering has been used in an attempt to gather private information such as bank account numbers, social security numbers, credit card information, and the list could go on. For instance, an email with a touching story seeking financial help is one example where social engineering is used. In this case, the sender attempts to invoke a specific set of emotions so that the receiver responds to the email with the requested information, thereby, using social engineering to acquire the desired information. Social engineering is a very common tactic for any hacker. They depend on human behavior and habits to carry out their strategy. (Hadnagy 13) Though this is a huge way for hackers to get what they want, it is only one piece of executing a cyber attack. There are many other types of exploits that hackers can use such as viruses, worms, Trojan horses, spyware, and other methods in order to extract information or simply cause damage to a computer.

Malware

Viruses, worms, Trojan horses, and spyware fall under the umbrella term, *malware*. A virus, much like a virus in medical terms, can easily spread to other programs and files that are common among other computers. The viruses can cause significant damage by slowing down a computer or even causing the computer to crash, thereby prompting the computer user to lose any data that was stored. A worm, akin to a virus, is able to travel to different computers. (“4 different types of malware: Explained”) The key difference between a virus and a worm, however, is that a worm “doesn’t require the help of a human or host program to spread. Rather,

they self-replicate and spread across networks without the guidance of a hacker or a file/program to latch onto" ("4 different types of malware: Explained"). Trojan horses are frequently used to steal more sensitive information like those related to finances and private data. The last piece of malware that will be examined is spyware. Spyware is also used to steal private information, but more along the lines of credit card data, and passwords. ("4 different types of malware: Explained") Even though malware is most often used in cyber attacks, it only accounts for 60% of these attacks. Many times, a computer operating system or software has what is called a "backdoor" – this is usually what hackers use in the other 40% of attacks. ("CrowdStrike | Next-Generation Endpoint Protection") A backdoor is essentially a loophole in the operating system that gives control to the hacker, allowing them to steal the information they desire. (Harris 92) In any case, each type of malware and hacking technique depends – at least to some degree – on social engineering, especially malware used for extracting information. Without the proper knowledge of what malware is or how the first stages of a cyber attack looks like, the hacker can easily take advantage of the computer user to plant viruses, worms, Trojan horses, spyware, or through the use of backdoors to begin their cyber conquest.

Since its beginnings, cyber attacks have no doubt become significantly more advanced today than ever before. Through the use of the various types of cyber hacking strategies, and other tactics like social engineering, cyber attacks pose a great threat to companies and businesses around the globe. To see how far along cyber attacks have come, a historical analysis of some the most prominent cyber attacks will be discussed.

Historical Overview of Cyber Attacks

Since the advent of the personal computers, cyber attacks were inevitable. The first worm was introduced in the 1980s. This cyber attack was a defining moment in cyber history, as it was

considered one of the very first, large-scaled attacks. **(**"The history of cyber attacks - a timeline") Since then, there have been copious numbers of cyber attacks against well-known companies, and governments around the world have fallen prey to these attacks. From the Morris worm to viruses, and the recent Stuxnet case, and Target breach, cyber attacks have progressively become more complex. The first real cyber threat came in the form of a computer worm discussed in the following section.

Worms

An inquisitive college student, Robert Morris, created the Morris worm in the 1980s. He created the worm using vulnerabilities in the operating system, Unix, in an attempt to discover the vastness of the Internet. A worm basically duplicates itself and travels to other computers allowing it to greatly damage a computer system, often leaving the system useless. Due to the large impact this had on computer users, "Robert became the first person to be tried and convicted under the US' computer fraud and abuse act" **(**"The history of cyber attacks - a timeline"). The Morris worm was one of the first cyber attacks that caused extensive damage, primarily in the United States. The attacks following this incident have evolved to quite advanced viruses and worms. (Julian)

Viruses

The next stage of cyber attacks to hit the world of technology and businesses were viruses during the 1990s. Viruses became a significant issue – both to companies and personal computer users. Ted Julian, an industry analyst for International Data Corporation, states that, "…it became clear that if viruses were to spread from corporate email accounts, questions about the security and integrity of the company could be brought into the public eye." Subsequently, antivirus software was created to help solve the issues of viruses. Though viruses may have

seemed to be of great threat to an organization, the next stage of cyber attacks involved greater exploits – credit cards. (Julian)

Credit Card Cyber Attacks

With viruses and worms still affecting computer users around the globe, cyber attacks became more specific. Hackers began to move their focus to accessing and gaining credit card information from a number of businesses' customers by the early 2000s. Companies and businesses were used to dealing with cyber attacks like viruses; however, many organizations were ill equipped to handle the data breaches that included stolen credit card information. This resulted in an ongoing two-year syndication led by the ringleader in the group of hackers who carried out these attacks – Albert Gonzalez – in which approximately data from 46 million credit cards was appropriated. The information was taken from shoppers of TJ Max, and its international subsidiaries. (Julian) Following the TJ Max incident was Stuxnet.

Present Day Cyber Attacks

Stuxnet has become a notable cyber attack, which resulted in plenty of news coverage as well as several documentaries. In simple terms, Stuxnet was essentially a worm, but it did not exactly play by the same rules a typical computer worm follows – making Stuxnet one of the most infamous viruses to this day. (Zetter) According to an article published by WIRED, Stuxnet "[hijacked] targeted computers or [stole] information from them, it escaped the digital realm to wreak physical destruction on equipment the computers controlled." This unique worm was discovered after various computers in Iran were continually powering off and then restarting (Zetter). Stuxnet was designed to target mainly programmable logic controllers (PLC), and "had the ability to remain dormant within a computer until it realized it was inside a PLC system" (Fleming). Originally, Stuxnet was created to "interfere with Siemens industrial control systems"

("The history of cyber attacks - a timeline"). When Stuxnet reached some of the main computers of a nuclear plant in Iran, "it was able to configure various settings that controlled the nuclear centrifuges and caused them to spin out of control" (Kelly). Stuxnet required the aid of a USB to proliferate through the Siemens network system; therefore, anytime someone plugged a USB into an infected computer, Stuxnet would attach itself to that USB. This resulted in a series of chain reactions, and one that puzzled computer technicians, since they could not find the source of the worm on the infected computers. (Zetter) It is crucial to note the sophistication of Stuxnet. The worm strayed from the original idea of what a worm was capable of doing and trampled over those perceptions. Stuxnet was able to travel from computer to computer in a stealth manner, while rendering the systems it came into contact dysfunctional.

Tactics Companies Use to Combat Cyber Attacks

Businesses and companies have implemented certain cyber security protocols that serve as preemptive strategies against cyber attacks. Some examples include, requiring customers to create a password comprised of a certain number of characters and symbols, numbers, lower-case, and upper-case letters. Organizations also employ a team of IT specialists who are responsible for creating strategies to prevent cyber attacks, and monitoring the company's network and computer systems. External threats however, are not the only attacks that companies should be on the look out for. According to an article published by *Harvard Business Review*, internal threats are just as much a threat as external cyber attacks. Non-employees execute external threats while internal threats are carried out by the employees themselves, and can be just as disastrous due to the amount of information available to them. As a result, companies need to have strategies in place to avert insider threats in addition to external threats.

As far as external threats, companies have already begun to heavily invest in security measures to prevent external cyber attacks. In fact, many companies are coming together to create strategies to avoid these security breaches. According to a survey conducted by Pricewaterhouse Cooper, 91% of organizations have executed a "risk-based" security protocol when it comes to preventing cyber attacks. Two of the most commonly used security strategies are the ISO 27001 and the US National Institute of Standards and Technology (NIST); the two strategies are described as "guidelines [that] enable organizations to identify and prioritize risks, gauge the maturity of their cyber security practices and better communicate internally and externally" ("Global State of Information Security®"). There are a variety of tactics that companies are actively undertaking to follow these standards.

One of the techniques businesses are using, especially those who gather sensitive information, is the use of various authentications as opposed to a password. For instance, some organizations are now using fingerprint scans and even facial recognition technology in order to access certain kinds of data. Other methods companies are using are information sharing and employing a Chief Information Security Officer (CISO). Companies engaging in collaboration say that it "allows them to share and receive more actionable information from industry peers….many also report that information sharing has improved their threat awareness and intelligence" ("Global State of Information Security®"). Partnering and working with other organizations has helped businesses tackle the proliferating issue of cyber attacks. With the increased threat of data breaches and cyber attacks, companies have opted to hire a CISO who specifically handles all issues related to cyber security, and to ensure the safety of private and proprietary information ("Global State of Information Security®").

Employees responsible for handling an organization's data and a plethora of sensitive information have a significant amount of power. With a few simple actions, they can easily access extremely valuable information. Interestingly enough, the majority of companies do not have "adequate safeguards to detect or prevent attacks" (Upton and Creese**)**. The prime reason that companies do not have as many "safeguards" for internal cyber attacks is simply because organizations do not realize the extent of damage these attacks can cause or do not expect these dangers to come from their own employees. More than 80 million internal cyber attacks take place every year in the U.S. The many tactics and strategies that companies have created help to combat external threats; however, they do not hold the same strength when it comes to internal threats (Upton and Creese). Consequently, further measures must be taken to avoid these types of threats.

The best way companies can prevent insider threats is to take a proactive approach in ensuring that employees are not putting sensitive information at risk through the use of USBs, emails, and portable devices. Hackers are easily able to upload viruses onto USBs, which employees will often then plug into a computer (i.e. Stuxnet). Michael Goldsmith, an associate director of Oxford's Cyber Security Centre asserted, "The best way to get into an unprepared company is to sprinkle infected USB sticks with the company's logo around the car park." Cellphones and tablets are widely used now on the job, therefore, companies should be sure to communicate the cyber risks associated with using these devices since the majority of these devices are vulnerable to malware. Furthermore, companies are recommended to train employees regularly and inform them of how to recognize threats and how to better complete tasks in regards to cyber safety. Though several companies already practice protocols protecting against

internal threats, not enough companies are cognizant of internal cyber risks and lack adequate security for these specific attacks (Upton and Creese).

Companies in the Cyber Security Industry

Many companies have come up that have changed the landscape of cyber security in the business world. Technology has completely changed the way businesses operate. With programs and systems like cloud computing technology or online records, businesses have found it easier to utilize these kinds of resources to aid in organizing and keeping information structured and easily accessible. Unfortunately, the dark side to the increase in technology is the amount of data that can be exposed or exploited by hackers. Through the high occurrence of cyber attacks in the past few decades, especially in the last few years, many companies have been created that specialize in cyber attacks. There are some that exist in the grey area, and sell coding that takes advantage of weaknesses in a particular software or computer system called zero day vulnerabilities. Zero day vulnerabilities are "unknown flaws for which no defense has been built. (The target has had 'zero days' to prepare for the attack)" (Harris 94). Others, however, strive to help companies strengthen their cybersecurity by finding flaws in the company's computer system and then fixing the vulnerabilities. Examples of such companies include: Vupen, Endgame, and Crowdstrike. (Harris 96, 104, 108)

Vupen specializes in selling zero day vulnerabilities to a variety of organizations, including governments. In fact, the NSA has been known to procure a number of the zero day vulnerabilities Vupen markets. Although the company claims that they only sell these codes to reputable organizations, there is a concern about the vulnerabilities falling into the wrong hands. Businesses like Vupen, though intently helpful, can also inadvertently cause cyber damage to a company. (Harris 96-97) Companies that are most at risk involve: "electrical power plants,

nuclear facilities, natural gas pipelines, and other critical infrastructures, including banks and financial service companies" (Harris 98). These companies are often the most frequently targeted organizations for cyber attacks and a company with a gamut of codes that expose vulnerabilities in the network of these businesses elevates the level of cyber threats the business can receive. Another company that is similar to Vupen is Endgame.

Endgame has a comparable model to Vupen in that it too sells zero day vulnerabilities; however, the company goes a bit further by providing specific locations of vulnerable computers through its exclusive program known as Bonesaw (Harris 103). Forbes describes Bonesaw as a "Google maps for hackers. With a few clicks a user can zero in on a computer and see its vulnerabilities along with a list of publicly available techniques to hack it." (Greenberg). As one can imagine, this tool poses a myriad of serious threats to any company. Though, the majority of Endgame's customers are government entities, the idea that a tool like Bonesaw exists, shows just how vulnerable computers and networks are now. Recently, Endgame has dramatically changed its business model, and has now shifted towards providing a proprietary software tool that collects data, and works with Endgame's software to find potential cyber risks. The company, however, is still engaged in business practices that fall into the grey area. (Greenberg) Though companies like Vupen and Endgame are not directly carrying out cyber attacks, they essentially are supplying any subscriber with the resources and tools needed to execute the attacks themselves. On the other side of the spectrum, are companies that position themselves to directly help businesses design a more robust cybersecurity like Crowdstrike.

Crowdstrike provides products and services that focus less on malware cyber security and more on the entry points of cyber attacks. The company also offers services to assist other business in responding to cyber breaches. According to their official website,

> Protecting endpoints [is] critical, because that is where the data resides in any organization…To collect endpoint data…we designed an extremely lightweight sensor that could be deployed rapidly and seamlessly across even the largest customer environments…by employing a cutting-edge Graph Data Model in the cloud, we could look at billions of individual endpoint events simultaneously and analyze them in real time…to spot anomalies, identify patterns, and prevent attacks ("CrowdStrike | Next-Generation Endpoint Protection").

Companies like Crowdstrike are becoming more prevalent, as the demand for these types of services are increasing and even becoming a requirement. In this day and age, the idea of a data breach is no longer simply a hypothetical scenario, but a reality. Crowdstrike, and companies analogous to it, have developed new strategies especially made for today's cyber security issues. As cyber attacks become increasingly more intricate, the security measures and strategies have to change as well. ("CrowdStrike | Next-Generation Endpoint Protection")

Methods

Analyzing the ethics behind a company's cybersecurity strategies required a qualitative case study of three large companies in North America that were the targets of cyber attacks within the last two years. Following a framework explained in the book, *Qualitative Research Methods for the Social Sciences*, by Bruce L. Berg, organizations were chosen as the units of analysis. Utilizing an exploratory approach to the case study, research was conducted on various companies in North America that had been victims of cyber attacks. Ultimately, this led to a more explanatory case study, and a utilization of content analysis – defined as "any technique for making inferences by systematically and *objectively* identifying special characteristics of messages" (Berg 267). Through content analysis, a pattern was found among the cyber attacks

that all three companies encountered; those companies were: Ashley Madison (Canada), Target (United States), and Liverpool (Mexico). All three experienced a cyber security breach in which consumer data was put at risk, resulting in negative press and additional costs for the companies.

Given that there have been a host of cyber attacks and breaches against numerous companies around the world, I decided to narrow my focus on companies specifically in North America. My primary goal consisted of analyzing whether the companies were ethical in their response to the cyber attacks, and in their proactive cyber security tactics in general. To understand the various cyber security strategies, an investigation of the most relevant cyber attacks that pertained to the case study was carried out, in addition to the variety of tactics that organizations implement, or are encouraged to implement. Furthermore, looking at three different companies allowed for a closer examination if the behavior regarding cyber security was exclusive to one organization, or if the behavior was consistent across the board – thereby representing similar large organizations around the world.

Questions of Analysis

To begin the case study, I first organized a list of questions that I would apply to each company I researched. They are as follows:

- What type of cyber attack did each company experience?
- How did the company respond after the cyber attack was discovered?
- Why did this attack occur?
- How did this attack occur?
- What cyber security methods were in place before the cyber attack?
- How much did the attack cost the company?
- How was the company affected as a result of this cyber attack?

- What did the company learn?
- How is it applying the lessons learned?

Using these questions laid the groundwork for analyzing the different aspects of cyber security, and later using those questions to evaluate the ethical behavior of the company when it comes cybersecurity. After creating an outline of study questions (Berg 257) two ethical views were selected that served as the theoretical framework for analyzing the ethics of companies' decision-making regarding their cyber security after the cyber attacks.

Theoretical Framework

The next step in the case study of Ashley Madison, Target and Liverpool, involved a qualitative research approach in which an analysis was done of the different ethical views that are frequently applied to businesses– normative ethics. After probing the many ethical standpoints that are most often used in a business setting, an evaluation was needed for the situation of each company through the lens of utilitarianism, and Kantian ethics. Examining the views of each ethical perspective allowed a more overarching analysis of the ethics when it comes to cyber security, and one that would eliminate biases when evaluating the choices for each company's strategy in protecting their respective computer networks.

In essence, the research used a combination of an exploratory and explanatory case study, and the use of content analysis to find patterns among the units of analysis. Following the decision to taper the focus to the three organizations, Target, Ashley Madison, and Liverpool, qualitative research was used, relying on latent content analysis – or "interpretive reading" (Berg 273). The cyber security tactics that were mentioned in the literature review, along with the strategies that each company employed after the cyber data breaches, were examined, and then compared to the two preceding ethical theories, and codified cyber security standards.

Findings

For this section of the paper, information regarding the cyber attack on each company will be given, as well as their cyber strategies they had in place before the attack, and their response to the cyber breach. The questions listed under the *Methodology* will be applied to each company as well, and will be used as guide in analyzing Target, Ashley Madison, and Liverpool. Furthermore, the concepts for utilitarianism, and Kantian ethics will be defined, explained, and juxtaposed with the actions of each company – post-cyber breach.

Target Cyber Breach

In 2013, the second largest retailer suffered one of the most extensive cyber attacks in history. With an attack affecting well over 40 million customers – jeopardizing private information – it was a highly publicized event. In the following days, scrutiny over Target's cyber security procedures and response plan took place, and nearly one-hundred lawsuits were filed, eventually leading up to the resignation of Target's CEO at the time. Though several cyber attacks have surpassed Target's cyber scandal in recent months, and even the past few years, it undoubtedly marked a new era of cyber security issues concerning credit cards.

Before the cyber attack ensued, Target had implemented a new cyber security program – one that had been notably used by government agencies across the globe. The program is known as FireEye, and was immensely effective in detecting sophisticated malware. Though Target met all cyber security standards held for retailers, the company went a step further in ensuring the security of its customers, especially during the holiday season – a time marked by high sales volumes and transactions. While FireEye detected an anomaly in Target's server, the security team did not act on this discovery. The hack was not unique, or original, in and of itself;

however, due to the absence of communication between the cyber security team and management, the hackers succeeded in their ruse. (Riley, Elgin, & Matlack)

Essentially, the hackers were able to steal customer credit card information by breaking into Target's server, most likely through one of Target's vendors. After the hackers found their place in the network, they were then able to plant the malware on Target's payment systems and extract customer data from there. The hackers, at that point, began transferring the data where "the malware was designed to send data automatically to three different U.S. staging points, working only between the hours of 10 a.m. and 6 p.m. Central Standard Time. That was presumably to make sure the outbound data would be submerged in regular working-hours traffic." (Riley, Elgin, & Matlack) The cyber attack occurred towards the end of November, but it was not until mid-December that Target issued a public statement, after Federal authorities informed them of the attack. Soon after, Target was inundated with lawsuits, fees, and its fair share of news coverage.

Shortly before Christmas of the same year, Target reported a 3-4% decrease in sales for the final weekend before the holidays. After further investigation of the cyber attack took place, Target confirmed that another 70 millions customers where affected. According to the Consumer Bankers Association and Credit Union National Association, the breach cost Target around $200 million; Target then committed to investing $100 million to revamp their cyber security systems, and incorporate the "chip-and-pin" technology, that has now been implemented throughout many retailers. (Clark) The CEO, Gregg Steinhafel, stepped down in May 2014, and a new chief executive officer was hired on. There are several key takeaways that are explained in the following paragraphs.

Lessons Learned from Target Breach

First, there is a lesson of communication. Due to the fact that there was a disconnect between the security department and higher management, Target looked to replace the CIO with someone who would create a more unified channel of communication. Second, it is clear that the retailer giant felt that their cyber security technology required an update, as they invested a large amount of capital to fund more advanced security. Another lesson learned, is the issue of response time. Many outlets suggested that the time between the attack and Target confirming the attack was too long. Therefore, one could say another lesson for Target is creating a greater and faster response strategy. (Burg) One question to ponder is: nearly three years later, has Target acted ethically in its reaction to the attack?

Ashley Madison Cyber Breach

Perhaps one of the largest, and most infamous cyber breaches spoken about in 2015 was the case of Ashley Madison, and similar websites under the parent company, Avid Life Media. The dating website, faced a massive data leak – one of the largest ever to take place – in July 2015. In the wake of this breach, one could imagine the uproar this unique situation ignited. The cyber attack revolved around customer data collection and storage, and affected over thirty million users.

To this day, it is not known who hacked into the database storing all of Ashley Madison's customers' information, other than they by the alias, Impact Team. Originally, the group was thought to have been a team of hacktivists, but the description has since been dropped once the hackers began to blackmail many of the website's users – portraying more black hat qualities. Ashley Madison used what has been described as one of the strongest password encryption strategies to protect their customers' accounts – one that would require years to break through. The strategy the company utilized is called bcrypt; this method muddles passwords into a

hodgepodge of different letters, numbers, and symbols. The cyber issue, however, came about at a later time when Ashley Madison reorganized the way it stored the accounts, and the matching passwords. ("Flaws found in Ashley Madison password protection") Ultimately, the new method of caching the passwords "stripped away the protection bcrypt bestowed on passwords" ("Flaws found in Ashley Madison password protection"). As a result, hackers had the ability to crack the various account passwords and gain access to user information, eventually publishing the information onto the Internet. In the preceding months, Ashley Madison and its parent company, Avid Life Media, had to face off rumors of suicides linked to the breach, lawsuits, and exploitation from the hackers. Moreover, private emails of employees were exposed through the different data dumps. The users also dealt with "scammers and extortionists" (Bisson). Several pieces of advice can be taken from the breach Ashley Madison went through.

Lessons Learned from Ashley Madison

One of the main points that came out of the Ashley Madison ordeal concerned the protection of passwords. An article published through Forbes online, asserted that companies, including Ashley Madison should take steps to "make security a priority, and get involved with [a] security provider (if not internal) to understand how it works and how [to] better secure…systems" (Basu). While the author of the article acknowledged that companies like Ashley Madison are highly susceptible to attacks by hacktivists, there are actions that can be taken to "mitigate the risk of a successful 'hacktivist' attack." In sum, the two fundamental lessons that can be directly pulled from this particular breach are: actively testing password encryptions, and reducing the impact hackers can have on breaking into the organization's network.

Liverpool Breach

Liverpool is one of the primary retailers and purveyor of credit cards in Mexico, and experienced a data breach in 2014. Though seemingly a fraction in comparison to the other cyber breaches, it speaks volumes about the nature of cyber attacks that occur in Mexico. Most cyber attacks against Mexican companies represent a small percentage of global cyber breaches, and the hacks mostly happen to smaller institutions. It is also important to note that there is less publicized information regarding Liverpool's cyber breach due to different cyber and privacy laws in the country. Nonetheless, there are a few details regarding the cyber attack on Liverpool.

In December 2014, Liverpool notified its customers and the public that it had experienced a cyber attack. Over three hundred thousand consumers were directly affected, as credit card numbers and other personal information was accessed. The breach was estimated to cost over $1 million U.S. dollars. The hacking group, by the name of "SicKillers", was found responsible for the hack in an "extortion" scheme ("Radiografía del Hackeo a Liverpool"). The company released a statement once the Mexican Stock Exchange (Bolsa de Valores) discovered the data breach. Other stakeholders included employees of Liverpool and higher management, whose emails were leaked. Details on the aftermath remain unclear, though Liverpool did express that it was increasing its cyber security and employing other measures to secure the information of consumers and employees.

Lessons Learned from Liverpool Data Breach

The Liverpool cyber breach was one of the biggest reported in Mexico. According to an article through PricewaterhouseCoopers called, *Cybersecurity in Mexico*, "the main obstacles to fight cybercrimes in Mexico are the constant lack of legislation to act immediately, the poor resources the police has to act, which effect the research and cause the lack of awareness among the society about cybersecurity." Thus, one glaring lesson from the Liverpool hack is one of

awareness. Even though the United States is one country that is frequently a main target for cyber attacks, the breach on one of the biggest companies in Mexico proves just how serious and prominent cyber crimes are becoming. Smaller companies are usually the primary targets in cybercrimes in Mexico (PricewaterhouseCoopers); therefore, larger companies in Mexico should evaluate their cyber defenses to ensure the safety of their consumers as well. Cyber attacks occur often in the country, albeit, not to the degree of those in the United States, or even Canada, as seen in the case with Ashley Madison. Nevertheless, organizations in Mexico should remain cognizant of the cyber threats that exist, and the advancement of certain cyber crimes.

Ethical Views Briefly Defined

Utilitarianism originated from Jeremy Bentham and John Stuart Mill, and holds the belief that "actions that provide the greatest amount of good over bad or evil are ethical or moral choices" (Carle). An example of Utilitarianism is given by a simple example of lying. If someone told a lie to help another person, and it brought more good than harm, then the actions of the person who lied would be viewed as ethical. Kantian ethics focuses on a more codified standard of behavior.

Kantian ethics, formed by the enlightened thinker, Immanuel Kant, believes that everyone should follow a standard code of conduct. For instance, under Kantian ethics, one has certain rights they can exercise, and rights that should not be imposed on such as, safety, privacy, and others. Kant also held that this standard of ethics should be universal, and that if the same criterion cannot be applied for everyone else, then the actions are considered unethical. For instance, using the lying example, Kant would assert that if lying was universally accepted, the action would be seen as ethical; on the other hand, if lying was only acceptable when committed by some, then the action would be viewed as unethical. ("Kantian Ethics") The third ethical view

that will be evaluated is virtue ethics. The following table organizes the ideas of Utilitarianism and Kantian ethics, and includes examples of their application to the three companies.

	Utilitarianism	**Kantian Ethics**
Brief Overview	Results-based	Duty-based
Description	An action is ethical if it brings the most amount of good or happiness for the largest number of people	An action is ethical if it can be applied universally, and does not infringe on certain rights that people hold.
Examples from Target	• Replaced CIO and CEO • Increased funds for tighter cybersecurity measures • Acted in the majority of stakeholder's best interest	• Investing in stronger cybersecurity coupled with the restricting of its executive board, Target exercised its duty to ensure that consumers would have greater protection moving forward
Examples from Ashley Madison	• Hired on a team of IT specialists following the cyber attack to address and repair vulnerabilities • Acted on behalf of the majority of stakeholders by ensuring consumer privacy	• Ashley Madison has a duty to keep consumer information private, and after the breach the company took steps to build up its password protection security
Examples from Liverpool	• Liverpool's actions are deemed unethical since the company has not established any concrete plans to heighten its cybersecurity	• Liverpool has a responsibility to its stakeholders to increase cybersecurity and make sure that the breach does not happen again. As of late, there have been no visible changes

Ethics of Post-Cyber Breach Actions

Since its breach in 2013, Target has allocated more funds to increase its cyber security, and restructured its upper management team – with the replacement of its CIO and CEO. Based off the theory of Utilitarianism, Target responded ethically by acting in the best interest of the

majority of its stakeholders, and prospective Target customers. In terms of Kantian ethics, it also acted ethically – it would be agreed that investing more resources to a cyber security team is a universally accepted response in the wake of such an extensive breach. Target expressed on numerous occasions that it strove to put its customers first, and regarded the safety of their consumers' information as a high priority. This was illustrated in the way it reorganized its executive management after the data breach. Through this restructuring, Target showed that it was adamant about keeping consumers safe and ensuring that the leaders of the organization best represented the values and goals Target sought to establish, especially after the attack.

While Ashley Madison went through the most controversial cyber hack, the cyber security implemented after the data breach was not as strong as many thought it would be post-cyber breach, according to a variety of sources. Specifically, an article through CBC news reported that the massive effect that Ashley Madison went through during the cyber breach scandal has faded, and that "there's no evidence the company has actually changed its protocols" (Loriggio). However, the company has worked with IT specialists to "close the unauthorized access points" (Loriggio). Using Utilitarianism as a lens, Ashley Madison does appear to be performing ethically, ensuring that their once existing vulnerabilities are no longer an issue, and seeking external help to increase it security for its growing customer base. Similarly, the company's actions appear ethical under Kantian ethics – with the increasing number of members joining the site because feel that their information is secure now. Also, the company has taken steps to make sure that they fixed their vulnerabilities, a strategy that is universally viewed as behaving ethically – protecting consumer data.

Since its cyber hack in 2014, Liverpool has remained quiet on any new cyber security measures. Akin to the situation of Ashley Madison, there is no clear indication that Liverpool has

implemented new cyber strategies for protecting information. Within the beliefs of a Utilitarian approach, Liverpool's actions seem unethical in that there have not been blatant changes in the cyber security systems, or even results from an investigation of how the information was taken. In essence, the actions Liverpool has carried out after the cyber attack does not bring a lot of benefit to the majority of its stakeholders. From a Kantian ethics perspective, the actions go against the belief system as well. Applying the same behavior of Liverpool after the cyber breach would create a sense of dishonesty between a company and its stakeholders for most companies. While Liverpool's actions could be considered ethical under the Kantian belief that people have the right to privacy, Liverpool is indeed keeping the issues tightly concealed ("Radiografía del Hackeo a Liverpool"). Regardless, because the set of actions cannot be applied universally without some concerns, Liverpool's actions are considered unethical under the premise of Kantian ethics.

Target, Ashley Madison, and Liverpool all faced scrutiny in the weeks and months following their cyber breaches. It was imperative to look at a few ethical views when analyzing a company's actions to impartially evaluate and determine whether the company is remaining responsible to its stakeholders after a data breach. Some ethical views considered the company's actions ethical, while others showed that the company was unethical in its response to the cyber breach. The findings also shed light on the cultural differences when it comes to the perception of cyber security and raised other questions regarding the future of cyber security.

Discussion

Information technology and cyber security was once viewed as an arcane topic – one that was only discussed by those with a strong interest in it or by professionals in the field. Through an analysis of various cyber attacks, defense strategies, and the cyber breaches that three major

companies experienced, one major question arose. The first one is whether there is a different cyber defense approach that companies categorically fall into and what this looks like. A recent model published through Deloitte Center for Financial Services Analysis, shed light on the type of cyber security approaches organizations typically practice – secure, vigilant, and resilient ("Transforming Cybersecurity").

Using a *secure* approach is essentially meeting the standards required for cyber security. A *vigilant* strategy requires more action on the company's part by increasing awareness of cyber threats and putting in place safeguards for potential cyber breaches. The final strategic approach, *resilient* "requires investment in traditional technology-based redundancy and disaster recovery capabilities, [and] the bigger picture includes a broad set of crisis management capabilities" ("With Cyber Risk, Secure, Vigilant and Resilient Are the Watchwords"). In a resilient approach, companies proactively test their security systems, and have plans in place to execute immediately after a cyber attack. In some ways, this method models a militaristic approach to combating cyber crime. The figure below illustrates where Target, Ashley Madison, and Liverpool fall under the above-mentioned strategies.

	Secure	**Vigilant**	**Resilient**
General Description	Meets cyber security standards and regulation. Implement preemptive strategies for common cyber attacks.	Builds off a secure strategy, but raises awareness for potential cyber attacks	Expands off of secure and vigilant strategies while regularly improving cyber security with the advancement of technology to prepare for possible newly developed cyber attacks.

Company Example	**Liverpool** - Met country standards for cyber laws - No other strategies to prevent more advance attacks were evident **Ashley Madison** - Met Canada's regulations for cyber security - Though advanced cyber security was used to protect passwords, company ultimately discontinued its use	**Target** - Implemented advanced cyber security software designed to detect sophisticated malware - Did not carry out frequent updates, tests, or communications between security team and management	

With Deloitte's description of the three main cyber defense strategies companies can take, it is important for companies to realize where they stand, and especially how their actions are viewed in the days, weeks, months, and even years after a cyber attack. The cyber attacks discussed in detail earlier in the paper are what most companies are prepared for and guarded against. Unfortunately, this means that when a much more advanced cyber breach does occur, the majority of companies are not well prepared to immediately respond to the attack. In turn, this can affect company's sales volume, and drive cautious consumers away. Today, the world is advancing at an incredibly fast pace, and the general culture is beginning to change as well.

Conclusion

The majority of people now have access to more information than ever before, and there is a growing concern for privacy and the ethics behind cybersecurity. For example, one contemporaneous issue germane to the topic of cybersecurity is the case of Apple and the company's refusal to provide the FBI with information of how to hack into an iPhone for

security reasons. The hot topic has had a tremendous response and indisputably brings the conversation back to the responsibility a company owes to its customers, and protecting consumer information. As technology continues to advance exponentially, there are a few key questions to contemplate. Will companies move towards a more resilient approach? How long before companies start abandoning the secure approach, and start adopting a more militaristic approach? To what extent should companies be allowed to practice a militarized cybersecurity strategy? In other words, should companies have the authority to counterattack, or strictly defend their networks? With the evolution of cyber attacks, and malware, cyber security will continue to spark conversations about the ethics and the responsibility a company has to its stakeholders and customers in an expanding digital world.

References

Basu, E. (2015, October 26). Cybersecurity Lessons Learned From the Ashley Madison Hack. Retrieved February 20, 2016, from http://www.forbes.com/sites/ericbasu/2015/10/26/cybersecurity-lessons-learned-from-the-ashley-madison-hack/#4626547aed99

Berg, B. (2001). Qualitative research methods for the social sciences (4th ed.). Boston, Massachusetts: Allyn and Bacon.

Bisson, D. (2015, September 01). The Ashley Madison Hack -- A Timeline. Retrieved February 15, 2016, from http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-ashley-madison-hack-a-timeline/

Burg, N. (n.d.). Five Lessons for Every Business From Target's Data Breach. Retrieved January 25, 2016, from http://www.forbes.com/sites/sungardas/2014/01/17/five-lessons-for-every-business-from-targets-data-breach/#775fedbc202b

Carle, Scott. (2003). Crossing the Line: Ethics for Security Professional. Retrieved March 1, 2016, from https://www.sans.org/reading-room/whitepapers/hackers/crossing-line-ethics-security-professional-890

Clark, M. (2014). Timeline of Target's Data Breach And Aftermath: How Cybertheft Snowballed For The Giant Retailer. Retrieved January 17, 2016, from http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056

Common Attacks - Security Through Education. (2015). Retrieved October 17, 2015, from http://www.social-engineer.org/framework/general-discussion/common-attacks/

CrowdStrike | Next-Generation Endpoint Protection. (2015). Retrieved from

http://www.crowdstrike.com

Ethical Hacking Defend against Cyber Attacks. (2014). Retrieved November 1, 2015, from http://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/crs/CY_Risk_EthicalHackingServicesFlyer_Noexp.pdf

FactSheet. (n.d.). Retrieved March 1, 2016, from http://www.elpuertodeliverpool.mx/eng/docs/FactSheet.pdf

Flaws found in Ashley Madison password protection - BBC News. (2015, September 11). Retrieved November 06, 2015, from http://www.bbc.com/news/technology-34221863

Fleming, R. (2010, December 2). Bits before bombs: How Stuxnet crippled Iran's nuclear dreams. Retrieved October 22, 2015, from http://www.digitaltrends.com/computing/bits-before-bombs-how-stuxnet-crippled-irans-nuclear-dreams/

Greenberg, A. (2014, March 3). Inside Endgame: A Second Act For The Blackwater Of Hacking. Retrieved October 22, 2015, from http://www.forbes.com/sites/andygreenberg/2014/02/12/inside-endgame-a-new-direction-for-the-blackwater-of-hacking/

Global State of Information Security® (2015). Turnaround and transformation in cybersecurity : Key findings from The Global State of Information Security® Retrieved from PricewaterhouseCoopers: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html

Hadnagy, C. (2010). Social engineering: The art of human hacking. Indianapolis, IN: Wiley Publishing.

Julian, Ted. "Defining Moments in the History of Cyber-Security." *Infosecurity Magazine*. N.p.,

04 Dec. 2014. Web. 10 Oct. 2015. <http://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/>.

Harris, S. (2014). @WAR: The rise of the military-Internet complex. New York, New York: Houghton Mifflin Harcourt Publishing Company.

Kantian Ethics. (n.d.). Retrieved March 01, 2016, from http://www.csus.edu/indiv/g/gaskilld/ethics/Kantian Ethics.htm

Kelley, M. (2013, November 20). The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. Retrieved October 22, 2015, from http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

Levine, K. (2015, November 4). Here's why companies are still getting hacked. Retrieved November 5, 2015, from http://www.cnbc.com/2015/11/04/cybersecurity-heres-why-companies-are-still-getting-hacked-commentary.html

Loriggio, P. (2015, December 25). AshleyMadison hack fails to spur cybersecurity overhaul. Retrieved February 25, 2016, from http://www.cbc.ca/news/business/ashleymadison-hack-web-security-1.3380372

PricewaterhouseCoopers. (2015, June). Cybersecurity in Mexico. Retrieved February 25, 2016, from https://www.pwc.com/mx/es/knowledge-center/archivo/20150917-kc-cybersecurity.pdf

Radiografía del Hackeo a Liverpool | Última Palabra. (2015, January 10). Retrieved February 25, 2016, from http://www.ultimapalabra.mx/radiografia-del-hackeo-a-liverpool/

Riley, M., Elgin, B., & Matlack, C. (n.d.). Target Missed Warnings in Epic Hack of Credit Card Data. Retrieved January 05, 2016, from http://www.bloomberg.com/bw/articles/2014-03-

13/target-missed-alarms-in-epic-hack-of-credit-card-data#p2

The history of cyber attacks - a timeline. (n.d.). Retrieved October 2, 2015, from http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

The thin gray line - CNET. (n.d.). Retrieved October 29, 2015, from http://www.cnet.com/news/the-thin-gray-line/

Transforming Cybersecurity. (2014, February). Retrieved March 1, 2016, from http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/dttl-fsi-TransformingCybersecurity-2014-02.pdf

Upton, D., & Creese, S. (2014, September 1). The Danger from Within. Retrieved October 17, 2015, from https://hbr.org/2014/09/the-danger-from-within

Velasquez, M., Andre, C., Shanks, T., S., & Meyer, M. (2015, August 1). Thinking Ethically. Retrieved March 01, 2016, from https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/thinking-ethically/

With Cyber Risk, Secure, Vigilant and Resilient Are the Watchwords - Deloitte Risk & Compliance - WSJ. (n.d.). Retrieved March 01, 2016, from http://deloitte.wsj.com/riskandcompliance/2014/08/25/with-cyber-risk-secure-vigilant-and-resilient-are-the-watchwords/

Zetter, K. (n.d.). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Retrieved October 11, 2015, from http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

4 different types of malware: Explained. (2015, July 22). Retrieved October 11, 2015, from http://www.techadvisory.org/2015/07/4-different-types-of-malware-explained/