Are Ethical Hackers the Best Solution for Combating the Growing World of Cyber-Crime?

by

Devin Marsh

A thesis presented to the Honors College of Middle Tennessee State University in partial fulfillment of the requirements for graduation from the University Honors College

Spring 2017

Are Ethical Hackers the Best Solution for Combating the Growing World of Cyber-Crime?

by
Devin Marsh

APPROVED:

_____
Charles Apigian
Chair, Computer Information Systems

_____
Meredith Dye
Sociology and Anthropology

_____
Dr. John Vile
Dean, University Honors College

Table of Contents

Chapter 1: Introduction

Cyber-crime has become one of the top threats for government agencies, large corporations, and select individuals. Certain information, such as credit card numbers and identities are stolen regularly. What allows such information vulnerability in a world where everyone feels so secure? The answer is the information super-highway, which can be easily accessed through any computer, tablet, or cellphone, better known as the Internet. According to Dictionary.com, the Internet can be defined as, "the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link billions of devices worldwide ("Internet")." The protocol suite TCP/IP is "the basic communication language or protocol of the Internet (Rouse, 2008)."

The people responsible for the theft of previously mentioned information are better known as computer hackers, specifically black-hat hackers. What is a black-hat hacker? According to PCTools.com, "A black hat hacker is an individual with extensive computer knowledge whose purpose is to breach or bypass internet security ("Black Hat Hackers")." Black-hat hackers are responsible for attacks on large corporations such as Target, where 40 million customer-credit card numbers were compromised in November of 2013 (Krebs, 2014), and Home Depot where 56 million-customer-credit cards were compromised in September of 2014 (Sidel, 2014).

What do companies do in order to prevent such powerful threats to not only the company itself, but also the customers of such companies? Some corporations rely solely on regular password rotation, by making employees change passwords on a regular basis. Other companies install extra firewalls to prevent malware from penetrating into the system. A large majority of

corporations have hired an IT Security department in order to monitor and prevent malicious threats. Another way to prevent black-hat attacks, is to hire a white-hat hacker.

A white-hat hacker is, “Internet slang referring to an ethical computer hacker, or a computer security expert, who specializes in penetration testing and in other testing methodologies to ensure the security of an organization's information systems (Rouse, Cobb, 2014).” It seems hard to believe that there can be a such thing as an “ethical hacker” considering the derogatory terms associated with the word, “hacker.” According to the EC-Council, the organization in charge of the training and certification of Ethical Hackers said, “To beat a hacker, you have to think like a hacker.” The training to become an ethical hacker includes learning about systems penetration testing. Penetration testing is, “the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit (also known as pen testing) (Gershater, Muheta, 2011).”

Are ethical hackers the best solution for combating a growing world of cyber-crime? There are differing beliefs throughout the information technology community that favor both sides of the discussion. However, the importance of data security differs based on the differing focuses of the individual businesses. The goal of this paper is to determine if companies are more secure hiring ethical hackers rather than just trying to use software, password updates, and an IT security department. In order to accomplish this, IT professionals were surveyed within the Middle Tennessee area who work in different types of businesses (healthcare, retail, etc.). Research was also conducted looking back on the history of some of the biggest cyber-attacks in history to look for relations within the businesses targeted.

Chapter 2: The History of Computer Vulnerability and the Origins of Hacking

Computers

Computers and comparable technology such as smartphones and tablets have made the modern generation reliant on these devices for everyday activities. However, this reliance opens up a whole new world of vulnerability for sensitive information that is stored and transferred via wireless networks. Computers, however, were not always a tremendous threat to everyday people. It was not until 1940 when the Complex Calculator was presented at Dartmouth College. During a demonstration, Stibitz used a "Teletype Terminal" to perform calculations on the Complex Calculator using specifically utilized telephone lines. This became the first historical account of remote accessing a computer ("Timeline", 2017).

In 1941, computers became more directly designed with the military in mind. The first Bombe computer was designed to decrypt Nazi ENIGMA-based communication from the German military during World War Two in 1941 ("Timeline", 2017). Following three years later in 1944, the first Colossus computer was designed to help decode Nazi cyphers ("The Colossus Gallery"). The machine would print all of the possible solutions to the code on a paper ribbon. It was believed that the Colossus machine greatly shortened the second World War.

Fast forward to 1950, the first commercial computer was produced by Remington-Rand computers ("Timeline", 2017). Although being branded for commercial use, the first predominant customers was the United States Navy. It was intended for high-speed computing and could hold up to one million bits. Later that same year the Standards Eastern Automatic Computer (SEAC) was invented. It was the first computer capable of storing programming. It also had an external memory stored on a magnetic tape that could hold the stored programs, coded subroutines, numerical data, and the programmed results (Garner, 2013). The capability

of being able to store information on computers made the threat of computer-based crimes grow exponentially.

In 1966, HP introduced its first modern computer, the 2116A. Customers could personalize their own computer to make it practical for their own uses. This was the beginning of the computerized revolution of businesses ("Timeline", 2017).

In 1981, IBM introduced its first personal computers, better known as PC. This allowed more people to gain access to the Internet and opened up a new world to smaller businesses that could not afford to purchase computers prior ("Timeline", 2017). Following shortly after, in 1984 Apple Computers Inc. introduce Macintosh. The Macintosh was the first mouse enabled system with a graphical user interface ("Timeline", 2017). Since IBM computers and Macintosh were still so expensive, one college student set out to lower the price of the hardware of computers. His name was Michael Dell, and he built hardware that was far less expensive than that offered by IBM, but still operated off the PC system. He later founded Dell Computers in the 1990s. The affordability offered by Dell, helped to allow more people to order computers for personal uses. Thus exposing people to a new world of information vulnerability ("Michael Dell Biography").

By 2000, cellphones were a growing trend all over the world. The Japanese company Softbank began incorporating small cameras into the phones it was manufacturing. Although the cameras were not expected to be a hit with consumers, they were widely accepted and most portable phones began to receive them. Although the camera phones were considered a privacy risk within businesses, cellphone manufacturers continued to develop on the trend ("Timeline", 2017).

In 2007, Apple Inc. released its first smartphone with the iPhone. It was a combination of web browser, phone, and multimedia device. These phones were given the capability that was previously unknown to phone users. Applications or "Apps" became available for download through an online store operated through Apple Inc. The capability of downloading and purchasing applications resulted in bank and credit card information being stored on devices and the individual user's personal accounts ("Timeline", 2017).

Throughout the history of computers, there was a continuous desire to make information and access to other people and businesses as convenient as possible for the general public. Most people, outside of the information technology field, did not realize the threat that was growing from the constant collection and storage of sensitive information until recent years. The attacks on large corporations such as Target and Home Depot showed how large amounts of valuable data are popular targets for computer hackers.

Hacking

Despite the "newness" of computers, the term hacking originates back to 1878. After Alexander Graham Bell invented the telephone, there was a need for people to work the telephone systems. One group of teenage boys were only interested in seeing how the telephone system worked, rather than connecting and directing calls. The boys were seen as trying to "hack" the system, thus the term "hacking" (Devitt, 2001).

In the 1950s and 1960s, commercial computers were still large and slow. So, programmers would spend large amounts of time trying to upload and edit their own programs. So in order to speed things up, they invented short cuts through the system or "hacks" to expedite their work.

It wasn't until the 1980s that the term "hacker" became a term with a negative meaning. When the Internet became more widely available to the public, some people began using that unmonitored openness for their own personal gain (Devitt, 2001).

The first known hacker went by the name "Captain Crunch," but his real name was John Draper. In 1971, he found a child's toy whistle the emitted the same tone as the 2600-hertz tone that is needed to open up a phone line for free use. He went on to get arrested numerous times for phone tampering. Inspired by Draper, two members of the Homebrew Computer Club, Steve Wozniak and Steve Jobs (who would later go on to found Apple Computers) wanted to help the public get free use of the phone system. They invented "blue boxes" that could emit different tones for home use of hacking the phone system (Devitt, 2001).

In 1984, hacking gained steam and popularity thanks to a growing number of computer users in the world. To help build this excitement was Eric Coley. Coley began publishing a magazine entitled: "2600: The Hacker Quarterly." The magazine basically gave tips and tricks on computer and phone hacking. The same year the Comprehensive Crime Control Act was put into place. Basically, it gave the Secret Service jurisdiction to investigate over credit fraud cases in the United States (Devitt, 2001).

However, in 1986, Congress passed the Computer Fraud and Abuse Act which made it illegal to hack into computer systems. However, the law did not apply to juveniles, who, at the time, were responsible for the majority of computer and phone breaches (Devitt, 2001).

The next year, 17-year old Herbert Zinn was arrested and pled guilty to hacking into AT&T phone networks. Investigators concluded that he was only a few steps away from completely shutting down the nationwide telephone operator switch, thus halting communication throughout most of the country. The same year, the virus referred to as "Brain" was released onto

the internet. While the virus was non-malicious, or non-threatening, it infected thousands of computers. The only change to the computer that users found was a small file that, when opened, contained the contact information for Brain Computer Services in Pakistan (Devitt, 2001).

However, in 1986, Robert Morris, a 22-year old from Cornell University, released a malicious, or dangerous, virus onto the Internet in order to exploit holes in the Unix operating system. The virus was known to infect about one-tenth of computers on the internet. That was enough however, to shut down the network for two days. As a result of the breach, the United States Government starts up the Computer Emergency Response Team with the mission of investigating attacks on Computer Networks (Devitt, 2001).

In 1990, the "Legion of Doom" which consisted of four hackers, presumed to be from the Southeastern United States, were arrested for stealing some of the technical specifications from the Bellsouth 911 emergency telephone system. The information stolen included usernames and passwords from 911 dispatchers across the country and could have disrupted the entire 911 Emergency Response unit across the country (Devitt, 2001).

In 1993, Kevin Poulsen, 28, and two others were charged with rigging promotional contests at three radio stations in Los Angeles, California. The hacked into the radio station main frame computer and redirected all incoming phone calls to the station to make sure that they were the only ones able to call through. The trio were able to win two porches, $20,000, and two trips to Hawaii, but were later caught (Devitt, 2001).

Two years later, in 1995, Vladimir Levin was arrested for using a laptop computer to break into Citibank's computer network and transferred between 3.5 and 10 million dollars into his own accounts (Devitt, 2001).

In 1996, the United States General Accounting office released a statement saying that there were 250,000 attacks on their system during 1995 alone. Out of those attacks, 65 percent were successful. Later that same year, hackers manage to break into the U.S. Department of Justice website and add things such as pictures of Adolf Hitler and renaming it the "Department of Injustice." They later got into the CIA and renamed it the "Central Stupidity Agency (Devitt, 2001)."

In 1998, the payroll and contact information of countless government employees was viewed and altered. Once again the hack was traced back to two teenagers living in California. That same year another teenager hacked into the Worchester, Massachusetts airport and interrupts the communication between the planes and the control tower. Although there were no accidents during the six-hour attack, the teen was charged for the attack. This was the first case of a juvenile being charged with a hacking offense (Devitt, 2001).

In May of that same year, members of the hacker group "L0pht" testified to Congress and explained the openness and vulnerability that they had found in the government computer network. They stated "if we wanted to, we could shut down the entire Internet in less than half-an-hour (Devitt, 2001).

In March of 1999, a hacker by the pseudo-name MagicFX breaches through to Ebay, the auction website. The attack was so large that he changed the home page of the site, was able to change prices on current auctions, and set up fake auctions. He also redirected visitors to external web sources (Devitt, 2001).

In 2001, multiple groups of Chinese hackers broke into the networks of major government entities such as: The White House, the CIA, and Department of Health. The attack

was suspected of being in revenge for a spy plane sent from the U.S. to China earlier that same year (Devitt, 2001)..

Fast forward to the present, hacking attacks occur almost every second at the largest corporations in the world. For example, in 2014, Sony experienced an attack that resulted in 47,000 files worth of employee and proprietary information being stolen (RBS, 2014). One year earlier, Target had a breach which ended with 110 million credit card numbers being stolen (Devitt, 2001).

Just like large corporations, our government is constantly threatened with outside cyberattacks from enemy nations. So how do companies and the government combat such an enormous, and steadily growing trend? Through store-bought and customized security software is one way. Through the use of ethical hackers is another.

Chapter 3: Literature Review

"Cyber-crime has become a growing concern in modern society due to the lack of governing bodies on the internet. The cyber world is a realm of no rules which allows cyber-attacks to happen on a daily basis." Dr. Joseph N. Pelton, the Director of the Space and Advanced Communications Research Institute (SACRI) at George Washington University, wrote his opinion of the threat of malicious hacking attacks in his article, *Who Will Control the Future, Black Hat Hackers or the Hacked* (2015). What is a black-hat hacker? A black hat hacker is defined as an individual with extensive computer knowledge whose purpose is to breach or bypass internet security according to PCTools.org. "The only chance that both companies and individuals have at preventing themselves from becoming victims, is done through the work of white-hat, or ethical hackers." Dr. Indu B. Singh (2015), an expert in Cybersecurity, has written numerous books pertaining to the threat of black-hat hackers and the need for white-hat hackers to fight back. Dr. Singh wrote the previous quote in his book entitled, *Digital Defense: A Cybersecurity Primer*.

An Ethical Hacker is defined as a person who hacks into a computer network in order to test or evaluate its security, rather than with malicious or criminal intent. A white-hat hacker is defined as a computer security expert, who specializes in penetration testing and in other testing methodologies to ensure the security of an organization's information systems. According to eSecurityPlanet, "The use of ethical hackers to test for security vulnerabilities is as old as the IT hills. But, unless there are clear goals outlining why and to what extent your organization is engaging them, the outcome could be useless information -- or worse (Bernard, 2004)." The website Help Net Security explains the need for Ethical Hackers to work more in businesses by stating, "As organizations of all sizes and sophistication levels can benefit from objective, expert,

third-party analysis, ethical hacking has become a more mainstream service in the past decade ("Importance, 2012)." The need for Ethical Hackers is best shown in the statement made on the Quality Crush blog, "Most of the benefits of ethical hacking are obvious, but many are overlooked. The benefits range from simply preventing malicious hacking to preventing national security breaches. The benefits include: fighting against terrorism and national security breaches, having a computer system that prevents malicious hackers from gaining access, having adequate preventative measures in place to prevent security breach (Shah, 2014)." To add onto this, Aasha Bodhani (2012) wrote, "With the rise of cyber-crime, ethical hacking has become a powerful strategy in the fight against online threats. In general terms, ethical hackers are authorized to break into supposedly 'secure' computer systems without malicious intent, but with the aim of discovering vulnerabilities in order to bring about improved protection," in her article Ethical Hacking: Good in a Bad Way which was published in *Engineering and Technology Magazine*. According to Convergence Network (2015) "Cyber hacking is a growing security problem for small and large businesses alike. So how do you prevent it? And after you've done your best to implement security to prevent it, how do you verify you're safe? There's actually an easy answer to that. The best way to keep a hacker out of your network is to hire a hacker to invade it. Let me clarify: an ethical hacker. Ethical hacking can test your networks using the same techniques the hacker will use and allow you to shut them out before the damage is done."

While some experts agree that ethical hackers are the answer to preventing both individual and corporate cyber-attacks, others disagree with this theory. Conrad Constantine, a writer of security software which are programs installed on the computer that protect against hackers or viruses, and Dominique Karg, co-founder and Chief Hacking Officer of Alien Vault Technology, are two information technology (IT) specialists who wrote an article in *Forbes*

Magazine titled, “Exploding the Myth of Ethical Hacking (2012).” In their article they write that “A hacker is a hacker is a hacker.” In other terms they are saying that all hackers are the same. Some people use the term white-hat hacker as an excuse to hack into company systems and steal information. Ian Sutherland (2016), an IT specialist who has held jobs in computer programming, a process that leads from an original formulation of a computing problem to executable computer programs, and IT consulting, advising organizations on how best to use information technology in achieving their goals, has written numerous books including *Invasion of Privacy* and *Social Engineering: Would You Trust a Computer Hacker*. Both of these books oppose the need for Ethical Hackers in corporations and even questions the legality of the actions carried out by these individuals. In his blog entitled, “Is Ethical Hacking Actually Ethical or Even Legal?” he writes, “Companies hire ethical hackers because they need to test their security. By granting their permission to the pen-test, they effectively cover their corporate eyes and ears while these tests are carried out. See no evil, hear no evil. And at the end, the ethical hacker presents a nicely polished report pointing out the weaknesses and associated recommendations. What the company has no idea about is how many laws they have enticed the ethical hacker to break to get to this point. The ethical hacker may not know or, more importantly, may not care about the laws that have been broken.” Pen-testing is slang for penetration testing. Penetration testing is defined as the practice of testing a computer system, network or web application to find vulnerabilities that an attacker could exploit. Brent Conran (2014), the Chief Security Officer of Intel Security, wrote in the online blogging forum called Security Magazine. The article titled, “Why Not to Hire an Ethical Hacker,” explained that, “White hat hackers use the same tools as black hat hackers, and have to keep their skills and knowledge up to date to make sure they understand the latest exploits. Many of them use personas when gathering the latest exploits so

that their real identity is not readily apparent to the underground. You're touching part of the shady underworld of hacking, even when going with white hats."

Despite the growing knowledge of what white-hat hackers attempt to accomplish, some companies are reluctant to grant trust to these individuals. According to CNBC News, an ethical hacker found a vulnerability in the system of United Airlines, who had recently started a program which rewarded airline miles to anyone who could find such vulnerabilities in their system and report it. CNBC wrote, "When Israeli researcher Yosi Dahan told United Airlines that he had found a security flaw in its website, he thought the company would be quick to act. So he was surprised when, two weeks later he had still not received a response from the company (Kharpal, 2015)." Later in the article, United Airlines responded and confirmed that the reason that they did not respond was out of fear of email bugs. Allen Jay Dumanhug found this out the prior to Yosi Dahan, when the company responded to him, accusing him of trying to breach the company. He wrote to CNBC, "One time, I found a bug. I tried to report it (but) they replied that I was trying to hack or get into their system. I had no intention to do bad, but they said I was trying to infiltrate the company.".

"Security software is any computer program designed to enhance information security. The defense of computers against intrusion and unauthorized use of resources is called computer security. Similarly, the defense of computer networks is called network security," as defined by Techopedia. Security Software is seen as an alternative to hiring an Ethical Hacker. The recognized benefits of this kind of software is that is can protect against black-hat hacker attacks as well as viruses and worms. Viruses and worms can be described as a piece of code that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

Ethical Hacking is viewed as both a positive and a negative based on the values of merit, honesty and integrity. Some people question whether or not ethical hacking is going to be the future law enforcement, other see ethical hackers as criminals using a fancy name to cover up for their actions. Cyber security is going to remain a growing concern for the future of our rapidly innovating society. The more devices that become connected to networks causes a growing field for black-hat hackers to harvest from and steal information.

Industry Specific Views on Ethical Hacking

Healthcare

According to Parameter Security, "The latest Ponemon Institute study reveals 60% of healthcare providers had more than 2 security breaches in the last year with the average breach costing them $2 million." However, 70% of healthcare organizations do not see patient information as a security priority. So, if healthcare companies rank patient information as a non-priority, why are ethical hackers barred from performing services for healthcare organizations? One of the main reasons for this, is lack of proper personnel to properly secure patient information. Ponemon Institute believes that the employment of ethical hackers will provide proper information security that has previously been lacking in the healthcare industry as long as the potential external ethical hacker is compliant with guidelines on new employee hiring procedures and extensive security experience (Chronister, 2015).

Some healthcare companies feel that the use of external ethical hackers to test the system can lead to an increased awareness of internal security measures that can protect patient information. Lucia Savage, the Chief Privacy Officer in the Office of the National Coordinator for Health IT, stated that she believes that ethical hacking can help properly probe and correct IT weaknesses for healthcare companies nationwide (Hall, 2016). Defense Secretary Ash Carter

bragged on the work that ethical hackers do for the United States military (Sarvestani, 2013). Our systems are deemed some of the most secure in the world. Carter and Savage feel that the use of ethical hacking services in healthcare, could lead to top-rate security for patient information (Hall, 2016).

Leaning away from strictly patient information vulnerabilities, in 2016, the Federal Bureau of Investigation warned the healthcare industry about the risks that some medical devices posed. Most hospital and medical devices operate on the Internet of Things (IoT). This means that devices automatically connect to the internet through a wireless connection and send and receive information that contribute to the proper functioning of the device. Some of these devices include heart monitors and insulin pumps. If these devices were compromised by hackers, it could endanger patient lives by causing the machines to malfunction because of coding changes. "Nordenburg, co-founder and executive director of the Medical Device Innovation, Safety and Security Consortium, stated 'pretty much every medical device out there is hackable (Spring, 2016).'"

Retail

While regular brick-and-mortar retail stores can still benefit from the services of ethical hackers by securing point-of-sale (POS) devices, and proper encryption of credit card information, the realm of the retail store has transformed into e-commerce. Almost every store has some form of website, most websites allow shoppers to buy things from the comfort of their home. In January of 2016, an e-commerce firm, located in India, realized a breach in its system that was allowing users to buy items for free, after hiring an ethical hacker. The ethical hacker later stated in an interview with *The Economics Times*, "We hacked in to the ecommerce platform from outside and were able to buy almost anything for free. It may be little complicated

for you to understand, but simply put, an algorithm was developed which manipulated the payment gateway in to reading duplicated discount codes (Sarkhel, Alawadhi, 2016).” Mobile application-based retail stores such as Amazon, Flipkart, SnapDeal, and Ola are starting to hire ethical hackers in order to prevent cyber-attacks. Hiring ethical hackers to try to hack into their systems from outside the physical company walls and report back and report their findings back to the CEO, CFO, CIO can be detrimental in preventing future loss of resources (Dave, Chaturvedi, 2016).

Dishant Shah, cofounder of Spherical Defense Labs which specializes in the prevention and understanding of cyber-attacks said, “Today hacks are highly targeted and lead to server crashes and corruption, implying massive losses for companies, and considering the massive movement towards e-commerce and mobile-application development, preventing these attacks is more of a priority than ever before (Dave, Chaturvedi, 2016).” One technique that is gaining popularity through the retail industry is the use of “honeypots.” According to Techopedia, a honeypot reroutes a hacker’s cyber-attack into a fake server. This technique used to be a way for hackers to hide by sending cyber-attacks through a fake server in order to conceal their location. For example, if a company in China wanted to hack into a company in the United States, they could use a honeypot server in Russia by routing the attack through a Russian server. When the company in the United States traces the attack, it would lead to the honeypot sever in Russia. Now, ethical hackers are helping companies set these up as a defensive maneuver against the hackers.

“One-fifth of breached companies are PCI (payment card industry) compliant (Sussman, 2008).” One example of a PCI Compliant company that was breached is the Target Breach of 2013. Target received PCI compliance status in September of 2013. Later that same year, on

November 12, 2013, Target was the victim of a cyber-attack that lasted eighteen days and resulted in around 40 million credit and debit card numbers being stolen (Krebs, 2014). Parameter Security, a firm that offers ethical hacking services, says that most ethical hackers have experience with securing credit and debit card information. Their motto is, "Compliant is good. Secure is better. Because if you are secure, you are compliant."

Finance

With ethical hacking being a security service to test an organization for potential exposure to cyber-attacks, the realm has opened up to many financial institutions. Financial institutions carry more wealth and personal assets than any other industry. Every industry including retail, healthcare, and hospitality rely on the financial industry to protect information and electronic funds. Many ethical hackers employ the use of social engineering tactics to test the employee of retail banks, investment banks, and insurance companies. Mark Hughes, the CEO of BT Security stated: "The prospect of accessing confidential financial information is a powerful lure for hackers so few companies attract as much online criminal attention as banks. We encourage all financial institutions to put themselves through a rigorous series of cyber-security simulations, whereby our ethical hacking consultants push the cyber defenses of financial institutions to the limit (Ball, 2015)."

However, some of the largest banks in the United States disagree with this new-generation belief of ethical hackers. "NPR (National Public Radio) contacted a dozen financial institutions. Like high-tech firms, financial institutions are under constant cyber-attacks, but only one of them said it has a method for outsiders (customers or researchers) to report a security issue to the company (Shahani, 2014)." The companies that had no comment on whether or not

they have methods for ethical hackers because they do not wish to discuss their cybersecurity measures with anyone from the public.

Chapter 4: Methodology

In order to understand if ethical hackers provide better security to businesses, a survey was conducted to gain weight into this matter. This survey was given to 20 professionals in the information technology industry. The survey was voluntary and the individuals are employed in the Middle Tennessee area. The sample group consisted of companies within different industries, such as: retail, healthcare, hospitality, financial, and other.

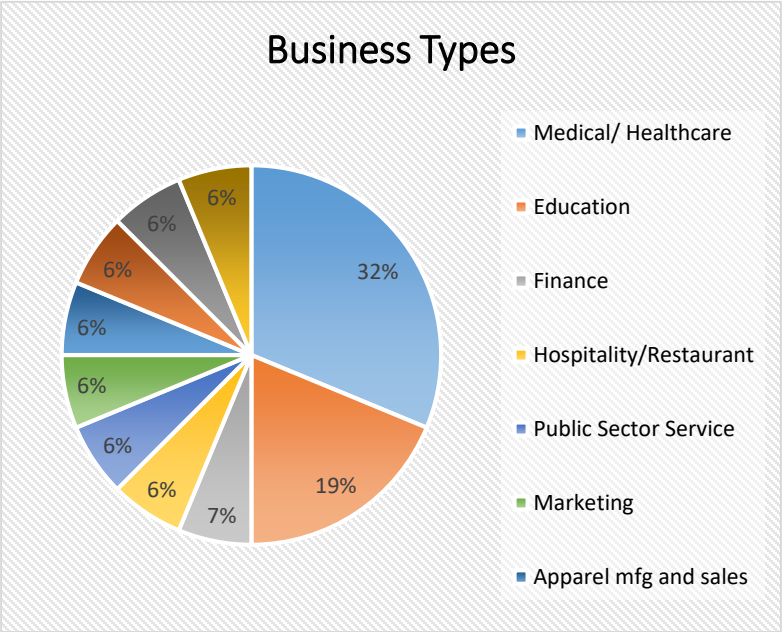
The survey consisted of multiple choice questions for demographic information. The questions regarding the use or lack of use of hackers consisted of yes/no answers. Finally, the opinion questions were on a Likert scale. The survey is in appendix A.

After the survey was conducted, the data was sorted into categories to see if there were any patterns. It was divided up based on company demographic information such as company industry, number of employees in the entire business, number of employees in the IT department, etc. The goal of organizing the data was to see if Ethical Hackers work better for specific industries.

Personal opinion data of the individual completing the survey was also collected. No personal information such as name or company identification were recorded.

Chapter 5: Results

Twenty-three IT professionals responded to the survey. After beginning the survey, only sixteen continued and provided answers. Of the sixteen individuals that responded to the survey the types of business were mostly different. The business types included: health care, finance, public sector services, higher education, education, medical, marketing, apparel manufacturing and sales, hospitality/ restaurant, and network administration. The most common business type was healthcare and medical information technology with five participants working in the industry. The second, most common business type was education with three participants working that industry.



Of the sixteen responses, ten participants had companies that had more than 1000 employees. Out of those ten companies, eight have information technology departments that have more than fifty employees. These include businesses in health care, finance, education, apparel manufacturing and sales, and hospitality/ restaurants.

Only two participants work for companies that employee less than 100 employees. Both of those companies had less than ten employees in the IT department. The company type for these two participants was retail and marketing.

Of the sixteen participants, ten work for companies that hire ethical hackers from an external firm. The reasons for hiring ethical hackers includes: having previous security breaches,

testing for potential software and hardware vulnerabilities, checking for company security compliance, provides confirmation or scrutiny of people, processes, and practices that are integral in operations, and seeing penetration testing from a different perspective than an internal employee would see it. The types of businesses that hire ethical hackers include: health care, finance, public sector services, retail, education, medical, hospitality/ restaurants.

Seven participants indicated that the company that he or she works for does not hire ethical hackers from external firms. The reasons behind this decision includes: budget restrictions, the company has an in-house penetration testing team, not part of the culture of the business, and smaller companies do not know what is an ethical hacker. The types of businesses that do not hire ethical hackers from external firms includes: education, medical, marketing, apparel manufacturing and sales and network administration.

Nine of the sixteen companies have an IT security department that works separately from the rest of the information technology department of the businesses. Of those nine, seven companies have more than 1000 employees, one company has less than 100 employees, and one has between 101 and 500 employees.

In response to the statement, “ethical hackers are an important part of information security,” five participants responded with the option of, “Strongly Agree,” ten selected the option of, “Agree,” and one participant selected, “Neither Agree nor Disagree.”

When asked the optional question about personal opinions of ethical hackers, the responses were:

- “We need to defend as a criminal would try to exploit. Ethical hacking that does not compromise business performance is a necessary tool in a layered security program.”

- “We use an external security firm to verify our internal security controls much like an organization uses an outside auditor for financial review.”
- “Ethical hackers can show vulnerabilities, but also the exploitation of systems. This is ultimately, risk being practiced.”
- “Because they are laser focused on key weaknesses and vulnerabilities present in security operations, and often are hired externally, they have the attention of senior leadership and management team members.”

Overall, the individuals that participated in the survey provided unique views of both the positives and negatives of hiring external ethical hackers with regards to different company cultures.

Chapter 6: Discussion

For myself, Ethical Hacking has grown into one of the topics that I consider to be most influential in the future of information technology. I was introduced to ethical hacking when I was a senior in high school and looking through potential college majors to pursue. I found the idea of working in security very interesting and began to look into the computer information systems major at MTSU with the intent to graduate and gain my certification in ethical hacking.

After I had been in the program for two years, we had a guest speaker in one of my classes talk about how ethical hackers were too large of a security risk to companies, and that anti-virus security software was better for businesses to use. This was the first person that since I had begun to look into my potential future career to disagree with the practice. This made me interested into seeing what the overall view of different types of businesses with the stance of ethical hackers being better for security purposes.

One of the reasons that hiring an ethical hacker from an external firm is more beneficial is the unique testing that comes with the penetration testing done by the individual performing the hack. While software can be cheaper if bought "off-the shelf," it is not unique to the operations of each business. If there are vulnerabilities within the software, it is not as likely to be found. Another problem with software is that it is susceptible to more human error. For example, if a company implements an ad blocker on all company computers, an employee could bypass the protocol and disable the ad blocker. Turning off the ad blocker could lead to someone being able to click on the links in potentially threatening emails.

Hiring ethical hackers from external firms is the best way to fight potential cyber-crime and prevent the breaches that happened to Target in 2013 and Home Depot in 2014. According to the survey administered to IT professionals, 93% either agree or strongly agree that hiring

ethical hackers from external firms is important to information security. Even though some companies do have in-house ethical hacking teams, I feel like there is a bias and lack of experience that could negatively impact the effectiveness of the pen-testing. External ethical hackers get to work with different businesses and learn about new ways to exploit vulnerabilities. Also with an external firm, there is a very small chance that the firm has a bias towards the company.

In the majority of articles arguing against hiring ethical hackers, the main concern was being able to trust people that consider themselves "hackers" with business critical information. However, people wanting to receive a certification in ethical hacking must go through a course that involves ethics while teaching the skills involved with hacking. Also, most companies require a background check before hiring an individual. If the person has any problems with burglary or cyber-threats, they will not be hired as a pen-tester or ethical hacker. Most ethical hackers provide their personal information to the higher-level information security management so that a background test can be done by the company considering using the services of the ethical hacking firm.

Ethical hackers are the best possible solution to combat the growing world of cyber-crime within the limits of current technology. When considering the need to hire ethical hackers, no company is too small. Ethical hackers are focused on finding key weaknesses and vulnerabilities present in security operations and fixing the problem before it becomes a real security threat.

Chapter 7: Conclusion

Although cyber-crime has grown throughout the years to become one of the top threats for government agencies, large corporations, and select individuals, the work of ethical hackers has helped diminish the threat. While hiring ethical hackers from an external firm may still be out of the financial means of smaller corporations, any company with the means to do so should employee the use of penetration testing services.

The history of malicious attacks on companies from hackers was largely due to the lack of penetration testing from external ethical hackers. The benefits of hiring ethical hackers include lack of internal bias, extensive knowledge of multiple systems and exploits, and laser focus on key weaknesses and vulnerabilities. While software is capable of preventing some attacks, the lack of uniqueness can provide a target for easy exploitation of systems.

The companies that were included in the interviewing process showed that while the trend of ethical hackers is growing, not every company in the area is using the method right now. However, even the companies that do not currently hire ethical hackers have IT professionals that feel it is important to partake in unbiased penetration testing to help prepare systems for potential malicious hacking attacks.

If this study were continued, a larger sample group would be taken. The field of participants would be extended to nationwide rather than in Middle Tennessee. A limitation of the survey sample was that it was a convenience sample. The survey was emailed and sent to a large group of participants, and only the ones that responded are considered participants. Another limitation of the information is that ethical hacking is a rather new topic. There are not many scholarly books or articles regarding the topic. Most of the current information about ethical hacking is found in online journals and blogs.

References

Ball, Alan. "BT Helps Global Financial Industry Keep Data Secure with New Ethical Hacking Service." *BT in US & Canada*. 16 Sept. 2015. Web. 21 Mar. 2017.

Bernard, Allen. "The Pros & Cons of Ethical Hacking." *ESecurityPlanet.com*. 02 Feb. 2004 Web. 20 Mar. 2017.

"Black Hat Hackers." *Browser Defender™ Powered by PC Tools*. PC Tools, 18 Oct. 2010. Web. 20 Mar. 2017.

Bodhani, Aasha. "Ethical Hacking: Bad in a Good Way." *Engineering and Technology Magazine*. 17 Dec. 2012. Web. 20 Mar. 2017.

"Certified Ethical Hacker (CEH)." *EC-Council*. Web. 20 Mar. 2017. <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>.

Chronister, Renee. "Healthcare and Security: A Hacker's Perspective." *Parameter Security*. May 2015. Web. 20 Mar. 2017.

"The Colossus Gallery." *The National Museum of Computing*. CodesandCiphers Heritage Trust. Web. 20 Mar. 2017.

Conran, Brent. "Why Not to Hire an Ethical Hacker." *Security Magazine*. 1 Mar. 2014. Web. 20 Mar. 2017.

Constantine, Conrad, and Dominique Karg. "Exploding the Myth of the 'Ethical Hacker'." *Forbes*. 31 July 2012. Web. 20 Mar. 2017.

Dave, Saschin, and Anumeha Chaturvedi. "E-commerce Firms like Amazon, Flipkart, Snapdeal \ Rope in Ethical Hackers to Tackle Cyber Attacks." *ETtech.com*. ET Bureau, 19 Feb. 2016. Web. 20 Mar. 2017.

Devitt, Michael. "Dynamic Chiropractic." *A Brief History of Computer Hacking*. 18 June 2001.

Web. 20 Mar. 2017. Dynamic Chiropractic fell victim to the "I love you" virus. They responded by hiring information security officer Michael Devitt. He used the company's newsletter as an outlet to spread the word about computer hacking.

Garner, Robert. "Early Popular Computers, 1950 - 1970." *Early Popular Computers, 1950 – 1970 - Engineering and Technology History Wiki*. IEEE Stars, July 2013. Web. 20 Mar. 2017.

Hall, Susan D. "HHS considering White Hat Hacking for 'security Hygiene'." *Fierce Healthcare*. 27 June 2016. Web. 20 Mar. 2017.

"The Importance of Ethical Hacking." *Help Net Security*. 19 Apr. 2012. Web. 20 Mar. 2017.

"Internet." *Dictionary.com*. Dictionary.com. Web. 20 Mar. 2017.

Kharpal, Arjun. "Ethical Hackers: Are Companies Ready?" *CNBC*. Tech Transformers, 19 June 2015. Web. 20 Mar. 2017.

Krebs, Brian. "Target Breach by the Numbers." *KrebsonSecurity*. 6 May 2014. Web. 20 Mar. 2017.

"Michael Dell Biography." *Biography.com*. A&E Networks Television, 06 Feb. 2015. Web. 20 Mar. 2017.

Pelton, Joseph, Indu B. Singh. "Who Will Control the Future: Black Hat Hackers or the Hacked?" *Digital Defense: A Cybersecurity Primer*. Springer International. 127-44. Print. Sept. 2015.

RBS. "A Breakdown and Analysis of the December, 2014 Sony Hack." *Risk Based Security*. 5 Dec. 2014. Web. 21 Mar. 2017.

Rouse, Margaret, and Michael Cobb. "What Is Ethical Hacker?" *TechTarget*. Nov. 2014. Web. 20 Mar. 2017. <http://searchsecurity.techtarget.com/definition/ethical-hacker>.

Rouse, Margaret, Johnathan Gershater, and Puheet Muheta. "What Is Pen Test (penetration Testing)?" *TechTarget*. 11 May 2011. Web. 20 Mar. 2017.

Rouse, Margaret. "TCP/IP (Transmission Control Protocol/Internet Protocol)." *TechTarget*. Oct. 2008. Web. 20 Mar. 2017.

Sarkhel, Aritra, and Neha Alawadhi. "Hacker Group Legion Calls Indian Banking System Deeply Flawed." *The Economic Times*. 13 Dec. 2016. Web. 20 Mar. 2017.

Sarvestani, Arezu. "Medical Device Cybersecurity Tools in the Real World – MassDevice." *Mass Device*. 21 Aug. 2013. Web. 20 Mar. 2017.

Shah, Ronack. "Ethical Hacking." *Quality Crush*. 24 June 2014. Web. 20 Mar. 2017.

Shahani, Aarti. "Banks Reluctant to Use 'White Hat' Hackers To Spot Security Flaws." *NPR*. 05 Nov. 2014. Web. 21 Mar. 2017.

Sidel, Robin. "Home Depot's 56 Million Card Breach Bigger Than Target's." *The Wall Street Journal*. Dow Jones & Company, 18 Sept. 2014. Web. 20 Mar. 2017. <https://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571>.

Spring, Tom. "IoT Medical Devices: A Prescription for Disaster." *Threatpost | The First Stop for Security News*. 15 July 2016. Web. 20 Mar. 2017.

Sussman, Bruce. "Mastering the Payment Card Industry Standard." *Journal of Accountancy*. 01 Jan. 2008. Web. 21 Mar. 2017.

Sutherland, Ian. "Is Ethical Hacking Actually Ethical or Even Legal?" *Ian Sutherland*. 2 May 2016. Web. 20 Mar. 2017.

"Threat of Hackers." *Convergence Networks*. Mar. 2015. Web. 20 Mar. 2017.

"Timeline of Computer History." *Computer History Museum*. Computer History Museum. Web. 20 Mar. 2017.

"What Is Honeypot (honey Pot)?" *Techopedia*. Web. 21 Mar. 2017.

"What Is Security Software?" *Techopedia* Web. 20 Mar. 2017.

Appendix A:

Ethical Hacking Thesis Survey

Type of Business (Retail, Hospitality/Restaurant, Medical, Finance, etc.) _____.

Approx. Number of Employees (Circle One) < 100 101—500 501-1000 1001 <

Approx. Number of Employees in IT Department < 10 11—20 21—50 51 <

Select One Answer

Does your company hire Ethical Hackers (Pen testers) from outside firm? Yes No

List specific reasons why your company does or does not hire ethical hackers

Does your company have a separate IT security department? Yes No

Has your company had an IT Security breach in the last 5 years? Yes No

Opinion Questions

Ethical Hackers are an important part of information security.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

An Ethical Hacker can truly be legitimate.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

I would hire an Ethical Hacker in the future.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

An ethical hacker would help mitigate a security breach.

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree

Do you have any other opinions on ethical hackers?