Looking Inside Rainbow Hacking: Tactics, Company Pitfalls and Preventative Security for the Public (December 2019)

Kevin J. Flanagan, Susanna S. Gottel, Tong H. Thao, Lauren A. Nguyen

***Abstract*—This paper will go over the sectors of rainbow hacking, and a brief history. There are companies that the public trust with their information, yet time and time again companies fail to protect our information. To then put the blame on the public for the company's pitfalls. Furthermore, if companies will not protect the publics information, it is for the public to choose how they want to protect themselves, and to educate themselves in the knowledge to protect their sensitive information.**

***Index Terms*— Computer Hacking, Computer Security, Internet of Things, Data Security, Encryption.**

I. Introduction

Often when people hear "hacker" they think of a malicious person who will take sensitive or secure information and exploit it for their own personal use. However, this is not always the case. There is a hacker rainbow where hackers are identified by the types of hat that they wear [1]. White hat hackers, are what one could call the 'good guys.' White hat hackers find vulnerabilities and then they report them to the owners [2]. On the other spectrum there are black hat hackers, or crackers [3]. These black hat hackers will find and exploit vulnerabilities that would be in systems and white hat hackers attempt to find these vulnerabilities and fix them before black hat hackers find them. There is a middle group called grey hat hackers. Grey hat hackers choose to gain unauthorized access to systems and their resources in order to help organizations find vulnerabilities and fix them as well, however; they are not authorized to enter these systems like other white hat hackers [4]. It is important to keep in mind that although hacking is technical, many hackers often trick people into giving their information to others.

In fact, many people are unaware that nearly anything that has connection to the internet or holds some sort of data can be hacked [5]. With that I mind, hackers have been using hacking to make profits and some entirely rely on the profits for business. But if companies took the time to employ 'the good guys' or white hat hackers to thoroughly investigate new software and find ways to update the companies legacy technology in order to stay patched and secure; it could be possible to prevent such hacks from happening again. However, due to the neglect of many companies and organizations neglecting to hire white hat hackers; and refusing to spend company finances to train and harden their people to find vulnerabilities within their systems, more companies and devices are prone to cyberattacks. Therefore, the public has a role in ensuring that their information is safe by being keen on where and who they are sharing information with.

Manuscript received October 9, 2001. (Write the date on which you submitted your paper for review.) This work was supported in part by the U.S. Department of Commerce under Grant BS123456 (sponsor and financial support acknowledgment goes here). Paper titles should be written in uppercase and lowercase letters, not all uppercase. Avoid writing long formulas with subscripts in the title; short formulas that identify the elements are fine (e.g., "Nd–Fe–B"). Do not write "(Invited)" in the title. Full names of authors are preferred in the author field but are not required. Put a space between authors' initials.

K. J. Flanagan is a student of Metropolitan State University, St. Paul, MN 55106 USA (e-mail: yww01ag@go.minnstate.edu).

S. S. Gottel is a student of Metropolitan State University, St. Paul, MN 55106 USA (e-mail: susanna.gottel@my.metrostate.edu).

T. H. Thao is a student of Metropolitan State University, St. Paul, MN 55106 USA (e-mail: tong.thao@my.metrostate.edu).

L. A. Nguyen is a student of Metropolitan State University, St. Paul, MN 55106 USA (e-mail: lj3959hl@go.minnestate.edu).

II. HISTORY OF HACKING AND METHODOLOGY

A. Brief History of Hacking

According to the Merriam Webster dictionary, a hacker is an individual who is an expert at solving problems with a computer [6]. A second definition is one who illegally gains access to and sometimes tampers with information in a computer. As shown in this report, there are many types of individuals that choose to hack and are commonly labeled as a Black Hacker, a White Hacker, or a Grey Hacker. One of the first hacks recorded in modern time was in 1966. The crime was committed in Minneapolis and entailed the altering of bank documents. This crime was federally prosecuted and eventually led to laws being written to hold hackers responsible for their criminal behavior. However, it is fair to say that the hacking of technology did not begin with computers, but with phone lines. In the 1970's, hackers found ways to connect to long distance and international phone lines by using a 2600-hertz signal [7]. These hackers were known as

Phreaks, a combination of the words phone and hackers. They have a direct link to two of Apple's founders, Steve Jobs and Steve Wozniak [8].

According to David Kim and Michael Solomon, Writers of Fundamentals of Information Systems Security, a hacker is someone who "modifies something, particularly related to computer systems." This tinkering and finding ways to explore and possibly interfere with new technology led to the Morris Worm. In 1988, Robert T Morris, a graduate student at Cornell University, created and released a worm that infected as many as six thousand network computers. Because of the Computer Fraud and Abuse Act of 1986, Morris was removed from the university and fined 10,000 dollars [9]. Robert is one of the first hackers to be held federally liable for his illegal hacking.

More recently, hackers have increased the amount of attacks towards, what David Kim and Michael G. Solomon, "…clueless employees…", who may, "…set off a company-wide virus attack by clicking a 'harmless' email link" [10]. They express how crucial it is for organizations to properly train and help staff understand the importance of email safety. This is a major access point for many criminals and hackers to exploit. In fact, by not securing email and allowing viruses to spread, your organization will be added to the botnet web that hackers hope to control. Using botnets, a web of computers controlled by an individual hacker, the attacker can wreak havoc on our daily lives and prevent an easy way of detecting and finding the perpetrator [11].

B. Attack Types and Patterns

As discussed previously, there are two major types of hackers; white Hackers and black Hackers. Since White Hackers are mainly on the defensive side and try to prevent Black Hackers from exploiting company information, this portion of the paper will not directly relate to them. However, many of the processes discussed here could be used by security professionals to help find and later close vulnerabilities within the network.

To begin, most black hackers use very similar software to organize and commit and attack on an organization or government agency. The goal of the initial software and probing of the network is to find vulnerabilities in the organizations software so that hacker will be able to access the company's intellectual property, customer's private data, or the organizations financial data. These hacker tools generally fall into two categories. The first category is analyzers and scanners. They include tools like Protocol Analyzers that can determine what type of software is being used and can see data that is not encrypted in plain text. One of the largest attacks in recent history was from 28-year-old Albert Gonzalez who used packet sniffing technology to steal credit card information and sell it to criminals on the web, as mentioned by David Kim and Michael Solomon [9]. Packet sniffers are usually run alongside port scanners that will expose the different ports that are open within IP host devices as well as individual terminals. Once the scanners determine what operating system the network computers are running, vulnerability scanner software will check for known vulnerabilities within companies operating system and provide the black hacker knowledge of how best to access the system. The vulnerability scanners lead to the second important software type which is using exploit software. Criminals will use this software to see how far into the organizations network they can access. If the hackers can gain system access, the hackers have found a "critical risk exposure" [12]. Finding this type of access in todays' security driven atmosphere would be challenging, so many criminals rely on other types of hacks.

C. Malicious Attacks

The previous section of a Black hacker's tools focused on the preliminary work needed to be completed to provide a better chance of a successful attack. Nevertheless, we have seen that hackers can be lucky and access private data when companies are careless with their network and credit card transactions. The following strategies discussed are more of a direct act to try and steal a company's assets and are referred to as active threats. There is one prominent type of malicious attack called fabrication. Using a fabrication attack, involves tricking the user into believing that they are on a real cite when in fact it is a dummy cite or tricking a user into providing private information to the hacker. Examples of these attacks are IP address spoofing, masquerading, social engineering, phishing, and pharming. Each of these deceptive attacks has their own unique twist and should be reviewed so that there is a complete understanding of how they are accomplished.

IP address spoofing will trick the network into believing that the IP address on the hacker machine is within the network and should have access to servers and data. By gaining knowledge and assessing vulnerabilities from the preparation stage this attack can be very effective.

Masquerading uses IP address spoofing to monitor network communications by faking network access. The disguised computer can monitor usernames, passwords, and other personal information in hopes that a mistake will be made within the network and the masquerading computer will be able export the user credentials for personal use.

Social engineering attacks are used to trick employees into giving up more information than they would normally release. The main idea is for the hacker to pretend that he is working within the organization and needs to gather information from the user to help fix a problem. Generally, this type of deception is used on new employees or individuals like receptionists and front desk employees. The goal is to "appeal to employees' natural instinct to help", as mentioned by David Kim [13].

Phishing and pharming are very similar and are used frequently to deceive users to provide personal information about themselves or the company that they work for. A phishing email acts as if it is coming from a real site, for example a bank. The purpose of the email is to hook the user into thinking that private information should be given to the fraudulent email. This may include passwords, social security numbers, credit card numbers, and banking information. These emails are generally easy to spot, and no information should be given to a reputable organization through an email request. Pharming attacks are harder to spot because they replicate a real website and will gather all your private information at once. Both types of attacks are easy ways for hackers to gain

private information. It is easy to send out thousands of emails to known bank users and only a few need to respond for the scam to work [14].

As seen, there are many ways in which hackers can gain either user private information or corporate account information. In many cases the process begins with the preparation stage and then continues into the malicious stage. However, there is another phase of attacks that can do as much harm as using fabrication attacks. These attacks perpetrated by malicious software or malware for short. Malware is an inserted program designed to cause damage, to disrupt, and divulge private data. David Kim and Michael Solomon describe the two groups of malwares as infecting programs and hiding programs [15]. Viruses are well-known types of infecting programs that will attach itself to other files and are a common way to trick users into sharing information without their knowledge. Every time a user runs the infected program it may attach to other running software and spread like a biological virus. Another type of infecting software is called a worm. The purpose of a worm tends to be causing network lag or for targeting a specific company and causing a Denial of Service (DOS) attack. Worms will repeatedly replicate themselves and wreak havoc throughout the network. As previously stated, the first reported worm attack was in 1988 by Robert Morris and it replicated itself so quickly that the computers infected became unusable [16].

Viruses and worms are well known malicious software and have a predictable path and can usually be found and cleaned out of a system without too much trouble. The problem intensifies when the discussion starts to move towards hidden software or programs. These attacks are even more dangerous because they are not as easily found. Take for example a Trojan Horse attack, named from historical trickery from the Greeks towards the people of Troy. This software replicates itself as something useful and without the user knowing, executes malicious software to spy or damage data. Of course, spying on users and corporations is left for another malicious program called Spyware. Spyware is usually, "…bundled as a hidden component of freeware or shareware programs that users download from the internet" [17]. The benefit of this method of disbursement, is that users don't even know that they have downloaded malicious content. Unlike infectious programming, the purpose of this software is to provide the hacker with user activity including things like monitoring keystrokes, snooping on other applications, and reading cookies, small files that will hold information about websites that have been visited.

As hackers become more sophisticated with the ways in which they can access private data from both individuals and corporations, their awareness of the human psyche plays a critical role. The reason is because cybersecurity is moving to protect data at a similar speed and hackers will need to find ways to trick people into sharing critical company or personal data. Using social engineering attacks like familiarity when interacting with employees daily, and trust by developing a level of trust with an employee of the company. Hackers may find a weak link in the corporate security chain. This is where the Black hacker will pounce on the "…clueless employee…" [18].

III. KEEPING THE PUBLIC INFORMATION PROTECTED, AND THOSE WHO NEED TO FIX IT

A. Keeping Company Data Protected and those who Have Failed

Although the digital information age arrived quicker than companies and corporations can adapt there are a few things that are being done to help secure consumer information in today's digital era. The first of those is ensuring that data information is being encrypted. Encryption is a must for any company or business that handles customer information.

> "Encryption tackles two common data protection vulnerabilities in today's global economy: a work force always on the move and the rise of remote work. With devices frequently leaving the safety of company networks, encryption ensures that, in case of theft or loss, the sensitive data they contain is inaccessible to outsiders" [19].

Encryption keeps information secure by rendering it unreadable by those that want to access the information illegally. Along with the mentioned issue of losing workplace assets, encryption will also keep those items secure by making the information inaccessible without a proper password or security credentials. Another important part of a company is the workforce. These are many employees that work in the companies and there are other ones that are handling day-to-day data exchanges where information can be lost or insecure. Humans are the weakest link when it comes to information security. Whether it is be ignorance or negligence employees account for 54% of data breaches [20]. In order to mitigate these problems, many companies are making sure to keep their employees up to date on policies and are providing essential training on the topics of cybersecurity. Even with top of the line software, security can be rendered useless if employees are not properly aware and trained. Aside from these things, companies should have comprehensive policies and procedures put in place along with ways to handle bring your own device policies. This may help in reducing the amount of vulnerabilities and providing access only to those who we want to have access to that data.

B. What is Not Being Done

It seems that what is being done still is not enough to resolve or provide a closer solution to the issues of data security within these companies. It is also clear that "existing research suggests that most organizations do not have sufficient protection to prevent data breaches, deal with notification responsibilities, and comply with privacy laws" [21]. Although many things can change within a year this still holds true today. Many companies are still struggling to prevent data breaches and notification of responsibilities. The steps that are being taken by the companies are just simply not working enough towards data security. The repercussions that come with data breaches such as fines and loss of profit does

not seem large enough to leave a dent. “Despite legal, reputational, financial, and survival threats, prevailing research suggests that private organizations are not significantly changing their behavior” [22]. Without significant changes these organizations are vulnerable to the same attacks and future security breaches. It seems that organizations are failing to put the correct measurements in place to prevent these kinds of breaches. There are not enough resources being devoted into this new area of the digital era. The only way to function correctly is with the correct vision and leadership. Some studies show that many organizations seem to lack both clear leadership and strategies for tackling the security threats they face. Some of the major companies to date that have been breached so far are Capital One, Evite, Door Dash, and many more others as mentioned by Dan Rafter [23]. Capitol one being the largest one with 106 million records breached. This breach allowed for the hacker to gain access to hundreds of thousands of social security numbers and bank account numbers. About 100 million customers were affected by this breach as shown by Dan Rafter [24]. This is not the last of the breaches to happen. Many more of these problems will arise if organizations do not take the necessary step to mitigate these issues.

IV. EDUCATION AND PROTECTION FOR THE PUBLIC

A. White Hat

White hat hacking is also referred to as ethical hacking. In present times, ethical hacking is picking up as a legal profession. Ethical hackers are granted access to highly sensitive and confidential information through penetration testing [24]. Nevertheless, the potential of misusing the data may rise. As such, a need to ensure professionalism is maintained throughout the process is critical in ensuring that competence and ethical behavior is stable. Nowadays, digital devices such as computers are networked to share information, and the number of security threats and information vulnerability is reported daily. Therefore, the use of ethical hackers’ aid in the battle of securing crucial information. This practice is a significant development in a world of communications and information sharing that is not entirely secure. The white hat hackers use their computer expertise to creep into systems in an effort of identifying weaknesses in them rather than exploiting them [25]. If a defect is found in a system, the ethical hackers report back to the system administrators for further intervention that includes amending the security gaps. The ethical hackers are significant because they possess skills, processes, and the tools that the black hat hackers use allowing system managers to deal with the issue of cybercrime exhaustively.

B. Black Hat

Black hat hacking is also referred to as malicious hacking. It involves activities of hackers breaking into systems, stealing information, manipulating data or even compromising security for their selfish reasons [26]. Their motivations are usually strong desires to access data from individuals such as usernames, passwords, and bank accounts to manipulate them for their beneficial interests. Black hat hackers can also hack foreign or their competitor's systems. This conduct is illegal and can never be justified as beneficial since malicious hackers would attack even very critical systems to satisfy their interests and wants. Despite that white hat hacking is ethical, the personnel can be proclaimed as black hat hackers if they access restricted networks when solving security issues in databases of various companies [27]. As such, it is vivid that the description of a hacker is determined by his or her intentions ones permitted to access a system by a client.

C. Grey Hat

In between a white and black hat hacker is a grey hat hacker. A grey hat hacker does not have malicious intentions toward the systems they hack. They find vulnerabilities in systems without the permission of the owner and patch any holes available to eradicate risks hacking possibilities [28]. Grey hackers have no malicious intentions since no real benefits to them exist [29]. Nevertheless, they exploit data and may also cause losses. For example, a hacker might hack into a banking system and unveil all the information about the bank to everyone. This hacker is classified as a grey hat hacker because he or she did not gain any personal benefits but might mess with the information from the bank system. As such, these issues might distinguish risks or further damages that depict total losses. Therefore, the significance of grey hat hacking is determined by whether the result will minimize or intensify the vulnerability of the systems.

D. How the Public can Protect their Information

The public needs to take precautions to protect their information from online vulnerabilities since they can never predict whether they will be victims of cyberattacks. Despite how strong the systems may appear; hackers can always detect a weakness that increases the vulnerability situation. One of the remedies is that the device owners should employ white hat hackers to regularly test their devices and systems for any faults [30]. This strategy helps them to patch the gaps before the hackers access them. The weaknesses sometimes emanate from the attempts of opening insecure sites on the internet by users. As such, users should always analyze the vulnerability of websites of interest and be sure of the security details irrespective of the provided information [31]. Another agenda is that public Wi-Fi also exposes the user’s data to vulnerabilities. Such connections are less secure compared to the private ones because it is difficult to identify the intention of the subscribers. Therefore, public members should ensure that the internet connection at reach is secure or opt for private internet services.

Another situation is that hackers try to access accounts by guessing passwords. As such, setting weak password intensifies the ease of black hat hacking. This challenge can be resolved by ensuring that users limit the accessibility to their user accounts or confidential information on social networking sites. In cases where the emails or usernames must be exposed, it is advisable to rotate and utilize strong passwords that reduce the ability of hackers to penetrate the security systems of the service providers [32]. Also, using password managers can help in enhancing the security of

accounts and information. They generate long and difficult to guess passwords leaving no room for hackers to crack them.

Educating the public should also assist in learning to seclude their personal information from emails, text messages and other online conversations. Laws should also be developed to counter unethical hacking practices in schools and at public levels [33]. Persons should also decide to set up security measures as well as using the internet in a safe and responsible manner.

V. Conclusion

Therefore, this paper has discussed the various types of hacking and how the public can protect their information. Hacking is seen as an unlawful activity. However, this discussion posits that ethical hacking is not for any malicious gains, and it is legal. Black hacking is illegal, and their interests always lead the hackers behind it. On the other hand, Grey hat hackers operate with no own interests. They may alter the confidential information but still patch the weaknesses in systems. Again, the public plays a crucial role in ensuring that data is safe. Verifying people who access personal information, public network connections, the security of websites, and the nature of password is significant in protecting confidential data from black hat hackers. Still, people should learn how to scan devices and identify weaknesses and vulnerability.

.

Acknowledgment

L.A. Nguyen thanks Jennifer Grant. For all their help and inspiration to complete this paper. If it were not for the influence of the wise. The desire to learn and explore the further depths of cyber security, and various methodologies of hacking was sparked by your inspiration.

References

[1] A. Knowles, and Ibm, “How Black Hats and White Hats Collaborate to Be Successful,” Security Intelligence, 01-May-2018. [Online]. Available: https://securityintelligence.com/how-black-hats-and-white-hats-collaborate-to-be-successful/.

[2] M. W. Kranenbarg, T. J. Holt, and J. van der Ham, “Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure,” SpringerLink, 19-Nov-2018. [Online]. Available: https://link.springer.com/article/10.1186/s40163-018-0090-8.

[3] A. lukegalbraith, “Hackers – The Need to be Smart Online,” My thoughts, feelings and opinions, 07-Sep-2016. [Online]. Available: https://lukeygal.wordpress.com/2016/09/07/hackers-the-need-to-be-smart-online/.

[4] M. Burgess, “What is the Internet of Things? WIRED explains,” WIRED, 16-Feb-2018. [Online]. Available: https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot.M. Webster, "Merriam Webster," Merriam-Webster Incorporated, 9 December 2019. [Online]. Available: https://www.merriam-webster.com/dictionary/hacker?utm_campaign=sd&utm_medium=serp&utm_source=jsonld.

[5] D. Fiery, Secrets Of A Super Hacker: The Knightmare, Port Townshend: Loom Panics Unlimited, 1994.

[6] P. staff, "CNN.com/sci-tech," Time Warner, 19 November 2001. [Online]. Available: http://www.cnn.com/2001/TECH/internet/11/19/hack.history.idg/?related.

[7] P. staff, "CNN.com/sci-tech," Time Warner, 19 November 2001. [Online]. Available: http://www.cnn.com/2001/TECH/internet/11/19/hack.history.idg/?related.

[8] D. K. a. M. G. Solomon, Fundamentals of Information Systems Security Third Edition, Burlington: Jones & Bartlett Learning LLC, 2018.

[9] D. K. a. M. G. Solomon, Fundamentals of Information Systems Security Third Edition, Burlington: Jones & Bartlett Learning LLC, 2018.

[10] D. K. a. M. G. Solomon, Fundamentals of Information Systems Security Third Edition, Burlington: Jones & Bartlett Learning LLC, 2018.

[11] D. K. a. M. G. Solomon, Fundamentals of Information Systems Security Third Edition, Burlington: Jones & Bartlett Learning LLC, 2018.

[12] D. K. a. M. G. Solomon, Fundamentals of Information Systems Security Third Edition, Burlington: Jones & Bartlett Learning LLC, 2018.

[13] D. K. a. M. G. Solomon, Fundamentals of Information Systems Security Third Edition, Burlington: Jones & Bartlett Learning LLC, 2018.

[14] D. K. a. M. G. Solomon, Fundamentals of Information Systems Security Third Edition, Burlington: Jones & Bartlett Learning LLC, 2018.

[15] D. K. a. M. G. Solomon, Fundamentals of Information Systems Security Third Edition, Burlington: Jones & Bartlett Learning LLC, 2018.

[16] D. K. a. M. G. Solomon, Fundamentals of Information Systems Security Third Edition, Burlington: Jones & Bartlett Learning LLC, 2018.

[17] Coos, A. A. (2019, February 15). 5 Ways Big Companies Protect their Data. Retrieved December 7, 2019, from https://www.endpointprotector.com/blog/5-ways-big-companies-protect-their-data/.REPLACE https://www.observeit.com/ponemon-report-cost-of-insider-threats/

[18] Talesh, S. A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as “Compliance Managers” for Businesses. *Law & Social Inquiry*, *43*(2), 417–440. https://doi.org/10.1111/lsi.12303

[19] Coos, A. A. (2019, February 15). 5 Ways Big Companies Protect their Data. Retrieved December 7, 2019, from https://www.endpointprotector.com/blog/5-ways-big-companies-protect-their-data/.

[20] Rafter, D. (n.d.). 2019 Data Breaches: 4 Billion Records Breached So Far. Retrieved December 7, 2019, from https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html.

[21] Rafter, D. (n.d.). 2019 Data Breaches: 4 Billion Records Breached So Far. Retrieved December 7, 2019, from https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html.

[22] Marsh, Devin. "Are Ethical Hackers the Best Solution for Combating the Growing World of Cyber-Crime?." PhD diss., University Honors College, Middle Tennessee State University, 2017. 5

[23] Porterfield, Jason. *White and Black Hat Hackers*. The Rosen Publishing Group, Inc, 2016. 7.

[24] Marsh, Devin. "Are Ethical Hackers the Best Solution for Combating the Growing World of Cyber-Crime?." PhD diss., University Honors College, Middle Tennessee State University, 2017.4

[25] Ibid., 7

[26] Nanda, Sanchit. “World of White Hat Hackers.” *International Journal of Scientific & Engineering Research* 10, no. 5 (May 5, 2019): 4

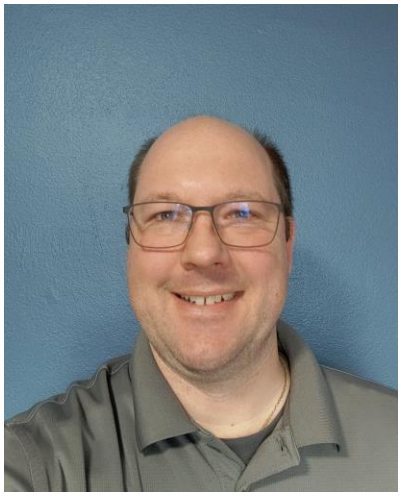
[27] Buch, Rachna, Dhatri Ganda, Pooja Kalola, and Nirali Borad. "World of Cyber Security and Cybercrime." (2017). 20

[28] Marsh, Devin. "Are Ethical Hackers the Best Solution for Combating the Growing World of Cyber-Crime?." PhD diss., University Honors College, Middle Tennessee State University, 2017.

[29] Buch, Rachna, Dhatri Ganda, Pooja Kalola, and Nirali Borad. "World of Cyber Security and Cybercrime." (2017).

[30] Marsh, Devin. "Are Ethical Hackers the Best Solution for Combating the Growing World of Cyber-Crime?." PhD diss., University Honors College, Middle Tennessee State University, 2017.

[31] Jaksa, Joseph J., and Anne R. Tapp. "Hackers: What Role Does Education Play?." *US-China Education Review* 6, no. 8 (2016): 508-512.



Kevin J. Flanagan, was born in Rochester, NY in January of 1974. Kevin has received an Associate Arts degree from Saint Paul College, Saint Paul, MN, United States of America in 2014. Kevin major field of study is in computer information technology.

He has worked for Seasonal Concepts where he helped install and train the GERS Point of Sale user side software. He has worked for Independent School District 622 as a paraprofessional helping manage behaviors and develop Individual Behavior Plans for children and youth. He is now currently employed with Metropolitan State University in Saint Paul, MN, United States of America. He works as an IT specialist that assists with the implementation of user hardware and software. He has helped write an article regarding Data Mining and the protection of Private Data for his ICS 311 Database Management Systems class.

Mr. Flanagan has not received any recognition or awards yet for his efforts as he is still working towards his Bachelor of Science Degree.

Susanna S. Gottel was born in Minneapolis, Minnesota in November of 1984. Susanna as earned her Associates of Arts degree from North Hennepin Community College in Brooklyn Park, MN, United States of America in 2010. Susanna's major field of study is in cybersecurity.

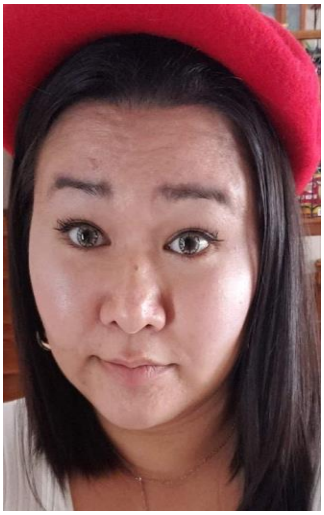
She has worked as a Radiological Technician at the VA Hospital and a Human Services Technician. She currently works for the Minnesota Department of Veteran Affairs in Minneapolis, MN United States of America as a Scheduling Coordinator for the Nursing department. She has researched and supported the transition of implementing a new database management system for the Minnesota Department of Veteran Affairs.

Ms. Gottel has not received any recognition nor awards yet as she is still pursuing her Bachelor of Science Degree.

Tong H. Thao was born in a refugee camp in Chiang Kham, Thailand in 1993. Tong is currently pursuing his Bachelor of Science Degree in Computer Information Technology at Metropolitan State University with plans to graduate in the spring of 2020.

He is currently employed at Metropolitan State University as an Endpoint Support Assistant. He has also complete many short projects ranging from implementing POS systems to setting up ID card machines. Aside from that, He also works as a sound technician for a local church. He is also familiar with many audio visual set ups, along with any needed computer set ups. In his free time He studies for a network security certificate and is currently working towards a few others as well.

Mr. Thao has not received any recognition nor awards yet and is still pursuing his Bachelor of Science Degree.



Lauren A. Nguyen (M'76–SM'81–F'87) was born in St. Paul Minnesota in May 1994. Lauren has graduated Century College in White Bear Lake, Minnesota with an Associate of Science in Computer Information Systems and Health Science, Broad Field. In addition, Lauren has earned a certificate in Internet Programming and Gender Studies. Currently, Lauren is studying computer information systems at Metropolitan State University.

She has worked at HealthPartners as a Support Desktop Specialist Intern. Where she would help with deployment on new infrastructure for the entire corporation. Currently, she is interested in helping others gain knowledge in the ever growing IoT world and hopes to achieve her bachelor's degree. She is hoping to start her own company with a focus on security and development.

Ms. Nguyen has not received any recognitions nor awards yet and is still in pursuit of her Bachelor of Science Degree