How have past cyberattacks affected how different social groups use and interact with software technology today?

A Research Paper Submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Michael J. Kosar

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor
Rider W. Foley, Department of Engineering and Society

Introduction

People and governments have become increasingly reliant on digital systems. This increasing reliance has led to an increase in cyber vulnerabilities throughout the world as more people switch to digital systems to store information and complete daily tasks. In cyberspace, nefarious actors and groups attempt to take advantage of flaws in software design for their own personal gain. Some of the largest and most damaging attacks in recent history include cyberattacks on the Colonial Pipeline, the Ukraine power grid, and the WannaCry ransomware attack (Atkins, 2022). The social groups behind these attacks can be anyone from a singular person in their basement to a criminal syndicate sponsored by a foreign government. Their intentions are often malevolent and can be motivated by money, political power, or personal espionage. Although the common perception of hackers is that of malevolent intentions, an often overlooked group involved in cyberattacks are certified hackers, or "whitehat" hackers. This social group does not carry out cyberattacks with the intent to disrupt or destroy, but instead with the goal of preventing future attacks by penetration testing, which is the act of scouring a computer network in search of bugs or vulnerabilities (Slayton, 2018). These different social groups, among others, can have either an adverse or beneficial effect on technology depending on their objective.

Whoever the actor is and whatever their purpose, they can cause major damage to global social systems. Because of this, major corporations and governments have begun to put an emphasis on cybersecurity and making sure their systems and information are secure. This is a difficult problem to solve due to the vast array of methods used to infiltrate software systems. Some basic methods include DDos, phishing, and sniffing attacks. While DDos attacks are blatant, large-scale attacks determined to deny the service of software, phishing and sniffing

attacks are less obvious and try to hide from plain sight to obtain information covertly. Among these attacks, there are various delivery methods such as trojan horses, viruses, and worms (Chapman, Leblanc, & Partington, 2011). These methods and modes of delivery are improving everyday and malware is constantly evolving. One reason for these vulnerabilities is because of the software designers themselves. Around 60% of vulnerabilities in code are due to the developers lack of careful development and maintenance. High consumer pressure and the demand to deliver features and requirements quickly forces developers to allow security to take a back seat (Larios-Vargas et al., 2022).

In order to address these issues posed by hacker groups and new malware, I chose to look back at real world examples of these attacks, their effects on society, and the subsequent response to them. This will allow us to develop methods based on past experience and knowledge that will enable detection and prevent future attacks. By using real-world case studies and Pinch and Bijker's Social Construction of Technology framework (Pinch & Bijker, 1984), I will be discussing how past cyberattacks have affected how various social groups interact with the technology they use.

Case Context

In today's world, there is a large effort to determine how we can effectively analyze, acknowledge, and prevent cyberattacks before they occur. With cyberattacks on the rise, the biggest issue for companies is data security and ease of access for cyberattacks, according to the Cyber Security Challenges Model (Khan et al., 2022). Companies that hold large amounts of personal data or those with critical infrastructure roles are most at risk of this exploitation. According to Pew Research, many Americans do not trust private institutions such as banks and

hospitals to protect their personal data. This is most likely because 64% of Americans have experienced some form of personal data breach (Olmstead & Smith, 2022). Because of this, companies have started requiring software developers to complete mandatory cybersecurity training in order to improve their skills and better secure their code (Gasiba, Beckers, Suppan, & Rezabek, 2019). In addition to the private sector, the federal government is having similar issues. The majority of the United States Air-Force's technologies rely on radar and transmission data. Typical aircraft have around 180 touch points across several networks as well as a variety of onboard processors (Maybury, 2015). This makes them prone to cyberattacks and interference from adversaries which has led to a conscious effort to secure their systems and find ways to identify threats before they occur.

A commonly used adage is to learn from your mistakes. There are thousands of mistakes caused by software developers, whether intentionally or unintentionally. Vulnerability in computer code is almost always a given. Even the largest companies such as Google and Microsoft are still finding bugs in their code. These vulnerabilities leave companies open to attacks. If we can learn how these attacks happened, who was responsible, and what was done in response, we may be able to eliminate commonalities and major errors that occur and thus prevent future attacks. Simply preventing attacks is difficult because there are so many different exploits and delivery methods for attacks. An example of one method is called a brute force attack. It is a very simple but common attack that uses large amounts of computing resources to typically break passwords by trying as many different combinations as possible. Although it is very time consuming, it is effective due to the fact that people generally don't take the time to create secure passwords. This attack is easily countered by strong password security but there is no type of standardized education to teach users basic online safety. This issue falls right back on

the shoulders of software developers when they develop the interface that people use to create passwords. Some say that it is the software developers responsibility to remind or brief the user on password security and make them aware of the clear vulnerability they face when failing to create a strong password. After all, they are the ones creating the software to encrypt and store the passwords. Others say that it is the responsibility of the government to create a standardized response to this issue by requiring developers or companies to teach or advise users on this issue. The issue of cyberattacks is relatively new with the rise of modern communication devices and the Internet of Things. The government has been slow to catch up and implement proper safety measures.

The consequences of cyberattacks can include internal chaos, widespread disruption in the administration of the country, severe damage to the national economy, and many others (Li & Liu, 2021). They affect aviation, banking, defense, energy, water, power, and many other sectors of society. All of these areas have had recent, prominent attacks to learn from (Malik et al., 2022). Making sure that we evolve and learn from our past mistakes has the potential to save money and lives in the future. In order to describe the human and social dimensions of this project, I will use the social construction of technology to help bridge our understanding of how different social groups can influence the evolution of technology.

Social Construction of Cybersecurity Defense

Pinch and Bijker's Social Construction of Technology (SCOT) will be used to analyze the effects of cyberattacks and the social groups that design the software in use today. SCOT is a framework that analyzes how different social groups in society have affected the construction, design, and implementation of various technologies. In a cyberattack, there are many different

social groups involved. The term ‘hacker’ was originally used to describe someone who explored the full-range of capabilities of themselves and their machine but has since become a term for someone who deliberately attempts to undermine and infiltrate another person or company’s computer system for their own gain (Kleen, 2001). This group is the main social group influencing the design of software as they usually cause the most damage and bring awareness to vulnerabilities. Another smaller social group is the ethical or “whitehat” hacker. These are hackers with good intentions who perform penetration testing on software with the permission of the owner with the aim of finding and fixing any vulnerabilities in the software. Then there are governments and legislative bodies who form rules and regulations that can influence how software is created and hold it to certain standards. The next group are the software developers themselves who actually write the code and create the software that is being exploited. Finally, there are the software users who are affected by cyberattacks or data breaches. Keeping these social groups in mind, we can now use SCOT to analyze the problem.

The first step in SCOT analysis is demonstrating that the technology is culturally constructed and interpreted. Software is constantly evolving. As people’s needs and wants change, software changes with it. The popularity of Instagram and Twitter today versus MySpace and AOL 15 years ago is clear evidence that software is culturally influenced and constructed. The developer takes into account common cultural trends that will fulfill the modern user’s appetite.

The second step of SCOT is mapping mechanisms for the stabilization of an artifact. The main way that these cyberattacks are being countered is from a law and regulation standpoint. Both federal and state governments have taken responsibility to enforce stronger cybersecurity by passing bills such as California’s Notice of Security Breach Act and the federal government’s

2002 Homeland Security Act (Srinivas, Das, & Kumar, 2019). Another mechanism for stabilization is for users to take it upon themselves to learn better online safety practices such as creating safer passwords and securely storing them. Finally, the software developers can prevent attacks by simply taking more time and putting more effort into writing secure code and using safer practices amongst themselves.

The third and final step is describing technologies by focusing on the meanings given to them by social groups (Pinch & Bijker, 1984). When a cyberattack is carried out by malicious hackers, there is an immediate effect on society. This effect, which is almost always a negative one, prompts companies and government agencies to spring into action and find ways to prevent these attacks in the future. For hackers, the purpose of cyberattacks is to gain data, cause disruption, or in the case of ransomware, make money. These different intentions vary based on who the hackers are, what kind of malware they have access to, and who they intend to target. A sophisticated state-sponsored hacking group has a large array of available malware and typically targets foreign entities, their critical infrastructure, and companies with large quantities of data. Smaller groups or lone hackers may be limited by ability and target smaller companies or individuals using ransomware to make money. Ethical hackers define cyberattacks as ways to infiltrate software without the negative effects that are associated with most cyberattacks and in turn provide key data that will help prevent those negative effects in the future. From the perspective of a governmental or legislative body, the ability to prevent cyberattacks is a key issue. They have constituencies and large populations to protect from these attacks. This leads to various bills, laws, and regulations that are put forth to mitigate the threat of another attack as well as for political gain (Cavelty & Egloff, 2019). These regulations and laws affect how software developers are able to design their software which in turn affects the users.

From a software developers standpoint, cyberattacks are a direct result of their own inability and inaction to prevent them. These attacks result directly from their software being flawed or bugged whether intentionally or not. Although software developers tend to do everything they can to prevent these attacks, it is often unsuccessful and better practices and awareness are needed. Finally, from a user's perspective, cyberattacks are designed to affect human behavior by causing chaos, confusion, and fear. This in turn affects how users interact with technology and, subsequently, how software developers design their systems by being more cautious and conscious when securing their product (Cayirci & Ghergherehchi, 2011). Users can leave themselves vulnerable to attacks in many ways, but may also be able to prevent them by practicing stronger online safety measures.

Research Questions and Methods

How have past cyberattacks affected how different social groups interact with software today? This is an important question because cyberattacks have become so prevalent in today's society and preventing them is at the front of most software developers' agendas. Analyzing how past events have shaped our current methods and interactions will allow software developers to develop a clearer picture of why they do what they do and how they can improve it in the future. I researched this question by analyzing four case studies that cover past cyberattacks as well as how they impacted society. I collected data on past attacks and, specifically, data on who the attacker was, their motive, how they infiltrated their target, and what the consequences of the attack were. This data will allow me to analyze the different social groups involved, what their role in the attack was, and how they responded if they were affected.

The four cases that will be covered are the recent Colonial Pipeline cyberattack, the WannaCry attack of 2017, the Marriott hotels breach of 2014, and the Office of Personnel Management data breach of 2015 . These four attacks will give us an insight into both foreign and domestic attacks. While two of the attacks affected mainly the United States, the other two had effects that were felt worldwide. This gives a broader understanding of the differences in response between countries. I will first analyze the group that was responsible for the attack as well as the users who were directly affected. After looking at the actual attack and what happened, I will then analyze the response by governments and legislature, if there was any. This allows us to see an objective response to the attacks and the effect the response had on software development. Finally, I will analyze how the software developers responded to the attack. By analyzing various software developer chat rooms and websites, we can understand if the attack had changed their approach to developing at any point or if any change was a direct result of legislation that was passed. I aim to determine what change in software development was brought about by these attacks and what role each social group played in that change.

Results

Each social group played a role in how the attack unfolded and what was learned from it. Users were at fault in at least two of these attacks due to a lack of public knowledge regarding computer safety. These attacks weren’t exactly the result of software developers' failures, but rather due to poor public education regarding password security and keeping systems up-to-date with the latest updates. When looking at the hackers and their intentions, two of these attacks were ransomware attacks and the other two were large scale data breaches. This emphasizes the importance of multiple motivating factors in the cyber field: money, data, and geopolitical gain.

While large foreign governments are more drawn toward bulk data collection and geopolitical targets for means of national security and espionage, smaller countries and hacker groups are drawn toward ransomware as a means to obtain money. When looking at the government as a social group, although there was some oversight and enforcement following a few of these attacks, they haven't done much to enforce better security practices. They've left the responsibility to software developers who, besides putting a stronger emphasis on writing secure code, haven't changed much in their development process. This is because among the attacks discussed, either the means of exploitation is unknown or the fault lies with the software users. Developers can write very secure code but if a user does not secure their password, the system can be compromised. Finally, as discussed later, there is a need for transparency when cyberattacks occur in order to learn from mistakes and provide a better response to future attacks.

Colonial Pipeline is the largest supplier of oil on the east coast of the United States and on May 6th, 2021, a hacker group by the name of DarkSide was able to gain access to their IT system. According to Kerner (2022), they used an out-of-date VPN password that was obtained from a separate data breach. Using this password, the hackers were able to steal over 100 gigabytes of data and install ransomware on the system. This meant that unless Colonial Pipeline paid a ransom, they would not be able to access their own system. Colonial Pipeline immediately paid the $4.4 million dollar ransom in Bitcoin and the pipeline restarted a week later. During the shutdown, the main groups affected were automobile and truck drivers who experienced long waits, increased prices, and shortages at the pump. Airlines were also affected as they did not have the fuel necessary to fly their normal schedules. In response, the federal government implemented a series of laws and regulations beginning with an executive order to strengthen cybersecurity through various steps such as implementing the use of a software bill of materials.

This is essentially a list of software components used in a system which allows system administrators to quickly identify parts of the system and any new vulnerabilities (Kerner, 2022). The other main response by Congress was the passage of the Strengthening American Cybersecurity Act of 2022 which set in place regulations such as the requirement for critical infrastructure companies and agencies to notify the federal government of any threats in a timely manner (Strengthening American Cybersecurity Act, 2022). Software developers responded to this attack by repeating the need to secure passwords and not reuse passwords across different sites. They also highlighted a greater need for IT resilience (Mello, 2022).

According to Kaspersky (2022), a group of hackers believed to be from North Korea took advantage of a known exploit in Microsoft Windows systems in 2017. This attack was known as the WannaCry attack. Although Microsoft knew about this vulnerability and had issued a patch for it, many people and organizations were slow to update their computer systems and were left vulnerable. Using this vulnerability, the hackers were able to place ransomware in the users computer and take control of all of the users files and data until a payment of $300-$600 was made. This breach affected about 230,000 Microsoft users globally. The victims were mainly in Europe but the attack eventually spread to over 150 countries. Multiple entities were affected, from hospitals to phone companies, causing an estimated $4 billion in losses globally (Kaspersky, 2022). Because this was a global event, there was little governmental response. The blame was put on the United States because the National Security Agency had actually discovered and developed the tools used in this exploit. They were blamed for not privately discussing the exploit with the appropriate entities until the tools were stolen and leaked by a group of hackers known as The Shadow Brokers. As a result, the United States proposed the PATCH Act which would allow an independent board to review exploits in order to balance

public trust and national security (PATCH Act, 2017). The response by software developers was to reiterate the need to update systems regularly. There was a lack of communication between the public and private sectors in regards to the known vulnerability and its potential severity. If there is a known vulnerability, it is essential to update the system immediately when the fix is sent out (Vigliarolo, 2017).

The third attack was the Marriott hotels breach in 2014. According to Fruhlinger (2020a), although this attack occurred in 2014, it wasn't discovered until 2018 when a security system tool discovered an unusual database query. Upon further investigation, Marriott discovered that the database of a company they had merged with, Starwood, had been compromised four years ago. Throughout these four years, almost 500 million personal records of Marriott and Starwood clients had been compromised. These included credit card numbers, passport numbers, and other personal information. Although information like this typically ends up on the dark web, the perpetrator of this crime had other intentions. It is believed the Chinese government was behind the attack and that the personal information stolen could be linked to other data breaches, such as the Office of Personnel Management breach that will be discussed later. These attacks were believed to be a Chinese attempt at stealing large amounts of data on U.S. personnel and government officials, many of which used Marriott services during their trips. The governmental response to this was minimal, with the United Kingdom imposing a fine of about $120 million on Marriott for their negligence. One main software development flaw was that not all the records were encrypted and the ones that were encrypted had their encryption keys stored on the same server which allowed easy access (Fruhlinger, 2020a). Not much is known publicly about how the breach actually occurred, which means software developers have not been able to publicly respond to this event, but there has been a push by large corporations to thoroughly vet

the systems of a company that they may be buying or merging with in order to protect clients data (Poston, 2019).

In 2015, it was discovered that Chinese state-sponsored hackers had gained access to and exfiltrated data from the Office of Personnel Management (OPM). OPM is in charge of storing the data of every government employee and contractor in the United States. Because of this breach, the hackers stole 21.5 million social security numbers and 5.6 million fingerprints (Office of Personnel Management). This largely affected government employees, especially those who work undercover overseas. Fruhlinger (2020b) states that in response, the U.S. federal government offered free credit monitoring and held multiple congressional hearings which resulted in the firing of OPM top executives. This attack had two motivating factors: data collection and geopolitical gain. It is also widely believed that the group connected to this attack were also responsible for another hack of Marriott Hotels which leaked the data of millions of Marriott clients. This clear connection between attacks helps to draw a picture of the desires of a nation state hacker such as China. Due to national security interests, how OPM was breached is not exactly known. Their poor security practices, such as not implementing two factor authentication, are believed to be the main cause (Fruhlinger, 2020b).

The final aspect to analyze is the lack of technical information available in at least two of these cases. In the Marriott and OPM cases, there is little to no information on how exactly the hackers exploited each system. For reasons unique to each company or agency, major victims of cyberattacks don't often report on the technical details of attacks. This presents a major problem if we want to improve and advance in the field of cybersecurity. Without knowledge about how these attacks happened, it is very difficult for the software development community to put in place safer practices and techniques. Software development relies heavily on learning from

previous implementations of similar software, both good and bad. Without the information needed to learn, it is hard to make meaningful change.

Discussion

This research reinforces the idea that it is up to the users to make the change needed. Software developers can only do so much to secure their systems. The general public, or users, are the ones that are tasked with securing their data by implementing proper online security practices. There is also a sentiment when it comes to cyberattacks that it won't happen to me. This research helps to illuminate how easy it is to fall victim to these attacks and shows the reach that these attacks can have worldwide. It is not a matter of if you'll be affected by a cyberattack, but when. By giving valuable information to a company whether it is a hotel, bank, or even the government, you are placing a large amount of trust in them to store your data safely. If these companies or governments don't take the necessary precautions, your information can be stolen. It takes a large scale team effort from the software developers, companies, government, and users in order to safely and securely operate online. This research also backs the push for more transparency in regards to cyberattacks in order to learn from others' mistakes.

The limitations of this research would be that only four case studies are analyzed. There are thousands of cyberattacks everyday and due to time limitations, I could only go in depth for four cases. This severely limits the amount of data taken in and can skew results and findings. By analyzing a more diverse set of attacks there may have been different results or possibly more concrete conclusions. It would also be beneficial to speak directly with a current software developer or cybersecurity expert in the field to get their opinion on the matter, as they are the ones facing these issues daily. The majority of information regarding cyberattacks is not

disclosed publicly in order to protect company assets and vulnerabilities. This means some information is missing which limits the analysis. The true underlying factor of how these attacks occurred may never be known to the public and therefore this paper. Without inside sources, we may not be able to make definitive statements on some aspects of the attacks.

In the future, I would like to have tried to talk with experts in the field such as business leaders, software developers, and cybersecurity experts. These people would be able to give me more insight into the everyday battle they fight to protect their systems. The business leaders could give us insight into the measures they are taking to protect their assets and their clients assets as well as possibly discuss any threats they've faced in the past and how they responded. The software developers and cybersecurity experts would be able to discuss how they've responded to attacks in the past as well as the measures they're taking to better secure their systems. I also would have gone more in depth on the actual software systems in place and looked into how the software itself has changed over time. This would have been difficult to do without direct access to a company's software system but some companies have open source code and it would have been beneficial to take that information into account as well. Finally, I would have analyzed more cases from a geopolitical perspective in order to understand the driving forces behind nation-state attacks such as international relations and trust in political figures.

This information will allow me to grow as a software developer by giving me insight into real world problems that software developers face. People generally think of software development as simply coding a program in order to achieve a goal but they don't often think of the security aspect of it. This research made me realize the amount of trust that is put into software and therefore the responsibility that developers have to make sure it is safe and secure. I

now have a better understanding of various reasons why and how people and companies are attacked. Using this information I can better understand which systems are likely to be targeted and how to mitigate any potential vulnerabilities. This newfound awareness will help me to educate my peers as well as the general public regarding online safety practices and potential vulnerabilities.

Conclusion

There has been an increase in cyberattacks across the world due to the rise of technology use in everyday life. These attacks affect every aspect of society and can change the way we function, with some arguing that the psychological effects of cyberattacks can rival those of traditional terrorist attacks (Gross, Canetti, & Vashdi, 2016). The results of this paper can have much broader significance than simply research data to look at. It can have real world implications by using the data gathered, analyzing the conclusions, and forming a better understanding of how we have responded to attacks in the past. Using that information, entities in charge of securing the world's networks, from software developers to national governments, can implement better techniques and safeguards to prevent future attacks. The next steps in this research would be to pull information and analyze a much broader array of cyberattacks. This paper only analyzes four case studies but with the addition of more cases from a broader range of scenarios, we can get a more in depth and complete comprehension of the global response to cyber incidents. The biggest takeaways from this research are the need for more public education of online safety practices as well as more transparency and disclosure of data when it comes to figuring out how the attack happened. This allows software developers to learn from mistakes

and for society to put more trust in technology. This will enable us to move forward as a society and ensure we have a safe and secure future in the use of technology.

References

Atkins, H. (2022, March 24). The Biggest Cyberattacks in History. Retrieved September 25, 2022, from https://www.historyhit.com/the-biggest-cyberattacks-in-history/

Cayirci, E., & Ghergherehchi, R. (2011). Modeling cyber attacks and their effects on decision process. *Proceedings of the 2011 Winter Simulation Conference (WSC)*. doi:10.1109/wsc.2011.6147970

Cavelty, M. D., & Egloff, F. (2019, June 20). The Politics of Cybersecurity: Balancing Different Roles of the States. *St Antony's International Review, 15 (1),* 37-57.

Chapman, I., Leblanc, S., & Partington, A. (2011). Taxonomy of Cyber Attacks and Simulation of Their Effects. *Proceedings of the 2011 Military Modeling & Simulation Symposium (MMS '11)* . doi:10.5555/2048558.2048569

Fruhlinger, J. (2020a). Marriott Data Breach FAQ: How did it happen and what was the impact? Retrieved March 1, 2023, from https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html

Fruhlinger, J. (2020b). The OPM Hack explained: Bad security practices meet China's Captain America. Retrieved March 1, 2023, from https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists, 72*(5), 284-291. doi:10.1080/00963402.2016.1216502

Gasiba, T. E., Beckers, K., Suppan, S., & Rezabek, F. (2019). On the requirements for serious games geared towards software developers in the industry. *2019 IEEE 27th International Requirements Engineering Conference (RE)*. doi:10.1109/re.2019.00038

Kaspersky. (2022, March 09). What is WannaCry ransomware? Retrieved March 1, 2023, from https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry

Kerner, S. (2022, April 26). Colonial pipeline hack explained: Everything you need to know. Retrieved March 1, 2023, from https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know#:~:text=The%20attackers%20stole%20100%20gigabytes,prevent%20the%20ransomware%20from%20spreading

Khan, A. W., Zaib, S., Khan, F., Tarimer, I., Seo, J. T., & Shin, J. (2022, June 02). Analyzing and evaluating critical cyber security challenges faced by vendor organizations in software development: SLR Based Approach. *IEEE Access, 10*, 65044-65054. doi:10.1109/access.2022.3179822

Kleen, L. J. (2001). Malicious hackers: A framework for analysis and case study. Retrieved October 27, 2022, from https://scholar.afit.edu/etd/4646/

Larios-Vargas, E., Elazhary, O., Yousefi, S., Lowlind, D., Vliek, M., & Storey, M. (2022, May 24). DASP: A framework for driving the adoption of software security practices. doi:10.48550/arXiv.2205.12388

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. doi:10.1016/j.egyr.2021.08.126

Malik, A. W., Abid, A., Farooq, S., Abid, I., Nawaz, N. A., & Ishaq, K. (2022). Cyber threats: Taxonomy, impact, policies, and way forward. *KSII Transactions on Internet and Information Systems, 16*(7). doi:10.3837/tiis.2022.07.017

Maybury, M. (2015). Toward the assured cyberspace advantage: Air force cyber vision 2025. *IEEE Security & Privacy, 13*(1), 49-56. doi:10.1109/msp.2013.135

Mello, J. P., Jr. (2022, June 07). How the Colonial Pipeline Attack has changed cybersecurity. Retrieved October 27, 2022, from https://www.csoonline.com/article/3662776/how-the-colonial-pipeline-attack-has-changed-cybersecurity.html#:~:text=Another%20government%20reaction%20to%20the,ransomware%20payments%20within%2024%20hours

Olmstead, K., & Smith, A. (2022) Americans and Cybersecurity. Retrieved February 5, 2023, from https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artifacts: Or how the sociology of science and the Sociology of Technology might benefit each other. *Social Studies of Science, 14*(3), 399-441. doi:10.1177/030631284014003004

Poston, H. (2019, August 7). Lessons Learned: The Marriott Breach. Retrieved March 1, 2023, from https://resources.infosecinstitute.com/topic/lessons-learned-the-marriott-breach/

S.1157 - 115th Congress (2017-2018): PATCH Act of 2017. https://www.congress.gov/bill/115th-congress/senate-bill/1157?q=%7B%22search%22%3A%5B%22patch+act+2017%22%5D%7D&s=3&r=1

S.3600 – 117th Congress (2021-2022): Strengthening American Cybersecurity Act. (2022, March 1). https://www.congress.gov/bill/117th-congress/senate-bill/3600

Slayton, R. (2018). Certifying "ethical hackers". *ACM SIGCAS Computers and Society, 47*(4), 145-150. doi:10.1145/3243141.3243156

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in Cyber Security: Framework, standards and recommendations. *Future Generation Computer Systems, 92*, 178-188. doi:10.1016/j.future.2018.09.063

U.S. Office of Personnel Management. (n.d.). Cybersecurity Incidents. Retrieved March 1, 2023, from https://www.opm.gov/cybersecurity/cybersecurity-incidents/

Vigliarolo, B. (2017, July 25). Report: The IT response to Wannacry. Retrieved March 1, 2023, from https://www.techrepublic.com/article/report-the-it-response-to-wannacry/