Increasing the Cybersecurity Standards of Websites and Applications

(Technical Paper)

The Line Drawn in Ethics in Cybersecurity

(STS Paper)

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree

Bachelor of Science, School of Engineering

Samantha Jade Chiang

Fall, 2020

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

Signature ____ Date __________

Samantha Jade Chiang

Approved ____ Date __________

Aaron Bloomfield, Department of Computer Science

Approved ____ Date __________

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction

As the workspace classes move towards an online space, a multitude of issues and challenges arise, such as adapting to a new learning and working environment, widespread internet connectivity problems, and much more. Online platforms such as Zoom have recently come into the forefront, not only because of its prominence in the online classroom, but because of the cyber attacks that it has been facing. This include accounts being leaked and sold, as well as "... 'Zoombombing' (in which uninvited attendees break into and disrupt meetings with hate-filled or pornographic content), [which has lead to] Zoom's security practices have been drawing more attention --along with at least three lawsuits against the company" and have reignited the discussion around cybersecurity (Chawla, A., 2020, p. 6). If these problems in the cybersecurity of such widely used applications are ignored, this could possibly lead to more people's sensitive information being leaked or even the shutdown of the application's or a company's servers. There are many challenges to the actual implementation of strong cybersecurity practices, but the most basic of which concerns the current standards currently in place. Though the federal government has released a framework for companies to follow, it has been proven to lack the details and refinement needed to adequately protect digital assets.

The technical topic of this paper will address this lapse in cybersecurity by outlining a project aiming to create a detailed, up-to-date framework that can be modified depending on the company or individual following it. The STS topic will then focus on the morality of such practices. This moral issue is harder to evaluate and find a conclusion to, unlike the technical topic. Users place trust in the people who test the security of systems, who have access to the sensitive information of these users. Additionally, the methods in which they use to test these systems can possibly be sketchy and unethical. Though morality can differ from person to person, the way to resolve this problem is to create standards that clearly define appropriate testing measures.

Technical Topic: Increasing the Cybersecurity Standards of Websites and Applications

In 2014, the National Institute of Standards and Security (NIST) released the first version of its cybersecurity framework in order to provide guidance in assessing cybersecurity systems and increasing them in order to respond to cyber attacks. It outlines five basic principles: “Identify” -- basics of cybersecurity in the scope of people, assets, and data; “Protect” -- methods of defense against attacks; “Detect” -- what to look for when identifying an attack; “Respond” -- actions to take in the event of an attack; and “Recover” -- plans for addressing the aftermath of an attack. The five further break down into 23 categories and subcategories, which go more in depth for each of the principles. Though it is not the only guide for cybersecurity practices, it is the most common framework used in the US. Many companies, and even other governments, use this framework in order to protect their digital platforms. In the time since release, it has only been updated once, first circulating for public comment in 2017, then finally published in 2018. This presents an issue, as technology and practices within the cybersecurity landscape changes rapidly.

Proponents of this framework will argue that it would not be worth the time and resources to update the contents every year, and that the suggestions set forth are not meant to be a replacement for a security policy, but rather a baseline to build off of. However, many experts agree that the framework is severely lacking. In his analysis of the NIST framework, Hitchcox outlines four of these criticisms, “(a) guidance too high-level and outdated, (b) limitations negatively affect guidance implementation, (c) lacking understanding of cybersecurity importance, and (d) compliance is not security” (Hitchcox, 2020, p. iii). These are problems that must be addressed sooner rather than later, as it is the basis of security of many companies and people, as well as their information.

As we have seen in the past, failure to put adequate effort into creating a strong cybersecurity system can lead to devastating consequences, not just in a financial sense, but productivity or even psychological damage or strain as well. Attacks can result in "...damage and destruction of data, forensic investigation, restoration and deletion of hacked data and systems, fraud, post-attack disruption to the normal course of business, stolen money, lost productivity, theft of personal and financial data, embezzlement, and reputational harm and theft of intellectual property" (Ahmad, T. 2020, p. 1).

Though it is obvious why the guidelines set forth within the NIST framework are not enough for a complete cybersecurity system, it provides a good starting point to expand upon. The technical project will be exactly this, an expansion of the NIST framework that will incorporate the previous iteration's idea while modifying them so that the contents are up to date. The wording must also be changed to both emphasize the importance of following the best practices outlined in the document and simplified so that more potential readers will be able to understand the proposed recommendations.

One of the main challenges faced with the reconstruction of the framework is the overhead that such an undertaking would require. For example, this could be the time needed to collect the proper information in order to consolidate it. Additionally, different experts in the field would likely have differing opinions on the definition of best practices and prefer one methodology over the other. If a best solution cannot be universally agreed upon, the new framework should list all possible solutions when dealing in a particular topic within cybersecurity, as well as the pros and cons of each. The user of the framework would then be able to find whichever works best for them depending on the particular situation they are faced with.

STS Topic: The Line Drawn in Ethics in Cybersecurity

The topic of morality has been heavily debated within the cybersecurity field. On the one hand, there are “white hats”, users who are employed to test a system and work within clearly set limitations in order to do so. “Black hats” are the polar opposite, working in order to cause damage, such as by stealing information or by shutting down systems through weak points in their code. The last is the “grey hat”, which stands between the previous two on morally ambiguous grounds. C. Dianne Martin phrases this best when she describes them as “...those who break the law but without criminal intent …. [which] may include cyber vandals who deface websites and so-called rogue security researchers who publicly share discovered vulnerabilities without notifying or receiving prior permission from their targets” (C. Dianne Martin, 2017, p. 34). The similarity between all three, however, are the applications and other assets, both software and hardware, at their disposal. What separates them is the reason behind their actions, and if they have permission to test the networks or applications in which they are trying to access and test.

In this morality debate, some of these “grey hat” individuals may argue that, even if they use methods that could be seen as questionable or even illegal, they are working for the ultimate good to find flaws in systems and improve the overall cybersecurity of whatever system they are trying to access. However, this sets a shaky precedent about the limitations one can go to in order to perform actions that they believe are just and morally sound. The “grey hat”, for example, might not be as experienced as a “white hat” who is hired to perform the test on the same program. This inexperienced vigilantes can cause serious damage, as “without prior knowledge and experience with the computer system in question, the actions of the hacker may well break the functionality of crucial software and/or hardware, and … any destruction of the computing … regardless of whether not it is done accidentally, is a bad consequence and a morally wrong action" (Falk, 2004, p. 2).

Currently, the Information Systems Security Association (ISSA) has a Code of Ethics for cybersecurity professionals to follow, and it highlights important points such as adhering to laws and not intentionally doing harm. However, these codes are general and are not enforced. The deliverable of this section will focus on researching the ISSA's Code of Ethics, as well as other documents and records concerning the ethics in cybersecurity. This is to gain a better understanding of the conversation surrounding this debate.

If this question about the morality of cybersecurity practices is not addressed and decisively answered, it could lead to any amount of morally ambiguous "gray hats" imposing their own definition of security onto these systems, which may end up causing more damage than good. Instead of these "grey hats" offering their unprompted help, companies should be in charge of their own security and have the freedom to determine which methods they wish to use in order to protect their digital assets. This does not relinquish them from the responsibility of not providing adequate security, or perhaps not protecting their system altogether. When a user uses a company's product or services, they do so with the assumption that the company will adequately protect the information that they entrust to them.

Conclusion

The creation of a new cybersecurity framework, or rather an extension of the NIST framework and other guidelines, would help to drastically improve the cybersecurity standards of many companies. This would mean that companies would have better preventative measures against cyberattacks and be better prepared to respond and recover in the case that such an event does occur. This helps the company face fewer losses in the cases where their systems might be shut down or their databases leaked, as well as the people whose information is in their systems, such as passwords, emails, social security numbers. Additionally, if the framework is written in text that is easier to read for people who are not as familiar with technical terms, it will help to promote the spread of good cybersecurity practices as well. The issue of safety on the online sphere is not one that should be taken lightly. As the world moves more and more towards the online workplace, cyberattacks become increasingly more frequent. If steps are taken to educate everyone, then people will have the knowledge to better prevent, but also better recover from these cyber attacks.

References

Ahmad, T. (2020). Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3568830

C. Dianne Martin The George Washington University, Martin, C., University, T., Profile, T., College, H., Cross, C., . . . Author: C. Dianne Martin The George Washington University The George Washington UniversityView Profile Authors Info & Affiliations. (2017, February 01). TAKING THE HIGH ROADWhite hat, black hat: The ethics of cybersecurity. Retrieved October 15, 2020, from https://dl.acm.org/doi/10.1145/3043955

Chakravarty, A., & Melendres, J. (2020). *Cybersecurity Risks Increasing During COVID-19 Pandemic | JD Supra*. JD Supra. Retrieved 8 October 2020, from https://www.jdsupra.com/legalnews/cybersecurity-risks-increasing-during-38481/.

Chawla, A. (2020). Coronavirus (COVID-19) – 'Zoom' Application Boon or Bane. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3606716

Cheung, K. (2020). *Cybersecurity in Cyber Warfare: The Application of Demon Game Models*. INFORMS. Retrieved 8 October 2020, from https://www.informs.org/Publications/OR-MS-Tomorrow/Cybersecurity-in-Cyber-Warfare-The-Application-of-Demon-Game-Models.

Falk, C. (2004). Gray Hat Hacking: Morally Black and White. Cyber Security Group (CSG) Training Conference. doi:https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/bibtex_archive/2004-20.pdf

Hitchcox, Z. (2020). *Limitations of Cybersecurity Frameworks that Cybersecurity Specialists must Understand to Reduce Cybersecurity Breaches* (Order No. 28086762). Available from ProQuest Dissertations & Theses Global. (2438613763). http://proxy01.its.virginia.edu/login?url=https://www-proquest-com.proxy01.its.virginia.edu/docview/2438613763?accountid=14678

Jalali, M., Landman, A., & Gordon, W. (2020). Telemedicine, Privacy, and Information Security in the Age of COVID-19. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3646320

Macnish, K., & Ham, J. V. (2020). Ethics in cybersecurity research and practice. Technology in Society, 63, 101382. doi:10.1016/j.techsoc.2020.101382

Nicol, D. (2020). In the Petri Dish: Cybersecurity Pushed to the Edge. *IEEE Security & Privacy*, *18*(3), 4-5. https://doi.org/10.1109/msec.2020.2983357

Okereafor, K., & Marcelo, A. (2020). Addressing Cybersecurity Challenges of Health Data in the COVID-19 Pandemic. *International Journal In IT & Engineering*, *8*(6). Retrieved 8 October 2020, from https://www.researchgate.net/profile/Kenneth_Okereafor/publication/341894685_Addressing_Cybersecurity_Challenges_of_Health_Data_in_the_COVID-19_Pandemic/links/5ed84885299bf1c67d3bb1f3/Addressing-Cybersecurity-Challenges-of-Health-Data-in-the-COVID-19-Pandemic.pdf.

Shen, L. (2014). THE NIST CYBERSECURITY FRAMEWORK: OVERVIEW AND POTENTIAL IMPACTS. *Journal of Internet Law, 18*(6), 3-6. http://proxy01.its.virginia.edu/login?url=https://www-proquest-com.proxy01.its.virginia.edu/docview/1639830271?accountid=14678

Vagle, J. (2020). *Zoom and the Problem of Cybersecurity Moral Hazard*. Reading Room. Retrieved 8 October 2020, from https://readingroom.law.gsu.edu/faculty_pub/2961/.

Williams, C., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity Risks in a Pandemic. *Journal Of Medical Internet Research*, *22*(9), e23692. https://doi.org/10.2196/23692