Thesis Project Portfolio

Exploration of Cybersecurity Vulnerabilities and User Awareness on Social Media Platforms

(Technical Report)

A Socio-Technical Analysis and Critique of the NIST and NICE Cybersecurity Frameworks and How They Can Be Improved

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Samantha Jade Chiang

Spring, 2021

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

(Executive Summary)

Criticisms of the Cybersecurity Field Through a Socio-Technical Lens

As cybersecurity threats become seemingly more pervasive, it becomes more important to study the field and understand how such cyberattacks can be carried out so persistently. Both my work in the STS research paper, as well as the technical report, are heavily based in this field, however they do not talk about the exact same subject matter. My STS research paper focused on the shortcomings in the field of cybersecurity, specifically citing and critiquing the NIST framework, which was created by the National Institute of Standards and Technology, an agency of the government designed to promote innovation and industrial competition. The framework aimed to highlight central cybersecurity practices, as a large contributor to this issue. On the other hand, my technical report analyzed the relationship between cybersecurity and social media. When it came time to decide on a topic for the technical project, my partner and I decided it would be best to focus on a different subject as it would allow us to study a different aspect of the cybersecurity field. As the use of the internet grows, the topic of cybersecurity grows more important, which creates many different facets to be studied within this broad field.

My technical project narrowed the focus of the topic of cybersecurity to its relationship with social media. Through a literature review of eight papers on cybersecurity in social media, we found that, as social media becomes more and more prominent in the online sphere, social media users become increasingly more susceptible to cyberattacks. While most social media platforms have some sort of security measures, as well as privacy options for user profiles, this does not prevent all forms of attacks. For example, a user could fall victim to a phishing attack, having their information stolen because of a fake email. It is, instead, up to the user aid in the protection of their own confidential information and data when using these sites. While they cannot do much if the website’s information is leaked as a result of a database breach, for example, they can control aspects such as the strength of their passwords, as well as being careful of the information they post to the public.

In my STS Research, I wrote about the flaws in both the NIST and NICE frameworks, the latter being a guide written by the same branch of government, but focused on the education of employees on cybersecurity. I also touched on how both frameworks contribute to lacking cybersecurity plans, as the NIST framework is widely used yet is outdated and lacks depth and the NICE framework, being published later, does not fill all the flaws that are found within the first framework. After analyzing critiques from cybersecurity experts, I found that the NIST framework fails to cover non-technical issues and does not properly account for companies that are unable to implement the framework as a whole. This presents a problem, as the non-technical aspects of cybersecurity are frequently just as problematic. Additionally, the lack of scalability means that smaller companies will not be able to benefit much, if at all, from the framework. I proposed the creation of a new framework, that will build upon previous work done in both the NIST and NICE frameworks, and will be both up to date and more thorough in the advice that it provides.

It is clear to see the link of cybersecurity between these two projects. However, both approach the subject matter in wildly different ways and broadened my view on the cybersecurity field as I had to research not only the technical facets of cybersecurity, but the non-technical as well. Together, these projects highlighted the themes that we saw in STS 4500, by delving into how society interacts with technology, such as cybersecurity through social media. It also briefly highlights ethics, which we talked about in STS 4600, by discussing the responsibilities that the government body behind the NIST framework owes to those using the framework, as well as the responsibilities due to users by social media platforms.