Adrian A. Valencia

Professor Kirkpatrick

CYSE 200

2 December 2025

**Synthesis of attacks through a predictive knowledge lens**

**BLUF**

The constant updating of technology and cybersecurity reflects how we adapt to threats such as phishing, DDoS, and SCADA system vulnerabilities. However, the way we adapt also reveals gaps that require improvement in predicting attacks. These topics discuss reliable forecasting within the realms of human behavior, digital ecosystems, and engineering infrastructure. A topic that needs to be addressed more is the practice of cybersecurity and the insight required to predict and adapt to new situations of uncertainty, complexity, and inevitability of different scenarios.

**Topic 1 - Phishing Attacks**

In module 4 of class, phishing attacks are a form of social engineering attack where a fake and disguised trustworthy entity communicates in a way to gain access to a user's account information, like logins and other information. There are many phishing methods and strategies that attackers use and exploit. For example, there is spear phishing, clone phishing, whaling, and other types of phishing methods that attackers use. Overall, the goal of phishing is to target the trust of humans rather than the technical side of technology. Phishing is a form that attacks the psychological side of a person's mind and how they react to certain situations under pressure. Going more in depth, spear phishing is the most common type, where an attacker targets certain victims with information about their workplace or recent activity online as leverage to gain their

trust. Additionally, clone phishing is a form of an attacker sending a realistic-looking message; however, they change around certain links or disguise things to get victims to access malicious links. Then there is whaling, a form of attack that targets high-value targets like business executives to bypass internal communications within a system or organization. These forms have many things in common, for instance, disguisement, urgency, and authority that all work on the psychology of the human mind through the attacks.

Mitigation techniques that can be used to counter or prevent phishing attacks can be done through Intrusion Detection Systems (IDS), Two Factor Authentication (2FA), training and awareness, and access controls. IDS are the frameworks within the systems that scan for any malicious activities or policies that are detected through anomalies or signature-based monitoring. 2FA involves a system-based way of authentication where a second layer of protection is added to verify the identity of the user. The 2FA system is commonly used as a basic security measure in today's online society in order to protect information. Awareness training is something that should be taught to everyone, as it is the best form of security. This requires people to become more aware of the different types of attacks for they to prevent being victim to phishing or other forms of attacks.

**Topic 2 - Distributed Denial of Service (DDoS)**

Distributed Denial of Service (DDoS) is an intentional attack that works by overloading resources in a server to conflict with a user from accessing the services being used. DDoS is a common attack that directly hits the availability pillar of the CIA Triad, where the attacks obstruct access to information systems. From the module slides, an example of an attack is the Mirai botnet attack in 2016. In the attack, hundreds of thousands of devices were brought down along the East Coast. During this attack, many devices were brought that had default logins and

were rarely serviced. These devices were then infected, creating large amounts of malicious traffic towards servers with great volume, causing stress in the systems.

Some ways to mitigate the attacks of DDoS are traffic monitoring, firewalls, and VPN segmentation. By monitoring traffic within systems, we can identify any ongoing anomalies within the network and see how components of software, like the CPU, are being used in malicious or harmful ways. By installing and implementing firewalls, networks will be more secure by having layers of protection that don't allow for a single vulnerable point of control to be attacked. Furthermore, using VPN's allows for stronger and secure connections and communication channels where everything will be encrypted, reducing the risks of vulnerable attacks occurring. These methods help shift the reactive monitoring to proactive by taking actions and preventing attacks by being more secure.

**Topic 3 - SCADA System Vulnerabilities**

Supervisory Control and Data Acquisition (SCADA) systems are the physical software and hardware structures and systems that were created to help control processes of manufacturing, water systems, utilities, and other physical operations that go on. The SCADA systems are made of different components like sensors and actuators, PLCs, RTUs, Telecommunication channels, and SCADA servers. Each component has different functions; for example, the sensors and actuators help maintain pressure, temperature, flow meters, and other factors that contribute to the maintenance of the structures. PLCs are programmable logic controllers that are you for deterministic control of the systems to change the systems, while the RTUs exchange the data from the systems. Finally, the SCADA servers are used to scan and detect the servers for analysis to make a decision on what's best for the infrastructure. These components support the monitoring of the industry by having evaluations for the processes of the

critical infrastructure. Some vulnerabilities of SCADA include weak physical protection, limited computational power, and outdated devices. Due to the fact that infrastructure is widely distributed, the physical security of systems like power grids and agricultural systems is weak and vulnerable to outside threats. Additionally, the controllers used within SCADA are commonly lacking the power to encrypt advanced defense methods, leaving vulnerability gaps. The sensors and data are vulnerable to spoofing, replay attacks and are capable of denying service disruptions. Furthermore, outdated devices leave SCADA vulnerable to new operating systems, physical inaccessibility, or out-of-production devices.

Mitigation techniques for these vulnerabilities can be simple solutions, like design principles and cybersecurity controls over the industrial systems. For example, creating a basis where assumptions of errors will occur can be a quick solution for repairing designs and systems. This allows for a smooth system to be run without any logical errors that the operators run into when trying to fix the systems or create adjustments. On the cybersecurity side, implementing programs and conducting vulnerability checks and scans allows for a more secure work environment by patching areas that are vulnerable. A factor that should always be considered is the education and awareness of the staff of cybersecurity to be alert to the possible errors that can occur.

The vulnerabilities of SCADA connect with phishing and DDoS attacks through human weakness, insecure devices, and unpredictable errors within the complex systems used in the world today. From weak passwords and training, human weaknesses leave more vulnerabilities than the complex system designs themselves. The physical components and outdated devices limit the traffic and networking of both SCADA and organizations all around. In essence, the

problems lead to understanding the systems and the vulnerabilities by predicting the possible vulnerabilities that are out for attack.

**Philosophical Discussion**

The philosophical question asked is, How far can prediction take us? And where does it fail due to complexity, uncertainty, or human behavior? Through phishing, the prediction of limits in human behavior is exposed, showing the unreliability. While being aware can reduce the risk, room for error still exists in the cognitive mind through things like trust, emotions, and assumptions. Due to phishing being mainly cognitive, many people fall for the attacks and become victims due to their decision-making and forecasting of the possibilities. Adding on, Limits across the digital systems through DDoS can be seen through the Mirai botnet case. The case shows the importance of engineers and their inability to predict the vulnerabilities within the devices. It dives into how unreliable the physical software devices can be when outdated and out of system in the current world. This leads to the broad problem of being unable to predict the possibilities of new attacks that are created and how they can be prevented. DDoS attacks expose how a random attack can occur at any time and emerge in the systems and grow within them. SCADA helps show the predictive limits within systems through the engineers. The SCADA systems developed long ago have vulnerabilities to exposure, environmental factors, and hardware life expectancy. Because of the many weaknesses of SCADA, the design principles help us learn and acknowledge the errors and flaws within the design for the future.

These three factors show how the prediction in cybersecurity fails due to the human mind, technological complexity, and constant threats to the system structure. Something that should be highlighted more is the power of prediction, in addition to the awareness, resilience, and adaptability of the people within the realms of protection, where prediction will seem to fail.

## Conclusion

In essence, phishing attacks, DDoS, and SCADA systems show the vulnerabilities and highlight the parts of cybersecurity that build security into systems. That being said, human involvement, network, and industrial aspects all fall into play in the structure of cybersecurity. Through a philosophical lens, the short arm of predicting knowledge becomes clearer as time and errors begin to show within the field of study. It becomes apparent that we must not only rely on models, but all aspects, like the human mind and logical values that come into play for the attackers. The field of cybersecurity must emphasize the importance of resilience, mitigation, and constant updating and learning within the field. By practicing and staying up to date with the possibilities, a more secure environment can be able to take place with the alertness to threats.

**References**

CYSE/IT-200 Mid-Term Exam Guide

CYSE-200 Final Exam Guide

ChatGPT

**Appendix A**

Originally, when thinking of topics for the paper, I was wondering which ones to pick and how I could relate the topics together. First, I was thinking about companies and organizations' problems specifically, and then turned to a broader view of attacks and systems. I narrowed my topics down to three things: phishing, DDoS, and SCADA systems. I was first having difficulty connecting the three; however, after reviewing the module slides through the exams, I connected them through the online systems and ecosystem in the technical world. When writing, something I got confused about was connecting SCADA system vulnerabilities to the other two topics. Ultimately, I dug deeper into SCADA to see its weaknesses within prediction and tied all three topics to prediction in cybersecurity. I asked ChatGPT: “What are some of the vulnerabilities SCADA systems have when it comes to prediction in cybersecurity?” I used the response from ChatGPT to make a connection between the response and the other two topics. Essentially, I wrote about the other two topics solely on my own, while ChatGPT helped me with the topic of SCADA systems.