Unit 1 Cybersecurity Concepts

**Corey Crooks**

**Purdue University Global**

**IT484—Cybersecurity Policies**

**Preston Rich**

**December 13, 2023**

**Part 1**

A compromised cybersecurity foundation may have the potential to ruin all infrastructure—digital and physical. Cybersecurity lays the ground work for much of what we do today. Private organizations deal with no insignificant amounts of data throughout their essential functions. Corporations may handle client information, and sensitive topics such as credit card numbers and security information. Cybercriminals may target this data specifically in order to gain the funds found within. A breach of this informational flow may devalue the trust that clients find in the company, and forever tarnish the brand name. To mitigate this issue, Cybersecurity concepts like social engineering are best utilized proactively. Smaller business may find that they are highly at risk from these attacks, as they may not know to look for them. They may not understand that certain individuals may pose as government personnel to gather that information, and moreso may not understand that concepts like spoofing do exist today.

Public organizations are no less at risk. Public Organizations have the potential to be some of the highest earning hits on the market. Amazon just recently experienced a round of intensive cybersecurity attacks in the form of Phishing in order to uncover sensitive information to sell to third parties (Madeksho, 2022). Due to the massive number of clients and customers served by Amazon, cybersecurity targets are plenty. Some of those using the platform, are not digitally literate enough to determine scams from the genuine website, and thus will do Amazon’s reputation harm alongside those seeking compensation from Amazon to allow such attacks to happen in the first place.

Government Organizations have a concerning risk factor as well. Given their status in society, they garner new types of both attacks, and motivations behind them. Given this, it is imperative that cybersecurity specialists are part of regular operations working to mitigate damages being imposed upon the governments of the world. Cybersecurity policy can help mitigate those exact situations in that they play a vital role in every step of the process. In January of 2023, a hacker was able to obtain the United States national No-Fly list, and leaked the names within on public forums (Factora, 2023). This caused chaos within the respective government agencies that could have been mitigated with simple Cybersecurity policies in place. The government may have been able to implement heightened security and prevent this accident from occurring simply with more robust security architectures. The hacker in question was able to retrieve a Comma-Separated-Value sheet that displayed the names of no-fly participants in plain-text. This could have been stopped by integrating some proprietary cryptography. This would have halted the hacker, despite having her retrieve the information in question. Using cryptography would have made the data acquired completely illegible without the highly specific cryptographic key, which would take an extreme amount of effort to obtain, and require more advanced disciplines such as social engineering.

Finally, our nation as a whole would benefit from enhanced cybersecurity policies to bolster our infrastructure. Our military is under siege from constant threats throughout every moment of every day—such is the requirement of having our flourishing combative forces. However, these fights are not only on the fields and hills. We are under attack, and attacking through, multiple cyber avenues (The United States Army, n.d.). The cybersecurity battlefield has a number of malicious actors with skills far past their own renown. Enhancing our own cybersecurity policies and workflows may help to vary the skills required to combat our personnel, which in turn makes each citizen more safe and secure in their homes. Additionally, a number of critical systems such as the White House, State Capitols, and more utilize technological systems connected to the internet that are potentially vulnerable. Such systems have rigorous cybersecurity infrastructures attached to increase the security of an attack—although no system can ever be hack-proof.

**Part 2**

* **What are the main categories of an in-depth cybersecurity policy** (Fabro, 2006)**?**
  + In-depth cybersecurity policies come in a number of layers. These layers may be explained succinctly into a number of different controls. Administrative controls oversee the logistical development of the systems behind the software in use. These controls are required to heighten organization, and increase productivity workflows without sacrificing security. This can be useful to develop specific policies to see how administrative functions may be swapped, or replaced without requiring a complete reworking of other sectors in the system. Critically, these systems also include some framework idealization to determine which goes best with the systems that are necessary to build. This further synergizes development platforms in case of a swapped component, and ensures security is maintained while keeping the entire system agile. First and foremost, it is important that proprietary tools are leveraged here, as a security flaw in administrative platforms may compromise the entire system as a whole. Indeed, Third-Party services may include their own security risks, and as the company or organization that is working on this particular platform may not be able to make adjustments to the backend of those services, such vulnerabilities may be a permanent addition to the system utilizing these services. Physical controls determine those components that are part of the real-world integration of the platform in question. These can take the form of a number of tools from a combination lock, a keycard, or even ID badges for employees interacting with them. Technical controls are the last of them. They oversee the software end of a system. Commonly, this could take the form of anti-malware and malicious behavior observation tools. As these are particularly popular even in home systems, it is important to not overlook the importance of the other control options available. A mixture of all three may help bolster security to an extent that wouldn’t be possible without them.
* **How would a well-designed cybersecurity policy program help secure a government agency, such as the Department of Homeland Security (DHS)** (EC-Council University, n.d.)**?**
  + Cybersecurity policies serve as an effective baseline to any kind of system. It is important to consider what system is to be integrated, however. The Department of Homeland Security is a complex organization that requires careful planning in order to ensure it may run optimally to continue its operations without issue. Additionally, the amount of potential security concerns may be overwhelming for the DHS without a carefully planned cybersecurity strategy. Thankfully, this is not an impossible feat to plan for. A number of administrative controls will help to ensure should one system fail, another may be able to take its place, although crucially, administrative controls should be put in place to mitigate the potential of failure in the system that is being overseen, though agile developments may be able to secure the reliability of the service. Physical controls will help bolster the security of the DHS systems in regards to attacks such as social engineering. Physical barriers of varying checks will ensure an individual will need thorough verification in order to access critical systems. Finally, technical controls will help the DHS to combat digital threats. As the digital battlefield will be instantaneous no matter the physical ground separating actors, fast action and response is crucial. Well documented automation software may help deal with surface-level threats as they pop up, but it is important to consider well nested attacks as well. All these controls and more should provide a thorough background to help Homeland Security to function safely and securely.
* **What are some challenges to making sure everyone in an organization follows the cybersecurity policy** (Rabinowitz, 2023)**?**
  + Cybersecurity policies are extremely challenging to implement no matter the organization. One key reason for this is the human element of the system. As personalities, viewpoints, and motives grow more and more diverse, a diverse system is required to help everyone understand the importance of the cybersecurity policy, and the heuristics required for it. For this reason, it would be wise to implement rigorous training and awareness programs to help everyone operate with the same amount of information regarding the potential dangers of the digital world. Although it may suffice to stop there, it would be recommended to provide additional resources on how this policy in particular may help with the aforementioned threats. Information alone is not enough, however. Stacking skills on top of that should help bolster the aptitude and motive of the individuals that must interact with these policies being drafted. Training materials should be made in order to ensure the people within the organization are comfortable with the UI of software and tools needed for the cybersecurity policies being implemented. This training should cover all basic routes that people working in the organization would need in order to protect the organization in any aspect they may encounter threats to during their normal job functions. As part of this training, it is recommended to implement a support structure so that employees may go through a specific resource in order to resolve issues or questions relating to the ideas or actions they may be required to perform during their jobs.

# **References**

EC-Council University. (n.d.). *How to Develop a Comprehensive Cybersecurity Strategy*. Retrieved from eccu.edu: https://www.eccu.edu/blog/cybersecurity/how-to-develop-a-cyber-security-strategy/

Fabro, D. K. (2006, May). *Control Systems Cyber Security: Defense in Depth Strategies*. Retrieved from Idaho National Laboratory: https://nsarchive.gwu.edu/sites/default/files/documents/3121326/Document-06.pdf

Factora, J. (2023, January 23). *A Trans Hacker Was Able to Access and Leak the No Fly List* . Retrieved from them.us: https://www.them.us/story/trans-hacker-leaks-no-fly-list

Madeksho, C. (2022, July 11). *Cybersecurity Scam of the Week -- Amazon Prime Day*. Retrieved from The University of Tennessee's Health and Science Center: https://news.uthsc.edu/announcements/cybersecurity-scam-of-the-week-amazon-prime-day-dont-fall-victim-to-phishing/

Rabinowitz, R. K. (2023). *Section 5. Developing Personnel Policies*. Retrieved from University of Kansas: https://ctb.ku.edu/en/table-of-contents/structure/hiring-and-training/personnel-policies/main

The United States Army. (n.d.). *Defend the Nation Against Cyber Threats*. Retrieved from goarmy.com: https://www.goarmy.com/careers-and-jobs/specialty-careers/army-cyber.html