Unit 2 Cyber Security Policy Drafting

**Corey Crooks**

**Purdue University Global**

**IT484—Cybersecurity Policies**

**Preston Rich**

**December 20, 2023**

**Part 1**

An organization’s management poses and presents several key considerations and issues that must be addressed in any coherent cybersecurity policy. Firstly, the issue of compliance must be addressed in full if any security policy is expected to take root in the organization. Fortunately, there are many tools available to help motivational compliance take effect (Madnick, 2020). Classes may be started to educate employees as to the dangers of the cybersecurity threats they face in their daily lives. Additionally, classes may focus on an awareness angle to help employees understand the multitude of threats faced in the cybersecurity world. Threats to the organization concerning cybersecurity are plentiful and ready; the employees must understand that.

Another key consideration may be an employee’s background. Certain employees may not be used to the digital world. As such, the employee may not be accustomed to thinking about how exactly their actions may impact those around them. Due to this, classes on the matter may help educate employees on digital Ethics, but certain cultural sensitivities may need to be developed within the policy to accommodate different backgrounds in the organization’s employees (Madnick, 2020). After all an organization is made up of many different employees that may have diverse backgrounds compared to one another, and such backgrounds may come with a different method of interaction with the digital world. Certain cybersecurity attacks such as social engineering may seek vulnerabilities within these diverse backgrounds. During these attacks, careful research is done into potential targets to secure valuable information, physical acquisitions, and more. These targeted attacks can be very difficult to overcome, and disastrous for the organization affected. Because of considerations like this careful thought must be put into each of the employees within the organization to accommodate certain backgrounds that may be vulnerable to such attacks. Although it is never possible to be completely vulnerability-free, it is very possible to be prepared for an attack to mitigate the potential damage done. This is what careful planning within an organization’s cybersecurity policy is supposed to accommodate.

Another consideration may be the resources required to implement a policy as designed and constructed. An organization is not entitled to unlimited resources. Factors such as time, money required, and physical manpower all contribute to an organization’s total budget they may have on hand (Madnick, 2020). Each of these factors drains from this budget. For instance, it may be unreasonable to expect the average employee to understand cybersecurity policies to the degree of a senior engineer. Because of this when drafting educational policies surrounding cybersecurity, careful consideration must be put into the target audience of this information. It may not be within the budget to incorporate certain details above what may be expected of an employee to learn. Additionally, certain policies may be more or less realistic depending on the number of individuals and organizations may have at their disposal. Certain policies that may be more elaborate may make sense for a smaller-scale organization, however, such an elaborate requisition may not be possible for an organization on the scale of thousands to tens of thousands of employees. This may be because as an operation grows in scale, it becomes more difficult to manage individuals down to their minute level. Because of this, it is important to draft policies that may be simple yet effective in their depth in total.

**Part 2**

**What are the components of an effective cybersecurity training program?**

* ISC2 lists several criteria in its Code of Ethics. This criterion lists safety, the common good, a duty to principles, the duty to each other, and behavioral mechanisms (Wills, 2019). The safety criterion lists key concepts such as the physical, digital, or mental safety of individuals within the organization. This safety is stressed with cybersecurity and informational systems within the organization that may lead to accidents or risks with the organization’s personnel. The common good refers to the organization’s community and gathering of individuals there within. This implies inherent well-being and safety while all security measures within an organization Are working as expected. Duty to principles refers to the burden an individual may have to follow the lead of their superiors. This involves acting within job functions to do a duty as a sign. Assigning these job functions may need careful attention by the superiors to address any complications within the organization or particular problems the organization may be facing outside and externally. A duty to each other may be supplemental to this as it involves how an organization’s individuals may interact as a community. Heuristics within this category may be generated to further goals that may try to strengthen that sense of community within the organization. This communal relationship acts to keep all individuals within the organization secure by creating a cybersecurity network. Behavioral mechanisms focus on how individuals interact and behave within the organization on their jobs within their job functions. This outlines how an individual should behave according to work-appropriate actions. These actions could be ideas such as surfing the web and the restrictions upon that to eliminate the possibility of exposing the organization to malicious actors based on noncritical functions that the employee may have been engaged in at that particular moment in time.

**How do organizational best practices help minimize risk to an organization’s confidential data?**

* There are many ways malicious actors may gain access to an organization’s confidential data. There are many more reasons why malicious actors may need or want to gain access to that said data. One common way is through practices such as social engineering. These practices see malicious actors pretending to be individuals in power or close to the organization to gain access to systems or physical areas that are off-limits to those without ties to the organization (The University of Texas at San Antonio, 2020). This could take the form of an individual pretending to be a maintenance worker to gain access to the server room and download data from there, or more remote attacks such as an individual pretending to be part of a major organization such as the government trying to get a user within a business to click on a link that may automatically download a virus vector onto the machine to infect further systems within an organization and gather information from that. These attacks can be devastating for organizations that are not prepared for them. An organization may introduce best practices to mitigate the chances of such attacks gaining any traction in the future. These best practices may be something simple such as a verification system to ensure any employee that may be The target of a social engineering attack may have a superior or another individual within the organization to go to and ask questions to ensure that the individual is who they claim to be before they are led into any critical systems. Another may be a code of ethics when utilizing online systems such as Internet browsers to ensure that employees do not expose the organization to malicious vectors to cause further damage.

**What are some best practices to manage portable devices in an organization?**

* Portable devices require careful attention when used at and away from an organization or workplace. This is because using them in both places opens the device up to a new potential vector of attack (California State University at Long Beach, n.d.). Work done remotely away from the organization creates an opportunity for malicious actors to gain information about the organization without physically being inside of it. Because of this, it is important to be cognizant of how exactly an employee may use portable devices within an organization, as well as outside of the organization. Some best practices may include first-hand encryption. Encryption is a tool that scrambles data while it is not being directly used by the recipient. When implementing this technology it will be ensured that if a malicious actor happens to be able to copy data from the portable device onto their machine, the data would be scrambled in a way that the malicious actor would not be able to read it. This would further increase the security of an organization away from the physical location where the organization may take place. This also by proxy benefits all those that interact with the organization, because their data may be more secure Because of the encryption protocol that has been implemented. Another Best practice may be to introduce a remote host system for portable devices. A remote host system allows a user from outside of the workplace to be able to stream into a computer located physically within the organization to continue their work activities as if they were working on that computer specifically. This ensures that the documents and data that are relevant to the workplace remain physically within the workplace while being located on no other device and storage solution outside of the organization. Although this does include careful consideration as to credential management, this will ensure that any malicious actor that is trying to copy data from the storage solution of the portable device will not be able to access any confidential information.

# **References**

California State University at Long Beach. (n.d.). *How to Secure Your Mobile Phone: A Guide for Cyber Professionals*. Retrieved from cpace.csulb.edu: https://digitalskills.cpace.csulb.edu/cybersecurity/how-to-secure-mobile-phone/

Madnick, A. M. (2020, January). *Analyzing the Interplay Between Regulatory Compliance and Cybersecurity*. Retrieved from Cybersecurity Interdisciplinary Systems Laboratory of the Massachusetts Institute of Technology: https://web.mit.edu/smadnick/www/wp/2020-06.pdf

The University of Texas at San Antonio. (2020). *Common Scam Techniques: Social Engineering*. Retrieved from utsa.edu: https://www.utsa.edu/techsolutions/Cyber-Awareness/Social%20Engineering.html

Wills, M. (2019). *SSCP Systems Security Certified Practitioner Official Study Guide*. Retrieved from ISC2: https://viewer-ebscohost-com.libauth.purdueglobal.edu/EbscoViewerService/ebook?an=2110465&callbackUrl=https%3a%2f%2fresearch.ebsco.com&db=nlebk&format=EK&profId=eds&lpid=&ppid=&lang=en&location=https%3a%2f%2fresearch-ebsco-com.libauth.purdueglobal.edu%2fc