# Cybersecurity Education; A High-Level Overview

Robert Timmons

School of Cybersecurity

CYSE 425w: Cybersecurity Strategy and Policy

Professor Bora Aslan

February 7th, 2025

**Cybersecurity Education; A High-Level Overview**

Cybersecurity is a growing industry, with threats to cyber assets and infrastructure growing daily, there's a need for sound policy to better combat attacks. For this paper, Cybersecurity Education was chosen because of its importance in both physical system security and network system security. Despite firewalls, intrusion detection and prevention systems, the largest threats to networks remain the human factor. According to the World Economic Forum, they expand on this fact, reporting that businesses themselves face "…a reality where 95% of all incidents occur due to human error…" (Zhadan, 2022) This paper aims to explore cyber education more fully; describing the development and history of the policy, providing a practical policy example, and then explaining how it integrates into a broader national policy. There are a multitude of policies in cybersecurity, but cybersecurity education is one of the most essential policies in the information age. Knowledge is power, and as the field grows, public and private organizations alike need strong knowledge-based foundations to successfully ward off attacks.

Securing information technology assets as a concept is not entirely new and has been around for decades. The idea malicious code that could be downloaded or injected into unsuspecting computers was tested over four decades ago, and these cases displayed the potential for devastating results. As worms, viruses, trojans emerged and began threatening systems, hardware and software tools began taking form to combat these attack vectors. Since the turn of the twenty first century, digitization has taken place on a monumental scale, with more and more devices having internet facing services, creating an even larger attack surface for organizations to defend. Attackers have found new, more cost-effective ways to breach systems, developing and adopting social engineering techniques to prey on the nativity and good nature of their victims. A response was devised to make victims aware of these types of cyber threats, and this is where

cybersecurity education came to the fore. Cybersecurity education is the process of exposing individuals to common attacks a hacker or scammer may use. The curriculum can take many forms, explaining what hackers do, how they make money, what tactics they may employ, and how to spot hacking or scamming attempts. This training can be as basic as explaining how a computer system works, letting participants understand the why behind these attacks. Cyber security education is constantly improving, with researchers highlighting its importance, stating "Given such low awareness of basic security precautions, it is likely that improving educational offerings, raising awareness, and providing opportunities for training in cybersecurity are needed around the world." (Shillair et al., 2022) With a high-level understanding of cybersecurity education, specific scenarios along with the connection to broader policy can be detailed.

Actual application of cybersecurity education can be rather simple on a small scale. Take an organization of any kind. Their IT department or cybersecurity specialist surveys the security requirements for the organization, and tailor a curriculum to their needs. Employees would then go through scenarios identifying threats, potential risks, and workshop ways to counteract hacking attempts. Companies can then reinforce these concepts by sending dummy malware or penetration testers to see if employees can identify and report these potential threats. Some institutions take this a step further and have gamified the cybersecurity education process. Cybersecurity education is extremely effective when gamified, with reports saying "Comprehensive research has reported that gamification produced positive effects and benefits. Specifically applied to Computer Science and Cybersecurity, we have seen similar results when examining participant engagement, experience and learning outcomes." (Balon & Baggili, 2023) Using levels, point systems, tutorials, challenges and engagement loops, cybersecurity learning is

made fun and impactful. Companies can use cybersecurity education to strengthen their security posture, and using gamification, make it a fun and enjoyable experience.

On a national level, governments can assist the private sector in ensuring cybersecurity education through guidelines and frameworks. Various federal organizations provide documentation for cybersecurity, integrating their own cybersecurity postures into learning materials and symposiums. Cybersecurity education is a facet of the nation's national cybersecurity goals, which in turn is a portion of the larger national security policy. It is in the Federal government's best interest to encourage and promote this education. The government recognizes this, with the result being "Federal agencies spend a significant part of their annual IT funding on cybersecurity, which currently constitutes 16-17% (about one in every seven dollars) of agency IT budgets overall." (Fischr, 2016) A large portion of that money goes into cybersecurity research and development as well as workforce development. More specifically, the federal government fosters programs to improve size, skills, and preparation of cybersecurity workforce. Kinetic threats aren't being replaced entirely, but many assaults the DoD, DHS, and FBI defend against are increasingly digital. The investment into cybersecurity education from the government is all in service to the greater national security policy, with these initiatives resulting in a more prepared workforce to protect national interests and secrets. Cybersecurity education is essential policy not only in the private sector, but the public sector and the nation's national security posture.

Cybersecurity is essential in multiple areas of society. As every aspect of civilization goes online, it behooves IT departments to ensure the best and most efficient security. Implementing cybersecurity education builds a robust security standard from the ground up. Cybersecurity education prepares individuals for common threat identification and response. Using

frameworks, standards, and dynamic learning through processes like gamification, cybersecurity can be better instilled throughout the population. This point is driven by the widespread adoption of it in the federal government, where they invest heavily in cyber awareness programs, aimed towards reinforcing the larger national defense strategy. Cybersecurity is an industry based on knowledge, so policies like cybersecurity education are essential for a safe and secure digital future.

## References

Zhadan, A. (2022, January 18). *World Economic Forum finds that 95% of cybersecurity incidents occur due to human error | Cybernews*. Cybernews. https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/

Shillair, R., Esteve-Gonzalez, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & Solms, B. von. (2022, May 16). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. https://www.sciencedirect.com/science/article/abs/pii/S0167404822001511

Balon, T., & Baggili, I. (Abe). (2023, February 24). *Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education - education and information technologies*. SpringerLink. https://link.springer.com/article/10.1007/s10639-022-11451-4

Fischr, E. A. (2016, August 12). *Cybersecurity Issues and Challenge: In Brief*. a51.nl. https://a51.nl/sites/default/files/pdf/R43831.pdf