# Cybersecurity Policy and Strategy

Aaron Jones

CYSE 425W

Professor Teresa Duvall

9/17/2023

## Introduction

Cybersecurity has shown how linked our world is today and how much organizations, governments, and people rely on digital technology. Cybersecurity has become a top priority. In this essay, we will examine the formulation, implementation, and position of a cybersecurity policy/strategy in the context of more general national and international cybersecurity policies. The chosen cybersecurity policy for study is "Mandatory Cybersecurity Training." This policy requires that all employees to complete cybersecurity training to increase their knowledge of online dangers and advance a secure online environment. This essay seeks to present a clear summary of this policy.

## Mandatory Cybersecurity Training Policy

The policy requiring cybersecurity training was created in response to the increased risk of cyberattacks aimed to organizations public and private of all kinds. Our main objective is to provide employees with the knowledge and skills needed to secure sensitive data by educating them about the numerous cybersecurity dangers they may run across. Organizations want to lessen the risk of security breaches brought on by mistakes or ignorance by demanding cybersecurity training.

## Development and Rationale

Employees are frequently the weakest link in an organization's cybersecurity protection, which is why the policy was created. Cyberattacks like social engineering and phishing frequently prey on human weaknesses. This policy makes sure that every employee, regardless of level of technical proficiency, receives cybersecurity training to reduce these risks.

## Application

All personnel are required under this policy to regularly attend cybersecurity training programs. detecting phishing emails, making secure passwords, detecting malware, and reporting security issues are just a few of the subjects covered in these seminars. Additionally, employees are made aware of the organization's cybersecurity standards and their part in upholding a safe online environment.

## Integration of Cybersecurity Policies

The policy on mandatory cybersecurity training is consistent with more comprehensive national and worldwide cybersecurity initiatives. Governments at the national level understand the value of an educated workforce in boosting cybersecurity. International institutions like the United Nations support cyber rules and norms, putting a strong emphasis on the value of cybersecurity knowledge and education.

## Conclusion

In conclusion, the Mandatory Cybersecurity Training policy enhances education and awareness to reduce human-related security risks, which is a critical component of an organization's cybersecurity strategy. This policy supports worldwide and domestic cybersecurity initiatives, making the internet a safer place.

References

1. Martin Macak. 2020 "Process-aware Insider Threat Detection and Mitigation in Organizations", 1(1), 1-16

2. Probst, C. W., Hunker, J., Bishop, M., & Gollmann, D. (Eds.). (2010). *Insider threats in cyber security* (Vol. 49). Springer Science & Business Media.

3. Canepa, M., Ballini, F., Dimitrios, D., & Vakili, S. (2021, March 1). *ASSESSING THE EFFECTIVENESS OF CYBERSECURITY TRAINING AND RAISING AWARENESS WITHIN THE MARITIME DOMAIN*. Research Gate. https://www.researchgate.net/publication/349899295_ASSESSING_THE_EFFECTIVENESS_OF_CYBERSECURITY_TRAINING_AND_RAISING_AWARENESS_WITHIN_THE_MARITIME_DOMAIN