Cybersecurity Professional Career Paper: Cybersecurity Awareness & Training Specialist

Isaiah Seaborn
School of Cybersecurity, Old Dominion University
CYSE 201S: Cybersecurity and the Social Sciences
Instructor Name: Yalpi
Date: 11/14/25

Introduction

Cybersecurity is a field that focuses on protecting people, data, and systems from online threats. In today's world, almost everything we do is connected to the internet, which means the risks are higher than ever. One important area in cybersecurity is awareness and training, which deals with teaching people how to avoid mistakes that could lead to cyber attacks. The purpose of this paper is to explain how social science plays a big role in this career, how key class concepts relate to daily work, and how the profession interacts with marginalized groups and society. The paper also includes scholarly sources that help support these ideas.

Social Science Principles – Relation to Career

A Cybersecurity Awareness & Training Specialist depends heavily on social science research because their job is focused on understanding human behavior. Many cyber incidents are caused by people falling for tricks like phishing or scams, so professionals need to understand why people make risky choices. Social science research helps explain things like motivation, trust, fear, and decision-making, which are all connected to cybersecurity behavior (Workman, 2008).

Social science also guides things like human-computer interaction. If security instructions are confusing or too technical, people ignore them. Specialists use communication strategies and psychology to create training that normal people can understand.
For example, knowing how memory works helps them design short, simple lessons that people actually remember. Understanding group behavior also helps them build a positive "security culture" where coworkers remind each other to stay safe.

These professionals use social science insights all the time when creating awareness programs, sending reminders, designing training modules, or explaining social engineering attacks to employees.

Application of Key Concepts – Relation to Career

Several concepts from this class are used directly in this career:

Social engineering: Specialists teach employees how to spot phishing emails, fake messages, pretexting, and other manipulation methods. Attackers often rely on emotional triggers like fear or curiosity (Mitnick & Simon, 2011).

Human factors: We learned that people are the biggest cybersecurity weakness. Awareness professionals focus completely on reducing mistakes by giving clear instructions and simplified guidance.

Risk perception: People tend to think cyber attacks "won't happen to them." Specialists must adjust how risks are explained so employees understand the seriousness.

Security culture: This concept is about creating an environment where everyone cares about cybersecurity. Awareness workers do this by running campaigns, posters, training videos, and reminder emails.

Tools and techniques used in this career include phishing simulations, online training platforms, surveys that measure employee behavior, and policy briefings. These help specialists see where people make mistakes and fix them before attackers can take advantage.

Marginalization – Relation to Career

Cybersecurity does not impact everyone equally. Some marginalized groups—like older adults, immigrants, low-income communities, or people with limited digital literacy—are targeted more often by cybercriminals (FBI, 2023). These groups may struggle with complicated technology or might not recognize scams.

Awareness specialists have to consider these challenges when creating training. They must avoid using complex language and make sure materials are accessible. Some organizations are working to improve diversity in cybersecurity by hiring people from

different backgrounds or offering training programs to communities that lack digital education.

This career plays an important role in making sure cybersecurity protections are fair and do not leave certain groups behind.

Career Connection to Society – Relation to Career

Cybersecurity Awareness & Training Specialists contribute to society by reducing the number of attacks that happen due to human mistakes. Many important systems—banks, hospitals, schools, transportation—depend on employees knowing how to stay safe. One person opening a bad link can shut down entire systems, so these specialists help keep society stable.

Public policies such as data privacy laws, breach notification rules, and workplace cybersecurity requirements also shape the job. Awareness specialists help organizations follow these rules by training employees and making sure everyone understands legal responsibilities. Their work supports safer communities and more secure digital environments.

Scholarly Journal Articles

Source 1

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4), 662–674.
Key Finding & Relevance: The article shows how human behavior and emotional manipulation lead to successful phishing attacks. This supports the idea that social science is essential in awareness careers.

Source 2

Mitnick, K., & Simon, W. (2011). *The Art of Deception: Controlling the Human Element of Security*. Wiley.
Connection to Social Science: This book explains how attackers exploit psychology. It helps show why specialists must understand human behavior to train people effectively.

Source 3

FBI. (2023). *Internet Crime Report*. Federal Bureau of Investigation.

Connection to Society and Marginalized Groups: The report highlights which groups are targeted the most and how cybercrime affects the public. This supports the argument that awareness specialists must adapt training to protect vulnerable populations.