Article Review #2: Human Factor in Data Breaches

Student Name: Alessandro Arroyo

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Yalpi

Date: 5th November 2025

Introduction/BLUF

In Human Error – A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education it explains that human error continues to be a major factor on why there is a risk in system attacks and data breaches. I plan to explain how the authors of this article tested this question while also showing the data and explaining how the research relates to concepts / principles we have learned in class.

Relation/Connection to Social Science Principles

- Archival Study
- Poor Security Methods (Weak Passwords, Default IDs, etc.)
- Social Norms
- Cybersecurity Culture
- Risk Assessment
- NIST Cybersecurity Framework
- Quantitative and Qualitative Methods
- Cybersecurity Awareness

Throughout the article we see these connections to Social Science principles and the article even uses some of these terms in their study. Such as NIST Cybersecurity Framework and Quantitative and Qualitative to express their ideas / findings of the experiment and it makes it easy to understand as they are commonly used in cybersecurity culture. As for the other terms they are ideas that are explicitly said but are used in their research / findings which makes this a social science / cybersecurity experiment.

Research Question /Hypothesis/ Independent Variable/Dependent Variable

- Research Question: How easy or difficult it is to find the security policies on the Institution's websites? How much the policies incorporate and address the various aspects that encompass human error to identify gaps in cybersecurity education, training, and awareness programs amongst participation selected institutions? By using survey responses from faculty members and students at Institution A they will analyze and establish if students and Faculty have cybersecurity training?
- Hypothesis: "The work will articulate best practices that can guide higher education institutions about Information Systems and operational weaknesses with associated threats and avenues to address Cybersecurity risk and enhance an organization's cybersecurity posture through improved and implementable cybersecurity policies and practices to reduce human errors" (Amoresano & Yankson, 2023).
    - Independent Variable: Institutions A, B, & C
- Dependent Variable: Cybersecurity policies and training data that was able to be seen by anyone in the institutions' websites.

Types of Research Methods used

"Most of this work focuses on qualitative design, with some additional quantitative data" (Amoresano & Yankson, 2023). This is stated but as you read through the article you can see the methods in action as much of the data is collected from users and the very policies and training data that comes from the institutions.

Types of Data Analysis used

Qualitative Analysis and Descriptive Analysis as they used the first one to describe the survey data however overall, the article did the job of explaining the data rather than doing anything else. I would say the conclusion leans more to Prescriptive and there could be an argument for it however I believe the whole is more Descriptive than anything else.

Connections to other Course Concepts

- Scarcity
- Poor Security Methods
- Social Norms

These are the most important connections to other course concepts that I could find as I believe the article was trying to explain this however it was never directly said. Human error often starts with Social Norms and Poor Security Methods as it's not praised to have complex passwords and to change them every couple months. It often creates a scarcity of good polices and methods that we follow and leads to our jobs, companies, and life being compromised by the bad actors.

Connections to the Concerns or contributions of Marginalized Groups

This is valuable knowledge to the cybersecurity culture as a whole and possibly even any company that wants to eliminate human error from their workforce. The overall goal was to give information and knowledge to the world, and it accomplished this with various reviewed articles mixed in with their own research making it trustworthy and accurate.

Overall societal contributions of the study/Conclusion

In conclusion, the article shows that the human factor is becoming the most important part of a company's defense as they deal with the infrastructure and are the main causes of breaches. The

data shown in the article also shows that we should shift some of the technical aspects to human aspects and deal with problems in training and mitigating cyber-attacks. Changing a culture is a difficult process and may take a long time however “Understanding the value and purpose of the training makes the learning more meaningful and makes the users more likely to pay attention because they know what is at stake” (Amoresano & Yankson, 2023).

Reference

Amoresano, K., & Yankson, B. (2023). Human Error - A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education. *Holistica: Journal of Business and Public Administration*, *14*(1), 110–132. https://doi.org/10.2478/hjbpa-2023-0007

Article Link: https://doi.org/10.2478/hjbpa-2023-0007