Article Review #02: Toward Effective Learning of Cybersecurity: New curriculum agenda and learning methods

Student Name: Albreana Butler

School of Cybersecurity, Old Dominion University

CYSE201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 04/13/2026

Introduction

Toward effective learning of cybersecurity is an article that states a new curriculum agenda and learning methods. It focuses on improving how cybersecurity is learned by using more hands-on and interactive approaches in learning. The study uses traditional lecture-based instruction and methods like practical exercises and competitions to allow students to fully understand cybersecurity concepts.

Relation/Connection to Social Science Principles

The Social Science principles learned in this course can be easily applied to this study. Empiricism is used by collecting student data instead of opinions. Objectivism is shown through results based on measurable outcomes from student performance and surveys. Determinism is reflected because the learning outcome of the student relies on the kinds of instruction they receive. Parsimony is seen since the study explains various learning styles using clear and instructional methods. Skepticism is represented by testing whether traditional teaching is actually effective. Finally, it connects to relativism because learning effectiveness may rely on context and learning environment.

Research Questions/Hypothesis/Independent Variable/Dependent Variable

- Research Question: In what ways do different teaching styles contribute to student learning, productivity, and confidence
- Hypothesis: Students who participate in a more interactive learning will learn better and gain more confidence, and are taught using traditional lecture instruction.
- Dependent Variable: Student knowledge, performance, collaboration, and confidence

Types of Research Methods

Quantitative research is used in this study by conducting surveys and performance-based learning activities. Students engaged in cybersecurity training that included hands-on activities like capture the flag competitions. They then completed surveys to reflect on their learning experience and confidence levels. This approach is similar to the quasi-experimental method because students are introduced to an educational intervention and assessed afterward.

Types of Data Analysis used

Descriptive statistical analysis is also used to compare student performance and survey response percentages. Students are analyzed based on how they perform in cybersecurity challenges and how their confidence levels change after training. The focus of this analysis is identifying patterns in learning improvement between different methods of teaching.

Connection to other Cource Concepts

There are a few course concepts learned from the course CYSE201S that connect to this article. First, Social Science research methods like surveys and quasi experiments used to analyze human behavior. Second, Variables and hypothesis testing are used to show how independent and dependent variables interact. Third, models of explanation connect to the nomothetic model since it looks for general patterns across student groups. As learned in the course, psychological factors in cyber behavior also relate to this study, such as low self-esteem and decision making error that increase vulnerability to cyber threats. It also reflects on ideas from behavioral and cognitive theories that describe how people learn through situations. Additionally, it connects to the Big Five personality traits, influencing how individuals communicate in cybersecurity training and risk.

Connections to the Concerns or Contributions of Marginalized Groups

Contributions of marginalized groups are shown in this study by improving access to cybersecurity education through interactive learning. Students with little technical knowledge benefit the most from hands-on training because it decreases learning challenges. This helps by closing the gaps in student knowledge and promoting fair opportunities in cybersecurity education. It also supports inclusivity by making sure that students from different backgrounds can build cybersecurity skills.

Overall Societal Contributions of the Study/Conclusion

In conclusion, Interactive and practical cybersecurity education is shown to improve student learning, work ethic, and self-esteem. It outlines the importance of using real-life training methods to better prepare individuals for cyber threats. From a social science point of view, how human behavior and the learning environment influence knowledge development is demonstrated in this study. The study also connects to society by enhancing cybersecurity education, decreasing inequality in technology, and helping individuals better protect themselves in the real world of technology.

References

Toward effective learning of cybersecurity: New curriculum agenda and learning methods | journal of cybersecurity | oxford academic. (n.d.-b). https://academic.oup.com/cybersecurity/article/10/1/tyae018/7900964