Article Review #1

By Kevon Merritte

## Introduction

The article I’ve chosen to review is called “Impact of Cybersecurity and AI’s related factors on incident reporting suspicious behavior and employees stress: Moderating role of cybersecurity training”. This article aims to identify how incident reporting of suspicious behavior mediates relationships in the field of cybersecurity incident management, cybersecurity awareness, intention to use AI, perceived threat in AI, and employee stress level.

### Describe how the topic relates to the principles of the social sciences

 Being that one if the topics in the journal’s main focus is to identify how incident reporting correlates with employee stress levels, this falls into the categories of psychological and sociological principles because the whole idea of the principles is to examine the reaction or behavior in response to an issue or concern. In the article, it speaks on how the employees react to the impacts of cybersecurity and AI. Some more principles of social sciences would be the impact of technology on society and social systems and structures.

### Describe the study's research questions or hypotheses

 From what I gathered through the journal, the study’s research questions and hypotheses are mainly focused around how exactly does incident reporting suspicious behavior mediates the relationship between different issues. To explain, in the article, the questions were revolved around security incident management and employee stress levels, intentions to use AI and employee stress levels, security awareness and employee stress levels, etc.

### Describe the types of research methods used

 Throughout the article, the author used a quantitative method to conduct the research. Meaning the author collected data on different factors to provide a accurate finding or result. In the authors research, they asked different questions to around 229 different employees from areas like fast-food chains, e-commerce firms, and banks. This was done to ensure to get different views and opinions from people in different career fields.

### Describe the types of data and analysis done

 In regard to the data analysis, there were many statistical factors used that had a focus on cybersecurity. It included Cyber Security Incident Management , Cyber Security Awareness, Incident Reporting Suspicious Behavior, Cyber training, etc. With these factors, each were scaled from 1 to 5 with the average score being the typical or repeated responses given and the standard deviation represents the variability in responses.

### Describe how concepts from the PowerPoint presentations relate to the article

 Going back to the presentation of module 3, the multi method research seems like it would relate to this article. I say this because looking at the analysis for the research, it used multiple surveys, and different factors to assess and get the result of a hypothesis.

### Describe how the topic relates to the challenges, concerns and contributions of marginalized groups

 I believe the study puts an emphasis and need on cyber training workers and employees to handle things like stress with artificial intelligence. Having your workers aware of how it works, and decisions to make with it are crucial to both of them employees and companies. This also applies to marginalized groups who are uneducated about AI, it would be in either themselves or their companies’ best interests to educate them on the capabilities of artificial intelligence.

### Conclusion

 In conclusion, this research evaluates and explains why it would be necessary to provide efficient cybersecurity training as it can help them relieve the stress of not knowing exactly what it is, or what is capable of. I feel it accurately aims at the psychological points that are necessary to improve the health of employees.

# References

Muthuswamy, V, Esakki, S.(2024). Impact of Cybersecurity and AI’s Related Factors on Incident Reporting Suspicious Behaviour and Employees Stress: Moderating Role of Cybersecurity Training, 18(4), 83-107. <https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/330/99>