Jahmire Whitehurst 02/17/25

AI and Cyber Securities Use in Suspicious Behavior Reporting

Intro

BLUF: this review is about the relation of social sciences, research questions, research methods, types of data analysis, how the presentations align with the article, how the article relates to challenges, marginalized groups, and concerns, and the contributions of the study to society.

This is a review of the article Muthuswamy and Essaki (2024). It shows the relation of many different topics in cyber security and AI. The social sciences are also described in the article and have been alluded to.

Body

This article discusses how psychological factors increase the likelihood of cybercrime similar to the principle of relativism. The former is from research by Muthuswamy and Essaki (2024) they also led a study on high stress leading to a negative cybersecurity posture. This proves the principle of objectivity because when you have a hypothesis like the former you need to run a study on people to find what you believe is actually true. When referring to figure 1 of Muthuswamy and Essaki (2024) the relationship between perceived threat in AI, incident reporting suspicious behavior, and then employee stress levels. The figure was given to make things as simple as possible for anyone to understand. On the topic of understanding, AI has many uses in many different fields and incident reporting is only the beginning. AI technology being used to solve cybersecurity problems shows that technology development improves the cybersecurity field. Muthuswamy and Essaki (2024) also goes on to describe the hypothesis of another article that cyber attacks are not planned or controlled and they can lead to unintended consequences because of this poor planning. This also ties in with the motives of cybercriminals: a person doing cyber crime for entertainment is not thinking about planning or consequences at the moment. The reinforcement sensitivity theory also ties with this closely a cyber criminal who is looking for rewards for their actions will not be worried about the consequences and more so their goal. Muthuswamy and Essaki (2024) also writes another article on the relation of high workload, short time frames, and absence of manager figures leading to burnout in cybersecurity employees. This also goes to show that conscientious employees need to have a managing figure in order to work efficiently and longer. These studies were done using 229 employee questionnaires in multiple different fields according to Muthuswamy and Essaki (2024).Being that cybercriminals are the marginalized group who have not taken these tests, they are what we set out to understand to better protect against them.Now AI can be used to determine why they do what they do and maybe even predict when they might attack.

Conclusion

The studies being done with cybersecurity and AI can have the chance to change the world if technology can advance to the point to catch criminals before they are convicted. Further research into the psychology of cyber security employees will help improve working conditions and chance of catching cyber criminals. Overall, this is a great article and gives me lots of hope of the uses of AI for good.

References

1. Muthuswamy,V.V., & Essaki, S. (2024). Impact of Cybersecurity and AI's Related Factors on Incident Reporting Suspicious Behaviour and Employees Stress: Moderating Role of Cybersecurity Training. *International Journal of Cyber Criminology, 18.(1), 1-25.* 10.5281/zenodo.4766805