William Aydelotte
10/2/2024
CYSE 201S
Article Review #1

View of Impact of Cybersecurity and AI's Related Factors on Incident Reporting Suspicious Behaviors and Employee Stress: Moderating Role of Cybersecurity Training

This article looks into the impact of the many factors of cybersecurity and artificial intelligence on how employees report suspicious activity related to cybersecurity incidents. It also takes a look at the roles of these factors that may contribute to employee stress and how cybersecurity training may change the look of these relationships.

This article uses a mix of quantitative and qualitative methods in order to collect and analyze data to get answers to their questions. Employee surveys and interviewers were used to gather opinions and insight into their stress levels and incident reporting of peers who were exposed to artificial intelligence cybersecurity systems. The findings in the statistics would then be applied to identify the relationships between the variables. The variables include AI usage, incident reporting, stress levels and the overall impact of training.

The findings in the study showed that there were advantages of using AI in cybersecurity but it has also given an equal effect on the growth of stress in the workplace. Organizations need to invest in key training in order to keep office morale up to make sure that their employee wellbeing is taken care of.

Cyber victimization in The Healthcare Industry

In this article it talked about the Routine Activities Theory (RAT). This theory argues that the frequency of crime increases when three elements are part of the workplace. Those three elements are a motivated offender, suitable target and the lack of a capable guardian. This theory can be used in the space of cybersecurity when identifying the traits of a vulnerable system in the healthcare industry. The motivated offender can be a cyber criminal after healthcare data. The suitable target is the data or systems that the system is using. The lack of a capable guardian is the absence of a robust security team or system that monitors the data of the enterprise.

Health care systems have very large targets on their back because of the information that they hold. They have healthcare records, critical personal identifying information and financial records. Health care systems are huge targets when it comes to getting sensitive information. The critical nature of these records also make them large targets for ransomware. Healthcare systems most of the time cannot afford the downtime within their systems as patient care can be critical depending on who is being seen. This makes them very likely to pay off that ransom in order to get their critical systems back up and running.

William Aydelotte
10/2/2024
CYSE 201S
Article Review #1

Conclusion

In the end these articles were very informative on what they were trying to prove. As we see New AI security systems may cause employees to stress if not given the proper training on them. We also see that you can spot out the risks of healthcare security by using the Cyber RAT framework.

Praveen, Y., Kim, M., & Choi, K.-S. (2024). Cyber victimization in the healthcare industry: Analyzing offender motivations and target characteristics through routine activities theory (RAT) and cyber-routine activities theory (Cyber-RAT). *International Journal of Cybersecurity Intelligence & Cybercrime*, *7*(2). https://doi.org/10.52306/2578-3289.1186

Jaishankar, K. (2024). View of Impact of Cybersecurity and AI's Related Factors on Incident Reporting Suspicious Behaviors and Employee Stress: Moderating Role of Cybersecurity Training. *International Journal of Cyber Criminology*, *18*(1).