Clifford Osei Yeboah

Old dominion University

CYSE 201 Social sciences

February 20, 2025

Article Review #1: Impact of Cybersecurity and AI's Related Factors on Incident Reporting Suspicious Behaviour and Employees Stress: Moderating Role of Cybersecurity Training

In an era where cyber threats are growing more sophisticated, the intersection of AI-driven security measures and human behavior has never been more critical nowadays. The topic relates to the principles of social sciences by examining how cybersecurity and AI influence human behavior, workplace dynamics, and stress levels. Psychology helps explain how employees perceive threats, report incidents, and cope with cybersecurity-related stress. Sociology and organizational behavior explore how AI-driven security measures shape workplace culture, trust, and compliance. Additionally, ethical and social considerations highlight the balance between security, privacy, and employee autonomy in the digital workplace.The most important point to me with the topic is the aspect of Psychology, this plays a key role in understanding how employees perceive threats, assess risks, and decide whether to report suspicious activity.

Increased reliance on AI-driven cybersecurity measures negatively affects employees' willingness to report suspicious behavior due to stress or fear of false reporting. Additionally, higher cybersecurity-related stress leads to lower rates of incident reporting among employees. For this research, I used Quantitative methods, this include surveys and questionnaires. Experiments, statistical analysis and modeling were used too. Employees may be surveyed to assess their stress levels, perceptions of cybersecurity threats, AI-driven security measures, and willingness to report suspicious behavior. Standardized scales (e.g., Perceived Stress Scale, Technology Acceptance Model) could be used to measure stress, compliance, and trust. A group of employees might receive cybersecurity training while another does not, allowing researchers to compare the effects of training on reporting behavior and stress reduction. The growing prevalence of work overload in contemporary organizations has become a critical issue,

given its negative impact on employee attitudes, perceptions, behaviors, well-being, and overall performance at work. For instance, work overload has been shown to negatively affect employee job satisfaction, organizational commitment, self-esteem, intrinsic motivation, and helping behavior. Moreover, work overload has been associated with increased levels of job stress, emotional exhaustion, burnout, and turnover intention among employees (Barriga Medina, Campoverde Aguirre, Coello-Montecel, Ochoa Pacheco, & Paredes-Aguirre, 2021 [7]; Hon & Kim, 2018; [8]). In the powerpoint the slide about the psychological role of victims in cyber relates to this topic.

In marginalized groups, women came to mind. Women, people of color, and individuals from lower-income backgrounds are underrepresented in cybersecurity careers, which can limit their access to training and advancement opportunities. Women in cybersecurity may face additional workplace stress due to gender biases, lack of inclusion, and the pressure to prove their competence in a male-dominated field. Business works better when there is an equal number of women and men. Women are a critical part of the economy and of the global workforce. It is well known that gender diversity in firm leadership yields higher levels of organizational commitment from employees (Perryman et al., 2016).

As cybersecurity and AI-driven security measures continue to evolve, their impact on employees—particularly in areas such as incident reporting, workplace stress, and perceptions of surveillance—must be carefully examined. This study highlights the critical role of cybersecurity training in moderating these effects, helping employees navigate AI-based security systems while reducing stress and improving compliance. Furthermore, the research underscores the challenges faced by marginalized groups,

particularly women, who often experience barriers to career advancement, biases in AI security tools, and increased workplace stress. By fostering inclusive cybersecurity policies, improving training accessibility, and ensuring fair AI implementation, organizations can create safer, more equitable workplaces where all employees feel empowered to participate in cybersecurity efforts.

Sources

https://doi.org/10.1016/j.ject.2024.08.004

https://doi.org/10.1016/j.techsoc.2024.102543

https://doi.org/10.1016/j.bushor.2024.12.004