Lukas Ankney

10/2/24

**Article Review #1:**

***Impact of Cybersecurity and AI’s Related Factors on Incident Reporting Suspicious Behavior and Employee’s Stress: Moderating Role of Cybersecurity Training***

**Relation to the Principles of the Social Sciences**

The focus of the article is to discover what ways incident reporting of suspicious behavior mediates relationships in the realm of cybersecurity incident management, cybersecurity awareness, AI and its perceived threat, and employee stress levels. The fact that these are the main ideas indicate how strongly this article ties to social science, since “suspicious behavior” is a behavioral issue in the cyber realm, employees are a social factor to consider that isn't online while considering security, and AI and its effects in society and particularly breaches is a hot topic. The researchers employed multidisciplinary inquiry by gathering data from employees that work in many different fields, and empirical research by directly observing responses.

**Article Research Questions & Hypotheses**

The researchers utilized structural equation modelling with partial least squares estimation when analyzing their data and testing their hypotheses. They hypothesized that providing counselling services and financial advice can reduce stress, reducing risky behavior in turn. The researchers also hypothesized that to have successful incident reporting among employees, there should be a mechanism that allows one to provide feedback to employees in reference to their reports to ensure staff engagement.

**Research Methods Used**

Questionnaires were utilized to collect quantitative data from 229 workers from various sectors like retail, food, banking, and more. Selection of said employees was structured to encompass a wide array of organizational settings and job roles in order to accomplish a thorough exploration of the variables being researched.

**Types of Data and Analysis Done**

Quantitative data was gathered whilst conducting the aforementioned questionnaires. Each factor involved was rated on a scale from 1 to 5, where the average score reflects the most common response, and the standard deviation indicates the variety in responses; the factors include Cyber Security Incident Management (CSIM), Cyber Security Awareness (CSA), Intention to Use AI (IU-AI), Perceived Threats in AI (PT-AI), Cyber Training (CT), Incident Reporting Suspicious Behavior (IRSB), and Employee Stress Level (ESL). The analysis of said data involves computing descriptive statistics for those factors in relation to cybersecurity awareness and behavior.

**PowerPoint Presentation Relations**

The subject of the article heavily pertains to human factors (or Human Systems Integration) in cybersecurity, namely the employees. The endeavor to improve the training of these employees and reduce their stress levels plays into the psychological aspects of cybersecurity, wherein maintaining a sound human mind prevents data leakage and improves the effectiveness of incident reports. The researchers also employ social science cyber research methods, namely the questionnaire they used, which is the same as a survey.

**Relation to Concerns & Contributions of Marginalized Groups**

While the subject of the journal does not have much to do with marginalized groups, the potential for concern lies within the data gathering method used; it is very possible, as has been seen many times before, that when gathering information for their study that certain groups were underrepresented, such as women. Additionally, since the questionnaire was only conducted towards employees of various businesses, the unemployed are not represented in the data although they also access online spaces in most cases.

**Overall Contribution to Society**

Emphasizes how integrating psychological and technical facets in cybersecurity management helps to better protect employee safety and underscores the effectiveness of incident reporting and cybersecurity training advance general understanding of how cybersecurity practices can affect employee welfare. In simple terms, the study contributes ideas pertaining to employee training/safety and the effectiveness of incident reporting suspicious behavior in mediating a multitude of relationships.

**Conclusion**

The study highlights the effectiveness of both robust incident reporting systems and advantageous cybersecurity training to mitigate employee stress in relation to cybersecurity and AI issues. It suggests organized training improves employees’ abilities to cope with stressful situations and stress that arises due to AI implementation.

**References**

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