Abraham Perez
3/24/2024

Article Review #2: Seeing Social Science in Cyber Criminology (1157)

Introduction:

In this article review, I will cover the journal "Mitigating Ransomware Risks in Manufacturing and the Supply Chain: A Comprehensive Security Framework" which discusses valuable insights into the overall security resilience of enterprises and analyzes the dynamics of ransomware risk mitigation. I will also be going into how this journal relates to the principles of social sciences and covering the essentials needed in a research paper. This would include; research questions/hypotheses, the methods used, data/analysis, and the contribution this research made to society. There will additionally be parts discussing its relation to class and how it relates to the marginalized groups that are associated with this topic. Hopefully, this will be informal to the reader/audience.

Principles:

Many principles of social science can be applied to this journal. One of them would be ethical neutrality, with how much a company's employee can be trusted with certain "valuables". This could involve classified information that shouldn't be viewed by the public or having an evaluation of a team of administrators monitoring the company's network. Another principle would be the principle of determinism, in which for this journal, it comes down to how a company responds to the ransomware attack and if they've dealt with this kind of situation before. One other principle that comes to mind from this journal is parsimony, an example would be how it's a better choice to have simpler lessons for employees to be trained and not complex lessons that would be rather taught to an IT department employee.

Research Question/Hypothesis:

The journal has several hypotheses, with the majority of them involving the usage of employee training. One of these hypotheses is that “Employee Behaviour and Adherence play a role in the relationship between Employee Training and Awareness and Comprehensive Security Posture. The effectiveness of employee training and awareness programs relies on employees' ability to integrate and adhere to security rules, ultimately impacting the overall security level. Robust security frameworks require the implementation of effective employee training and awareness activities.” (Aljoghaiman et. al., 2023, page 2). Another hypothesis is that employee behavior/adherence plays a primary role in the relationship between Technological Solutions Implementations and Comprehensive Security Posture. This overall states that the employee’s role in maintaining the solutions of the technology is a key aspect of security. A third hypothesis observed the relationship between the Supply Chain Resilience Measures and Comprehensive Security Posture and proposed that this relationship also has a key factor of employee behavior in it. One final hypothesis is factoring in employee behavior into the relationship between Collaboration and Information Sharing Practices and Comprehensive Security Posture. It can be seen that the main takeaway from these hypotheses is that employee behavior has a major impact on the company.

Below is a diagram showing the framework of various relationships that employee behavior connects with a Comprehensive Security Posture.

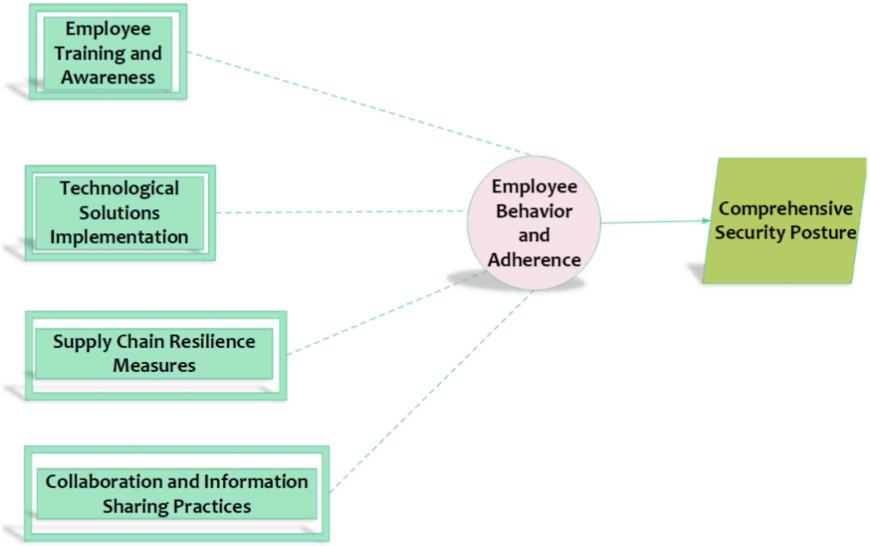
Employee Training and Awareness
Technological Solutions Implementation
Supply Chain Resilience Measures
Collaboration and Information Sharing Practices
Employee Behavior and Adherence
Comprehensive Security Posture

Figure 1: Conceptual Framework

Research Methods:

The data collected for this journal was in the format of a questionnaire/survey. This questionnaire was used to address multiple areas concerning the mitigation of ransomware risk, which includes organizational preparedness, security protocols, and prior knowledge. It was performed systematically and uniformly, thus guaranteeing all responses to an identical set of questions. The survey data helped gather insights into various perspectives regarding ransomware threats in a context focused on industry specifically. This data was also used to help create a security architecture to face challenges in the manufacturing and supply chain departments of Saudi Arabia.

Data Analysis:

Having the data being collected from the survey, the journal concluded that there is an emphasized importance of incorporating socio-technical elements into various security models, and acknowledging that solely relying on technology is not efficient. An example like this could be how it's better to "think outside the box" when dealing with technical issues and not solely relying on whatever device the employee is using. It also takes into consideration that employee training should be prioritized, integrating technology, establishing a firm supply chain, and implementing collaborative behaviors as tangible actions. Overall, this data helps prove that employee training and integrating technical solutions can improve a company's efficiency. Although there isn't much else to analyze for this journal, it can still prove useful when it comes to learning to improve a company's IT infrastructure.

Relation to Class:

With how this journal tackles mitigation and/or risk management, it allows for there to be some kind of relation to what we've learned in class. One big topic that can relate to this journal is human factors, with how it's imperative to establish employee training. Another topic would be the way the journal gains its data, that is by conducting a survey research method, which was discussed in module 1 of our class. Another correlation would be the principle of parsimony, as discussed earlier in this article review, with how it's better to "simplify" things to allow employees to not get confused when being trained. Although there is the topic of ransomware that hugely plays in the cyber-criminology world, the only correlation that can go with it is the human factors of preceding events. Overall, it can be seen that this journal can be its own thing but still have some correlation with our class.

Relation to Marginalized Groups:

This journal can be seen to help contribute to the entire business world, but who exactly can it correlate with? Given how its data proves that employee training is a key factor in preventing ransomware, it can be considered that this journal is to inform executive people on what to do with their company. Perhaps to the IT department as well with how there is an influx of socio-technical relationships. The relationships between each department of a company are incredibly important when it comes to technology. Especially if there is some kind of technological situation. Whether it's someone high up in the company or a completely new, first-day employee, it shows that this journal can be viewed by anyone who wants to improve their skills with technology and cybersecurity.

Overall Contributions:

Showing how this journal contributes to both employees and their companies, there is also the main takeaway on how it overall contributed to the world. It highlights how different security components and human variables are interconnected. The study also takes into account the major impact of employee behavior and how it offers a comprehensive insight that goes beyond conventional technology solutions. This contribution applies to businesses looking to improve their security frameworks as well as professionals in supply chain management and cybersecurity. This study adds significantly to the subject of cybersecurity by highlighting the necessity of a comprehensive and understanding approach that takes human factors and technological improvements into account. This research also highlights the ever-expansive understanding of human-centric elements in successful security measures by considering employee behavior in cybersecurity.

Conclusion:

This journal discussed how employee training is a key factor in the mitigation of ransomware and other technical situations. It went over various hypotheses that led to data being collected in uniform behavior to help prove its stance. There were also the relations to our class modules and the principles of social science that were covered, albeit there was some "independence" between the journal and class. There were additionally the contributions of this journal to society and perhaps what kind of marginalized groups it focused on. The main takeaway from this article review is that having employees knowledgeable in the technical world can prove to be beneficial to both themselves and the companies that they work for.

Works Cited

Aljoghaiman, A., & Kaliani Sundram, V. P. (2023, July-December). *Mitigating Ransomware Risks in Manufacturing and the Supply Chain: A Comprehensive Security Framework*. International Journal of Cyber Criminology. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/214/81