International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS)
ISSN : 2581-7930, Impact Factor : 5.880 , Volume 04, No. 01, January - March, 2021, pp 347-350

IMPACT OF AWARENESS, PREPAREDNESS, BEHAVIOR AND ATTITUDE OF RESPONDENTS TOWARD CYBER RISKS ON EXPERIENCE- A RESEARCH ON CYBER RISK MANAGEMENT

Subroto Panda*

ABSTRACT

This research paper aims to explore the impact of awareness, preparedness, behavior, and attitude of respondents toward cyber risks on their experience of cyber risk management. The study focuses on understanding how individuals' knowledge, level of preparedness, actions, and attitudes affect their ability to effectively manage cyber risks. A comprehensive research methodology was employed, including data collection through surveys and interviews, data analysis using statistical techniques, and interpretation of the findings. The results indicate that a higher level of awareness, preparedness, responsible behavior, and positive attitudes toward cyber risks positively influence individuals' experience of cyber risk management. The implications of these findings are discussed, and recommendations for improving cyber risk management practices are provided. The paper concludes with suggestions for future research in this area.

Keywords: *Cyber Risks, Awareness, Preparedness, Behavior, Attitude, Experience, Risk Management.*

Introduction

In today's digital age, cyber risks have become a significant concern for individuals and organizations alike. The increasing reliance on technology and the interconnectedness of systems have led to a rise in cyber threats, including data breaches, identity theft, and financial fraud. To effectively manage these risks, it is crucial to understand the factors that contribute to individuals' ability to mitigate cyber threats. This research paper investigates the impact of awareness, preparedness, behavior, and attitude of respondents toward cyber risks on their experience of cyber risk management.

Theory

The theoretical framework for this study draws on various concepts related to cyber risk management. It incorporates theories of risk perception, including the Protection Motivation Theory, which suggests that individuals' behavior is influenced by their perception of the severity and vulnerability to a threat. Additionally, the Theory of Planned Behavior emphasizes the role of attitudes, subjective norms, and perceived behavioral control in shaping individuals' intentions and actions. These theories provide a foundation for understanding how awareness, preparedness, behavior, and attitude influence the experience of cyber risk management.

* Research Scholar, Department of Management, Radha Govind University, Ramgarh, Jharkhand, India.

Data Analysis

To gather data for this study, a survey questionnaire was administered to a diverse sample of respondents. The survey included items related to respondents' level of awareness, preparedness, behavior, attitude toward cyber risks, and their experience of cyber risk management. Additionally, in-depth interviews were conducted with selected participants to obtain qualitative insights into their experiences and perspectives.

The collected data were analyzed using statistical techniques such as descriptive analysis, correlation analysis, and regression analysis. The quantitative analysis provided insights into the relationships between variables, while the qualitative analysis helped in understanding the underlying factors and motivations influencing individuals' experiences of cyber risk management.

Research Methodology

This study employed a mixed-methods research design, combining quantitative and qualitative approaches. The survey questionnaire was distributed to a random sample of participants, and the data were analyzed using statistical software. The interviews were conducted with a purposive sample of participants who exhibited diverse characteristics and experiences related to cyber risk management. The qualitative data were transcribed, coded, and analyzed thematically to identify patterns and themes.

Results

The data analysis revealed several important findings regarding the impact of awareness, preparedness, behavior, and attitude of respondents toward cyber risks on their experience of cyber risk management.

Firstly, there was a strong positive correlation between awareness and the experience of cyber risk management. Respondents who demonstrated a higher level of awareness regarding cyber risks reported a more positive experience in managing those risks. This finding emphasizes the significance of educating individuals about cyber threats, their potential consequences, and ways to mitigate them. Increased awareness can empower individuals to make informed decisions and take appropriate actions to protect themselves and their organizations.

Secondly, preparedness played a crucial role in shaping the experience of cyber risk management. Individuals who reported being well-prepared, equipped with knowledge, resources, and preventive measures, expressed a higher level of satisfaction with their ability to handle cyber risks. This highlights the importance of implementing proactive measures, such as regular system updates, robust security protocols, and employee training programs, to enhance preparedness and minimize vulnerabilities.

Thirdly, responsible behavior significantly influenced the experience of cyber risk management. Respondents who exhibited responsible behavior, such as adhering to security protocols, practicing safe online habits, and promptly reporting suspicious activities, reported better outcomes in managing cyber risks. This underscores the need for promoting a culture of cybersecurity awareness and instilling responsible behavior among individuals at all levels.

Lastly, positive attitudes toward cyber risks were associated with a more favorable experience of managing those risks. Respondents who maintained a positive mindset, viewing cyber risks as challenges that can be effectively mitigated rather than insurmountable obstacles, reported greater confidence and resilience in their cyber risk management efforts. Fostering positive attitudes through education, training, and creating a supportive organizational culture can contribute to more effective risk management practices.

Conclusion

Based on the findings, it can be concluded that awareness, preparedness, behavior, and attitude significantly impact the experience of cyber risk management. Individuals who possess a higher level of awareness, are well-prepared, exhibit responsible behavior, and maintain positive attitudes toward cyber risks are more likely to have a positive experience in managing those risks. These factors collectively contribute to enhancing individuals' ability to mitigate cyber threats, minimize vulnerabilities, and respond effectively to incidents.

Organizations should prioritize cybersecurity awareness programs, providing comprehensive training and resources to promote awareness and preparedness among employees. Encouraging responsible behavior through clear policies, regular communication, and incentives can foster a culture of cybersecurity consciousness. Furthermore, cultivating positive attitudes by emphasizing the importance

of proactive risk management and highlighting success stories can motivate individuals to take cybersecurity seriously and engage in effective risk mitigation practices.

Future Scope

While this research paper provides valuable insights into the impact of awareness, preparedness, behavior, and attitude on the experience of cyber risk management, there are several avenues for future research:

- **Longitudinal Studies:** Conducting longitudinal studies to assess the long-term impact of awareness, preparedness, behavior, and attitude on individuals' experience of cyber risk management would provide a more comprehensive understanding of their interrelationships and their effectiveness over time.
- **Comparative Analysis:** Comparing the experiences of different demographic groups, such as age, gender, occupation, and level of technological expertise, would help identify variations in the impact of awareness, preparedness, behavior, and attitude on cyber risk management. This would facilitate the development of targeted interventions tailored to specific groups.
- **Evaluation of Interventions:** Investigating the effectiveness of specific interventions and strategies aimed at enhancing awareness, preparedness, responsible behavior, and positive attitudes toward cyber risks would provide valuable insights into the most effective approaches for improving cyber risk management practices.
- **Cultural Influences:** Exploring the role of cultural factors in shaping individuals' awareness, preparedness, behavior, and attitude toward cyber risks would contribute to a more comprehensive understanding of how societal norms and values influence cybersecurity practices.
- **Technological Advancements:** With the rapid evolution of technology and emerging threats, future research should investigate the impact of new technologies, such as artificial intelligence, blockchain, and Internet of Things, on cyber risk management practices and individuals' experiences.

By addressing these areas of future research, we can further enhance our understanding of the factors that influence effective cyber risk management and develop more robust strategies to mitigate cyber threats in an increasingly interconnected world.

References

- ✓ Chen, L., & Lui, M. (2020). A systematic review of cybersecurity awareness research. Computers & Security, 88, 101663.
- ✓ Colwill, C. A., &Debevec, K. (2018). An examination of the relationship between cybersecurity knowledge and information security behaviors: A meta-analysis. Computers & Security, 78, 165-175.
- ✓ Egelman, S., & Peer, E. (2015). Why people fail to recognize their own incompetence in online tasks. Journal of Economic Behavior& Organization, 116, 30-43.
- ✓ Furnell, S., & Clarke, N. L. (2018). Exploring the relationships between cyber-risk awareness, cybersecurity investment, and organizational performance. Journal of Cybersecurity, 4(1), tyx019.
- ✓ Gerber, N., & von Solms, R. (2005). Management of information security awareness and its measurement. Computers & Security, 24(2), 108-118.
- ✓ Goel, S., Williams, K. D., & Konrath, S. H. (2018). Cybersecurity behaviors and the protection motivation theory. Computers & Security, 77, 249-263.
- ✓ Haddadi, H., &Awad, A. (2020). The role of awareness, behavior, and cybersecurity practices in mitigating cybersecurity risks: A survey study. Information Systems Frontiers, 22(5), 1107-1131.
- ✓ Hamari, J., Sjöklint, M., & Ukkonen, A. (2016). The sharing economy: Why people participate in collaborative consumption. Journal of the Association for Information Science and Technology, 67(9), 2047-2059.
- ✓ Han, H. S., & Han, I. (2018). Cybersecurity investment behavior: An empirical analysis of individuals' cybersecurity behaviors. Computers in Human Behavior, 80, 165-175.
- ✓ Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with

information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615-660.

- ✓ Jaeger, P. T., St. Jean, B., & Grimes, J. M. (2007). Information seeking and cybersecurity: Why do individuals turn to social sources for advice? Journal of the American Society for Information Science and Technology, 58(9), 1359-1370.
- ✓ Jensen, C., Potts, C., & Jensen, S. (2015). Privacy practices of Internet users: Self-report versus observed behavior. International Journal of Human-Computer Studies, 79, 101-112.
- ✓ Kirlappos, I., Sasse, M. A., & Harvey, N. (2018). "Never give up on your password": A study of user perceptions of multiple password use in everyday life. International Journal of Human-Computer Studies, 114, 52-63.
- ✓ Koronios, A., &Polatidis, H. (2006). Information security awareness in small and medium enterprises: A case study. Information Management & Computer Security, 14(5), 394-406.
- ✓ Liang, H., Xue, Y., & Li, H. (2017). Information security policy compliance in organizations: An empirical investigation of rationality-based beliefs and individualism. Information & Management, 54(7), 871-883.
- ✓ Martens, B., Tepe, M., & Haggerty, N. (2015). A meta-analysis of computer-based training in cyber security awareness: The influence of learning domain, frequency, and duration. Journal of Computer Information Systems, 55(4), 9-18.
- ✓ Naiakshina, A., Danilova, A., Krupp, J., & Smith, M. (2020). Understanding the impacts of information security awareness on employees' security behavior. Computers & Security, 91, 101685.
- ✓ Rainer Jr, R. K., & Turban, E. (2008). Introduction to information systems: Supporting and transforming business. John Wiley & Sons.
- ✓ Vroom, V. H. (1964). Work and motivation. John Wiley & Sons.
- ✓ Von Solms, R., & Von Solms, B. (2004). From awareness to action in managing information security. Computers & Security, 23(3), 167-177.