Cybersecurity Readiness within SMEs

Prafulkumar Chunilal Patel

Department of Computer Science, Monroe College, King Graduate School

KG604: Graduate Research & Critical Analysis

Professor Jonathan Kyei

2/28/2023

Assessing Cybersecurity Readiness within SMEs

Introduction to Literature Review

Small and medium enterprises (SMEs) encounter risks to cybersecurity safety as they implement technological processes in their business operations (Perozzo et al., 2021). Following the cybersecurity risks that SMEs face in the ever-growing business world, there is need for research to help determine the level of preparedness and offer possible remedies for the cybersecurity safety issue. The literature review comprised only research articles and literature about the status of readiness of SMEs when it comes to cybersecurity challenges. The factors that were reviewed in the study were the organizational readiness of SMEs, different cyber threats to SMEs and their impacts, and the possible preventive measures SMEs can use against cyberattacks. The literature review process was conducted in Monroe College Library databases like ProQuest, EBSCO Host, and Google Scholar. SMEs, cybersecurity organizational preparation, and cybersecurity were some of the search phrases used to locate pertinent publications for the literature review.

Review of Literature

Cybersecurity Awareness

Perozzo et al. (2021) conducted a qualitative multiple-case study in Italy to explore existing literature on cybersecurity. This study was published in the Complex Systems Informatics and Modeling Quarterly (CSIMQ) journal as article 185 and issue number 33, from pages 53 to 66. The paper follows a multiple case study using multiple resources to explore real-life cases over time. The authors aimed to explore the limitations of the readiness models of small and medium enterprises (SMEs) for cybersecurity and proposed a framework that may be used. The authors use a qualitative multiple-case study method to understand the socio-cultural

context of the study participants. Perozzo et al. (2021) collected data through semi-structured interviews and reviewed secondary and internal resources. The interviews were recorded, transcribed, and annotated after taking 45 minutes each. Taking into consideration their expertise and experience, the research participants were chosen. Three Italian manufacturing SMEs were included in the study. The article used the data from the literature and socio-technical perspectives to propose a Cyber Security Readiness Model (CSRM-SME). The CSRM-SME helped assess the readiness of SMEs for cybersecurity. The model can help professionals and firms determine their readiness for cyberattacks. The model also helps companies understand their contextual environment and plausible cyberattack prevention strategies. SMEs can become more resilient in preventing and managing the risks of cyberattacks.

Neri et al. (2022) carried out a study in Italy to determine the degree of preparation of SMEs for coping with cyber threats. This study had similar goals to Perozzo et al. (2021). The researchers used a survey administration to collect data between December 2020 and February 2021. To get more thorough, insightful data regarding how SMEs are prepared cybersecurity-wise, the researchers conducted quantitative and qualitative assessments. The survey, which the authors divided into four components, was subjected to a quantitative data analysis. Each of these categories was important in identifying the essential characteristics that firms need to evaluate and enhance their cyber preparedness. According to the study's results, SMEs in Italy have both strengths and shortcomings when it comes to cybersecurity. Neri et al. (2022) discovered that Italian-based SMEs had the ability to understand the importance of crucial information. SMEs also benefit from the ability to recognize cyber risks coming from both inside and outside the firm. In terms of disadvantages, the long-term planning of SME decision-makers is limited because they are concerned with day-to-day activities. Also, SMEs face cyber threats

because of the need for a cybersecurity budget. For SMEs to be able to avoid cyberattacks on their own, they require a specific budget for cybersecurity. Lack of money results in ignorance and shifts attention away from the company operations' operational components. The challenge with SMEs is that they need to consider themselves targets or anticipate safety measures against cybercriminal acts.

Similarly, Rawindaran et al. (2022) conducted a survey in Wales in the year 2022. The study was purposed to help understand the importance of cybersecurity awareness and how it helps SMEs to address cyber threats. The authors followed a survey methodology to collect data. The paper methodology was a quantitative survey questionnaire that follows positivism. Several Businesses in Wales received the surveys. 122 individuals who took part in the survey were chosen by convenience sampling. The survey was successfully created and distributed using Qualtrics. Rawindaran et al. (2022) found out that workers in SMEs have a substantially low level of awareness of cybersecurity. The study participants explained that they did not need to understand machine learning because they needed more support from their information technology (IT) teams. SMEs relied on IT companies to sort out their technological needs. Respondents affirmed that they either used simple antivirus or were not aware of the expiry of their software licenses. Some SMEs allowed university organizations to handle their software needs. The researchers revealed that SMEs faced challenges when using machine learning in cyber security packages. While 72% were unaware of machine learning, 10% attested challenges to technical expertise barriers, and 8% blamed the high cost of implementing and using those packages.

Impact of Cyberattacks on SMEs

A different study from the above was also conducted concerning the impact of cyberattack damage. In Saudi Arabia, 296 respondents from small businesses participated in a survey that Alharbi et al. (2021) performed. Between December 2020 and March 2021, the authors gathered data to determine the impact of cybersecurity procedures with reference to cyber threats. The data collection for the survey was from 3 December 2020 to 18 March 2021. Of the 296 respondents, 14 were excluded due to incompleteness leaving 282 final respondents' data for use. The research findings showed that some organizations lost vital data during attacks, but there was minimal financial damage, with 20.5% and 14.2%, respectively, for the former and the latter. Organizational recovery times after cyberattacks were different. 22.3% of the enterprises took days to recover, while 9.6% of the cases took months. The inspection team and recovery strategy had an influence on the damage. Data loss was also linked to pay of specialists, understanding of the harm, and cybersecurity awareness. In the event of cybersecurity assaults, SMEs that have a team for inspection and a recovery plan were less likely to sustain major financial harm. Saudi Arabian SMEs must abide with the Capital Market Authority by assembling a team to examine the information security measures.

Analysis of Literature

The issue of cyberattacks has persisted in many Italian Enterprises. Semi-structured interviews and survey questionnaires were two main research methodologies used by the reviewed articles. The authors also had other preferences for quantitative and qualitative methods. Perozzo et al. (2021) and Neri et al. (2022) researched SMEs' readiness for cybersecurity concerns in Italy. Perozzo et al. (2021) used a qualitative multiple case study approach, while Neri et al. (2022) chose both quantitative and qualitative methods in four

sections. These two studies present the challenges SMEs in Italy face when faced with cybersecurity issues. The challenges of SMEs in Italy include the need for a long-term plan for proper cybersecurity measures since the decision-makers only deal with daily problems. Additionally, SMEs have the challenge of not setting aside a cybersecurity budget which lowers the level of readiness when such risks happen. Neri et al. (2022) established that SMEs do not usually anticipate facing cyberattacks, which is another risk factor since they need to prepare. A similar study was conducted by Rawindaran et al. (2022) in Wales. A quantitative survey showed that many SME workers need to be aware of the safety measures for preventing cyberattacks. The research showed that many SMEs need to be mindful of the importance of cybersecurity measures in preventing cyberattacks. In another study, Alharbi et al. (2021) showed cyberattacks' impact on SMEs. The authors showed that most Saudi Arabian organizations take days to recover from cyberattacks, while few escalate this period to months. Perozzo et al. (2021) were unique because they offered the CSRM-SME model to support SMEs in staying ready for cyberattacks.

References

Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. *Sensors, 21*(20), 6901. https://doi.org/10.3390/s21206901

Neri, M., Niccolini, F., & Pugliese, R. Assessing SMEs' cybersecurity organizational readiness: Findings from an Italian survey. *Online Journal of Applied Knowledge Management* https://www.researchgate.net/publication/363741932_Assessing_SMEs'_cybersecurity_organizational_readiness_Findings_from_an_Italian_survey

Perozzo, H., Ravarini, A., & Zaghloul, F. (2021). Assessing Cybersecurity Readiness within SMEs: Proposal of a Socio-Technical based Model. *Internation Workshop in Soci-Technical Perspective in IS Development,* 19-21. https://ceur-ws.org/Vol-3239/paper3.pdf

Rawindaran, N., Jayal, A., & Prakash, E. (2022). Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime. *Computers*, *11*(12), 174. https://doi.org/10.3390/computers11120174