Journal of Information Systems Engineering and Management
2025, 10(7s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

An Empirical Study on the Economic Impact of Cybersecurity Breaches and Computer Fraud on SMEs

Dr. Nidhi Sonkar[1], Dr. Nivedita Verma[2], Dr. Arun Kumar[3], Dr. Doa Naqvi[4], Dr. Zaibun Nisa[5]

[1]Assistant Professor, [1]Institute of Management Studies, Ghaziabad U.P. (India); nidhisonkar1605@gmail.com

[2]Assistant Professor, School of Management Sciences, Varanasi U.P. (India); neetumanu@gmail.com [3]Assistant Professor, Department of Commerce, Bundelkhand P.G. College, Jhansi, U.P. (India); bhuarun@gmail.com

[4]Assistant Professor, Department of Business Administration, Khwaja Moinuddin Chishti Language University, Lucknow U.P. (India); drdoakmc@gmail.com

[5]Assistant Professor, Department of Commerce, Khwaja Moinuddin Chishti Language University, Lucknow U.P. (India); zaibunrizvi@gmail.com

ARTICLE INFO

Received: 10 Oct 2024

Revised: 06 Dec 2024

Accepted: 20 Dec 2024

ABSTRACT

An empirical study of the economic impact of cybersecurity breaches and computer fraud on Small and Medium Enterprises (SMEs) is presented in this research paper. As the need for digital infrastructure continues to rise, SMEs are ever increasingly finding themselves being hit by cyber attacks, resulting in huge financial losses and operational disruptions. Using SME data from various sectors, the study examines the extent and nature of these impacts. We examine key areas of focus associated with breaches, including direct financial costs, indirect costs (such as reputational damage) and broader impacts on business continuity. The research is done by employing quantitative analysis methods to identify trends and correlations of frequency of cyber attacks and financial resilience of SMEs. These findings highlight the need for robust cybersecurity measures as well as provide lessons for policymakers and business owners on how to reduce risks. As such, it further contributes to the increasingly voluminous SME cybersecurity literature by providing a foundation for further research and strategic policy development.

Keywords: Cybersecurity, SMEs, Economic Impact, Cyber-attacks, Computer Fraud, Financial Loss, Business Continuity, Risk Mitigation.

INTRODUCTION

Small and Medium Enterprises (SMEs) are today heavily dependent on technology for growth, operation streamlining and competitive edge. Unfortunately, as SMEs grow more dependent on digital infrastructure, demanding more distributed mobile devices, and more deliveries made, they all have become prime targets for cyber breaches and computer fraud. SMEs are often not the resources nor the expertise to implement comprehensive cybersecurity measures making them particularly vulnerable to cyber threat.

Cybersecurity breaches and computer fraud have a very significant cost for SMEs. These include direct financial losses like theft of funds or data ransom, as well as indirect ones like reputational damage, loss of customer trust, and legal liabilities. The combined damage can seriously weaken an SME's capacity to operate, with adverse effects on the SME's future.However, research on the economic impact of cyber-attacks on SMEs is scarce and more empirical evidence is required given the recent growing threat landscape. Evading more attention, 'while, large organizations in particular, given cautious study, SMEs are a vital fragment of the worldwide economy as well deal with insurance claims that must be examined all the more fittingly.' To this end, understanding the economic implications of cyber threats to SMEs is essential in the development of specific cybersecurity strategies and policies that can help protect this most essential part of the economy.This thesis seeks to address this research gap by investigating the economic impact of cybersecurity breaches and computer fraud on SMEs. Drawing on the combination of quantitative data analysis and case studies, the research aims to uncover the scale and nature of the financial damages caused to SMEs, the processes for recovery from that, and the strategies utilized by SMEs to prepare for and respond to cyber threats. This study sheds light on these aspects in order to draw actionable insights for SME owners, policymakers, and cybersecurity professionals who would like to improve cyber-resilience against cyber-attacks.

LITERATURE REVIEW

Research on cyber breaches and their effects on firms is an important part of strategic management courses (Ashibani et al., 2017; Lezoche and Panetto, 2020; Chronopoulos, Panaousis and Grossklags, 2018; Fielder, 2016). An attack on a company's information systems (IS) isn't the only ill effect it can have: For instance, legal ramifications, damage to the company's brand, effects on supply chains, and business continuity are all also becoming more important. Moreover, businesses attempt to quantify how secure they are and how probable it is that they might suffer a cyber breach, which could, in the worst case scenario, significantly harm its financial and economic standing.a footnote1 for instance is contained in Pirounias, Mermigas, and Patsakis (2014).Considered in this framework, the causes and consequences of data breaches in businesses have been studied (Heartfield et al., 2018; Conteh and Schmick, 2016; Gatrner Group, 2014). Despite such remarkable progress, there exists very little knowledge about what correlations can be made between breaches and the potential damage to businesses (in particular, conclusions around this relationship so far have been mixed and insufficiently informed) (e.g., Couce-Vieira, Insua, and Kosgodagan 2020). This is caused from a number of things. Sahoo and Gupta(2019), Heartfield, Mahmud and Pickett (2018), Choo (2011), Bland et al.(2020), Wang and Zhang(2020) and Seibold et al.(2020) also affirm that the issue lies in identifying a breach in corporations. However, the whole scope of the threats that firms might have to face has not been considered by most previous studies investigating certain types of assaults and single firms (Garre, Pérez, and Ruiz-Martínez 2021; Dahiya and Gupta 2020). Moreover, research on cyber-breach effect on business has been rare, whereas little has been done on how cyber-breach would impact businesses on an economic, financial, and managerial perspective (Couce-Vieira, Insua, and Kosgodagan 2020). Firm cybersecurity management is not very permeable and this is how it happened. The complexity and technological uniqueness of cybersecurity make managers difficult to get engaged (Ahmad et al. 2019; Cavusoglu et al. 2015; Srinidhi, Yan, and Tayi 2015).In the absence of that knowledge vacuum, this article will explore consequences of cyber intrusions on business. To accomplish this, we make a number of assumptions in establishing the parameters of our study. Rather, let's pretend for now that there are a number of different types of cyber breaches that occur in businesses, each with different outcomes. This paper draws from a statistical study of breach types and of their consequences for firms, thus differing from other analyses of this type. We will moreover fill a gap in the literature by considering SMEs who've been neglected in nearly all preceding research (Ponsard, Grandclaudon, and Dallons 2018; Osborn 2015; Valli, Martinus, and Johnstone 2014; Hayes and Bodhani 2013). It is widely known, that SMEs are important for the global economy. At an example, in European nations they generate 60% greater than GDP and hire 6 out of seven people (Müller, Buliga, and Voigt 2018). SMEs represent about 72% of breaches (Fielder et al., 2016), but relatively little attention has been accorded to the SME sector relative to organisations with elaborate IT departments and greater available resources (Osborn, 2015). In the case of cyber attacks, sixty percent of small businesses shut down within the first six months after a cyber attack, and of course, this number goes up along with the intensity of the attack. Therefore, SMEs encounter glitches that affect the company's workings and make it hard for workers to do their daily activities. Thus, finally, this work employs a systematic cause and effect analysis (Somya Sahoo and Gupta 2019). To do so, we use artificial neural networks (ANNs) for prediction and simulation, exploring the relationships between breaches and their consequences for SMEs. Arranz and Fernandez de Arroyabe (2010) and Somers and Casal (2009) state that machine learning approach can be applied to the analysis of many complex business and management research topics with high measurements of interactions. In the case of the corporate cybersecurity management, it is especially true given that the breaches spread far and wide, all resonated from the complex web of interrelated factors (Couce Vieira, Insua, and Kosgodagan 2020). However, prior research on cybersecurity in firms has been based on survey data which suffers from a low response rate (Cyber Security Breaches Survey 2017) due to the difficulties of recognising assaults and threats as well as their impact on businesses. Furthermore, Somers and Casal (2009) and Minbashian, Bright, and Bird (2010) claimed in situations where the response is low, connection can be established by using a solution which has high resilience, like machine learning methods.Cybersecurity breaches and their effects to companies still remain unclear, especially to small and medium sized enterprises (SMEs). Less attention has been paid in literature available to specific limitations of SMEs that have been discussed mostly in relation to big firms. The study of larger economic and financial consequences of breaches has been ignored in favor of studying the technical parts. Furthermore, few studies exist that combine strong approaches, such as machine learning, in a cause and effect sense between breaches and their outcomes. Using sophisticated statistical approaches, this research fills in several gaps in our understanding of the economic effects of cybersecurity events. It considers SMEs, considers a whole range of cyber breaches and tries to provide a holistic view.

Objectives of the study

- To analyze the prevalence and types of cybersecurity breaches affecting SMEs.
- To assess the direct and indirect economic impacts of cybersecurity breaches on SMEs.
- To evaluate the relationship between cybersecurity preparedness and the financial resilience of SMEs.

Hypothesis:

There is a positive relationship between cybersecurity preparedness and the financial resilience of SMEs, such that higher levels of cybersecurity preparedness are associated with greater financial resilience in the face of cybersecurity breaches.

RESEARCH METHODOLOGY

This research uses a mixed method research design to assess the economic impact of cybersecurity breaches on SMEs. In the quantitative part, data is being collected using structured surveys and from the financial records of SMEs in several industries related to the frequency, types and impacts of cyberattacks. Methods of statistical analysis such as regression models and correlation analysis, will be performed to find patterns or relationships between cybersecurity preparedness and financial resilience. Furthermore, artificial neural networks (ANNs) will be trained to predict the likely damage incurred by future breaches. The part of this is qualitative—it is based on in-depth interviews with SME owners and cybersecurity experts to learn about the challenges and strategies pertaining to cybersecurity. This combination of quantitative (to some degree, qualitative) approaches ensures that we obtain a holistic view of the issue and can make robust conclusions and actionable recommendations in this project.

Data analysis and discussion

Table 1 – Descriptive statistics

Variable	Mean	Median	Standard Deviation	Minimum	Maximum
Cybersecurity Preparedness Score	75.4	78.0	12.3	45	95
Financial Resilience Index	82.6	85.0	10.8	50	98
Number of Cybersecurity Incidents	3.2	3.0	1.5	1	7
Downtime Due to Breaches (hours)	12.5	10.0	8.4	2	40
Financial Loss Due to Breaches (Rs.)	25,0000	20,0000	15,0000	5,0000	75,0000

An overview of key variables concerning SMEs' cybersecurity preparedness and financial resilience can be given through descriptive statistics as shown in Table 1. On average, the Cybersecurity Preparedness Score was 75.4 with a moderate spread as shown by a standard deviation of 12.3, showing that SMEs sampled are generally highly prepared in cybersecurity. The Financial Resilience Index has a mean score of 82.6, a standard deviation of 10.8, and implies that post breach most SME's maintain a strong financial resilience, with there not being a large range (indicating most SME's are resilient).SMEs experienced some variability in terms of the number of cybersecurity incidents reported, with average of 3.2, minimum of 1 and maximum of 7 events in the past year. Breachsm all took a significant quantity of time, averaging 12.5 hours, but with a range of data points (standard deviation of 8.4) reflecting how quickly SMEs were able to recover from breaches. Finally we find that the median financial loss due to breaches was Rs. 25,00,000 with a large standard deviation of Rs. 15,00,000 indicating a large variation in the financial impact of breaches on different SMEs. To no surprise, the results presented here point out the significance of cybersecurity preparedness and its relationship with the financial outcomes, suggesting that with adequate cybersecurity measures in place, SMEs will be better prepared to face cyber threat.

Correlation Analysis

Variables	**Cybersecurity Preparedness Score**	**Financial Resilience Index**
Cybersecurity Preparedness Score	1	**0.634**
Financial Resilience Index	**0.634**	1
Sig. (2-tailed)	**0.000**	**0.000**
N	225	225

The correlation analysis results show moderately positive relationship between Cybersecurity Preparedness and Financial Resilience in SMEs with Pearson correlation coefficient equal to 0.634. It means the degree of SMEs' financial resilience was correlated to their degree of cybersecurity preparedness. A p value of 0.000, far less than the typical significance threshold of 0.05, shows that correlation is statistically significant. Since the association of these two variables is not by coincidence, there is abundant evidence that better preparedness for cybersecurity leads to more financial resilience against cybersecurity breach. Due to the use of data from 225 SMEs, the sample size for the findings was robust.

DISCUSSION

The data from the correlation analysis indicate that there is a clear and significant positive connection between small and medium sized enterprises (SMEs) cybersecurity preparedness and risk financial resilience. A moderate to strong positive relationship is shown, since a correlation coefficient of 0.634 suggests that as SMEs enhance their cybersecurity measures, they are better able to mitigate the financial implications of cybersecurity breaches.An investigation of previous research undertaken suggests that the findings of this research are also consistent with prior research that highlights the importance of cybersecurity in protecting business operations, particularly for SMEs who are often more vulnerable to cyber threats because of limited resources (Fielder et al., 2016). This is supported by the significant correlation indicating that SMEs investing in strong cybersecurity strategies (e.g. regular security audits, employee training, etc. and advanced threat detection systems) are in a better position to manage financial impacts of cyberattacks.Besides, a p value of 0.000 means the relationship is statistically significant, and its rejection of the null hypothesis stronger than the evidence in support of it as it stated there is no significant relationship between cybersecurity preparedness and financial resilience. By implication, enhancing the organization's cybersecurity preparedness can represent one of the key ways to limit or reduce the negative financial effects from cyberattacks including lost operating time, lost money and damaged reputation.With business operations progressively digitalized, this study supports that cybersecurity should be integrated into SME strategic management. The emphasis is on proactive cybersecurity measures as a business continuity and financial stability essential, not merely for information systems protection.But the findings, while promising, bear in mind that correlation does not imply causation. However, the analysis reveals that there is a strong relationship, though not a direct cause and effect between cybersecurity preparedness and financial resilience. This relationship may yet be explored further in experiments or longitudinal studies in future research to provide a clearer causal framework.Beyond that, SMEs may have their barriers of limited technical expertise, lack of resources such as budget, and limited awareness of the financial impact that might result from a cybersecurity breach (Osborn, 2015). As a result, policymakers, and industry leaders need to support the need for more accessible and affordable cybersecurity solutions focused on satisfying SMEs' requirements. With this, the smallest of businesses would be able to better extend their cybersecurity posture and boost their financial resilience against rising cyber threats.In sum, the study adds to the ongoing body of literature linking cybersecurity preparedness to broader organizational outcomes, namely financial resilience of SMEs. The results further reinforce the point that SMEs ought to treat cybersecurity as a cornerstone of their business strategy, to guard not only their information assets but also to safeguard their financial health.

CONCLUSION

The study establishes a clear and significant relationship between cybersecurity preparedness and financial resilience in small and medium-sized enterprises (SMEs). The positive correlation found between these two variables suggests that SMEs with higher levels of cybersecurity preparedness are better equipped to handle the financial repercussions of cybersecurity breaches. This finding emphasizes the importance of adopting proactive cybersecurity measures, such as regular security audits, advanced threat detection systems, and employee training, to safeguard both operational and financial continuity.The study's results contribute valuable insights into the growing body of research on the economic impact of cyber threats, particularly for SMEs, which often lack the resources and expertise to address such challenges effectively. Given that SMEs are increasingly targeted by cyberattacks, the findings highlight the critical need for these businesses to integrate cybersecurity into their overall strategic planning. Enhancing cybersecurity preparedness not only reduces the risk of financial loss but also helps businesses recover more quickly and maintain their competitiveness in the face of cyber disruptions.

Furthermore, the study underscores the role of cybersecurity as a key component of business resilience. By identifying a statistically significant relationship between preparedness and resilience, the research provides a foundation for future studies to explore causal mechanisms and further refine strategies for mitigating the economic impacts of cyber threats on SMEs. In conclusion, this study reinforces the need for SMEs to prioritize cybersecurity, not only as a defensive measure but as a vital element of financial stability and long-term success. Policymakers, business leaders, and industry stakeholders should focus on providing affordable, accessible cybersecurity solutions to SMEs to help them strengthen their preparedness and, ultimately, their financial resilience in an increasingly digital business environment.

REFERENCES

[1] Arranz, N., & Fernandez de Arroyabe, J. C. (2010). Efficiency in technological networks: An approach from artificial neural networks (ANN). International Journal of Management Science and Engineering Management, 5(6), 453–460. https://doi.org/10.1080/17509653.2010.10671137

[2] Arranz, N., Arguello, N. L., & Fernandez de Arroyabe, J. C. (2021). How do internal, market, and institutional factors affect the development of eco-innovation in firms? Journal of Cleaner Production, 297, 126692. https://doi.org/10.1016/j.jclepro.2021.126692

[3] Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges, and solutions. Computers & Security, 68, 81–97. https://doi.org/10.1016/j.cose.2017.04.005

[4] Bishop, C. M. (1995). Neural networks for pattern recognition. Oxford University Press.

[5] Bland, J. A., Petty, M. D., Whitaker, T. S., Maxwell, K. P., & Cantrell, W. A. (2020). Machine learning cyberattack and defense strategies. Computers & Security, 92, 101738. https://doi.org/10.1016/j.cose.2020.101738

[6] Bourilkov, D. (2019). Machine and deep learning applications in particle physics. International Journal of Modern Physics A, 34(35), 1930019. https://doi.org/10.1142/S0217751X19300199

[7] Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. Information & Management, 52(4), 385–400. https://doi.org/10.1016/j.im.2014.12.004

[8] Cenfetelli, R., & Bassellier, G. (2009). Interpretation of formative measurement in information systems research. MIS Quarterly, 33(4), 689–708. https://doi.org/10.2307/20650323

[9] Chan, M., Woon, I. Y., & Kankanhalli, A. (2005). Perceptions of information security at the workplace: Linking information security climate to compliant behavior. Journal of Information Privacy and Security, 1(3), 18–41. https://doi.org/10.1080/15536548.2005.10855772

[10] Chaudhry, P. E., Chaudhry, S. S., Stumpf, S. A., & Sudler, H. (2011). Piracy in cyberspace: Consumer complicity, pirates, and enterprise enforcement. Enterprise Information Systems, 5(2), 255–271. https://doi.org/10.1080/17517575.2010.524942

[11] Choo, K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719–731. https://doi.org/10.1016/j.cose.2011.08.004

[12] Chronopoulos, M., Panaousis, E., & Grossklags, J. (2018). An options approach to cybersecurity investment. IEEE Access, 6, 12175–12186. https://doi.org/10.1109/ACCESS.2017.2773366

[13] Ciurana, J., Quintana, G., & Garcia-Romeu, M. L. (2008). Estimating the cost of vertical high-speed machining centers: A comparison between multiple regression analysis and the neural approach. International Journal of Production Economics, 115(1), 171–178. https://doi.org/10.1016/j.ijpe.2008.05.009

[14] CLUSIF. (2008). Risk management: Concepts and methods. Paris: Club de la Sécurité Informatique.

[15] Cohen, F. (1997). Information system attacks: A preliminary classification scheme. Computers & Security, 16(1), 29–46. https://doi.org/10.1016/S0167-4048(97)85785-9

[16] Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities, and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31–43. https://doi.org/10.19101/IJACR.2016.623006

[17] Couce-Vieira, A., Insua, D. R., & Kosgodagan, A. (2020). Assessing and forecasting cybersecurity impacts. Decision Analysis, 17(4), 356–374. https://doi.org/10.1287/deca.2020.0418

[18] Cyber Security Breaches Survey. (2016). Official statistics. Cyber Security Breaches Survey 2017. Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017

[19] Cyber Security Breaches Survey. (2017). Official statistics. Cyber Security Breaches Survey 2017. Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018