Multidisciplinary Reviews

CONFERENCE PAPER
Published Online: May 12, 2024
https://doi.org/10.31893/multirev.2023ss080

Innovations in Strategic Management: Navigating Complexity and Driving Organizational Success

Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review

Lubna Ambreen[a] ✉ | **Manjula Jain**[b] | **Rakesh Kumar Yadav**[c] | **Shweta Loonkar**[d]

[a]Department of Entrepreneurship and New Venture Creation, JAIN (Deemed-to-be Univesity), Bangalore, Karnataka, India.
[b]Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India.
[c]Maharishi University of Information Technology, Uttar Pradesh, India.
[d]Department of ISME, ATLAS SkillTech University, Mumbai, Maharashtra, India.

Abstract Small-to-medium-sized enterprises (SMEs) make up a significant portion of the economies of many nations. However, research shows that many companies fall short when establishing cyber security, making them vulnerable to assaults. In addition, while accounting for a sizable share of firms, studies on cyber security focus on SMEs. This study reviews the latest evaluation on the cyber security of SMEs, emphasizing how well this experiment aligns with the well-known National Institute of Standards and Technology (NIST) and Cyber Security Framework (CSF). The report begins by underlining the crucial necessity of cybersecurity in the digital era and the particular issues that SMEs confront. It emphasizes the financial and reputational dangers associated with cyber events, emphasizing the importance of solid cybersecurity procedures. The review investigates several cybersecurity risk management approaches, strategies and frameworks, providing insights into their relevance and efficacy in the context of SMEs. We discovered that study in SME cyber security is sophisticated and specialized attention on the NIST and CSF recognize as well as defend tasks, with minimal effort spent on the other current activities. SMEs should be equipped to detect, react to, and recover from cybercrime. SMEs might not have appropriate information on responding to such occurrences if research in these areas is pathetic. In future studies in SMEs, there needs to be an excellent equilibrium in cyber security. Scholars ought to use firm, proven mathematical methods to improve and test their work, yet governments and academia are urged to invest in providing researchers with incentives to broaden their research horizons.

Keywords: Cybersecurity, Risk Management, Small and Medium-Sized Enterprises

1. Introduction

The implementation of agile methodologies in educational organizations is a topic that is getting more and more attention today. Colleges and universities have a responsibility to develop strategies geared at adaptable instruction due to the changing requirements in employment. Due to the global emphasis on lifelong learning, the problem is pressing. Agility is essential for staying abreast of the evolving needs of the industry (Yusuf et al 2020). Educational institutions' current interest in using agile approaches to create novel teaching tools is a sensible response to such issues. The primary goal must consider the developments established by the global society while developing a framework for creating information and measuring the quality of education (Agarwal et al 2023). However, the education process itself is not what the labor market is most interested in; instead, what emerges through the process takes the shape of educated graduates with abilities that are appropriate for present employment or capable of fast adapting to specifics. Industries are encouraged to take advantage of initiatives designed to ensure education quality, regardless of their insignificant impact on the manner of actual educational advances (Moi et al 2021). The building block for achieving the overall objectives of sustainability is considered to be education, which must cover the environmental, social and economic facets of sustainable growth. To long-standing conflicts and problems for recognizing non-sustainable modes in economic manufacturing and consumer behavior lead to ecological decomposition and worldwide warming, including an increase in natural events (Omer and Noguchi 2020). ESD and social educational methodologies are connected. Social learning methods enable learners to collaborate on projects related to real-world problems while developing Cyber threats target SMEs, regardless of their size, number of workers, or yearly turnover. Cyber attackers are more concerned with attractive rewards than the size of the corporate sector, making SMEs the main target of

cyber threats (Tabisa Ncubukezi et al 2020). Several financial and nonfinancial losses have occurred due to developing challenges, including information security and cyber hazards. In this line, it is believed that SMEs confront comparable levels of cyber security problems to those their larger competitors face. Their lack of resources and competencies makes them vulnerable to cyber risk. In other words, managing cyber risk that is ready for it becomes an essential skill for the survival and growth of small enterprises (Sukumar et al 2023). SMEs have become the new primary target for cyber crimes.

They are among the least resilient and least advanced countries regarding cyber security risk. SME businesses conduct thorough cyber-risk assessments and can encounter several internal challenges (Opitz 2018). Small Information Technology (IT) teams, insufficient security budgets and differences between IT and business leadership teams over cyber security risk management are factors worth considering when developing cyber-risk strategies (Boletsis et al 2021). In a globalized and digitized world, medium-sized IT enterprises face new challenges to remain competitive. The IT industry is critical for various sectors and it is a crucial driver for many others. SMEs in the IT industry focus on niche industries, which can disadvantage them in global competition (Lloyd 2020). Their products contain proprietary data formats and security gaps, which can slow digital transformation. This is true for German and European Union national market situations for IT SMEs. In contrast, the IT-based SMEs in the US focus on rapid standardization and platform thinking (Johannsen et al 2020). The most effective solution to address SMEs' data processing and decision-making demands is Collaborative Business Intelligence (CBI) or Business Intelligence (BI) in the cloud. The term "cloud-based BI" (CBI) refers to the data used by BI systems and the components of BI systems that are supplied as services. BI technology supports organizational decision-making in CBI, which refers to integrating two primary cloud computing architectures. Like traditional BIs, CBIs can offer management quality information based on analyzing significant internal and external data required in decision-making (Moyo et al 2019). Risk management is necessary for small and medium-sized enterprises (SMEs). The diagnostic level is essential because, through recognizing dangers, preventive measures can be developed. Lack of enterprise risk management can have adverse effects, including difficulty paying debts, a lack of job orders, poor financial indicators, tense interactions between management and staff. Insolvency and frequent foreclosure are possible outcomes of these harmful effects. An analysis of business risks and their relationship to future business orientation is done in light of SMEs' significant contribution to the European Union's economy as a whole (Dorsey et al 2021).

2. Related Work

The NISTs CSF has been utilized in Benz and Chatterjee's (2020) methodology for SMEs to gauge their cyber security risk and resilience. The process included a 35-question online survey. Using the five NIST framework categories to recognize, safeguard, observe, answer and come back, information technology directors ought to assess their maturity in each (Dvorsky et al 2021). It discusses whether to manage cyber security risks, how it works and what it means for practitioners. Alahmari and Duncan (2020) explore the role of cyber security risk management in SMEs, focusing on recent evidence. The authors aim to understand the current situation, reveal the management's role in addressing cyber security risks and recommend lines of inquiry. The review employs a tried-and-true methodology, beginning with a keyword search and fitness evaluation. Sukumar et al (2023) used a “Multi-Criteria Decision Analysis (MCDA)” approach to evaluate the security hazards in SMEs. Twenty-eight cyber-related threats are included in the report under the following five headings, protection, dependence on others, staff members, strategy and legal (Berry and Berry (2018). To create a risk assessor process, a comprehensive approach, the “Best-Worst Method” (BWM) and “Step-Wise Weight Assessment Ratio Analysis” (SWARA), were combined. It contributed to the body of literature on cyber risk control by outlining a fresh approach for managing cyber security risk for e-tailing SMEs.

Dey et al (2020) explore the link between Corporate Social Responsibility (CSR), the innovation that is Sustainability-Oriented Innovation (SOI), Lean Management Practices (LMP) and the economy's performance. The method of structural equation modeling was used to compare predictions with the data. While LMP facilitated sustainability and economic growth, SOI relays LMP to accomplish sustainable development performance. Even though CSR practices contribute to LMP to attain success for ecological sustainability, they mediate SOI. It attempts to close holes in knowledge to improve the SME sector's economic performance from a sustainability perspective. Sahoo and Yadav (2018) examined the consequences of lean management methods on the productiveness of operations among Indian small and medium-sized manufacturing enterprises. It reveals that process improvement and waste minimization affect operational efficiency (OP), with "5S-workplace organization" that is the most commonly used lean tool. The findings suggest that poor implementation can improve productivity in Indian SMEs. It is fundamental to comprehend how various lean tools and performance standards relate. Van Haastrecht et al (2021) claimed that SMEs are less equipped to handle threats because they possess cyber protection resources. Motivation to improve cyber security is low, as there is no necessary knowledge and awareness. A threat-based approach to determine security hazards should be provided to help SMEs handle cybersecurity risks. The strategy inspires users to act by elevating their perceptions of autonomy, competence and relatedness. The method's ability to convert SME data into prioritized, enforceable suggestions that satisfy the expectations stipulated by Self-Determination Theory (SDT) has been demonstrated through an actual-world application. Lyu et al (2019), before identifying technological discrepancies between demand and the real-world state of concerns regarding security and safety in CPS, this study reviews existing methodologies for evaluating and handling risks from the angles of safety, security and their combination. It summarizes the benefits and

drawbacks of each method. Due to their frequent interaction with tangible goods and computer networks, CPSs are safety and security-critical as CPS complex and system openness increase. Vitunskaite et al. (2019) assessed cyber security measures for smart cities, emphasizing technical standards and legal frameworks. It examined 93 safety measures and compared Barcelona, Singapore and London as instances of comparison. To assure security in cities with intelligent infrastructure at all levels, the study concluded with a recommended arrangement comprising technology needs, official input, an ethical framework and a promise of compliance. Tantawy et al (2020) proposed an integrated model-based approach for measuring Cyber-Physical Systems (CPS) security risk by employing a CPS test bed. The test bed was monitored by an exotherming container boiler that is agitated and used in the petrochemical, nuclear, water treatment, oil and gas industries. Network and data flow models are used to analyze the cyber security system and develop attack scenarios (Eling et al 2021) . The capacity of the hybrid automaton to transmit security risk assessment, the impact of hazardous time to development on security system design as well as the complex interaction between computer and physical systems for CPS were a few of the fundamental advances. Etemadi et al (2021) reviews analyzed block chain's significance in handling supply chain risk in cyberspace employing Systematic Literature Network Analysis (SLNA). It focused on potential concerns with intelligent contract security, monitoring for counterfeit goods and systems with databases for safeguarding food and transparency. This advances our knowledge of leveraging blockchain for supply chain resilience and CSRM.

In this section of writing, the enterprises are stressed as it covers the cybersecurity risk control in SME and Large enterprises (Section 2), Methods used in the Survey (Section 3), Discussion and Recommendations (Section 4) and Conclusion (section 5).

3. SME vs. Large Enterprises

SMEs are vulnerable to the same hazards as large organizations since cyber threats do not differentiate between different sizes of enterprises. Most of the time, more prominent entities have the personnel and financial resources to implement controls. However, they have an excellent attack surface due to increased employee and device counts. Larger organizations employ devoted cyber security personnel with the necessary levels of education. SMEs make smaller investments in internet safeguarding, but when it comes to the costs associated with effective cyber-attacks, they bear a higher proportional burden than big enterprises. However, SMEs could profit from their stature, speed and more flexible IT setups (Heidt et al 2019). Even though cyber risk has become a higher priority for larger organizations over the past few years, industry studies revealed that many firms cannot explain the method, although having the necessary staffing and funds to take action on cyber risk. Cybersecurity concerns for small firms must be regarded as a standard security problem. In Australia, where small enterprises govern a sizable amount of the industry and business, cyber-attacks on companies could harm buyers' confidence in online shopping and the economy (Bada et al 2019).

3.1. Cybersecurity Risk Assessments for SME

Due to their distinctive structural features, such as industry, place of residence and cybersecurity skills, SMEs deal with significant risks related to cybersecurity. The European Digital SME Network divides SMEs into four categories: entrepreneurs, online fitness instructors, SMEs with an excellent digital technology foundation and others. Although cybersecurity risk assessment techniques have been customized to meet the demands of SMEs, these methodologies call for a dedicated user with some level of cybersecurity experience. These techniques work for digital enablers and SMEs with a digital foundation. They will only work for startups and SMEs that rely on digital technology if they need more cybersecurity understanding and drive to make enhancements (Bada & Nurse 2019).

3.2. Evaluation of the Risk of Cybersecurity

From a managerial perspective, SMEs' Cybersecurity Risk Control (CRC) needs more attention. To present five different CRC vantage points. They are challenges, conduct, procedure, perception and decision-making.

According to this study, SMEs must pay more attention to cybersecurity in the decision-making process than other sectors because of the significance of its role in Cybersecurity Risk Control Investment (CRCI). Most experts agree that cyber-attacks pose the most significant risk to businesses, but decision-makers in SMEs continue to think their organizations are not at risk. The most recent cyber-attacks can cost billions of dollars to purchase, but many go unnoticed. Therefore, SMEs must prioritize understanding the possible effects of cybersecurity threats. Information Risk Management (IRM) decisions are the owners' and managers' responsibility, underscoring how vital their function is in minimizing the gravity of the effects of digital assault.

Decision-makers, executive managers, decide on the enterprise's information security strategies. For instance, chief executive officers of SMEs are involved in decisions on implementing cybersecurity (Pugnetti & Casián, 2021). SMEs make cybersecurity decisions that could have ripple effects on the entire industry. Decision-makers in the SME sector can make better choices as their awareness of cybersecurity grows. For instance, raising decision-makers' awareness might motivate them to invest more in cybersecurity.

Even with a bounty of previous investigations on CRC, qualitative studies have focused on CRCI making decisions in SMEs. The few published journals make a mathematical approach to the best option for such an exploratory case. Therefore, the absence of such a descriptive analysis that looked at curiosity hurdles to CRCI in SMEs can be viewed as a vacuum that the current study will aim to fill. In addition to gathering participant feedback and ideas for potential future study directions, the article will provide an overview of CRCI in SMEs (Yigit Ozkan et al 2021).

4. Methods used in the Survey

We keep talking about recent cyber-attacks on SMEs. Best practices for managing cyber security risk are outlined in cyber security frameworks. These frameworks standardize service delivery, create a single language internally as well as externally and increase efficiency. Various methodologies are used in the cybersecurity risk handling practices for SMEs survey.

4.1. Current cyber attacks

Because SMEs are thought to be inherently more vulnerable, (Eling et al 2021) discovered that they are becoming more and more targeted by cyber-attacks. Cybercriminals with less education and previous criminal activity target SMEs because they are simple targets. SMEs are responsible for this careless security since they planned computerization protection under the assumption that data and networks had been protected (Chidukwani et al 2022). Based on a 2020 Verizon analysis, the attacks are pervasive and affect every firm, regardless of size, industry, or sector. However, businesses involved in finance and health care are the most targeted internationally. The most common types of cyberattacks that SMEs encountered were supply chain attacks for e-commerce, web-based attacks, social engineering (such as phishing), computer hacking (such as credentials that are extracted, data theft), malware (such as ransomware) and misuse (such as malicious insiders). The hacking and attempts at social engineering were the most typical kinds of attacks experienced by SME respondents (see Figure 1 and Table 1 below).

Online application infrastructure is one of the IT components compromised in hacking attacks globally and across all organizations. This is because more services consume cloud-based software-as-a-service platforms, leading to a shift towards web-based applications. Users' desktop and laptop computers, email servers, database servers and even themselves are attack targets. According to several analysts, IoT and mobile devices are the most prone to invade the SME environment and provide access to the network to attackers. Unsecured online electronics can be converted into firearms to launch sophisticated attacks on additional companies. In particular, devices can be forced into Botnets, where they must wait for Instruction to join distributed denial of service (DDoS) activities that are undertaken online. 70% of recent worldwide hacks were the work of outside actors or attackers who were not firm employees. Intrusion or obtaining unauthorized access was involved in over half of all incidents. The vast majority (86%) of these hacks had financial motivations. However, there are a number of additional reasons why cyber events and data breaches occur, such as amusement, ideology, resentment, espionage, state-sponsored activity and human mistakes. Insider attacks are occurring in 16% of SMEs. For instance, the district of the regional colleges in Maricopa County experienced a data breach in 2011 when some of the students' information databases were made available for purchase on the phantom web. Investigations established that an employee was responsible for the problem but did not establish whether the data leak was deliberate or unintentional. A total of 11% of data breaches reported to the Australian authorities were the result of hostile insiders or rogue personnel "Office of the Australian Information Commissioner" (OAIC).

4.2. Cyber Security Challenges

Due to financial limitations, concerns with regulatory compliance and a lack of talent, SMEs need help implementing cyber security. Their cybersecurity posture can be impacted by a lack of training, a shortage of IT staff and misconceptions about mitigating cyber-attacks. Because they restrict their online websites, contact details and social media presence, SMEs underestimate the risk of cybercrime. Cyber threats, however, include email communication, internet-connected devices, sensors and the Internet of Things (IoT) to these platforms. Digital supply networks introduce new cyber dangers, yet many firms must be aware of the threat they offer to their supply chain. The biggest problems for SMEs are a lack of resources, inadequate staff and cybersecurity knowledge. Due to their low wealth, they need more devoted IT workers and cybersecurity expertise, which makes it challenging for them to adhere to rules and implement cutting-edge technology like machine learning. SMEs should embrace security models incorporating numerous security features, like the Centria cyber security manager idea and affordable, simple-to-implement solutions to handle this. SMEs need help in risk management due to technology's development and a lack of knowledge of security solutions (Lloyd 2020). Despite growing business risk awareness of cybercrime, many Australian SMEs need more information on where to turn for assistance when cybercrime incidents occur, according to a 2017 Australian survey. SMEs can get confused and apprehensive because of the quantity of internet material on cyber security, which financial industry groups have complained about due to conflicting standards. Effective cybersecurity can be hampered by negative associations with data breaches, fines from the government and company interruptions. Studies must demonstrate consistent use of security measure and difficulties in responding to new threats.

4.3. Cyber Security Framework

The core of the literature is NIST's CSF; it was created to enhance the protection of crucial infrastructure companies in the USA. It is an offered structure created by combining regulations, legislation and rules that are already in place with government and business sector suggestions. The framework offers businesses a policy framework for monitoring and improving their capacity to stop, recognize and react to cyber-attacks. The framework has proven to be extendable and helpful for multiple businesses, despite being first intended for critical infrastructure enterprises. By implementing the plan of action, businesses can better manage technology-related risks and maximize the return on their security spend. NIST offers established language that simplifies ignorance about the language of treaties and other policies (Opitz, 2018). Figure 2 represents the SME internet security in NIST and CSF functions the security research in NIST and CSF functions and its categories are:

1. Identifying: Property awareness, risk evaluation, administration and compliance with the law, obligations, risk administration, risk management in the logistics network, working alongside exterior partners and hiring.
2. Protect: Client control of access and identification security, education and formation, data security includes methods and procedures for information protection, encryption, repair, patch, change management and protective technology.
3. Detect: Security ongoing surveillance, anomalies, the detection procedure for security incidents and events (SIEM).
4. Respond: Prepare an answer. Management of data, impact analysis and forensics, disaster planning, catastrophe control, experiences acquired and ongoing improvement.
5. Recover: Improvements, communications, business continuity management (BCP), disaster recovery (DRP).

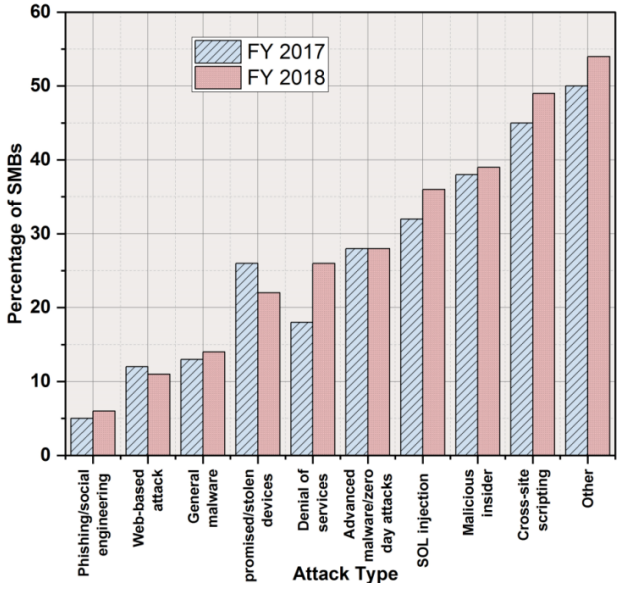

Figure 1 Varieties of attacks that SMEs have suffered. The most widespread attack is social engineering, which has been rising for the past few years.

Table 1 Different assault that SMEs had been faced to. The practice of social engineering has become the most persistent attack throughout the course of the last few years.

Attack Type	Percentage of SMBs	
	FY 2017	FY 2018
Phishing/social engineering	5	6
Web-based attack	12	11
General malware	13	14
Compromised/stolen devices	26	22
Denial of services	18	26
Advanced malware/zero day attacks	28	28
SOL injection	32	36
Malicious insider	38	39
Cross-site scripting	45	49
Other	50	54

For SMEs, NIST developed a condensed version of the CSF that includes ten recommended practices and addresses systems, networks, personnel, recovery from crises, disaster preparation and security of operations.

4.3.1. Identifying

The determining feature of the NISTs CSF is designed to support firms to be aware of their background, essential resources and related cyber security risks. Early studies concentrated on cyber dangers, vulnerabilities, hazards and practices. Some researchers targeted manufacturing industries because they faced particular difficulties due to the adoption of digitization and IoT (Kaila 2018). SMEs are a desirable target for cyber security research because of their compact, adaptable and flexible IT infrastructure. While some studies investigated risk management procedures, others investigated breach prevention techniques. Armenia et al (2021) looked at the information security rules and practices needed by SMEs as part of their focus on governance. Cybersecurity hazards, behavior, immigration, information and decisions are the five viewpoints that SME management must consider when making cybersecurity-related decisions.

4.3.2. Protect

The Protect function in SME tries to reduce the effects of future cyber security incidents. It includes privacy, authorization of entry, servicing and safeguarding devices are some of the information preservation processes and procedures. Studies have shown that IT personnel need better cyber security awareness due to a lack of education and competing objectives, SME cyber security research emphasizes these issues. By establishing policies and procedures, SMEs can align their facilities and assets for data compliance with safety criteria. However, a lack of human and financial resources can hinder the creation, enforcement and adherence to accurate privacy and security laws. Berry & Berry (2018) have examined SME protective cyber security technologies, including machine learning, that are successful at fending off cyber-attacks. SMEs should invest in training and awareness campaigns, align their information systems and resources with security requirements and put defensive cyber security technologies like machine learning into place to solve problems in adopting cyber security.

4.3.3. Detect

In order to identify and implement the proper operations to detect cyber security occurrences, businesses must use the detect function. Anomalies and events, security, continuous monitoring and detection processes are a few of the categories included. Continuous monitoring is essential for effective security management in SMEs and it can be done with the help of a Security Information Environment (SIEM). Researchers Mercl and Horalek (2020) investigated two SMEs deploying IBM Security QRadar SIEM and detected that the procedure's difficulty needed assistance from experienced specialists for duty. SMEs in the UK have a poor adoption rate for Machine Learning Cyber Security (MLCS), according to the research by Rawindaran et al. Kaila and Nyman emphasized the significance of monitoring for SMEs to find breaches and respond intelligently. After adopting, controlling, minimizing risks, regulating assets, monitoring vulnerabilities and ensuring business continuity, information security tactics should be utilized in conjunction with detection systems and ongoing monitoring.

4.3.4. Respond

The response function in cyber security is crucial for SMEs to develop and implement appropriate actions to respond to incidents. It includes response planning, communications, analysis, mitigation and improvements. However, many SMEs lack a disaster response strategy or have not implemented it. Cyber resilience is a holistic approach that helps SMEs anticipate, detect, withstand, recover and evolve after cyber incidents. Mitigation is essential in a compromised system, providing business benefits and compliance. Cybersecurity practices can reduce the financial damage caused by cyber-attacks. Rawindaran et al (2021) recommend improving SMEs after hearing about the role of AI and ML in privacy and security.

4.3.5. Recover

Following a cyber-security event, SMEs can follow the NIST CSF's recovery planning, improvements and communication standards to resume regular operations. However, there is little study on cyber resilience and little literature on this function (Tam et al 2021). SMEs depend on outside providers for infrastructure and security precautions but might need to be more responsible for recovery planning. Despite these attempts, these approaches yet to have real-world applications. Figure 2 and Table 2 show that most past and current studies have focused on the NIST CSF's identify and protect functions.

4.4. Data Collection Methods

According to the study's analysis of the data-gathering techniques employed by Feng et al (2021), research reviews (43%), quizzes (25%) and discussions (17%) were the most popular. A combination of approaches was used for 7% of the research, with surveys and experiments receiving the least attention.

Interviews utilize talking on the phone with the participant and the person conducting the research. A systematic

process for studying or evaluating printed and electronic written materials, as well as earlier research conducted by others, is known as an analysis of literature. They are evaluating the gathered facts without formulating inquiries. A questionnaire is a written list of inquiries used to learn details about specific people rather than spot trends. The subsequent examination of statistical evaluation is a list of demands distributed to broad specimens. Gathering, averaging and analyzing the responses to specific questions is a part of surveys. In an experiment, variables are changed and the results of those changes are recorded. They were combining the collected data using various data-gathering techniques. Figure 3 and Table 3 show the findings that indicate the primary strategy that SME cyber security researchers used for data collection is a literature review of the various data collection techniques.

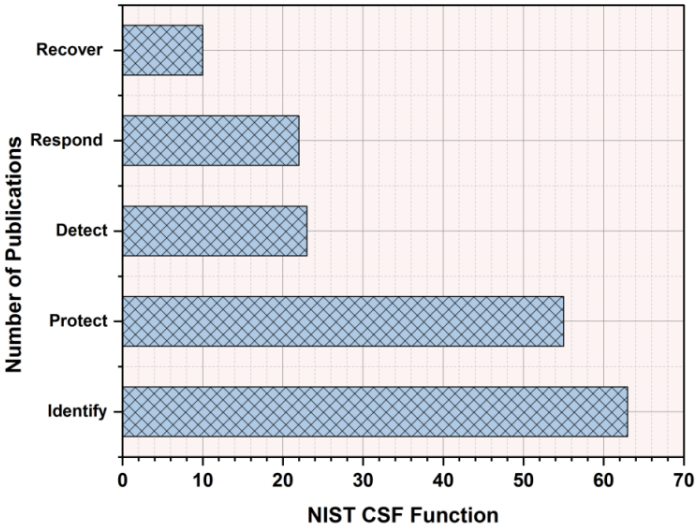

Figure 2 The primary area of study for SME internet security in NIST CSF functions.

Table 2 Lists the key NIST CSF functions for SME internet security research.

Number of Publications	NIST CSF Function
Identify	63
Protect	55
Detect	23
Respond	22
Recover	10

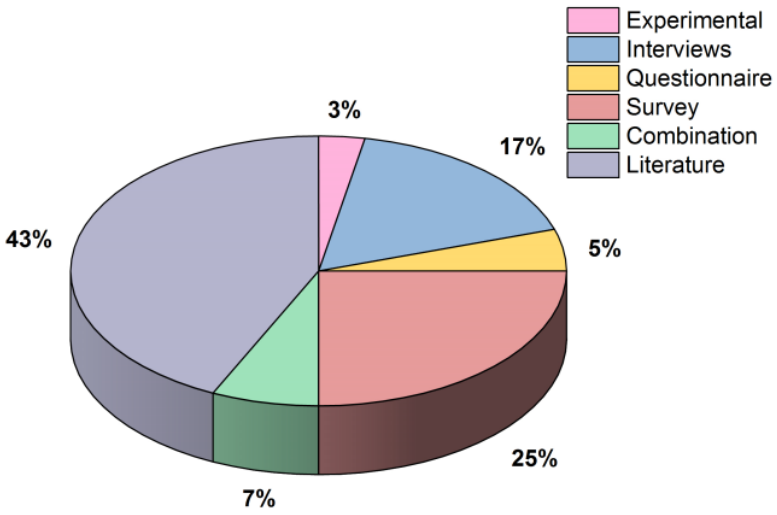

Figure 3 Data collection techniques. Reveals indicate that the primary strategy SME cyber security researchers use for data collecting is literature reviews.

Table 3 Data collecting is literature reviews.

Data Collection Method	Percentage
Experimental	3
Interviews	17
Questionnaire	5
Survey	25
Combination	7
Literature	43

4.5. Research Methods

70% of SME cyber security researchers utilize qualitative, 25% use quantitative and 5% use combined techniques. This is in line with earlier studies that examined risk assessment. Authors support using evidence-based research methodologies in cyber security, highlighting the need for cyber professionals to compute metrics for objective and accurate results. In 2019, 30% of firms, up from 17% in the previous two years, reported utilizing quantitative methodologies to express cyber risk exposures (Suryotrisongko and Musashi 2019). Few SME researchers employ combined methodologies, like McLauren's quantitative strategy, to examine 'how machine learning cyber security is applied in SMEs'. Figure 4 and Table 4 show the qualitative research techniques.

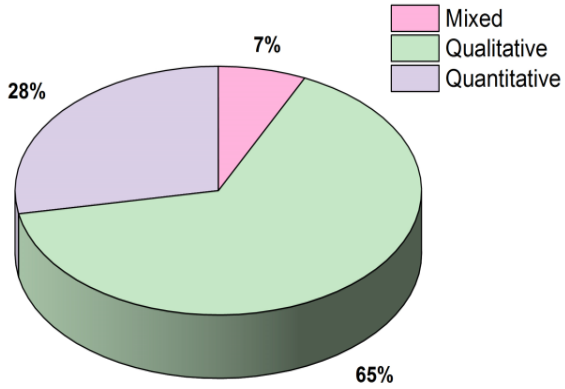

Figure 4 SME cyber security employs a qualitative research technique.

Table 4 SME cyber security makes use of an approach based on qualitative research.

Research method	Percentage
Mixed	7
Qualitative	65
Quantitative	28

5. Discussion

Most SME cyber security research uses qualitative techniques rather than original research such as case studies, polls and experiments. The need for empirical research challenges academics working in regional environments like Australia. Ransomware and other sophisticated tactics are used in cyber attacks, which have the power to disrupt corporations, supply systems and even entire countries. While some academics advise a balanced approach to preventive and reaction paradigms, others emphasize technology defenses and prevention without ignoring other actions that enhance cyber resilience. Cyber attacks are getting more sophisticated and pose severe risks to industries, supply chains and businesses. Researchers advise firms to take a harmonious strategy for security precaution and interaction. However, many concentrate on tech defenses and prevention while ignoring other actions that help to improve cyber resilience. It should be possible for SMEs to avoid, regulate and recover from cyber-attacks. It is suggested that companies employ an adequate information security system, rules for using desktops, instruction for safeguarding data, corporate antivirus and protection against malware. SMEs ought to prioritize adheres that will lessen the impacts of attacks via the internet, like spending money on a group of inspectors and a written recovery plan. SMEs and technology providers, notably those of cloud-based "Software-as-a-Service (SaaS)", have security requirements.

6. Conclusions

Research on cyber security for SMEs uses qualitative techniques rather than original research, such as stories, polls and exercises. The lack of empirical research presents difficulties for educational institutions in remote environments like Australia. Ransomware and other complex strategies are used in cyber-attacks, which have the power to disrupt big businesses, supplies and even nations at large. While some academics suggest employing a mixture of approaches to proactive and reaction paradigms, others emphasize technology defense and control without ignoring other measures that assist in building cyber security. SMEs should protect themselves from cyber attacks and resume regular business after an event. There is agreement on what excellent cyber security looks like and a complete information security system is a dependable and economical place to start. Other experts advise SMEs to concentrate on procedures that will lessen the impact of computer hacking, such as creating a clear restoration strategy and an inspection team. Security obligations are crucial for vendors and SME clients, such as cloud-based SaaS.

Ethical Considerations

Not Applicable.

Conflict of Interest

The authors declare no conflict of interest.

Funding

This research did not receive any financial support.

References

Alahmari A, Duncan B (2020). Cyber security risk management in small and medium-sized enterprises: A systematic review of recent evidence. In 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA) pp. 1–5). IEEE. DOI: 10.1109/CyberSA49311.2020.9139638

Bada M, Nurse JR (2019). Developing cybersecurity education and awareness programs for small and medium-sized enterprises (SMEs). Information & Computer Security. 27(3):393–410.DOI: 10.1108/ICS-07-2018-0080.

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cyber security evaluation tool for SMEs. Business Horizons. DOI: 10.1016/j.bushor.2020.03.010

Boletsis C, Halvorsrud R, Pickering JB, Phillips SC, and Surridge M (2021). Cyber security for SMEs: Introducing the Human Element into Socio-technical Cyber Security Risk Assessment. InVISIGRAPP (3: IVAPP) (pp. 266-274).

C. T. Berry & R. L. Berry (2018). ''An initial assessment of small business risk management approaches for cyber security threats,'' (in English) Int. J. Bus. Continuity Risk Manag., vol. 8, no. 1, pp. 1–10, DOI: 10.1504/IJBCRM.2018.090580.

Chidukwani A, Zander S, Koutsakis P (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. IEEE Access. 10:85701-19. DOI: 10.1109/ACCESS.2022.3197899

Dey PK, Malesios C, De D, Chowdhury S, Abdelaziz FB (2020). The impact of lean management practices and sustainably-oriented innovation on the sustainability performance of small and medium-sized enterprises: empirical evidence from the UK. British Journal of Management. (1):141–61. DOI: 10.1111/1467-8551.12388

Dvorsky J, Belas J, Gavurova B, Brabenec T (2021) Business risk management in the context of small and medium-sized enterprises. Economic Research-Ekonomska Istraživanja. 34(1):1690-708.

Eling M, McShane M, Nguyen T (2021) Cyber risk management: History and future research directions. Risk Management and Insurance Review. 24(1):93-125. DOI: 10.1109/CyberSA49311.2020.9139638

Etemadi N, Borbon-Galvez Y, Strozzi F, Etemadi T (2021) Supply chain disruption risk management with blockchain: A dynamic literature review. Information; 12(2):70. DOI: 10.3390/info12020070

Feng Y, Duives D, Daamen W, Hoogendoorn S (2021) Data collection methods for studying pedestrian behaviour: A systematic review. Building and Environment; 187:107329. DOI: 10.1016/j.buildenv.2020.107329

G. Lloyd (2020) ‘‘The business benefits of cyber security for SMEs,’’ (in English) Compute. Fraud Secure, vol. 2020, no. 2, pp. 14–17, DOI: 10.1016/S1361-3723(20)30019-1.

Suryotrisongko H, Musashi Y (2019) ‘‘Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective,’’ in Proc. IEEE 12th Conf. Service-Oriented Comput. Appl. (SOCA), Kaohsiung, Taiwan, pp. 162–167, DOI: 10.1109/SOCA.2019. 00031.

Heidt M, Gerlach JP, Buxmann P (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments. Information Systems Frontiers. 21:1285-305. DOI: 10.1007/s10796-019-09959- 1

Johannsen A, Kant D, Creutzburg R (2020) Measuring IT security, compliance and data governance within small and medium-sized IT enterprises. Electronic Imaging. 2020(3):252-1.

Lyu X, Ding Y, Yang SH (2019) Safety and security risk assessment in cyber-physical systems. IET Cyber-Physical Systems: Theory & Applications. 4(3):221-32. DOI: 10.1049/it-cps.2018.5068

Mercl L, Horalek J (2020) SIEM implementation for small and mid-sized business environments. J. Eng. Appl. Sci. 14(9):10497-501. DOI: 10.36478/jeasci.2019.10497.10501

Moyo M, Loock M. (2019) An Analysis of Small and Medium-Sized Enterprises' Perceptions of Security Evaluation in Cloud Business Intelligence. In International Conference on Cyber Warfare and Security (pp. 554-XIII).

Opitz EL (2018) Cybersecurity for the board of directors of small and midsized businesses. Board Leadership. 2018(159):4-5. DIO: 10.1002/bl.30115

Pugnetti C, Casián C (2021) Cyber risks and swiss smes: an investigation of employee attitudes and behavioral vulnerabilities. DIO: 10.21256/zhaw-21478

Rawindaran N, Jayal A, Prakash E (2021) Machine learning cybersecurity adoption in small and medium enterprises in developed countries. Computers; 10(11):150. DOI: 10.2290/computers10110150

S. Armenia, M. Angelini, F. Nonino, G. Palombi, and M. F. Schlitzer (2021) ‘‘A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs,’’ (in English) Decis. Support Syst., vol. 147, Art. no. 113580, DOI: 10.1016/j.dss.2021.113580

Sahoo S, Yadav S (2018). Lean implementation in small and medium-sized enterprises: An empirical study of Indian manufacturing firms. Benchmarking: An International Journal; 25(4):1121-47. DOI: 10.1108/BIJ-02-2017-0033

Sukumar A, Mahdiraji HA, Jafari-Sadeghi V (2023) Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. Risk Analysis. DOI: 10.1111/risa.14092

T. Tam, A. Rao, and J. Hall (2021), ‘‘The good, the bad and the missing: A narrative review of cyber-security implications for Australian small businesses,’’ (in English) Comput. Secur., vol. 109, Art. no. 102385, DOI: 10.1016/j.cose.2021.102385.

Tabisa Ncubukezi, Laban Mwansa and Francois Rocaries (2020) International Journal of Computer Science and Information Security (IJCSIS), Vol. 18, No. 3.

Tantawy A, Abdelwahed S, Erradi A, Shaban K (2020) Model-based risk assessment for cyber physical systems security. Computers & Security; 96:101864. DOI: 10.1016/j.cose.2020.101864

U. Kaila (2018) ‘‘Information security best practices: First steps for startups and SMEs,’’ (in English) Technol. Innov. Manag. Rev., vol. 8, no. 11, pp. 32–42, DOI: 10.22215/timreview/1198.

Van Haastrecht M, Sarhan I, Shojaifar A, Baumgartner L, Mallouli W, Spruit M (2021) A threat-based cyber security risk assessment approach addressing SME needs. In Proceedings of the 16th International Conference on Availability, Reliability and Security (pp. 1-12). DOI: 10.1145/3465481.3469199

Vitunskaite M, He Y, Brandstetter T, Janicke H (2019) Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. Computers & Security; 83:313-31. DOI: 10.1016/j.cose.2019.02.009

Yigit Ozkan B, van Lingen S, Spruit M (2021) The cybersecurity focus area maturity (CYSFAM) model. Journal of Cybersecurity and Privacy. 1(1):119-39. DOI: 10.3390/jcp1010007