IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 7 July 2022, accepted 26 July 2022, date of publication 10 August 2022, date of current version 19 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3197899

SURVEY

A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations

ALLADEAN CHIDUKWANI, SEBASTIAN ZANDER, AND POLYCHRONIS KOUTSAKIS, (Senior Member, IEEE)

Discipline of Information Technology, Media and Communications, Murdoch University, Murdoch, WA 6150, Australia

Corresponding author: Alladean Chidukwani (alladeanc@outlook.com)

This work was supported by the Australian Government Research Training Program (RTP) Scholarship.

ABSTRACT Small-to-medium sized businesses (SMBs) constitute a large fraction of many countries' economies but according to the literature SMBs are not adequately implementing cyber security which leaves them susceptible to cyber-attacks. Furthermore, research in cyber security is rarely focused on SMBs, despite them representing a large proportion of businesses. In this paper we review recent research on the cyber security of SMBs, with a focus on the alignment of this research to the popular NIST Cyber Security Framework (CSF). From the literature we also summarise the key challenges SMBs face in implementing good cyber security and conclude with key recommendations on how to implement good cyber security. We find that research in SMB cyber security is mainly qualitative analysis and narrowly focused on the Identify and Protect functions of the NIST CSF with very little work on the other existing functions. SMBs should have the ability to detect, respond and recover from cyber-attacks, and if research lacks in those areas, then SMBs may have little guidance on how to act. Future research in SMB cyber security should be more balanced and researchers should adopt well-established powerful quantitative research approaches to refine and test research whilst governments and academia are urged to invest in incentivising researchers to expand their research focus.

INDEX TERMS Cyber security, small-to-medium business, security posture, cyber security threats, cyber security frameworks, security and privacy.

I. INTRODUCTION

On the global level, SMBs are responsible for more than 90 percent of the worldwide business economy [1]. In Australia in particular, SMBs make up 98% of all Australian businesses, producing one-third of the total GDP and employing 4.7 million people [2] whilst in the UK, SMBs make up 99.9% of all businesses [3]. Since there are varying definitions of SMBs or small-to-medium enterprises (SMEs) [4], [5], we are using the definition of the Australian Bureau of Statistics defining SMBs as businesses employing between 5 – 199 staff [6].

Based on the major role that SMBs play in the economy, it would be expected that they would adequately implement cyber security strategies. However this is not the case as explained in [7], and this makes them susceptible to financial, productivity and legal costs that can even lead to bankruptcy.

Attackers have now turned to the easy target of SMBs many of which are either unaware [8] or not well resourced to fortify their networks and information resources [9]. Despite there being well known measures to protect businesses from cyber-attacks, SMBs continue to be victims [10]. Statistics show that 62% of Australian SMBs reported to have been a victim of cyber-attacks [11]. This statistic is closely aligned with the 2017 global statistic where 66% of SMBs reported their organization experiencing a cyberattack in the previous 12 months. These statistics are not only a concern for SMBs but also a concern for suppliers and customers who do business with them [12].

Cyber security is defined as ''the art of protecting networks, devices, and data from unauthorised access or criminal use and the practice of ensuring confidentiality, integrity, and

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

availability of information'' [13]. Cyber security research is a growing field with numerous topics which authors such as Suryotrisongko and Musashi have tried to develop taxonomies for [14]. Our study was necessitated by the realisation that there was very limited literature available regarding the cyber security of SMBs – both in Australia and globally [15]. To the best of our knowledge, only two surveys of a similar nature have been done [15], [16] which we discuss in more detail in Section IV. None of the existing surveys aligned their surveyed research to a well-known security framework or analysed the geographic spread of the surveyed research.

This motivated our study on the available literature and its focus as well as areas of SMB research that are underrepresented. From our experience and assertions from others [17], the practical and cohesive application of cyber security practices in industry is accomplished through the adoption of cyber security frameworks which provide structure and methodology [18]. Many frameworks exist, among which the National Institute of Standards and Technology Cyber Security Framework (NIST CSF) is popular amongst SMBs. Using the NIST CSF as a benchmark, the aim of our research is to understand the focus of previous SMB cyber security research and identify areas that may be lacking. The secondary aim is to establish in which countries or regions SMB cyber security research is being conducted, what research methodologies are being used and which data gathering techniques are being employed. Another aim was to analyse what researchers identified as the challenges faced by SMBs and what the recommended cyber security practices are.

Our study asked the following questions:

1. What has been the focus of SMB cyber security research?
2. How does past and current SMB cyber security research align with the widely used NIST CSF?
3. What areas of SMB cyber security research need more focus?
4. What is the most common SMB cyber security research methodology?
5. What data gathering techniques are SMB cyber security researchers using?
6. What is the geographic spread of SMB cyber security research?
7. What are the common challenges affecting SMB implementation of good cyber security?
8. What are the recommended cyber security practices for SMBs?

Compared to [15], [16] our work discusses a much larger body of relevant literature and categorizes the literature using a taxonomy based on NIST CSF. Hence, our survey covers more depth and breadth than existing work.

We anticipate that the results of this study will be useful to SMB cyber security researchers, academic institutions, research institutions, governments, and policy makers. Researchers can adopt a more targeted approach to their SMB cyber security research by focussing more on the underrepresented research areas. Academic/research institutions and governments could also incentivise researchers to carry out research in the lacking areas to ensure a well-balanced approach and ultimately help secure SMBs and subsequently the economies.

In section II to set the scene we discuss the difference between SMBs and larger organisations, current cyber-attacks and their cost to SMBs. In section III we briefly discuss cyber security frameworks and standards applicable to SMBs with a focus on the NIST framework which we use to classify the existing literature. In section IV we discuss the few existing surveys in this area. In section V we explain the paper selection criteria for the survey. In section VI we present our survey in two parts. Firstly, we discuss the challenges identified in previous literature and secondly, we discuss the literature through the lens of the NIST framework. In section VII we discuss the findings and summarize the recommendations for a good cyber security posture of SMBs. Section VIII presents the conclusions of this work.

II. CYBER SECURITY SITUATION FOR SMBS

In this section we discuss the differences between SMBs and large organisations when it comes the cyber security situation. We continue to discuss current cyber-attacks against SMBs and their cost implications.

A. SMBS VS. LARGE ENTERPRISES

Cyber threats do not discriminate by organisation size, which means SMBs are susceptible to the same threats as large organisations [19]. Although larger enterprises have a larger attack surface with more employees and devices, larger organisations also, in most cases, have the human and financial resources to put in place controls [9], [20]. Larger organisations tend to have dedicated cyber security staff with appropriate levels of education [21]. SMBs invest less in cyber security [20], however when it comes to the financial impact of successful cyber-attacks, they suffer higher costs proportionately than large businesses [10], [22]. SMBs however have the potential advantage of being small and agile with more flexible IT arrangements [23].

Industry research revealed that although cyber risk became more firmly entrenched in larger organisations' priorities in the past few years, the confidence of many organisations in their ability to manage cyber risk had declined as they were found to still struggle to articulate, approach and act upon cyber risk despite having the relevant human and financial resources [24]. They were also found struggling to educate and train their employees on cyber security [25], a challenge also common in SMBs.

Williams and Manheke [26] argued that cyber security threats to small business should be treated as a matter of national security. They argued that in a country like Australia where much of the business and economy lies in the hands of small businesses, the financial well-being of large groups of society could be affected by cyber-attacks on the business

sector impinging on the confidence on e-commerce and the economy as a whole.

B. SMBS UNDER ATTACK

Hayes and Bodhani [27] found that SMBs are being increasingly targeted by online threats because they are perceived as being inherently more vulnerable. New and less experienced cyber criminals often attack easy targets among which SMBs are featured [28]. The authors attribute this lax security to SMBs planning their IT security under the misconception that their networks and data are already safe.

A 2020 report from Verizon indicated that the attacks are far reaching with every organisation no matter the size, industry or sector, falling victim [19]. It is noted however that globally, health care service providers and finance related businesses are the most targeted [29], [30]. Academia and industry reports reveal that the most common cyber-attack types experienced by SMBs included: social engineering (e.g., phishing), hacking (e.g., stolen credentials, data theft), malware (e.g., ransomware), misuse (e.g., malicious insider), web-based attacks and ecommerce supply chain attacks [19], [31], [32], [33], [34]. Fig. 1 below shows the results from the Ponemon Institute's 2018 study showing phishing or social engineering attacks as the most prominent types of attack experienced by SMB respondents [31].

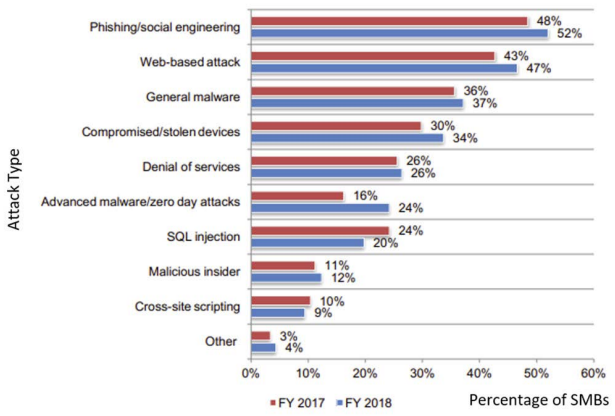

FIGURE 1. Types of attack experienced by SMBs from [31]. Social engineering is the most prominent attack and increasing from previous years.

Globally and across all organisations, web application servers appear to be the most targeted IT assets in data breaches largely due to the shift towards web-based applications due to an increasing consumption of services offering cloud-based software-as-a-service platforms. Other assets under attack are users' desktops and laptops, email servers, database servers and the end-users themselves [19]. Some researchers believe that mobile devices [35] and other IoT devices are the most vulnerable devices in the SMB environment which are most likely to be compromised and allow attackers entry into the network [8], [36], [37].

Unsecured online devices can also be weaponised to carry out sophisticated attacks on other organisations. For example, devices can be coerced into Botnets, awaiting instructions to join online distributed denial of service (DDoS) attacks [38].

As reported in [22], 70% of recent global breaches were perpetrated mainly by external actors, i.e., attackers from outside the company. Almost half of these attacks involved intrusion or gaining unauthorised access. The vast majority (86%) of these breaches were financially motivated, however cyber incidents and data breaches have several other motivators which include fun, ideology, grudges, espionage, state sponsored and human error [19].

Although most cyber-attacks were from external actors, in 2018, 16% of SMBs reported suffering an insider attack [31]. Williams and Manheke argued that human error both intentional and unintentional has a great impact on SMBs given that it affects many areas of protecting computer systems [26]. For example, in 2011 the Maricopa County Community College District (MCCCD) suffered a data breach with some of the college's databases being posted for sale on the dark web. Investigations revealed the issue was caused by an employee but did not reveal whether the data was intentionally or accidentally leaked [39]. In Australia, 11% of data breaches reported to the Office of The Australian Information Commissioner (OAIC) were the result of a rogue employee or insider attack [29].

C. COST OF POOR CYBER SECURITY FOR SMBS

Cyber-attacks are becoming more severe in terms of negative consequences such as financial impacts [40]. According to the Australian Criminal Intelligence Commission (ACIC), cybercrime is costing the Australian economy up to $1 billion annually in direct costs alone. The impact of cybercrime can be far reaching with other indirect costs coming in the form of damage to personal identity, loss of business or employment opportunities and significant impact on emotional and psychological wellbeing [41]. It is reported that about 60% of small businesses that were victims of a cyberattacks went out of business within six months [42]. This demonstrates that small businesses have a lot to lose if cyber threats materialise and it is in their best interest to have cyber defences in place.

Lost business was one of the largest costs for small business, along with financial loss, lawsuits, victim compensation, fines and internal investigations [30]. Once a data breach has occurred, the cost of compliance activities, training, research and upgrades to infrastructure could be signifinact [43]. In addition, businesses are susceptible to repeat attacks given hackers are likely to return. Research highlights that 28% of non-compliant victims are likely to suffer another breach within two years after the initial attack [44].

In the case of the payment and card industry, non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) could lead to be the business not being able to accept credit card payments for the goods sold or services rendered [45]. Other risks of fallout from not being compliant can be reputational. SMBs suffer a

disproportionately higher financial impact from cyber-attacks when their losses are adjusted to organizational size and revenue [22]. As of 2019, smaller organisations were found to have higher costs relative to their size than larger organisations, incurring an average cost of USD $3533 per employee, compared to USD $204 per employee for larger organisations [10]. The average cost of a data breach in Australia is $2.13 million while companies spend an average of $1.2 million due to damage or theft of IT assets and infrastructure. Additionally, disruption to normal operations cost an average of $1.9 million and these figures continue to increase from previous years [10], [31], [46].

Lloyd [47] claims that effective cyber security allows a business to demonstrate a high level of corporate social responsibility, showing customers commitment to security and privacy which leads to customer retention. Conversely it can be argued that ineffective cyber security demonstrates a lack of corporate social responsibility and disregard for customer security and privacy, leading to loss of customers.

Given many damaging data breaches are not reported, large organisations are now scrutinising the security practices of potential SMB third parties or suppliers to ensure a secure end-to-end supply chain can be achieved [12]. The US retailer Target suffered a large data breach in 2013 after hackers exploited the network access of a small heating, ventilation, and air-conditioning system supplier [48].

The existence of good cyber security practices in an SMB creates a competitive advantage for them in the market. It creates opportunities for lucrative supply chain contracts for which SMBs would not otherwise be a contender without good cyber security. A good example is the stringent cyber security compliance requirement that the US Department of Defence now imposes on defence contractors which is likely to preclude a lot of SMBs from bidding for defence contracts [49]. Effectively, SMBs who fail to invest in data security and governance miss out on market opportunities. When cyber security is not a priority it can become a growth inhibitor for an SMB.

III. CYBER SECURITY FRAMEWORKS

Cyber security frameworks define best practices that SMBs can follow to manage cyber security risk, establish a common language internally and externally, standardise service delivery and improve efficiency [50]. As pointed out by previous researchers, SMBs should adopt these frameworks to guide their cyber security implementations [15], [28].

A. NIST CYBER SECURITY FRAMEWORK

The taxonomy we use to classify the literature is based on the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) which was developed to help improve the security of critical infrastructure organisations in the USA [51]. It is a voluntary framework developed from existing standards, guidelines, and practices as well as with input from industry and government [52]. The framework provides a policy framework for organisations to assess and improve their ability to prevent, detect, and respond to cyber-attacks [53].

Although initially developed for critical infrastructure organisations, the framework has proven to be flexible and useful to other organisations [54]. By implementing the framework, organisations are better able to cost-effectively manage their cyber security risks, maximising their return on security investment [55]. Another notable benefit of NIST is that it provides a common language reducing confusion on the meaning of terms used in contracts and other agreements.

The components of the NIST CSF [116], [119] are summarised in TABLE 1 below.

TABLE 1. [53], [57] Nist CSF functions and categories.

NIST CSF Function	Category
Identify	Asset management; Risk assessment; Governance and compliance; Responsibilities; Risk Management; Procurement / supply chain risk management; Working with external partners; Recruitment
Protect	Identity management and user access control; Awareness and Training; Data Security; Information protection processes and procedures; Encryption; Maintenance; Patch and change management; Protective technology
Detect	Detection process; Security Incident Event Monitoring (SIEM) & anomalies; Security continuous monitoring
Respond	Response planning; Communications management; Forensics and impact analysis; Incident management; Emergency management; Lessons learnt and continuous improvement
Recover	Disaster recovery (DRP); Business continuity management (BCP); Improvements; Communications

NIST recognised that SMBs often do not have security experts at their disposal to interpret the cyber security framework and developed a simplified version of the NIST Cyber Security Framework specifically for SMBs which is published as the NIST Interagency Report 7621 (NISTIR 7621) [56].

NISTIR 7621 provides guidance to SMBs on how they can improve the security of information, including systems and networks, physical security, personnel security, contingency planning disaster recovery and operational security [56]. It prescribes actions that small businesses should take (Essential Practices) and adds ten highly recommended practices [58].

B. OTHER FRAMEWORKS

The Australian Signals Directorate (ASD) Essential Eight, International Standards Organisation (ISO) 27001/2 and the Payment Card Industry Data Security Standard (PCI DSS) are among other popular frameworks relevant for SMBs [28].

The ASD Essential Eight is an Australian framework which provides a baseline for organisations in order to protect themselves [59].

ISO 27001 is an international standard, providing specifications for a best-practice Information Security Management System (ISMS) [60]. ISO 27001 was developed to help organizations protect their information in a systematic and cost-effective way through the adoption of an ISMS [61]. The ISO 27001 standard groups the controls that organisations can select to tackle information security risks into 14 sets or domains [62]. ISO 27002 compliments ISO 27001 by providing more detailed guidance and a reference for selecting security controls within the process of implementing an ISMS [60].

The PCI DSS is the standard for the protection of cardholder data [45]. The PCI DSS controls framework helps SMBs to layer their defences around payment card data operations, improving their ability to maintain the confidentiality and integrity of customers' payment card details, in turn safeguarding the company's reputation. However, meeting PCI DSS compliance has been difficult for SMBs with only one in five managing to maintain their annual compliance obligations. Boese found that unlike larger corporations, small businesses lack the resources to become PCI DSS-compliant [45].

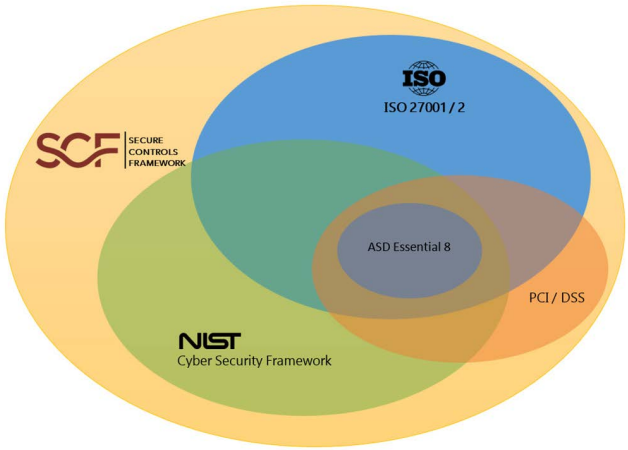

FIGURE 2. Relationship between cyber security frameworks. Note. This figure was adopted from Compliance forge [64] and enhanced to show the relationship with other frameworks such as PCI/DSS and ASD Essential 8.

SMBs may struggle to meet their business objectives as well as compliance requirements when adopting a single framework, thus some researchers recommend to adopt a hybrid framework [55]. The Secure Controls Framework (SCF) was developed as a hybrid framework to cover NIST CSF, NIST 800-53 and ISO 27002 [63]. Fig. 2 shows the SCF and how some of the frameworks and standards overlap. Essentially the SCF can be seen as a superset covering NIST CSF, ISO 27001/2, PCI DSS and ASD Essential Eight.

IV. RELATED SURVEYS

To the best of our knowledge, there exist only two surveys of a similar nature – one focussed on the UK [16] and one focussed on Australia [15].

Tam *et al.* discussed the research data challenges plaguing SMB cyber security researchers where the lack of publicly available data leads to little data being obtained largely from convenience sampling [15]. Self-reporting is also highlighted as an issue in SMB cyber research which causes awareness biases. They discuss challenges faced by SMBs as well as advantages or opportunities for SMBs. They also highlight the need for research data in businesses with less than 20 employees.

Alahmari and Duncan's review of SMB cyber security research was aimed at revealing the role played by SMB management in addressing cybersecurity risks [16]. They analysed 15 articles and identified threats, behaviours, practices, awareness, and decision making as the perspectives that play a role in SMB cyber security risk management.

Our survey differentiates itself by analysing a much larger body of literature and aligning the surveyed literature to a well-known cyber security framework which previous surveys have not done. Our survey categorizes the literature using a taxonomy based on NIST CSF. Unlike the previous studies, we also investigate the geographic spread of the surveyed research.

V. PAPER SELECTION CRITERIA

The literature analysed in this study consists of 40 scholarly academic and peer-reviewed publications, dating back to 2005 (see TABLE 5, Appendix A). For the search we used the Murdoch University Online library which indexes and searches popular academic databases and repositories such as Scopus, Web of Science and many other original research databases such as IEEE Explore. Outside the Murdoch University online library, Google Scholar was also used to widen the search. We set the inclusion and search criteria are as follows:

- Published: 2005 onwards
- Title Contains the terms: cyber security or cyber security or IT security or cyber risk AND small or medium AND business or enterprise
- Peer-reviewed journal paper, conference paper, doctoral dissertation or master's thesis
- Clearly articulated methodology

Each publication was categorised as journal paper, conference paper, doctoral dissertation or Master's thesis.

A qualitative systematic review of literature was carried out, paying attention to the focus of the research questions and themes of the research. We adopted the qualitative systematic review approach due to the difficulty of performing meta-analysis of studies within a particular topic. Qualitative approaches have been developed to review and assess the quality of research findings, as well as identify patterns and relationships amongst studies on a particular topic [65], [66].

Publications were shortlisted for analysis and reviewed to determine the SMB cyber security topic or theme, the country where the research was conducted, the research methods used as well as the data collection methods. The resulting process followed is depicted in Fig. 3.

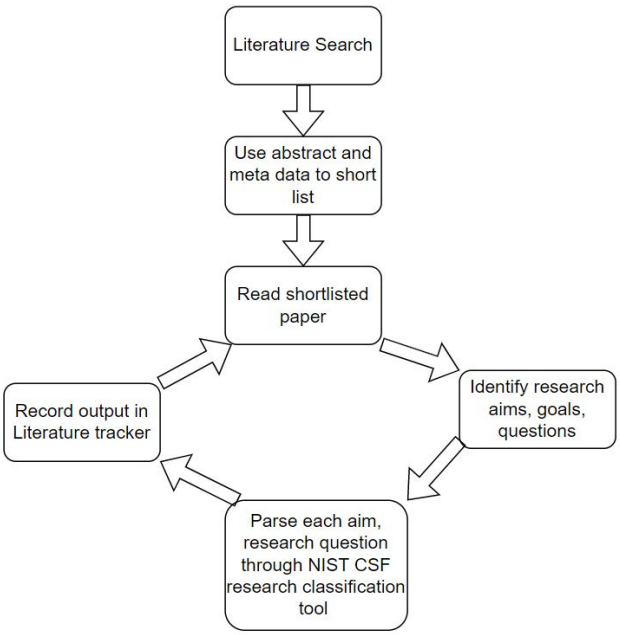

FIGURE 3. Methodology visualised. This figure visually depicts the process followed in this research.

We developed the NIST CSF Research Classification Tool (NCRCT) shown in Fig. 4 to help us align each publication with the functions of NIST CSF. For each included publication, the research aims, objectives and questions were parsed through the tool to help determine the NIST CSF category (Table 1) it aligned with. Using this tool, we determined the corresponding NIST Category or categories.

Furthermore, the research methodology and research design of each publication were reviewed to establish whether it was a qualitative, quantitative or mixed method approach and also to establish what data collection technique was used. The data collection methods are categorised as shown in Table 2.

Additionally, as each paper was analysed, the challenges faced by SMBs were noted and are discussed in Section VI.A Furthermore, we also identified recommended practices for SMBs suggested by the literature and discuss these in Section VII.

It should be noted that our literature search results are by no means exhaustive. Search results were limited to the repositories described above. Non-English research repositories could not be accessed and publications in other languages such as French, German, Chinese would have been precluded.

VI. SMB CYBER SECURITY RESEARCH

Our work investigated the alignment of SMB research to the popular NIST CSF framework. It also investigated the methods, data gathering techniques and the geographic spread of past SMB cyber security research. In the process we also examined the common challenges faced by SMBs in implementing good cyber security. This section discusses the findings related to the research questions.

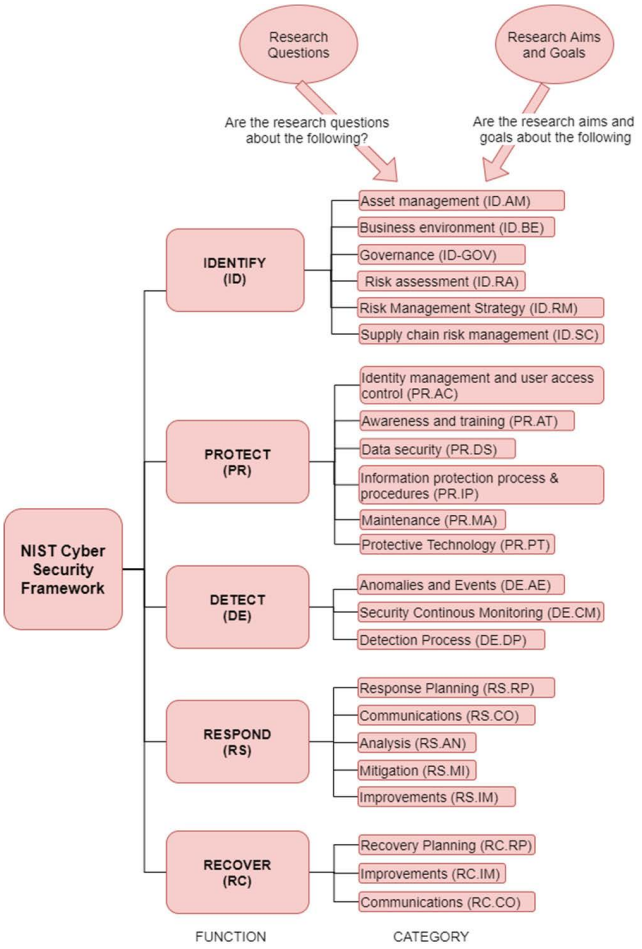

FIGURE 4. NIST CSF research classification tool (NCRCT). This figure shows the tool which was used to determine the focus of surveyed literature.

TABLE 2. Categorisation of data collection methods.

Method	Description
Interviews	Involves verbal communication between the participant and researcher
Literature review	Systematic procedure for reviewing or evaluating documents—both printed and electronic including previous research carried out by others.
Observation	Involves collecting information without asking questions.
Questionnaire	Written set of questions aimed at obtaining information about individuals and not used to look for trends.
Survey	Surveys are a set of questions typically deployed to a large sample for the purposes of statistical analysis. Surveys include the process of collecting, aggregating, and analysing the responses from those questions.
Experiment	Variables are manipulated and their effects on others are measured.
Combination	Combination of any data collection methods

A. CYBER SECURITY CHALLENGES

Previous research identified several challenges that SMBs face in implementing sound cyber security. In a recent study,

top challenges were found to be the lack of finances to pay for talent, issues with regulatory compliance as well as a shortage of professionally available talent [67]. Some researchers have categorised challenges faced by SMBs into technical, human, organisational, financial and legal challenges [15]. In the 2018 State of Cyber Security in SMBs study, the three main challenges faced by small businesses identified were: (i) not having the in-house expertise to mitigate cyber risk; (ii) IT budget constraints; and (iii) a general lack of understanding of how to protect against cyber-attacks [31].

Several other factors are suspected to also influence the poor cyber security posture of SMBs. Research by Deloitte [68] suggested that the age of the business owner or manager played a part in the security posture of their business, as well as their attitude and use of technology. The major factors influencing poor SMB cyber security posture are presented below.

1) UNDERESTIMATING THE RISK

Cyber risk transcends data breaches and privacy concerns. As Borenstein [69] alluded, the threats have evolved into more sophisticated schemes that prove very costly, disrupting entire businesses, industries, supply chains and even nations. Research has however shown that small business owners often have the tendency to underestimate cyber security risk [70], [71].

In Australia, almost half of the SMBs surveyed believed that they could protect their business from cybercrime by limiting their online presence. SMBs reported limiting their online presence to a business website, contact details and social media, with only 15% of survey respondents offering a business website with product viewing or purchasing functionality [43]. Notwithstanding the significant economic benefits of a greater presence online, the SMBs perception of cyber risk appears to be misguided. Cyber risks transcend websites and social media to include internet connected desktops, laptops, tablets, phones and nowadays internet connected devices and sensors (IoT) [19]. Any of these could expose the SMB to a cyberattack. Besides social media use, 55% of SMB owner-operators surveyed alluded to also using email to communicate, unknowingly exposing themselves to threats such as phishing and ransomware attacks [43]. They wrongly assumed limiting their online presence to be a safety measure preventing cybercrime, simultaneously unaware that email is the main vehicle for two thirds of malware related cyber security incidents globally [32].

A survey on small businesses in the US revealed the sector is more at risk than they think and is not taking necessary steps or investing in defending against cyberattacks [72]. Over half the businesses studied had not invested any measures to mitigate risks as they did not believe that they stored any valuable data, yet in fact they stored email addresses, phone numbers, postal addresses, home addresses, social security numbers and credit card details. This information which the SMBs perceived not to be of any value, is actually Personally Identifiable Information (PII), which forms the basis for most privacy regulation in Australia [73] and other countries. These findings demonstrate that there is an element of naivety in the operation of small businesses.

Another example from the US is that only one in five businesses are reported to be able to meet their annual obligations under the PCI DSS standard. Some do not believe that they have any valuable data assets or business impacting IT systems; some do not see the business benefits or return on investment in complying and ignore their obligations [12].

Digital supply chains also introduce new cyber risks for business [33], [74], [75]. Although many businesses were found to perceive the risk other supply chain partners introduce to them, they do not perceive the risk they pose to their supply chain [47].

Bhattacharya [76] asserted that small businesses are always going to be primarily focused on sales and revenues in order to survive and stay in business. With this being their core focus, cyber security issues are likely neglected as they are not seen as valuable contributions to the core business.

2) LACK OF SKILLS AND KNOWLEDGE

Academia and industry researchers have suggested that small businesses remain exposed and susceptible to attacks because they do not know what to protect [25], [58], [77], [78], [79]. The work in [77] and [79] found that SMBs are struggling with the complex demands of carrying out risk assessments and the manner in which to adopt cyber security best practices into their organizations.

The Australian Small Business and Family Enterprise Ombudsman alluded that the lack of awareness regarding cyber security is one of the biggest threats facing small business operators [80]. The lack of cyber security awareness is evident not only among employees but also among managers who are the decision makers but found to be unaware of the technical solutions available to address their cyber security challenges [16]. SMBs were also found to lack knowledge in assessing the capabilities of their IT service providers [28]. A common challenge with SMBs in the financial card payment industry is a lack of awareness and knowledge on how to become compliant even with mandatory regulations such as PCI-DSS [45], [81]. Thus SMBs require help with creating policies and complying with regulations [15]. SMBs also struggle to implement crucial monitoring and security systems (such as a SIEM) due to their complexity and the requisite skills and knowledge not available to SMBs. This is not surprising given that research found a lack of appropriate education amongst the IT professionals working in SMBs [21].

These assertions were confirmed in a 2019 survey of small businesses, citing insufficient personnel, insufficient budget and a lack of understanding around how to protect against cyber-attacks, as the biggest challenges for SMBs when trying to improve their cyber security posture [46]. This situation does not seem to have changed as recent studies consistently rated these as the main challenges [10], [31], [46].

3) LACK OF RESOURCES

SMBs are less likely to employ dedicated IT staff, let alone cyber security specialists [74]. A medium or large company may have sustainable resources for dealing with cyber-attacks, whereas the relatively low income of a small business generally equates to fewer resources allocated toward cyber defence strategies. Fewer human and financial [36], [71], [82] resources [36], [71], [82] make it difficult for most SMBs to comply [83] even with regulations such as PCI-DSS [45]. SMBs also fail to adopt more advanced cyber security technologies such as effective technical controls using machine learning due to the high costs [84]. Some researchers found that achieving a good level of cyber security awareness was one of the biggest challenges for organisations today [25], [79]. The problem is only compounded for SMBs because they face the same challenge but with much fewer resources [25]. As a consequence, some SMBs trust their IT service providers to take care of their cyber security, but without the necessary contractual arrangements in place or clear definition of the responsibilities [85]. McLaurin recommended SMBs should align the little resources they have to the threats that they face [28]. Thus, SMBs require cyber security solutions that are affordable, easy to implement and use [86], [87]. Onwubiko and Lenaghan recommend that SMBs adopt security models that combine multiple security facets together thereby reducing costs of implementation and management [9]. The Centria Cyber Security Manager concept is an example of this approach where SMBs can share cyber security expert costs [8] thus making it affordable.

4) RAPID PACE OF TECHNOLOGY ADVANCEMENT

Berry and Berry [88] found that small business owners struggle with risk management approaches for mitigating cyber threats due to the rapid pace of advancement in technologies. Some authors even argue that cyber security risks are evolving faster than the rate of digital technologies evolutions [24]. Thus, the inexperience with security technologies contributes to SMBs challenges [23]. In a recent study of cyber security incidents and data breaches, the Ponemon Institute found that SMBs are ill prepared to deal with risks created by third parties and the Internet of Things (IoT) which is growing at an increasingly rapid pace [10].

5) CONFLICTING / EXCESSIVE CYBER SECURITY INFORMATION

An Australian study in 2017 indicated that general awareness of cybercrime as a business risk was increasing amongst Australian SMBs, however many do not know where to get help from when responding to cybercrime events. They were found to be looking to multiple sources for help, ranging from Google searches to government and police [7]. Notably, 38% of respondents reported reaching out to an IT forensic consultant for help [43].

In a bid to improve the cyber awareness of SMBs, industry, government and other bodies make resources available, however as Renaud and Wier [7] found, the wealth of online information is at times conflicting, causing confusion and uncertainty amongst SMBs. It is possible the overwhelming availability of cyber security information hinders rather than helps SMEs. For example, in 2016 financial industry groups complained to NIST that banks are being burdened with a growing number of competing cyber security guidelines [89].

Another challenge with cyber security information or messaging is the negative connotations associated with the narrative of data breaches, regulatory fines and business disruption. Lloyd [47] suggests that business leaders need to reframe how they think about cyber security, with a focus on the opportunities that good cyber security presents rather than the consequences of its absence. For instance, effective cyber security allows companies to innovate, which drives revenue, profit and growth [15]. Good cyber security assists businesses to gain its customers' trust. Additionally, it gives businesses credibility in the supply chain, hence creating more opportunities [33], [74], [75].

6) LACK OF PERSEVERANCE

SMBs do care about cyber security despite the limited implementation of known security precautions [4], however businesses that start off implementing a number of security measures may, over time, become lax, especially since there is no visible benefit that accrues from the extra effort and expense. They can also inhabit a sense of false security, having not kept up with the emerging risks.

Renaud [90] found small businesses are inconsistent in their implementation of security measures based on their appraisal of threats and the ability to implement risk controls. Key findings from a 2019 cyber security benchmark report also showed small businesses are challenged with cyber security initiatives to ensure a quick response to emerging cyber threats [91].

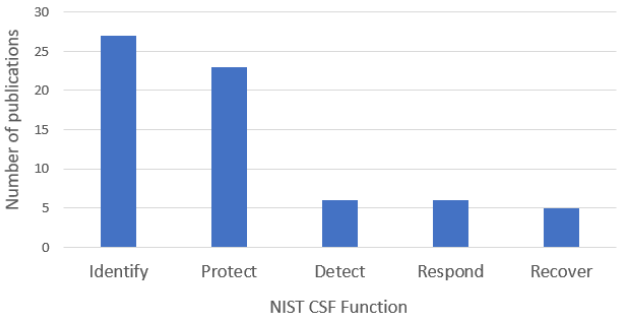

FIGURE 5. NIST CSF functions - focus of SMB cyber security research. This figure shows that the Identify and Protect functions of NIST CSF have been the focus of most previous and current research.

B. FOCUS OF CYBER SECURITY RESEARCH

Our results in Fig. 5 show that SMB cyber security research has largely been focussed on the Identify (27 out of 40) and Protect (23 out of 40) functions of the NIST CSF framework, with little work on the Detect (9), Respond (6) and

Recover (5) functions. In the Identify function, governance, risk management strategy and risk assessment were the most popular topics which researchers (see Table 5, Appendix a). In the Protect function, most publications researched the cyber security awareness and training of SMBs with Information protection processes and procedures being the second most popular category. Overall, across all of the NIST CSF categories, awareness and training has been the most popular topic.

The following sub sections will discuss the literature in relation to its respective NIST function and categories.

1) IDENTIFY

The identify function of the NIST CSF is meant to ensure that businesses understand the business context, the resources that support critical functions, and the related cyber security risks so that they can prioritize efforts, consistent with its risk management strategy and business needs. Four of the six categories of the Identify function [55] were represented in the literature reviewed. The functions Asset Management and Business Environment were not represented in the literature.

Early SMB cyber security research explored the cyber threats to SMBs, vulnerabilities, risks and practices [9], [26], [34], [79], [92], [93], [94]. Whilst other authors were industry agnostic in their studies, Heikkila *et al.* targeted their study to SMBs in the manufacturing industry [8] which had unique challenges due to digitisation and the adoption of the Internet of Things (IoT). Valli [95] targeted lawyers who require education on how to use encryption and were failing to report cyberattacks to the government's online reporting tool.

While most researchers focused on the challenges [25] faced by SMBs, others have found opportunities for SMBs when it comes to cyber security. Unlike large organisations, SMBs were found to have the advantage of being small, agile, and having flexible IT arrangements [15].

Some researchers studied risk management practices in SMBs whilst some explored strategies SMB use to prevent breaches, for example [96] and [97]. Several SMB cyber security researchers focused on the Governance category in the past decade. Aljumaili [98] explored information security policies and practices required by SMBs while Patterson [82] studied policy decisions in small businesses.

Researchers such as Burton-Howard [83] and others [45], [82], [87] focussed their research on governance and compliance including policies, legislation and compliance. Others concentrated on decision making related to cyber security amongst management in SMBs [82], [96]. Decision making approaches were found to depend on five perspectives which are cyber security threats, behaviours, practices, awareness and decision making in order to apply the correct remedies [16].

Additionally, the deficiency of existing laws was discussed with better laws to help protect SMBs being called for [83]. Tam *et al.* added that legal and policy work is needed to help SMBs become more cyber resilient [15]. Management is encouraged to ensure a good cyber security culture in their organisations [87].

Three studies [33], [74], [75] touched on cyber security supply chain risks – an emerging topic in SMB cyber security. Sangani *et al.* [74] developed a security and privacy architecture to help SMBs adopting cloud services. Cloud providers are part of the supply chain for SMBs adopting cloud, however their security responsibilities have limitations with some responsibilities falling in the hands of the cloud customers. Thus, in addition to understanding cloud benefits, SMBs are also urged to be aware of their responsibilities under these arrangements.

Some researchers based their research on cyber security frameworks such as the NIST CSF [28], [99]. Some designed new frameworks [74] whilst some identified shortcomings [94], [100], [101] with existing frameworks and suggested modifications or enhancements to existing frameworks that SMBs could adopt. Examples include the SME Cyber Risk Assessment suggested by Armenia *et al.* [99] and another by Emer *et al.* [102]. Benz and Chatterjee proposed an SME Cyber Security Evaluation Tool (CET) based on the NIST CSF targeting SMBs. Beachboard *et al.* [79] proposed an open development approach to develop a decision heuristic based risk assessment which allows SMBs to quantify costs and estimate probabilities for specific threats in their risk assessments. Considering the difficulty of practically implementing cyber security in SMBs, Borges and Carias proposed a more holistic framework which provides an implementation order for SMBs to follow [18]. Bada and Nurse proposed a framework for education and awareness to support SMBs [25]. Coertze *et al.* [101] proposed enhancements to the Information Security Management Toolbox to help SMBs with creating automated security policies and monitoring compliance. There is however very little evidence on the practical implementation of most of the proposed toolsets and frameworks.

2) PROTECT

According to NIST [103], the Protect function ''supports the ability to limit or contain the impact of a potential cyber security event''. Examples categories within this Function include Access Control (validating identities and access to different systems, facilities, etc.), Awareness and Training (giving employees and others the ability to be part of the cyber plan with education and training), Data Security (manage data according to company standards in order to mitigate cyber security risks, and protect its Availability, Integrity and Confidentiality proactively), Information Protection Processes & Procedures (putting in place the policies, processes, and procedures that are needed to manage protection of assets), Maintenance (continuously repairing information system components) and Protective Technology (deploying security solutions needed to protect assets in line with company policies).

Cyber security awareness has been a key focus of SMB cyber security research in early and recent

years [35], [81], [92]. Several works analysed by us had training and awareness as their key focus with authors like Valli *et al.* specifically focusing on the cyber awareness of lawyers [95] and Milos studying the awareness levels of IT professionals in SMBs [21]. According to Fehér [75], it is most important to improve the user's awareness. The argument is that SMBs should have a proper understanding of the threats their businesses face and how to mitigate them [74]. Cook [85] found that awareness in SMBs studied was broken into three themes which are: knowledge of third-party vendors, knowledge of protection and knowledge of strategic plans.

In general, training was found to raise the awareness and self-efficacy [81], [95]. Barosy identified making people aware of their responsibilities and roles in information technology as the critical factor in a cyber security awareness program for SMBs [97] and should be an ongoing exercise given the rapidly evolving threat landscape. Carnell [80] found that loss of sensitive data had a direct correlation with security awareness and knowledge of cyber security damage. Like large enterprises, SMBs struggle to educate and train their workforce except for SMBs the problem is worse due to a lack of resources [25]. However, cyber awareness and training is essential to keeping businesses cyber secure and Carias [18] suggested that every domain of a cyber security framework should be supported by training and awareness. Bada and Nurse [25] proposed a cyber awareness programme for SMBs with key areas of the programme being the initial engagement with SMEs, improving security practices and culture, programme and trusted third-party resources / services – all underpinned by a communication strategy.

Cyber security awareness levels of IT professionals in SMBs was found to be low due to a lack of appropriate education and conflicting priorities since they are not dedicated to cyber security tasks [21]. Lawyers in Western Australia were found to need education particularly on the use of encryption to help protect data in transit or at rest given their professional privilege and access to sensitive client data. [95].

Policies and procedures are seen as one of the ways SMBs can solve the challenge aligning their information systems and resources with requirements of security standards [98]. Several publications in our study were devoted to policies that SMBs could implement to ensure good cyber security behaviours in their organisation [96], [98]. McLaurin identified that SMB owners required assistance with writing cyber security policies [28] as research has shown that a lack of human and financial resources was a barrier to drafting, implementing, and complying with sound information security policies [101].

Most recently researchers have studied protective cyber security technologies in SMBs such as machine learning [84], [100] which are seen to be effective in protecting against cyber-attacks. Mercl and Horalek [104] examined the practical implementation of a Security Incident Event Monitoring (SIEM) in an SMB environment [104] with their results showing that SIEM implementation in SMB environments was both costly and complicated especially considering SMBs may not have the requisite knowledge and skills.

The challenges SMBs face when implementing cyber security is another popular theme [36], [71]. Deficiencies in SMB cyber security was a focal point of several studies. Examples such as the failure to implement firewalls on devices despite them being built into operating systems were attributed to the lack of knowledge and awareness [35]. The majority of SMBs were also found to not install anti-malware on mobile devices. SMBs were also found to be deficient in performing risk assessments in their environments [79].

3) DETECT

According to NIST [103] the Detect function helps ensure organisations develop and implement appropriate activities to identify the occurrence of a cyber security event.

The Detect function enables timely discovery of cyber security events. Examples of categories within this function include: Anomalies and Events (ensuring anomalies and events are detected, and their potential impact is understood), Security Continuous Monitoring (implementing security continuous monitoring capabilities to monitor cyber security events and verify the effectiveness of protective measures including network and physical activities), and Detection Processes (maintaining detection processes to provide awareness of anomalous events) [103].

Only six of the papers in our review had the Detect function as their focus [8], [18], [84], [86], [94], [104]. As shown in Table 5, four of them fell into the Security Continuous Monitoring category whilst the remaining two fell into the Detection Process category. The Anomalies and Events category was not represented.

Whilst virus and malware protection were found to create net benefits and encourage a positive user experience in SMBs [86], Heikkila *et al.* [8] argued that successful security management hinges on continuous monitoring and SMBs require easy to deploy security services offering such. They explored the Centria security laboratory as a low-cost solution for SMBs in the manufacturing industry to manage their cyber security including continuous security monitoring. Continuous monitoring of an IT environment is achieved using a SIEM which researchers Mercl and Horalek focused their study on [104]. They studied two SMBs implementing the IBM Security QRadar SIEM and found that such implementations required guidance and assistance from knowledgeable professionals due to the complexity of the implementation. The implementation of a SIEM in the SMBs was found to hinge on the following factors: the number of company employees; geological division of IT infrastructure; financial aspects and limitations of the company; the number and type of devices that are managed by the system and the audit reporting requirements.

Rawindaran *et al.* [84] investigated the challenges SMBs face in adopting Machine Learning Cyber Security (MLCS). Their study revealed that although MLCS has been

successfully applied in many monitoring applications, for example in network intrusion detection systems (NIDS), there was still poor adoption of MLCS techniques among UK SMBs.

Kaila and Nyman [94] stressed the importance of monitoring as it not only allows SMBs to uncover what happened in the event of a breach, but also helps them make informed responses to incidents. Carias *et al.* [18] focussed their study on the best implementation order for a cyber resilience framework in SMBs. They found that different experts have differing priorities, however a general consensus reached indicated that detection processes and continuous monitoring should be implemented together with information security techniques after implementing governance, risk management, asset management, vulnerability management and business continuity.

4) RESPOND

The Respond function involves activities that ensure organisations develop and implement appropriate activities to take action regarding a detected cyber security incident [103]. According to NIST, ''the Respond function supports the ability to contain the impact of a potential cyber security incident''. Examples of categories within this function include Response Planning (ensuring response planning process are executed during and after an incident), Communications (managing communications during and after an event with stakeholders, law enforcement, external stakeholders as appropriate), Analysis (analysis is conducted to ensure effective response and support recovery activities including forensic analysis, and determining the impact of incidents), Mitigation (mitigation activities are performed to prevent expansion of an event and to resolve the incident) and Improvements (the organization implements improvements by incorporating lessons learned from current and previous detection / response activities). The Respond function activities such as response planning, impact analysis and improvement from lessons learnt go a long way in ensuring cyber resilience in SMBs however in their study, Powell *et al.* [34] found that almost half of SMBs either did not have an emergency action plan or did not have it written and fully implemented. Given the threat landscape is ever evolving, traditional methods of protecting against known threats we seen not to be effective enough, thus Carias *et al.* [18] claimed that cyber resilience is a more holistic approach to cyber security which assists SMBs to anticipate, detect, withstand, recover and evolve after cyber incidents.

Seven out of 40 publications in our review were focused on the Respond function of the NIST CSF. The Mitigation category was the most popular category in this function accounting for over half of the papers. Analysis and Improvements were also represented; however, Response Planning and Communications were not.

Regarding Mitigation, Kaila and Nyman [94] identified logs as crucial in the event of a compromised system as they help uncover what happened and help inform SMBs on deciding on how to respond to incidents. Having good mitigation strategies also brings a business benefit where the organisation can demonstrate compliance and reasonable effort to protect the business, customer or staff data should a cyber incident occur [18]. Alharbi *et al.* [105] measured how certain cyber security practices can affect the level of harm caused by cyber-attacks and found that having a cyber security inspection team and recovery plan reduced the financial damage caused by cyberattacks in SMBs. For incidents that eventuate, SMBs were disinterested in reporting the incident or conducting forensic analysis due to the costs of the activities; SMBs simply wanted to move on rather than spend time determining the source or cause of attack [106]. Machine learning (ML) techniques and artificial intelligence (AI) were found to be very effective in the detection of anomalies and enhancing the functionality of modern network/host intrusion detection and prevention systems, however Rawindaran *et al.* [84] found that some SMBs were not aware or had disregarded that AI and ML were built into the cyber security solutions they invested in. Rawindaran recommended that awareness of AI and ML in cyber security should be improved amongst SMBs.

5) RECOVER

The recover function of the NIST CSF guides SMBs to put in place measures to ensure that they can recover normal operations after a cyber security incident [103]. Recommended activities under this function are designed to enable any business functions and capabilities affected by a cyber-attack to be able to be restored after the incident. This ability to recover from or adjust easily to misfortune or change part of cyber resilience [107]. For SMBs, not only should they be able to defend against cyberattacks, but they need to be able to return to normal operations after an incident. Categories under this function include Recovery Planning (recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cyber security incidents), Improvements (continuous improvements from lessons learnt and communications to ensure the organisation is well coordinated during cyber incidents [103]) and Communications (restoration activities are coordinated with internal and external parties) [103].

Only five [15], [18], [85], [94], [105] of the papers reviewed focussed on the Recover function with the Recovery Planning category being the most popular category. The Improvements category was not represented in the literature. Tam *et al.* highlighted the lack of research in cyber resilience which our study also validates. They noted that cyber security insurance was a challenge for SMBs given it is a new concept [15]. They added that highly expensive remediation costs of cyber incidents make it particularly difficult for SMBs to recover, hence cyber insurance would be the best approach; however, it is not well understood amongst SMBs. SMBs were also found to have a reliance on third party vendors for their infrastructure and security preventative measures [85], however this does not necessarily mean the third party takes ownership of the SMB's recovery planning. Cook's study [85] also revealed that SMBs were adopting preventative

and protective strategies, however our analysis of Cook's results revealed that planning for the worst was not quite evident amongst the SMBs studied. Planning for the worst is crucial for recovery in the event that a cyber-attack occurs and this can be achieved by having a business continuity plan in place [94]. In their research Alharbi *et al.* [105] found that having an inspection team and a recovery plan reduced the financial damage a cyber-attack had on SMBs in Saudi Arabia. Additionally, their research revealed having contact with cyber security authorities statistically reduced the restoration time following a cyber-attack. They recommended that SMBs should focus more on certain cyber security practices that can decrease the impacts of cyber security attacks. Carias *et al.* [18] claimed that cyber resilience was a more holistic approach which SMBs should adopt and they proposed a framework to make it easier for SMBs to implement cyber resilience practices. However, there is no data on the practical application of this framework.

C. RESEARCH AREAS REQUIRING MORE WORK

Several categories from the Detect, Respond and Recover functions were underrepresented whilst some categories were not represented at all. Underrepresented categories include Detection Process, Security Continuous Monitoring, Analysis, Improvements, Mitigation, Communications and Recovery Planning. Categories with no representation at all include Maintenance, Anomalies and Events, Response Planning, Communications, and Improvements.

It is quite evident from the results above that there is limited research on cyber resilience. Previous researchers have also found that in practice many organisations narrowly focus on technology defences and prevention of cyber risk but neglect other cyber resilience building activities like risk transfer and response planning aspects which are covered by the Respond and Recover functions of the NIST CSF [24]. Our results indicate that, overall, little research attention has been given to the Detect, Respond and Recover functions of the NIST CSF all of which are part of developing cyber resilience. In 2020, IBM Security reported that incident response preparedness was the highest cost saver for businesses when it came to data breaches, saving businesses on average of USD$2 million in the event of a data breach [30]. This highlights the importance of the Respond and Recover functions to businesses.

We believe that the narrow focus of SMB cyber security research is largely attributed to the limited quantity of research in the area, since most of the research to date has focused on large enterprises. Our study highlights the need for additional research in more categories.

D. GEOGRAPHIC SPREAD AND PUBLICATION TYPES

When considering the countries in which SMB-related cyber security research is conducted/published, the USA had the highest number of papers overall, accounting for 43% of publications analysed (Fig. 6). Together with other countries, Australia was found to be underrepresented in the SMB cyber security research literature, particularly in the academic literature of master's theses and doctoral dissertations. Outside the USA and Australia, the majority of the relevant research is conducted in Europe. Africa, Asia, the Middle East and South America are underrepresented with little to no publications on SMB cyber security. We suspect the lack of literature from Asia and South America may be due to non-English publications not accessible to us.

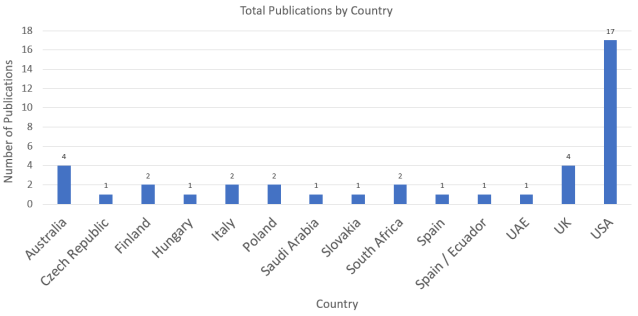

FIGURE 6. Total publications by country. This figure shows the geographic spread of literature surveyed in this study.

Table 3 shows that journal papers were the most popular type of publication accounting for 47.5% of the literature reviewed. They were followed in popularity by conference papers (20%) and doctoral dissertations (17.5%) and lastly master's thesis at 15%. Between 2005 and 2013, there were few publications examining SMB cyber security with an average of one publication each year. Between 2013 and 2014 there was an increase in the number of doctoral dissertations and master theses focused on the topic.

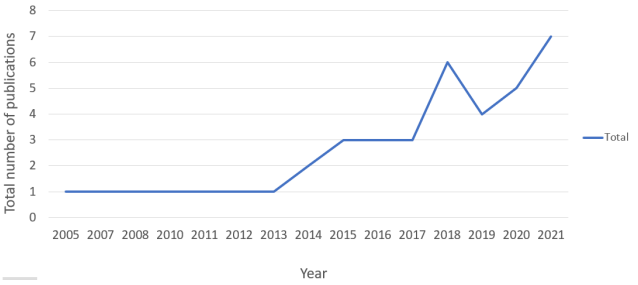

FIGURE 7. SMB cyber security research - Publications over time. This figure shows a gradual increase in SMB cyber security research since 2013.

It is encouraging that the number of publications on the topic has increased in recent years. Fig. 7 shows a general upward trend indicating a growing interest in the topic among researchers.

E. RESEARCH METHODOLOGY USED

As shown in Fig. 8, we found that SMB cyber security researchers have been predominantly using qualitative methods (70%) as opposed to quantitative (25%) and mixed methods (5%). These findings are consistent with previous research which found that a large proportion of cyber security research is focussed on risk with most researchers using

TABLE 3. Percentages of publication types.

Publication Type	Quantity	Percentage
Masters Thesis	6	15%
Doctoral Dissertation	7	17.5%
Conference Paper	8	20%
Journal Paper	19	47.5%
Total	**40**	**100%**

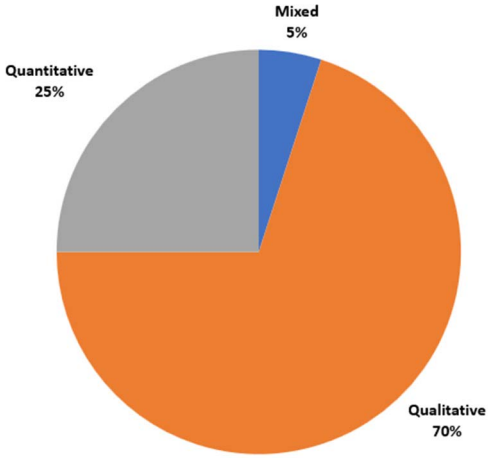

FIGURE 8. Research methodology used by SMB cyber security researchers. Most researchers are using qualitative methods to research cyber security in SMBs.

qualitative methods to assess cyber risk [108]. Information security is viewed as being too complex to model with quantitative methods but authors like Douglas and Seiersen [109] strongly advocate for evidence-based research methods in cyber security, as opposed to testimonial-based methods of identifying cyber security best practices and effectiveness of controls. They emphasise the role of cyber experts in computing cyber security metrics to ensure a factual and unbiased outcome. In 2019, 30% of organisations reported using quantitative methods to express cyber risk exposures, up from 17% in the previous two years. Marsh recommends that organisations should quantify cyber security risks to drive better informed investment, and performance measurements thus treating cyber security risks in the same economic terms as other enterprise risks [24].

Very few SMB cyber security researchers seem to use mixed methods [25], [84]. Rawindaran *et al.* researched cyber security technology using mixed methods to study the adoption of machine learning cyber security in SMBs. Although most researchers adopted qualitative approaches in their studies [8], [9], [15], [16], [18], [21], [26], [33], [45], [74], [79], [83], [93], [94], [97], [98], [101], [102], [104], [106], some adopted quantitative approaches [28], [34], [35], [71], [81], [82], [86], [95], [99], [100]. For example McLauren adopted a quantitative approach to study to which extent SMBs should implement a security framework to offer the most return on investment [28]. Alharbi *et al.* [105] also adopted quantitative methods to measure the impact that SMB cyber security practices have on cyber-attack damage. Their research indicated that having an inspection team and a recovery plan reduced the financial damage that a cyber-attack had on SMBs in Saudi Arabia.

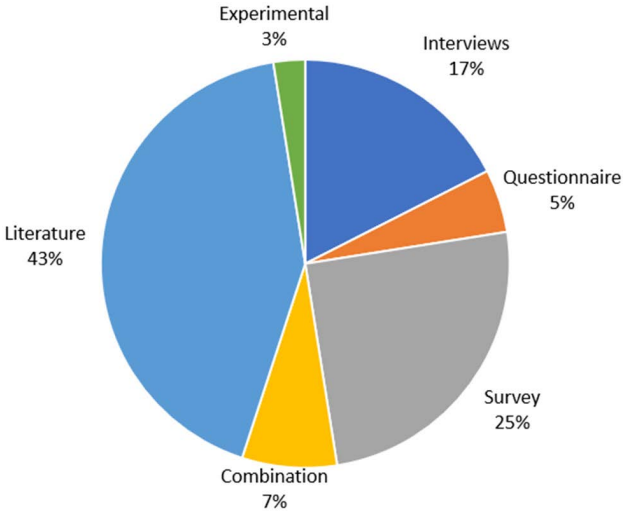

FIGURE 9. Data collection methods used by researchers. The figure shows the findings that literature reviews are the leading method for data collection by SMB cyber security researchers.

F. DATA COLLECTION METHODS USED

The data collection methods (Table 2) used by researchers were analysed and our results in Fig. 9 show that literature reviews were the most common method for data collection used by researchers (43%), followed by surveys (25%) and interviews (17%). A combination of methods was used for 7% of the research analysed with the methods least used being questionnaires (5%) and experiments (3%). It is interesting to note that none of the publications analysed used observation as a data gathering method. We believe this is due to the complexity of observing user interactions with computer systems and user behaviour profiling which requires capturing large amounts of data, in a process that can be intrusive [110]. With emergence of automated tools, this may however be more feasible in the future [111].

VII. DISCUSSION AND RECOMMENDATIONS

Many researchers of SMB cyber security use literature reviews for data collection whilst using largely qualitative methods. This indicates that there is limited original research in the field, such as case studies, surveys and experiments (all which can employ different data collection techniques including questionnaires, interviews, content analysis, observations [112]). While original field research is difficult in this highly sensitive area, it would be highly desirable to better understand the issues and provide better solutions. A literature-review-based approach also presents a challenge

to researchers when there is limited literature particularly in localised contexts such as in Australia.

Whilst qualitative methods are quick and cost-effective in prioritising cyber risks, Alahmari noted the need for empirical research on topics like cyber security risk management in SMBs [16]. Well-established and powerful quantitative methods can be used [113], however authors such as Edgar and Manz argue that the unavailability of objective data limits their applicability and credibility [114], [115]. Apart from a lack of data, the limited use of quantitative methods may also indicate a lack of maturity of research as quantitative methods are typically used to answer clear, predefined questions in the advanced stages of a study [116].

Despite the increase in SMB cyber security-related publications over recent years, several authors have suggested that more research is needed to understand the approaches to risk management SMBs undertake alongside their responses to cyber security threats. Such research will help highlight SMB cyber security activities for preparedness, the decision makers' perceptions of risk and approaches to improve their cyber security postures [70], [88].

Cyber-attacks are now moving beyond data breaches and privacy concerns to more sophisticated schemes, such as ransomware, that prove very costly, disrupting entire businesses, industries, supply chains and even nations. Some researchers such as Baskerville *et al.* have recommended strategies to ensure a balanced approach to the prevention and response paradigms of security [117]. However, many organisations narrowly focus on technology defences and prevention of cyber risk but neglect other cyber resilience building activities like assessments, risk transfer, response planning and training [24].

Very few papers analysed in this study touched on aspects of SMB cyber security related to the security incident management and business continuity management categories of the NIST CSF. Since the threats will always be there, whether external or internal, cyber security risks cannot be eliminated, but a business can mitigate, manage, and recover from cyber-attacks [69]. SMBs should not only be able to defend against cyber-attacks in the first instance but also to return to normal operations after an incident. Eilts [118] found that small businesses that were able to improve their cyber security posture were those that had committed to incorporating cyber security preparedness activities into their routine business.

Although suggested priorities may differ, there is consensus in the literature on what is good cyber security. Bryan [61] points out that a reliable and affordable starting point to good cyber security for SMBs is a comprehensive information security system which contains a computer-use policy, information security training and business virus and malware protection [86]. Kaila and Urpo [94] suggest the useful first steps for start-ups and SMBs should be: identifying assets and risks; protecting accounts, systems, clouds, and data; implementing a continuity plan; and monitoring and reviewing. Other researchers suggested SMBs should put more focus on practices that can decrease the impact of cyber-attacks such as investing in an inspection team and a documented recovery plan [105]. It is not only the SMB's responsibility, but also technology vendors who have been challenged to incorporate security into computing technologies to assist the likes of SMBs with limited knowledge and access to expertise [26]. There are security responsibilities for both vendor and SMB customer, for example for cloud-based Software-as-a-Service (SaaS).

Table 4 below sums up the practices that are recommended by researchers [15], [21], [24], [25], [28], [30], [33], [34], [35], [36], [47], [59], [75], [81], [86], [94], [96], [119], [120], [121], [122]. Practical implementation of these practices is somewhat difficult for SMBs, which is why authors like Carias and Borges proposed a framework for the implementation order of these practices [18].

TABLE 4. Good cyber security practices.

1. Allocating budgets for cyber security	19. Ensure backups can be restored when required
2. Create password policies	20. Use multi-factor authentication
3. Perform vulnerability assessments	21. Implement access control
4. Develop a strategy of training employees	22. Use passphrases in lieu of passwords
5. Invest in and sufficiently train staff	23. Invest in effective firewalls
6. Have regular awareness training	24. Implement anti-virus and anti-malware
7. Make cyber security an agenda topic for boards	25. Install antivirus countermeasures on mobile platforms
8. Treat cyber security like any other business risk	26. Review contracts and policies with suppliers
9. Develop a cyberattack response plan	27. Ensure suppliers have an accredited standard for cyber security for themselves and their partners to protect the supply chain
10. Grow cyber security as the business grows	28. Have an up-to-date incident response plan
11. Perform a risk management assessment	29. Practiced incident response plan regularly so that employees know what to do when they suspect there is an attempted breach or if an actual incident occurs
12. Develop and document an internal IT security or cyber security policy	30. Consider investing in cyber insurance to cover the exposure of data privacy and security.
13. Have simple, clear policies	31. Hire trustworthy employees
14. Ensure employees are familiar with the security policy	32. Secure remote access
15. Take inventory of software	33. Utilize encryption software
16. Ensure regular updates and patches of software	34. Employ dedicated cyber security staff
17. Perform automatic backups of all data	35. Implement multi-factor authentication
18. Securely backup business-critical data, such as customer data and financial information	

TABLE 5. Publications included in our study.

TITLE	YEAR	COUN-TRY	TYPE OF PUBLICATION	METHOD-OLOGY	Data Collection Method	ID	PR	DE	RS	RC
Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence[16]	2021	UK	Journal Paper	Qualitative	Literature	ID.RM				
Efficacy Of Small Business Cybersecurity [28]	2021	USA	Doctoral Dissertation	Quantitative	Survey	ID.GOV	PR.IP			
The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses [15]	2021	Australia	Journal Paper	Qualitative	Literature	ID.RM	PR.PT			RC.RP
The Impact of Cybersecurity Practices on Cyberattack Damage The Perspective of Small Enterprises in Saudi Arabia [105]	2021	Saudi Arabia	Journal Paper	Quantitative	Survey	ID.RA	PR.AT		RS.AN	RC.RP
A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs [99]	2021	Italy	Journal Paper	Quantitative	Experimental	ID.RA				
Machine Learning Cybersecurity Adoption in Small and Medium Enterprises in Developed Countries [84]	2021	UK	Journal Paper	Mixed	Survey		PR.PT	DE.CM	RS.IM	
A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises [102]	2021	Italy	Journal Paper	Qualitative	Literature	ID.RA				
Evaluating Self-efficacy Pertaining to Cybersecurity for Small Business [81]	2020	USA	Journal Paper	Quantitative	Survey		PR.AT			
Calculated risk? A cybersecurity evaluation tool for SMEs* [100]	2020	USA	Journal Paper	Quantitative	Survey	ID.RM				
Systematic Approach to Cyber Resilience Operationalization in SMEs [18]	2020	Spain	Journal Paper	Qualitative	Interviews	ID.GOV	PR.AT	DE.DP	RS.MI	RC.CO
Effective Information Security Strategies for Small Business [86]	2020	USA	Journal Paper	Quantitative	Survey	ID.GOV	PR.AT	DE.DP	RS.MI	
Cybersecurity threats of cloud and third-party services in small and medium-sized enterprise environment [75]	2020	Hungary	Conference Paper	Qualitative	Combination	ID.SC	PR.DS			
Developing cybersecurity education and awareness programmes for Small and medium-sized enterprises [25]	2019	UK	Journal Paper	Mixed	Survey		PR.AT			
Cybersecurity and Small to Medium Business [33]	2019	USA	Masters Thesis	Qualitative	Literature	ID.SC	PR.PT			
PCI DSS Compliance Challenges for Small Businesses [45]	2019	USA	Masters Thesis	Qualitative	Literature	ID.GOV				
SIEM Implementation for Small and Mid-Sized Business Environments [104]	2019	Czech Republic	Journal Paper	Qualitative	Combination			DE.CM		
Protecting Small Business Information From Cyber Security [83]	2018	USA	Doctoral Dissertation	Qualitative	Questionnaire	ID.GOV				
A Survey of Lawyers' Cyber Security Practises in Western Australia [95]	2018	Australia	Conference Paper	Quantitative	Survey		PR.AT			
Exploring the information security policies and practices required by small and medium sized enterprises [98]	2018	USA	Doctoral Dissertation	Qualitative	Survey	ID.GOV	PR.IP			
Economic and National Security Effects of Cyber Attacks Against Small Business Communities [106]	2018	USA	Masters Thesis	Qualitative	Literature				RS.AN	
Exploring SME cybersecurity practices in developing countries [71]	2018	South Africa	Journal Paper	Qualitative	Interviews	ID.RM	PR.IP			
Information Security Best Practices: First Steps for Startups and SMEs [94]	2018	Finland	Journal Paper	Qualitative	Literature	ID.RA	PR.IP	DE.CM	RS.MI	RC.RP
IT Security Management In Small and Medium Enterprises [36]	2017	Poland	Journal Paper	Qualitative	Literature	ID.GOV				
Cyber Security Policy Decisions in Small Business [82]	2017	USA	Doctoral Dissertation	Qualitative	Interviews	ID.GOV				
Effective Cyber Security Strategies for Small Businesses [85]	2017	USA	Doctoral Dissertation	Qualitative	Interviews	ID.RM	PR.AT			RC.RP
Determining Small Business Cybersecurity Strategies to Prevent Data Breaches [96]	2016	USA	Doctoral Dissertation	Qualitative	Questionnaire	ID.RM				
The Importance of the Security Culture in SMEs as Regards the Correct Management of the Security of Their Assets [87]	2016	Spain / Ecuador	Journal Paper	Quantitative	Literature	ID.GOV				
Security Challenges in Small- and Medium-Sized Manufacturing Enterprises [8]	2016	Finland	Conference Paper	Qualitative	Literature		PR.PT	DE.CM		
Cyber security Measures in SMEs: a study of IT Professionals' organisational cyber security awareness [21]	2015	Slovakia	Masters Thesis	Qualitative	Interviews	ID.RA	PR.AT			
The cyber security in SMEs in Poland and Tanzania [123]	2015	Poland	Conference Paper	Qualitative	Combination	ID.RM				
The value of Cyber Security in Small Business [92]	2015	USA	Masters Thesis	Qualitative	Literature	ID.RA	PR.AT			
Small to Medium Enterprise Cyber Security Awareness: An Initial Survey of Western Australian Business [35]	2014	Australia	Conference Paper	Quantitative	Survey		PR.AT			

TABLE 5. *(Continued.)* **Publications included in our study.**

Analyzing and mitigating cybersecurity risks faced by small businesses. [93]	2014	USA	Masters Thesis	Qualitative	Literature	ID.RA	PR.IP			
Successful Operational Cyber Security Strategies for Small Businesses [97]	2013	USA	Doctoral Dissertation	Qualitative	Interviews	ID.RM	PR.AT			
Security & Privacy Architecture as a service for Small and Medium Enterprises [74]	2012	UAE	Conference Paper	Qualitative	Literature	ID.SC	PR.IP			
A web-based information security management toolbox for small-to-medium enterprises in Southern Africa [101]	2011	South Africa	Conference Paper	Qualitative	Literature	ID.GOV				
Small Business - A Cyber Resilience Vulnerability [26]	2010	Australia	Conference Paper	Qualitative	Literature	ID.RA				
Improving Information Security Risk Analysis Practices for Small- and Medium-Sized Enterprises -A Research Agenda [79]	2008	USA	Journal Paper	Qualitative	Literature	ID.RA				
Managing Security Threats and Vulnerabilities for Small to Medium Enterprises [9]	2007	UK	Journal Paper	Qualitative	Literature	ID.RM	PR.IP			
Information Security Threats and Practices in Small Businesses [34]	2005	USA	Journal Paper	Quantitative	Interviews	ID.RM	PR.DS		RS.MI	

VIII. CONCLUSION

Continuous on-going research is required to support the development of cyber security solutions for SMBs [15], [102]. Research in cyber security is however rarely focussed on SMBs, despite them representing a large proportion of business. SMBs contribute immensely to the global economy, and in particular in Australia they make up 98% of all businesses contributing one third of the GDP. Despite their large number and importance, our study shows that research in SMB cyber security is rather limited and narrowly focussed. This is consistent with previous findings of other researchers [15].

We also found SMB cyber security research to be concentrated in the USA despite other nations having similar high proportions of SMBs and facing similar threats but in different environments. This is in part due to our study only including English publications, but it may also indicate that not enough attention is being paid to SMB cyber security in many countries, despite SMBs representing the backbone of the nations and the global economy.

Our results show that significant attention and effort has been made towards research around security strategies and policies for SMBs, however there appears to be only limited work in the areas of practical implementation, detection, response and recovery.

Researchers have recommended that a deeper analysis of how SMBs implement security controls is required [28]. Our study found a lack of quantitative data in SMB cyber security research. In future work researchers should adopt more powerful well-established quantitative research approaches to investigate SMB cyber security.

When considering the popular NIST CSF, our study found that research related to the cyber security of SMBs is focussed on aspects of information security policies and operational security. Topics relating to cyber security incident detection, response and recovery are hardly accounted for in past and current research. In Australia, 62% of small businesses have been a victim of a cyber-attack [11]. Given that past research has been mainly directed towards the prevention paradigms, researchers need to focus their work more on cyber resilience in order to ensure a more balanced approach to cyber prevention, response and recovery. Globally, governments should invest in incentivising research and initiatives to promote the resilience of SMBs. Cyber-attacks are inevitable, but when they do happen, SMBs should be able to respond and recover.

There is a need for governments and academic institutions to incentivise researchers to conduct more studies into SMB cyber security. The findings of our work can be used as guidance for researchers, academic and research institutions, governments and policy makers when selecting the focus of SMB cyber security research.

APPENDIX A

Table 5 lists the papers included in our study sorted by year of publication. It also shows the country of publication, methodology, data collection method used, as well as the NIST category that it fell under when analysed with our NCRCT tool.

REFERENCES

[1] A. Vives, "Social and environmental responsibility in small and medium enterprises in Latin America," (in English) *J. Corporate Citizenship*, vol. 2006, no. 21, pp. 39–50, Mar. 2006, doi: 10.9774/GLEAF.4700.2006.sp.00006.

[2] G. Gilfillan. *Small Business Sector Contribution to the Australian Economy*. Parliament of Australia. Accessed: Apr. 8, 2021. [Online]. Available: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1819/SmallBusinessSector

[3] Small Business. *What is an SME? Here's an SME Definition*. Accessed: Apr. 8, 2021. [Online]. Available: https://www.simplybusiness.co.uk/knowledge/articles/2021/05/what-is-an-sme/

[4] Organisation-for-Economic-Co-operation-and-Development. *OECD Glossary of Statistical Terms-Small and Medium-Sized Enterprises (SMEs)*. Accessed: Apr. 8, 2021. [Online]. Available: https://stats.oecd.org/glossary/detail.asp?ID=3123

[5] S. Ward. *What Are SMEs?*. Accessed: Apr. 8, 2021. [Online]. Available: https://www.thebalancesmb.com/sme-small-to-medium-enterprise-definition-2947962

[6] Australian-Bureau-of-Statistics. *Small Business in Australia, 2001*. Australian Bureau of Statistics. Accessed: May 13, 2021. [Online]. Available: https://www.abs.gov.au/ausstats/abs.nsf/mf/1321.0

[7] K. Renaud and G. R. S. Weir, "Cybersecurity and the unbearability of uncertainty," in *Proc. Cybersecurity Cyberforensics Conf. (CCC)*, Amman, Jordan, Aug. 2016, pp. 137–143, doi: 10.1109/CCC.2016.29.

[8] M. Heikkila, A. Rattya, S. Pieska, and J. Jamsa, "Security challenges in small- and medium-sized manufacturing enterprises," in *Proc. Int. Symp. Small-Scale Intell. Manuf. Syst. (SIMS)*, Narvik, Norway, Jun. 2016, pp. 25–30, doi: 10.1109/SIMS.2016.7802895.

[9] C. Onwubiko and A. P. Lenaghan, "Managing security threats and vulnerabilities for small to medium enterprises," in *Proc. IEEE Intell. Secur. Informat.*, New Brunswick, NJ, USA, May 2007, pp. 244–249, doi: 10.1109/ISI.2007.379479.

[10] L. Ponemon. *What's New in the 2019 Cost of a Data Breach Report*. Security Intelligence. Accessed: Jul. 12 2021. [Online]. Available: https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

[11] ACSC. *Small & Medium Businesses*. Australian Cyber Security Centre. Accessed: Aug. 12, 2020. [Online]. Available: https://www.cyber.gov.au/acsc/small-and-medium-businesses

[12] Better-Business-Bureau. *State of Cybersecurity Among Small Businesses in North America*. Accessed: May 10, 2021. [Online]. Available: https://www.bbb.org/stateofcybersecurity

[13] CISA. *Security Tip (ST04-001)*. Cybersecurity & Infrastructure Security Agency. [Online]. Accessed: Mar. 10, 2022. Available: https://www.cisa.gov/uscert/ncas/tips/ST04-001

[14] H. Suryotrisongko and Y. Musashi, "Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective," in *Proc. IEEE 12th Conf. Service-Oriented Comput. Appl. (SOCA)*, Kaohsiung, Taiwan, Nov. 2019, pp. 162–167, doi: 10.1109/SOCA.2019.00031.

[15] T. Tam, A. Rao, and J. Hall, "The good, the bad and the missing: A narrative review of cyber-security implications for Australian small businesses," (in English) *Comput. Secur.*, vol. 109, Oct. 2021, Art. no. 102385, doi: 10.1016/j.cose.2021.102385.

[16] A. Alahmari and B. Duncan, "Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (CyberSA)*, Dublin, Ireland, Jun. 2020, pp. 1–5, doi: 10.1109/CyberSA49311.2020.9139638.

[17] M. Syafrizal, S. R. Selamat, and N. A. Zakaria, "Analysis of cybersecurity standard and framework components," (in English) *Int. J. Commun. Netw. Inf. Secur.*, vol. 12, no. 3, pp. 417–432, 2020.

[18] J. F. Carias, M. R. S. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes, "Systematic approach to cyber resilience operationalization in SMEs," (in English) *IEEE Access*, vol. 8, pp. 174200–174221, 2020, doi: 10.1109/ACCESS.2020.3026063.

[19] S. Widup, D. Hylender, G. Bassett, P. Langlois, and A. Pinto, "Verizon: Data breach investigations report 2020," (in English) *Comput. Fraud Secur.*, vol. 2020, no. 6, p. 4, 2020, doi: 10.1016/S1361-3723(20)30059-2.

[20] M. Heidt, J. P. Gerlach, and P. Buxmann, "Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments," (in English) *Inf. Syst. Frontiers*, vol. 21, no. 6, pp. 1285–1305, Dec. 2019, doi: 10.1007/s10796-019-09959-1.

[21] M. Zec, "Cyber security measures in SMEs: A study of IT professionals organisational cyber security awareness," M.S. thesis, Dept. Technol., Linnaeus Univ., Växjö, Sweden, 2015.

[22] Y. Itai and E. Onwubiko, "Impact of ransomware on cybersecurity," *Int. J. Comput. Technol.*, vol. 17, no. 1, pp. 7077–7080, Jan. 2018.

[23] T. Tam, A. Rao, and J. Hall, "The invisible COVID-19 small business risks: Dealing with the cyber-security aftermath," *Digit. Government, Res. Pract.*, vol. 2, no. 2, pp. 1–8, Apr. 2021, doi: 10.1145/3436807.

[24] Marsh. *Global Cyber Risk Perception Survey Report 2019*. Accessed: Jun. 16 2021. [Online]. Available: https://www.marsh.com/uk/risks/global-risk/insights/global-risks-report-2021.html

[25] M. Bada and J. R. C. Nurse, "Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)," (in English) *Inf. Comput. Secur.*, vol. 27, no. 3, pp. 393–410, Jul. 2019, doi: 10.1108/ICS-07-2018-0080.

[26] P. A. H. Williams and R. J. Manheke, "Small business—A cyber resilience vulnerability," *Presented at the 1st Int. Cyber Resilience Conf.*, Perth, AU, USA, Aug. 2010, pp. 1–9.

[27] J. Hayes and A. Bodhani, "Cyber security: Small firms under fire," *Eng. Technol.*, vol. 8, no. 6, pp. 80–83, Jul. 2013, doi: 10.1049/et.2013.0614.

[28] T. McLaurin, "A study on the efficacy of small business cybersecurity controls," Ph.D. dissertation, College Bus., Innov., Leadership, Technol., Marymount Univ., ProQuest Dissertations Publishing, 2021.

[29] Office-of-the-Australian-Information-Commissioner. *Notifiable Data Breaches Report: July–December 2020*. Accessed: Apr. 5, 2021. [Online]. Available: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2020/

[30] IBM-Security. *Cost of a Data Breach Report 2020*. Accessed: Jun. 26, 2021. [Online]. Available: https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

[31] Ponemon-Institute. (2018). *State of Cybersecurity in Small & Medium-Sized Businesses (SMB)*. [Online]. Available: https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

[32] Verizon. (2016). *Data Breach Investigations Report*. [Online]. Available: https://conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/10/2016/10/2b_Verizon_Data-Breach-Investigations-Report_2016_Report_en_xg.pdf

[33] K. E. Krahl, "Cybersecurity and small to medium business," M.S. thesis, Utica College, ProQuest Dissertations Publishing, 2019.

[34] S. Keller, A. Powell, B. Horstmann, C. Predmore, and M. Crawford, "Information security threats and practices in small businesses," (in English) *Inf. Syst. Manag.*, vol. 22, no. 2, pp. 7–19, Mar. 2005, doi: 10.1201/1078/45099.22.2.20050301/87273.2.

[35] C. Valli, I. Martinus, and M. Johnstone, "Small to medium enterprise cyber security awareness: An initial survey of Western Australian business," *Presented at the Int. Conf. Secur. Manag.*, Las Vegas, Nevada, Jul. 2014, pp. 1–6.

[36] Z. Polkowski and J. Dysarz, "IT security management in small and medium enterprises," (in English) *Sci. Bull.-Econ. Sci.*, vol. 16, no. 3, pp. 134–148, 2017.

[37] Keeper-Security. (2019). *Global State of Cybersecurity in Small and Medium-Sized Businesses*. [Online]. Available: https://www.keeper.io/hubfs/PDF/2019%20Keeper%20Report%20V7.pdf

[38] Norton. *What Is A Botnet?*. Accessed: Apr. 8, 2021. [Online]. Available: https://au.norton.com/internetsecurity-malware-what-is-a-botnet.html

[39] Z. Walker. *Data Breaches and Small Businesses*. Rippleshot. Accessed: Apr. 3, 2021. [Online]. Available: https://info.rippleshot.com/blog/data-breach-small-businesses

[40] IBM-Security. (2019). *Cost of Data Breach Report*. [Online]. Available: https://www.ibm.com/account/reg/au-en/signup?formid=urx-42215

[41] Australian-Federal-Police. *Cybercrime*. Accessed: May 15, 2021. [Online]. Available: https://www.afp.gov.au/what-we-do/crime-types/cyber-crime#:~:text=Cybercrime%20offences%20are%20found%20in,including%20denial%20of%20service%20attacks

[42] J. Galvin. *60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack Here's How to Protect Yourself*. Accessed: May 15, 2021. [Online]. Available: https://www.Inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html

[43] NSW-Small-Business-Commissioner. (2017). *Cyber Aware*. Accessed: Jul. 6, 2021. [Online]. Available: https://www.smallbusiness.nsw.gov.au/sites/default/files/2019-07/Cyber-Aware-full-report.pdf

[44] C. Bucolo. *Get PCI Compliance Right the First Time*. PCI Compliance Guide. Accessed: Aug. 2, 2020. [Online]. Available: https://www.pcicomplianceguide.org/get-pci-compliance-right/

[45] R. F. I. V. Boese, "PCI DSS compliance challenges for small businesses," M.S. thesis, Utica College, ProQuest Dissertations Publishing, 2020, Art. no. 27672228.

[46] Ponemon-Institute. (2017). *State of Cybersecurity in Small & Medium-Sized Businesses (SMB)*. Keeper Security. [Online]. Available: https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html

[47] G. Lloyd, "The business benefits of cyber security for SMEs," (in English) *Comput. Fraud Secur.*, vol. 2020, no. 2, pp. 14–17, 2020, doi: 10.1016/S1361-3723(20)30019-1.

[48] B. Krebs. *Target Hackers Broke in Via HVAC Company*. Accessed: Aug. 8, 2021. [Online]. Available: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[49] A. House, "The price of a cybersecurity culture: How the CMMC should secure the department of defense's supply chain without harming small businesses and competition," (in English) *Public Contract Law J.*, vol. 50, no. 3, pp. 449–470, 2021.

[50] Reciprocity. *What is a Cybersecurity Framework?*. Accessed: Apr. 1, 2021. [Online]. Available: https://reciprocity.com/resources/what-is-a-cybersecurity-framework/

[51] National-Institute-of-Standards-and-Technology. *Evolution of the Framework*. Accessed: Jul. 23, 2021. [Online]. Available: https://www.nist.gov/cyberframework/evolution
[52] N. Kshetri, *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*. Switzerland: Springer, (in English), 2016.
[53] National-Institute-of-Standards-and-Technology. *New to Framework*. Accessed: Jul. 23, 2021. [Online]. Available: https://www.nist.gov/cyberframework/new-framework
[54] National-Institute-of-Standards-and-Technology. *NIST Releases Version 1.1 of its Popular Cybersecurity Framework*. Accessed: Aug. 2, 2021. [Online]. Available: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework
[55] A. Calder, *NIST Cybersecurity Framework: A Pocket Guide*. Ely, U.K.: IT Governance, 2018.
[56] National-Institute-of-Standards-and-Technology, *Fundamentals of Small Business Information Security*, 1st ed. U.S. Department of Commerce, Gaithersburg, Maryland, 2020, pp. 1–4. Accessed: Apr. 11, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
[57] National-Institute-of-Standards-and-Technology. *An Introduction to the Components of the Framework*. Accessed: Aug. 30, 2021. [Online]. Available: https://www.nist.gov/cyberframework/online-learning/components-framework
[58] C. Paulsen and P. Toth, "Small business information security: The fundamentals," U.S. Dept. Commerce, Gaithersburg, MD, USA, Tech. Rep. IR7621r1, 2016. Accessed: Jul. 10, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
[59] Australian-Cyber-Security-Centre. *Essential Eight Explained*. Australian Government. Accessed: Jul. 12, 2021. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/essential-eight
[60] Information Technology, Security Techniques, *Code of Practice for Information Security Management*, Int. Org. Standardization, Geneva, Switzerland, 2005.
[61] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for information security management," *J. Inf. Secur.*, vol. 4, no. 2, pp. 92–100, 2013. [Online]. Available: https://www.scirp.org/journal/paperinformation.aspx?paperid=30059
[62] (in English) *Information Technology—Security Techniques—Information Security Management Systems—Requirements*, Standard ISO 270001, 1st ed. Sydney, AU, USA: Standards Australia, 2015.
[63] T. Cornelius. *Understanding Cybersecurity & Privacy Best Practices*. Accessed: May 1, 2021. [Online]. Available: https://www.linkedin.com/pulse/understanding-cybersecurity-privacy-best-practices-tom-cornelius/
[64] Compliance-Forge. *NIST 800-53 vs ISO 27002 vs NIST CSF*. Accessed: Jun. 10, 2021. [Online]. Available: https://www.complianceforge.com/faq/nist-800-53-vs-iso-27002-vs-nist-csf.html
[65] D. Tranfield, D. Denyer, and P. Smart, "Towards a methodology for developing evidence-informed management knowledge by means of systematic review," in English *Brit. J. Manag.*, vol. 14, no. 3, pp. 207–222, Sep. 2003, doi: 10.1111/1467-8551.00375.
[66] M. J. Grant and A. Booth, "A typology of reviews: An analysis of 14 review types and associated methodologies," (in English) *Health Inf. Libraries J.*, vol. 26, no. 2, pp. 91–108, Jun. 2009, doi: 10.1111/j.1471-1842.2009.00848.x.
[67] A. Asti, "Cyber defense challenges from the small and medium-sized business perspective," GIAC Certifications, SANS Inst., 2017, p. 16, Art. no. 38160. [Online], Available: https://www.giac.org/research-papers/38160/
[68] Deloitte. *Connected Small business 2017*. Deloitte Access Economics. Accessed: Jul. 14, 2021. [Online]. Available: https://www2.deloitte.com/au/en/pages/economics/articles/connected-small-businesses-google.html
[69] J. Borenstein. *Overview of the Marsh-Microsoft 2019 Global Cyber Risk Perception survey results*. Accessed: Aug. 5, 2020. [Online]. Available: https://www.microsoft.com/security/blog/2019/09/18/marsh-microsoft-2019-global-cyber-risk-perception-survey-results
[70] E. Rohn, G. Sabari, and G. Leshem, "Explaining small business InfoSec posture using social theories," (in English) *Inf. Comput. Secur.*, vol. 24, no. 5, pp. 534–556, Nov. 2016, doi: 10.1108/ICS-09-2015-0041.
[71] S. Kabanda, M. Tanner, and C. Kent, "Exploring SME cybersecurity practices in developing countries," (in English) *J. Organizational Comput. Electron. Commerce*, vol. 28, no. 3, pp. 269–282, Jul. 2018, doi: 10.1080/10919392.2018.1484598.
[72] M. Grevey. *Survey: How Prepared are Small Business Owners for Cyber Attacks*. Experian. Accessed: Apr. 1, 2021. [Online]. Available: https://www.experianpartnersolutions.com/2016/05/survey-how-prepared-are-small-business-owners-for-cyber-attacks/
[73] Office-of-the-Australian-Information-Commissioner. *What is Personal Information?*. Accessed: Jul. 13, 2021. [Online]. Available: https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/
[74] N. K. Sangani, P. Velmurugan, T. Vithani, and M. Madiajagan, "Security & privacy architecture as a service for small and medium enterprises," in *Proc. Int. Conf. Cloud Comput. Technol., Appl. Manag. (ICCCTAM)*, Dubai, United Arab Emirates, Dec. 2012, pp. 16–21, doi: 10.1109/ICCCTAM.2012.6488064.
[75] D. J. Fehér, "Cybersecurity threats of cloud and third-party services in small and medium-sized enterprise environment," in *Proc. 8th Int. Conf. Manag., Enterprise, Benchmarking*, 2020, pp. 36–41.
[76] D. Bhattacharya, "Evolution of cybersecurity issues in small businesses," in *Proc. 4th Annu. ACM Conf. Res. Inf. Technol.*, New York, NY, USA, Sep. 2015, p. 11, doi: 10.1145/2808062.2808063.
[77] E. Osborn and A. Simpson, "Risk and the small-scale cyber security decision making dialogue—A U.K. case study," (in English) *Comput. J.*, vol. 61, no. 4, pp. 472–495, Apr. 2018, doi: 10.1093/comjnl/bxx093.
[78] C. Paulsen, "Cybersecuring small businesses," (in English) *Computer*, vol. 49, no. 8, pp. 92–97, Aug. 2016, doi: 10.1109/MC.2016.223.
[79] J. C. Beachboard, A. Cole, M. Mellor, S. Hernandez, K. Aytes, and N. Massad, "Improving information security risk analysis practices for small- and medium-sized enterprises: A research agenda," (in English) *J. Issues Informing Sci. Inf. Technol. Educ.*, vol. 5, pp. 73–85, Jan. 2008, doi: 10.28945/996.
[80] K. Carnell. *Cyber Security a Growing Issue for Small Business*. Accessed: Aug. 8, 2021. [Online]. Available: https://www.asbfeo.gov.au/news/news-articles/cyber-security-growing-issue-small-business
[81] E. M. Raineri and J. Resig, "Evaluating self-efficacy pertaining to cybersecurity for small businesses," (in English) *Appl. Bus. Econ.*, vol. 22, no. 12, pp. 13–23, 2020.
[82] J. Patterson, "Cyber-security policy decisions in small businesses," Ph.D. dissertation, College Manag. Technol., Walden Univ., Minneapolis, MN, USA, 2017.
[83] V. Burton-Howard, "Protecting small business information from cyber security criminals: A qualitative study," Ph.D. dissertation, Colorado Tech. Univ., ProQuest Dissertations Publishing, 2018, Art. no. 10928879.
[84] N. Rawindaran, A. Jayal, and E. Prakash, "Machine learning cybersecurity adoption in small and medium enterprises in developed countries," (in English) *Computers*, vol. 10, no. 11, p. 150, Nov. 2021, doi: 10.3390/computers10110150.
[85] K. D. Cook, "Effective cyber security strategies for small businesses," Ph.D. dissertation, College Manag. Technol., Walden Univ., Minneapolis, MN, USA, ProQuest Dissertations Publishing, 2017.
[86] L. L. Bryan, "Effective information security strategies for small business," *Int. J. Cyber Criminology*, vol. 14, no. 1, pp. 341–360, Jan. 2020.
[87] A. Santos-Olmo, L. Sánchez, I. Caballero, S. Camacho, and E. Fernandez-Medina, "The importance of the security culture in SMEs as regards the correct management of the security of their assets," (in English) *Future Internet*, vol. 8, no. 4, p. 30, Jul. 2016, doi: 10.3390/fi8030030.
[88] C. T. Berry and R. L. Berry, "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, 2018, doi: 10.1504/IJBCRM.2018.090580.
[89] L. Clozel, "Banks get (yet another) cybersecurity framework, this time from G-7," American Banker, 2016, no. 196. [Online]. Available: https://www.proquest.com/newspapers/banks-get-yet-another-cybersecurity-framework/docview/1828205806/se-2
[90] K. Renaud, "How smaller businesses struggle with security advice," (in English) *Comput. Fraud Secur.*, vol. 2016, no. 8, pp. 10–18, 2016, doi: 10.1016/S1361-3723(16)30062-8.
[91] Hiscox. (2019). *Hiscox Cyber Readiness Report*. Hiscox, Bermuda. [Online]. Available: https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF
[92] R. D. Feagin, "The value of cyber security in small business," M.S. thesis, Utica College, Utica, NY, USA, ProQuest Dissertations Publishing, 2015, Art. no. 1599731.
[93] J. Hogg, "Analyzing and mitigating cybersecurity risks faced by small businesses," M.S. thesis, Utica College, Utica, NY, USA, ProQuest Dissertations Publishing, 2014.

[94] U. Kaila, "Information security best practices: First steps for startups and SMEs," (in English) *Technol. Innov. Manag. Rev.*, vol. 8, no. 11, pp. 32–42, Nov. 2018, doi: 10.22215/timreview/1198.
[95] C. Valli, "A survey of lawyers cyber security practices," *Brief*, vol. 44, no. 10, pp. 34–35, 2017.
[96] J. A. Saber, "Determining small business cybersecurity strategies to prevent data breaches," Ph.D. dissertation, College Manag. Technol., Walden Univ., Minneapolis, MN, USA, 2016.
[97] W. Barosy, "Successful operational cyber security strategies for small businesses," Ph.D. dissertation, College Manag. Technol., Walden Univ., Minneapolis, MN, USA, ProQuest Dissertations Publishing, 2019.
[98] T. Al-Jumaili, "Exploring the information security policies and practices required by small and medium-sized IT enterprises," Ph.D. dissertation, Colorado Tech. Univ., Colorado Springs, CO, USA, ProQuest Dissertations Publishing, 2018, Art. no. 10975031.
[99] S. Armenia, M. Angelini, F. Nonino, G. Palombi, and M. F. Schlitzer, "A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs," (in English) *Decis. Support Syst.*, vol. 147, Aug. 2021, Art. no. 113580, doi: 10.1016/j.dss.2021.113580.
[100] M. Benz and D. Chatterjee, "Calculated risk? A cybersecurity evaluation tool for SMEs," (in English) *Bus. Horizons*, vol. 63, no. 4, pp. 531–540, Jul. 2020, doi: 10.1016/j.bushor.2020.03.010.
[101] J. Coertze, J. van Niekerk, and R. von Solms, "A web-based information security management toolbox for small-to-medium enterprises in Southern Africa," in *Proc. Inf. Secur. South Africa*, vol. 2, no. 11. Johannesburg, South Africa: IEEE, 2011, pp. 1–8, doi: 10.1109/ISSA.2011.6027515.
[102] A. Emer, M. Unterhofer, and E. Rauch, "A cybersecurity assessment model for small and medium-sized enterprises," (in English) *IEEE Eng. Manag. Rev.*, vol. 49, no. 2, pp. 98–109, Jun. 2021, doi: 10.1109/EMR.2021.3078077.
[103] *Framework for Improving Critical Infrastructure Cybersecurity*, National-Institute-of-Standards-and-Technology, Gaithersburg, MD, USA, Apr. 16, 2018, doi: 10.6028/NIST.CSWP.04162018.
[104] L. Mercl and J. Horalek, "SIEM implementation for small and mid-sized business environments," *J. Eng. Appl. Sci.*, vol. 14, no. 9, pp. 10497–10501, Jan. 2020, doi: 10.36478/jeasci.2019.10497.10501.
[105] F. Alharbi, M. Alsulami, A. Al-Solami, Y. Al-Otaibi, M. Al-Osimi, F. Al-Qanor, and K. Al-Otaibi, "The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia," (in English) *Sensors*, vol. 21, no. 20, p. 6901, Oct. 2021.
[106] M. S. Gordon, "Economic and national security effects of cyber attacks against small business communities," M.S. thesis, Utica College, Utica, NY, USA, ProQuest Dissertations Publishing, 2018, Art. no. 10935780.
[107] *Resilience*, Merriam-Webster.com Dictionary, Merriam-Webster, Springfield, MA, USA, 2020.
[108] J. Pamula, S. Jajodia, P. Ammann, and V. Swarup, "A weakest-adversary security metric for network configuration security analysis," in *Proc. 2nd ACM Workshop Quality Protection (QoP)*, New York, NY, USA, 2006, pp. 31–38, doi: 10.1145/1179494.1179502.
[109] D. W. A. Hubbard and R. A. Seiersen, *How to Measure Anything in Cybersecurity Risk*. Hoboken, NJ, USA: Wiley, 2016.
[110] S. Ouaftouh, A. Zellou, and A. Idri, "User profile model: A user dimension based classification," in *Proc. 10th Int. Conf. Intell. Syst., Theories Appl. (SITA)*, Rabat, Morocco, Oct. 2015, pp. 1–5, doi: 10.1109/SITA.2015.7358378.
[111] J. A. Iglesias, P. Angelov, A. Ledezma, and A. Sanchis, "Creating evolving user behavior profiles automatically," (in English) *IEEE Trans. Knowl. Data Eng.*, vol. 24, no. 5, pp. 854–867, May 2012.
[112] M. Balnaves and P. Caputi, *Starting the Inquiry: But What Happened then?*. London, U.K.: SAGE, 2001.
[113] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel, "Quantitative cyber risk reduction estimation methodology for a small SCADA control system," in *Proc. 39th Annu. Hawaii Int. Conf. Syst. Sci. (HICSS)*, Kauai, HI, USA, 2006, p. 226, doi: 10.1109/HICSS.2006.405.
[114] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," (in English) *Comput. Secur.*, vol. 56, pp. 1–27, Feb. 2015.
[115] T. W. A. Edgar and D. O. A. Manz, *Research Methods for Cyber Security*. Cambridge, MA, USA: Elsevier, 2017.
[116] B. Pritha. *What Is Quantitative Research? | Definition, Uses & Methods*. Accessed: May 22, 2021. [Online]. Available: https://www.scribbr.com/methodology/quantitative-research/
[117] R. Baskerville, P. Spagnoletti, and J. Kim, "Incident-centered information security: Managing a strategic balance between prevention and response," (in English) *Inf. Manag.*, vol. 51, no. 1, pp. 138–151, Jan. 2014, doi: 10.1016/j.im.2013.11.004.
[118] D. Eilts, "An empirical assessment of cybersecurity readiness and resilience in small businesses," Ph.D. dissertation, College Comput. Eng., Nova Southeastern Univ., Fort Lauderdale, FL, USA, ProQuest Dissertations Publishing, 2020, Art. no. 27831857.
[119] E. L. Opitz, "Cybersecurity for the board of directors of small and midsized businesses," (in English) *Board Leadership*, vol. 2018, no. 159, pp. 4–5, Sep. 2018, doi: 10.1002/bl.30115.
[120] Canon. *The Canon Business Readiness Index—Security*. Accessed: Jul. 20, 2021. [Online]. Available: https://www.canon.com.au/business insights/business-readiness-index-2018-security
[121] I. Pagura, "Law report: Small business and cyber security," *J. Austral.-Traditional Med. Soc.*, vol. 26, no. 1, pp. 38–39, 2020.
[122] G. Gilead, "Managing cybersecurity governance," *Governance Directions*, vol. 71, no. 5, pp. 267–270, 2019.
[123] M. Nycz, M. J. Martin, and Z. Polkowski, "The cyber security in SMEs in Poland and Tanzania," in *Proc. 7th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*, Jun. 2015, pp. 25–27, doi: 10.1109/ECAI.2015.7301182.

ALLADEAN CHIDUKWANI was born in Gokwe, Zimbabwe, in 1983. He received the Advanced Diploma degrees in information technology and technology education from the Chinhoyi University of Technology, Chinhoyi, Zimbabwe, in 2004 and 2005, respectively, and the master's degree in IT management from Murdoch University, Perth, WA, in 2017, where he is currently pursuing the Ph.D. degree in cyber security. From 2006 to 2020, he has worked in numerous roles, including a network systems administrator, a technical it trainer, an assistant training manager, a technology training officer, and an IT security consultant. He provides cyber security mentoring for small-medium-businesses through an Australian government funded project delivered by Belmont Enterprise Centre. He also casually lectures the cyber security bootcamp course at The University of Western Australia as well as penetration testing courses at the Australian Government's Vocational Education Training (VET) Institution South Metro TAFE. His research interest includes cyber security in small-to-medium sized businesses. He is a member of the Australian Information Security Association (AISA). He is also a Technical Reviewer for Packt Publishing's CompTIA Server + and Security + books.

SEBASTIAN ZANDER received the Ph.D. degree in telecommunications engineering from the Swinburne University of Technology, Australia, in 2010. He is currently a Lecturer at Murdoch University. Previously, he has worked as a Research Fellow at the Swinburne University of Technology and a Scientist at Fraunhofer FOKUS, Germany. He has coauthored the Wiley book *Information Hiding in Communication Networks*, over 50 peer-reviewed journal and conference papers, two IETF RFCs, and one patent held by Hitachi Ltd. His research interests include cyber security and networking, in particular information hiding and covert channels, network traffic classification, network measurement, transport protocols, and IPv6.

POLYCHRONIS KOUTSAKIS (Senior Member, IEEE) received the Ph.D. degree in electronic and computer engineering from the Technical University of Crete, Greece. From July 2006 to December 2008, he was an Assistant Professor at the Electrical and Computer Engineering Department, McMaster University, Canada. In January 2009, he joined the School of Electronic and Computer Engineering, Technical University of Crete, where he received tenure as an Associate Professor, in 2014. In January 2016, he joined Murdoch University. He has authored more than 120 peer-reviewed papers and is the co-inventor of one U.S. patent acquired by Blackberry Ltd. He has been honored three times as an Exemplary Editor of the IEEE Communications Society, for his work as an Editor of the IEEE Communications Surveys and Tutorials journal. He has served as the General Chair for the IEEE WoWMoM 2018.