Not all SMEs are the same: Categorizing Security Needs of SMEs

Murray E. Jennex
West Texas A&M University
mjennex@wtamu.edu

Jeffry Babb
West Texas A&M University
jbabb@wtamu.edu

Amjad Abdullat
West Texas A&M University
aabdullat@wtamu.edu

Abraham Abby Sen
West Texas A&M University
aabbysen@wtamu.edu

Kareem Dana
West Texas A&M University
kdana@wtamu.edu

Abstract

This paper presents a novel categorization and maturity model for Small and Micro Enterprises (SMEs), designed to address their unique cybersecurity challenges. Based on a detailed analysis of 40 cybersecurity audits, the proposed model categorizes SMEs into five levels of IS/IT usage: Basic, Minimal, Competitive, Integrated, and Strategic. Each level identifies specific risks, threats, knowledge requirements, and cybersecurity controls, providing a clear roadmap for SMEs to enhance their cybersecurity maturity. The model not only simplifies cybersecurity evaluation for non-technical SME owners but also equips auditors with a standardized framework for assessing preparedness This study makes significant theoretical contributions by extending maturity model literature to the SME context, emphasizing the socio-technical interplay of technology adoption and organizational readiness. Practically, it provides actionable guidance for resource allocation, promotes proactive cybersecurity cultures, and fosters ecosystem collaboration through partnerships with universities and Managed Service Providers (MSPs). These collaborations offer SMEs cost-effective access to expertise, training, and advanced tools, enabling them to mitigate vulnerabilities and ensure compliance with regulatory standards. The findings emphasize the growing importance of addressing SME-specific cybersecurity needs, particularly in critical sectors such as healthcare and childcare. Future research will focus on incorporating emerging technologies, such as AI and IoT, and expanding the model's applicability to diverse geographic and industrial contexts.

Keywords: cybersecurity, SME, maturity models, university partnerships, IS/IT usage, regulatory compliance

Introduction

In 2004 Jennex, et al. (2004) and Dimopoulos, et al. (2004) identified several reasons to explain why Small and Medium Enterprises, SMEs, under performed on their cybersecurity programs when compared to larger organizations. The consensus was that SMEs don't have the resources or knowledge to tackle both their information systems needs and their cybersecurity needs. Jennex and Babb (2024) found that SMEs still have a lack of resources and knowledge based on a study on the results from 40 cybersecurity audits of SMEs. However, it was also noticed that the subject SMEs had various levels of IS/IT in their organizations and various levels of IS support. A quick review of cybersecurity frameworks from NIST, ISO, and academia found that they are based on analyzing organizational risk and the identification of sets of controls. While these are good frameworks, they aren't real easy for non-cybersecurity specialists to apply to their organizations. They are best for large and medium organizations, but not so good for small and micro organizations, leading this paper to redefine SME as Small and Micro Enterprises. Given that SME organizations tend to have limited resources and knowledge, it is our position that an easier way of judging SME cybersecurity preparedness needs to be developed. This paper reviews the data from Jennex and Babb (2024) to determine and propose a maturity model/scale that is easy for SME owners/operators to review, understand, and apply. Also, this maturity model/scale needs to be easy for cybersecurity auditors to utilize to develop audit plans and determine cybersecurity preparedness.

Literature Review

SME Cybersecurity Research

This section examines recent research with respect to SMEs (note that this literature uses the traditional definition of SME). A common theme found within the literature is that the threats and risks that SMEs encounter are on the rise while, at the same time, many SMEs are underwired and not cognizant of these increasing threats and risks. The consequence of this misalignment is that, for many SMEs, a significant breach or attack will lead to that business' failure. Many researchers have concluded relatively simple ameliorations such as further threat and risk training is needed. However, most studies, including our own, have found that SMEs lack knowledge and resources to adequately address the increasing threats and risks. Other sources have suggested that audits, similar to those conducted in this study, bring illumination and attention cybersecurity has a positive impact on helping an SME better prepare itself to protect its network and data/information/knowledge assets.

SMEs are increasingly being targeted by cyber-attacks (Bada and Nurse, 2019) where a major issue for SMEs is in providing cybersecurity awareness training to their employees. Bada and Nurse (2019) provide a framework for SME cybersecurity training and awareness programs based off a case study done by the London Digital Security Centre (LDSC). The LDSC also proposed self-evaluation similar to the cyber security audits done for this paper as a part of their framework (Bada and Nurse, 2019). In their work, Bada and Nurse (2019) found that the LDSC improved cyber security outcomes for the SMEs they assisted with their program.

Auyporn, et al. (2020) identified factors that influenced the implementation of cybersecurity in an organization. These factors include available resources, cybersecurity awareness, knowledge, having a risk management culture, and management support internal to the organization. They also identified external factors such as external threats, industry readiness, and the legal/regulatory environment as influencing the organization in implementing cybersecurity.

Kajiyama, et al. (2017) and Nagahawatta, et al. (2021) found that cyber security concerns within SMEs can influence SME decision-making with respect to the adoption of cloud computing. These cybersecurity concerns can limit SMEs' the ability to expand and potentially benefit from cloud computing technologies to further innovate their processes. This is among the examples that demonstrate how limited knowledge resources within SMEs prevents many SMEs from leveraging the benefits of new innovations.

Chidukwani, et al. (2022) found that that attackers have now focused on SMEs as a target due to their belief that SMEs are ill prepared and under protected (e.g. easy marks): many SMEs are either unaware or not well resourced to fortify their networks and information resources. Additionally, Chidukwani, et al. (2022) reviewed recent research on the cyber security of SMEs, with a focus on the alignment of this research to the popular NIST Cyber Security Framework (CSF). From the literature they found that most

of the qualitative guidelines employed failed to effectively address issues associated with SMEs. Their conclusion was that SMEs need more concrete and actionable guidance on how to address cyber security issues in ways that are immediately implementable and actionable, and they encourage that future research focus on SME cyber security issues.

Alahmari and Duncan (2020) found that while SMEs have been encouraged to take advantage of any possible business opportunities by utilizing and adopting new technologies such as cloud computing services, significant misunderstanding of cyber security threats from the management perspective remains an impediment to effective use. Underestimation of cybersecurity threats by SMEs leads to a propensity to employ strategies that increase exposure to vulnerabilities and risks, which often exacerbate challenges inherent to SMEs, their partners, and their affiliates. Jennex, et al. (2022) found that COVID-19 further amplified these risks as businesses, including SMEs, rapidly adopted new technologies in order to sustain operations, often ignorant of the risks involved in adopting those technologies.

Antunes, et al. (2021) discuss an information security and cybersecurity management project, based on the ISO-27001:2013 standard, that was designed and implemented in fifty SMEs located in the center region of Portugal. The project was conducted by a business association located in central Portugal, assisted by the Polytechnic of Leiria and an IT auditing/consulting team. The project resulted in improved cyber security in the participating organizations.,

Alharbi, et al. (2021) measured the effectiveness of security practices at SMEs in Saudi Arabia in the event of a cybersecurity attack. A total of 282 respondents were used to measure the effectiveness of 12 cybersecurity practices in three aspects: financial damage, loss of sensitive data, and restoration time. Their findings indicate that having an inspection team and a recovery plan may limit the financial damage caused by cybersecurity attacks on SMEs. The results also show that cybersecurity awareness, knowledge of cybersecurity damage, and professionals' salaries were related to the loss of sensitive data. Furthermore, the results indicate that contact with cybersecurity authorities and having an inspection team have statistically significant effects on restoration time.

Ashley and Preiksaitis (2022) found that the number of cyberattacks affecting United States SMEs has increased substantially; with an average per-breach loss of $500,000 USD. Cyber-breaches most often result in business closure within six months of the breach. They found that awareness training was critical to surviving a data breach and proposed other strategies to help SMEs focus attention on cyber security.

Finally, while all the above are finding increasing risk and threats to SMEs, Wilson, et.al. (2023) found that SMEs; in an online survey of 85 U.K-based SMEs that explored their threat and coping appraisals toward five common types of cyber-attack: Network being hacked; Data being stolen or encrypted; malware infection; mobile devices being compromised; and phishing e-mail attack; were not concerned. Overall, SMEs' reported assessment of the risk of an attack was low, particularly for the possibility of their business network being hacked or their data being stolen or encrypted. However, while they believed the risks to be low, they reported that the impact would be high.

Categorizing SMEs for Cybersecurity

Pawar and Palivela (2022) used a survey of one hundred and fifteen SMEs to understand the current cybersecurity controls implementation posture for different SMEs, along with the challenges faced during the planning and implementing of these cybersecurity controls. The challenges identified by Pawar and Palivela (2022) include: lack of financial resources, inability to reconcile appropriate and suitable cybersecurity controls, and lack of skilled resources. To assist SMEs, they propose the use of their Least Cybersecurity Control Implementation (LCCI) framework. The framework is based on identifying the most critical asset for a SME, then determining the minimum overall cybersecurity controls implementation for the SME to ultimately determine the least cybersecurity controls necessary to support defense in depth to meet confidentiality, integrity, and availability (CIA), priorities.

Carias, et al. (2020) created a cybersecurity resilience framework that cyber synthesized SME cybersecurity into 10 domains and 32 policies for SMEs to follow and implement. This framework did not differentiate between different types of SMEs.

Eilts (2020) created a taxonomy for assessing SME cybersecurity preparedness by classifying the SME based on its business continuity preparedness.

Perozzo, et al. (2021) proposed a Cybersecurity Readiness Model (CSRM) based on a Socio-Technical view of organizations. Factors looked at were company size, leadership, technical skills possessed, tangible or intangible product, degree of servitization, dependence on third parties, current availability of protection systems, and legal environment. The model was tested on three Italian companies.

Van Haastrecht, et al. (2021) also proposed a socio-technical SME cybersecurity model where organizations were classified as: startups, digitally dependent, digitally based, and digital enablers. This model was based on literature review.

De Arroyabe, et al. (2023) investigated cybersecurity resilience in SMEs, focusing on three key aspects: the capacity to handle potential cyber incidents, the ability to recover from such incidents, and the capability to adapt in the face of possible cyber threats. The study utilized a survey of 239 UK SMEs. Key findings were the lack of SMEs' engagement with the management of cybersecurity and finds cybersecurity incidents to be the most important factor in driving resilience, as compared to cybersecurity capabilities.

Shojaifar and Järvinen, (2021) realizes that SMEs are not homogenous and created a classification scheme using five SME types based on their characteristics and specific security needs: cybersecurity abandoned SME, unskilled SME, expert-connected SME, capable SME, and cybersecurity provider SME. The framework proposes solutions for each class to approach cybersecurity awareness and competence more consistent with SME needs. This framework takes a similar approach to that used in the framework proposed by this paper. Differences will be discussed later.

Maturity Model Literature

A maturity model describes how organizational processes might grow and appreciate over time such that their effectiveness increases. These are models that usually focus on describing ideal maturity pathways for processes where a measurement approach to validate the improvements is common. Maturity models can be described as a risk management approach designed to increase reliability and predictability of the outputs or outcomes for a given business process. From an IS perspective, maturity models provide a means of both a quantitative and qualitative understanding of the sociotechnical structures of organizational effectiveness where that effectiveness is described as a function of processes and operations (Mettler, 2011).

The subject-matter of maturity models remains timely as it is common for both practitioners and researchers find them useful. The paper exams what the literature tells us about the evolution and adoption of maturity models (Becker et al., 2010; Mettler and Ballester, 2021). Whereas the impetus for maturity model uptake has been characterized as related to the perturbations and waves of diffused innovations and related disruptions (Röglinger et al., 2012), there are likely deeper and broader change and culture issues that lie at the heart of the appeal and uptake of maturity modeling. Usually, inflection points related to desired (or undesired) environmental change present the need or opportunity to reevaluate operations and engagement in the sensemaking that underlies the capture, description, analysis and improvement in business processes. Such an approach allows for a reflective and evaluative appraisal of the organizational and technological advance that characterizes the very nature of information systems (Poeppelbuss et al., 2011). SMEs dwell within the midst of information systems and are ensconced within them in both an overt and covert manner. The literature on maturity models provides some guidance on how an iteration and evolution of this comprehension is possible.

To suggest a maturity model perspective in the case of SME cybersecurity may not be without controversy and the very topic of maturity modeling is not universally embraced (Mettler and Ballester, 2021). There are also scholarly treatments designed to develop comprehensive understanding of maturity models that can be useful. The cases described in this manner are consistent with other scholars' characterization of maturity modeling as being socio-technical in nature and justly situated within the IS discipline (Mettler and Ballester, 2021). In the case of SME cybersecurity, should exact prescriptions be lacking in this work, maturity models are offered for consideration as a generative metaphor designed to highlight why the exploration for maturity models for SME Cybersecurity is a worthwhile endeavor (Schön, 1979).

The strength of maturity modeling is its foundations as being practice-driven an amenable as a complement to empirical scholarly work. In the case of SME Cybersecurity, maturity modeling is an approach that may assist in the discovery of how policy and operational controls can be understood in terms of SME comprehension and sensemaking of their current and potential future state. The

opportunity with respect to the findings of this study exists where maturity models typical adopt both a practitioner and managerial/organizational viewpoint. At issue at times, is whether harmony can be struck between our theoretical understanding of maturity modeling with the pragmatic and prescriptive aspects of maturity models. If a maturity model is simply a snapshot of a current state, then their utility to demonstrate the investments and costs of growth are somewhat stilted.

Another issue here is that maturity models require some design and that design should have ample subject matter and domain experts as authors. Whereas over all expertise in Cybersecurity increasingly resides within the realm of certified expertise, the confluence of this expertise along with domain expertise is a core challenge. For this reason, any maturity modeling to provide an improved framework for SMEs to navigate their Cybersecurity challenges stands to be a fractured and fragmented effort. One approach is to consider the need to develop and use a domain specific language from which the basis of maturity model development and comprehension may develop. While domain specific language development has some formalism (Kosar et al., 2008), again we offer the domain specific language as a supportive concept to underscore the necessity of the infusion of domain expertise and Cybersecurity expertise should any maturity modeling effort be considered.

Becker et al. (2009) provide a process for the development of maturity models whose steps provide a reasonable basis for why this paper recommends a maturity model approach as a next step in developing and strengthening provisions of Cybersecurity management for SMEs. Overall, Becker et al. (2009 make the case that maturity models, and the process for their development, hold potential to develop exploratory and explanatory power for comprehension and sense-making of emergent phenomena. This affords to conceptualize that maturation is a process of comprehension and action-planning. From a scholarly sense-making perspective, maturity models are more commonly conceived, developed, and adopted as technically rational instruments (Poeppelbuss et al., 2011) rather than a learning process of the type that Argyris and Schon (1997) describe as "organizational learning." Of course, in your treatment of relevance, you site the utility of a maturity model exactly for comprehension. Our recommendation to consider maturity models as a next step are less motivated as checklist/process guides and more as opportunities for self-appraisal and awareness on the part of the SME. However, without adequate Cybersecurity and SME partnerships, it is likely that only the technically rational elements of any maturity model would be utilized.

We realize maturity modeling as a learning system, a maturity modeling approach would advocate, much as has been the case with Agile methods, that maturity model designers and users are cast as reflective practitioners (Schön, 2017; Babb et al., 2014). This is so as those effectively using a maturity model would likely be operating from generalizations and abstractions of tacit knowledge gained from experience. In this manner, it can be argued that the elements of maturity models become a "design pattern" to characterize and spot familiar aspects in emergent phenomena (Gamma et al. 1994).

Becker et al. (2009) offer a few guidelines for the overall design considerations and concerns of maturity modeling, from these, we can perhaps understand how a maturity modeling approach may be helpful as a future step and in response to the outcomes of the research findings of this paper.

Methodology

Jennex and Babb (2024) analyzed 40 cybersecurity audits on SMEs to identify common issues in SMEs. The audits were conducted by students following a standard methodology and audit plan. The subjects of the audits were a variety of SMEs and were selected by the students based on availability and familiarity. Issues were identified by how many SMEs had the issue.

During the analysis in Jennex and Babb (2024) it was noticed that there was a great variety of types of SME organizations that were audited. The analysis identified the categories of SMEs as follows (numbers in parentheses are the number of SMEs audited in the category):

- Small professional office (financial/tax/law) (12)
- Small retail (gas station, café, pawn broker, etc.) (10)
- Small services provider (non-professional) (4)
- Small manufacturing (3)
- Healthcare/daycare (3)

- Church/Church bookstore (3)
- Apartment complex (2)
- Car/trailer dealership (2)
- Nonprofit (1)

Additionally, Jennex and Babb (2024) were able to determine that 11 of the 40 (27.5%) audit clients had at least one full time IT/IS support person. We also determined that 3 of the 40 (7.5%) had more than one full time IT/IS support person. The remainder, 29 of 40 (72.5%) had a combination of part time support, contract support (for special functions), and did the IT/IS support themselves. The issues, level of IS/IT support, and the types of SMEs led to the research question of if there was an easier and more logical way of categorizing SMEs and cybersecurity needs. To answer this question, we reviewed the previous findings while also considering the audit reports to find patterns in SMEs that could lead to a classification framework.

To check how well the model fits it was compared to the results of 21 SME audits performed in the fall, 2024 semester by cybersecurity students. Comparison was done by using a survey administered to the audit performers. The survey was created based on the model without mentioning the model. A review of the survey results showed that the model was basically okay but a few modifications were made with respect to the basic technologies being used to define the different levels.

Additionally, the audit survey collected information on the organizations with respect to employee numbers and revenue, threats and risks observed, and security knowledge needed by the organizations.

Results

The analysis identified a categorization scheme/ maturity model based on the IS/IT used by the SME consisting of five levels with each level defined by the IS/IT used by the SME for business. The five levels with their associate risk level are:

1. Basic: This level uses basic/ubiquitous IS/IT that any individual could be using. SME may use any of the following: phones, email, cloud-based storage (such as one drive and drop box), IoT based devices (such as cameras, ring door cameras) personal Bluetooth devices (such as headphones), and personal computer connected to the Internet (including any software such as Microsoft Office and AI enhanced tools built into the browser and personal computer software). The organization has minimal IS/IT support, usually a part time support person. Overall, risk very low and is commensurate to what a connected household would see.
2. Minimal: This level expands basic IS/IT usage to provide some business support by including payment systems. SME may use any of the same technologies as the Basic level, plus a payment system or basic point of sale system including card readers, network support, data processing and storage (which may be supplied/managed by a 3rd party vendor). Overall, risk is low including low supplier risk.
3. Competitive: This level expands IS/IT usage to include the software/tools needed to enhance organizational effectiveness and competitiveness. SME may use the technologies from the Basic and Minimal levels, plus packaged or custom bought systems such as ERP, CRM, AI, managed web sites, vendor apps, expanded network support, etc. Overall risk is medium including third party and expanded network risk.
4. Integrated: This level expands IS/IT usage to include in-house built IS/IT systems that can support competitive advantages. SME may use any of the technologies from the Basic, Minimal, and Competitive levels, plus customer data is being used strategically and the organization may create and manage its own apps (including AI) and web sites. Overall, risk is high including third party/supplier risk and risk introduced by internal system development.
5. Strategic: This level relies on IS/IT for sustained competitive advantage and market position. SME may use technologies from the Basic, Minimal, Competitive, and Integrated levels plus it may rely on cutting edge technologies such as custom purchased or internally developed AI tools/applications, data is used to create information/knowledge to manage the organization and/or support clients/customer. Additionally, the SME may be subject to special cybersecurity requirements such as HIPAA, GDPR, etc. Overall, risk is very high due to

cutting edge technology use and unknown risk, expanded network use, internal use of customer data, legal risk, and third party/supplier risk.

The full model is shown in Table 1, SME levels and descriptions, risks, threats and risk level, and Table 2, SME Knowledge needs, IS/IT support, and controls that are attached at the end of this paper.

Table 1: SME Use Levels, Threats and Risks

Rank	Attributes	Risks	Threats	Risk
Basic	SME may use phones, email, cloud-based storage, IoT based devices, personal Bluetooth devices, and personal computer connected to the Internet	Disclosure of data/information/ Knowledge via communications Unavailability of email/phone communications	Business email compromise Phishing Ransomware Physical break ins and theft Lost phones Loss of phone service Loss of email service	Very low
Minimal	SME may use any of the above technologies plus a payment system package or basic point of sale system with associated equipment.	All previous plus Disclosure of Modification of Payment process Unavailability of Payment process	All previous plus Network threats to payment system, Unauthorized modification of payment process, Physical threats to payment card readers	Low
Competitive	SME may use any of the above technologies plus packaged or custom bought systems such as ERP, CRM, AI, managed web sites, vendor apps, expanded network support, etc..	All of the above plus Disclosure of data/ information/ knowledge through 3rd party attacks Unavailability of packaged systems Unexpected modification of packaged systems	All previous plus: Cyber-attacks through vendors Packaged systems maintenance leads to new and/or different features and abilities causing new threat vectors Dependence on vendor knowledge leads to loss of ability to manage packaged systems	Medium
Integrated	SME may use any of the above technologies, plus customer data is being used strategically and the organization may create and manage its own apps (including AI) and web sites.	All previous plus: Disclosure of data/ information/knowledge through cyber-attacks on the organization Unauthorized modification of data/ information/knowledge Unauthorized modification of self-maintained apps and websites Unavailability of self-created apps, websites and data/information/ knowledge stores	All previous plus: Attacks on vulnerabilities created by the organization All forms of attacks on apps, websites, data/ information/knowledge Denial of service attacks Configuration mistakes in settings for devices, apps, databases, web sites, etc.	High
Strategic	SME uses any of the above technologies plus it may rely on cutting edge technologies such as custom/purchased or internally developed AI tools/applications, data is used to create information/knowledge to manage the organization and/or support clients/	All previous plus: Disclosure, modification, unavailability of systems and data/ information/knowledge due to noncompliance with regulations	All previous plus: Vulnerabilities created through noncompliance with regulations Risk assessments that miss critical threats and/ or control identifications	Very High

	customers. Additionally, the SME may be subject to special cybersecurity requirements such as HIPAA, GDPR, etc.			

Table 2: 2 SME Knowledge, IS/IT Support and Cybersecurity Controls

Rank	Knowledge Needed	Potential Controls	IS/IT Support
1 - Basic	Physical security/ protection Basic cybersecurity knowledge	Phishing and business email compromise training Create process for handling email payment requests Secure premises (locks, alarm system, cameras) Ransomware recovery plan Backup essential data Use MFA where possible	Nothing special, do suggest physical security assistance Rely on vendors for ransomware recovery
2 - Minimal	All above plus: Network security principles Fraud detection principles System modification principles	All above plus Payment process fraud training Payment process management training Ransomware/DR/BC Planning	physical security assistance ransomware recovery plan. managed service provider for payment system possible onsite support for local computers, hardware, networks, etc
3 - Competitive	All previous plus: Knowledge of packaged system design, operation, and evolution Knowledge of vendors security plan/approach	All previous plus: Maintenance and support contract with system providers Change management process implemented Contingency/Incident Response planning Backup planning and management CIO or manager charged with coordinating organizational strategy with IS/IT needs Cybersecurity training on data protection, attack methods, organization requirements Periodic auditing to ensure controls are properly implemented	All previous plus: MSP contracts with package vendors On site support for updating and managing packaged software Some help desk On site support of local computers, hardware, networks, etc. CIO/IS Manager
4 - Integrated	All previous plus: IS project management IS development process. Secure coding Cybersecurity management How attacks occur Vulnerability analysis Risk assessment	All previous plus: Full security plan Incident response procedure preparation and training Regular auditing to ensure security plan implementations are what is expected	All previous plus: Contract or onsite app/website developers, testers, and maintenance Contract or onsite data, information, knowledge managers Contract or onsight CISO/Cybersecurity analysts/managers
5 - Strategic	All previous plus: Knowledge of compliance practices for applicable regulations	All previous plus: Implementation and compliance testing for cyber regulations Document preparation for all applicable cyber regulations Regular auditing to ensure compliance is being met	All previous plus: Contract or onsite compliance experts for all applicable cyber regulations

Discussion

The SME cybersecurity categorization/maturity model identifies 5 categories of SMEs based on IS/IT usage in the organization. Additionally, each level identifies risks, threats, knowledge requirements, IS/IT support needs, suggested controls, and a risk level. All this is identified by an analysis of cybersecurity audits reported on in Jennex and Babb (2024). A discussion of each level follows.

Level 1, Basic, is primarily focused on micro organizations that don't really use IS/IT. Since no organizations were audited that had no IS/IT usage, the basic level reflects an organization that relies on basic IS/IT such as phones, email, and personal Internet usage. The Basic level can also include utilizing cloud-based storage and IoT devices. Both cloud-based storage technologies, such as Microsoft OneDrive and Dropbox, and IoT devices have become ubiquitous that micro-organizations with limited IT reliance still have easy access to them. Two audit subjects are used to represent this level, a welding shop and a calligraphy shop. Both subjects were home based offices that used phone, email, personal Internet, and basic software such as Microsoft Office. We don't expect to see many at this level, and expect that all examples will be home-based, single-to-family-sized organizations. Neither had dedicated IS support and both kept paper records. Cybersecurity focus was on physical security as most cybersecurity risk has been transferred to service providers. The risk is considered very low and is mitigated by awareness training and using qualified providers.

Basic organizations, typically micro-businesses with minimal IS/IT usage, should focus on foundational cybersecurity measures. Physical security controls such as locks, alarms, and surveillance cameras are critical to safeguarding assets and premises. Basic cybersecurity awareness training should be conducted to help employees identify phishing attempts and other common threats. Additionally, SMEs at this level should use strong, unique passwords, enable multi-factor authentication (MFA) where possible, and back up essential data periodically to prevent data loss. Partnering with reputable service providers for internet and cloud services ensures minimal exposure to risks.

Level 2, Minimal is focused on small to micro businesses that primarily use IS/IT to handle payments. Examples of these organizations come from several coffee ships that were audited. An interesting example was the coffee shop that had fake security cameras on their premises. None of the audit subjects had dedicated IS support but were aware of their payment system vendor. It is expected that there will be many micro-organizations that fit this criterion, everything from small retail and service providers, gas stations, food trucks, coffee shops, etc. Again, the cybersecurity focus is on physical security, with an awareness of vendor issues. The risk is considered low and is mitigated by awareness training and using qualified providers and vendors.

Minimal businesses, which rely on IS/IT primarily for payment systems, ensuring the security of these systems is a top priority. SMEs should regularly check and update payment systems to maintain compliance with industry standards and mitigate risks such as fraud or unauthorized access. Staff should be trained on secure payment handling, fraud detection, and recognizing suspicious activities. Replacing fake security measures like dummy cameras with functional systems can further deter physical theft. SMEs at this level should also implement basic firewalls and antivirus software and limit access to payment systems to authorized personnel.

Level 3, Competitive is a common category where organizations use communication and packaged solutions. Several audit clients fit this category. Examples include larger restaurants, small gas station chains, book keeping firms, small stores/church bookstores, small apartment complexes, artisans, home based legal firms, etc. IS support varied, a few had a dedicated person managing all IS with vendor support as needed, but many relied on managed service providers (MSP) and vendor support as needed. There is still a focus on physical security but there is also a focus on systems and operational data. All had managed web sites and some had hosted apps, a few had packaged solutions (more common in professional organizations). Risk is considered medium risk is and is mitigated by awareness and basic cybersecurity training, backup/ contingency plans, change management plans, doing regular auditing to ensure controls are properly implemented, and using and managing qualified providers and vendors.

Competitive organizations, which use packaged solutions and communication tools, should focus on protecting operational and customer data. Regular backups and contingency plans are essential to recover quickly from potential incidents. Change management processes should be established to monitor and

approve modifications to packaged systems, reducing the risk of accidental vulnerabilities. Engaging managed service providers (MSPs) for ongoing cybersecurity support ensures consistent protection. Additionally, periodic audits should be conducted to verify the effectiveness of implemented controls, and network segmentation can help isolate critical systems to limit the impact of potential breaches.

Level 4, Integrated, uses all forms of IS/IT, including developing custom apps and websites, but doesn't have special regulatory requirements, common with the larger small organizations such as small IS support organizations, consulting firms, car rental franchisees, churches/megachurches, large apartment complexes, etc. All had dedicated IS support with additional support from contractors and possibly a MSP as needed. This level can generate their own apps and websites, so support includes programmers and web masters. Also, since data is being used for competitive purposes, support can include data analysts/scientists. The examples audited all had critical data and many had custom apps and websites. Risk is considered high as it is now managed by the organization, perhaps using an MSP, and not by product vendors. Risk is mitigated by doing all previous actions plus developing incident response plans, a full security plan, and conducting regular auditing of security plan implementation.

Integrated, SMEs utilize advanced IS/IT, including custom applications and websites, necessitating more robust cybersecurity measures. Developing comprehensive incident response plans and training employees on their roles during cyber incidents is vital. Regular vulnerability assessments and penetration tests should be conducted to identify weaknesses in custom-developed applications. Establishing a full security plan with protocols for access control, data encryption, and threat monitoring ensures proactive risk management. SMEs at this level should also employ or contract with skilled professionals such as data analysts, developers, and cybersecurity managers to manage their more complex cybersecurity needs.

Level 5, Strategic, uses all forms of IS/IT and is also subject to special regulatory requirements. We had few audit examples but what we had were small medical facilities, medical professionals working out of home offices, and childcare facilities. Some of these clients had dedicated IS support (medical facilities) but most didn't (medical professionals working out of home offices, childcare facilities). Contract/MSP support was commonly used. We observed that only one had regulatory support. Risk is considered very high due to possible non-compliance issues. Risk is mitigated by using all previously discussed actions plus doing compliance testing and auditing.

Strategic businesses, which rely on cutting-edge IS/IT and are subject to regulatory requirements, must prioritize compliance and advanced threat protection. Regular compliance audits are essential to ensure adherence to regulations like HIPAA, GDPR, or other industry-specific standards. Maintaining detailed documentation of cybersecurity and compliance processes supports regulatory inspections and readiness. SMEs should invest in AI-driven threat detection tools and advanced encryption technologies to safeguard critical systems and data. Organization-wide training on regulatory requirements can foster a culture of compliance, while a dedicated governance structure ensures alignment of cybersecurity policies with business goals.

Observed issues were seen in all SME levels but we did observe a couple of well managed and resourced SMEs. It is observed that the categorization model fits the observed organizations. Additionally, the model serves as a SME cybersecurity maturity model, illustrating how SMEs can progress their cybersecurity programs based on changing IS/IT usage. The proposed model is similar to that of Shojaifar and Järvinen, (2021) but with a few key differences. Shojaifar and Järvinen, (2021) based their classification on cybersecurity knowledge in the SME and how to progress that knowledge. This model is based on actual IS/IT usage in the SME and at providing generic analysis of risk, threats, needed cybersecurity knowledge, needed IS/IT resources, and generally accepted cybersecurity controls and actions. Likewise, Pawar and Palivela (2022) provide their LCCI model of least common controls. This model supports that but expands to include direction on cybersecurity knowledge and IS/IT resource needs and provides a generic assessment of risks and threats. Finally, the models of Perozzo, et al. (2021) and Van Haastrecht, et al. (2021), also addressed portions of what the proposed model provides but not the completeness this model provides.

Theoretical Contributions

This study makes theoretical advancements by extending the existing maturity model literature to the unique context of SMEs. While prior models, such as those by Shojaifar and Järvinen (2021) and Pawar

and Palivela (2022), address general cybersecurity frameworks, they lack specificity in categorizing SMEs based on IS/IT usage. The proposed model bridges this gap by introducing a structured, IS/IT-driven classification system that aligns with real-world cybersecurity audit data. Moreover, the integration of socio-technical principles into the model emphasizes the dynamic interplay between technological adoption and organizational readiness. This reflects the evolving landscape of SME operations and their corresponding risk profiles. By grounding the model in a robust theoretical foundation of maturity models (e.g., Becker et al., 2009; Mettler, 2011), this research contributes to a deeper understanding of how SMEs can transition across cybersecurity maturity levels while balancing resource constraints and operational priorities.

Practical Contributions

The practical contributions of this study provide actionable insights for improving SME cybersecurity preparedness in real-world contexts. By leveraging the proposed categorization and maturity model, SMEs can better understand their cybersecurity needs, allocate resources efficiently, and address risks commensurate with their level of IS/IT usage. The model not only serves as a valuable tool for SME owners and operators but also supports auditors, policymakers, and ecosystem collaborators in developing targeted strategies to enhance cybersecurity resilience. These contributions are particularly significant given the limited resources and expertise that SMEs typically possess, offering scalable solutions to meet their diverse and evolving needs.

Guidance for SMEs: The categorization provides SMEs with a clear roadmap to identify their cybersecurity needs based on their IS/IT usage. For example, SMEs at the "Minimal" level can focus on vendor management and basic network security, while those at the "Strategic" level must address complex regulatory requirements and advanced threat mitigation. This structured approach demystifies cybersecurity for SME owners who may lack technical expertise, enabling them to make informed decisions about their security investments.

Resource Allocation: By linking each maturity level to specific knowledge, IS/IT support, and controls, the model enables SMEs to allocate limited resources effectively. For instance, organizations at lower levels are encouraged to rely on Managed Service Providers (MSPs) for cost-effective cybersecurity management. This not only optimizes operational expenses but also ensures that SMEs receive expert support tailored to their unique needs, reducing the likelihood of costly security breaches.

Auditor Tools: For cybersecurity professionals, the model serves as a practical framework to assess SME cybersecurity maturity during audits. This facilitates consistent evaluations and tailored recommendations, ensuring SMEs receive actionable insights to enhance their security posture. By standardizing audit practices, the model also helps auditors efficiently identify critical vulnerabilities and recommend pragmatic solutions aligned with the SME's operational capacity.

Improving Resilience in Critical Sectors: The model provides specific recommendations for sectors with higher cybersecurity risks, such as healthcare and childcare, where compliance with regulations like HIPAA and GDPR is critical. SMEs operating in these sectors can use the model to identify gaps in their regulatory compliance and implement targeted controls to reduce risk. This focus on compliance and risk management not only protects sensitive data but also ensures business continuity in highly regulated environments.

Promoting Proactive Cybersecurity Culture: A key practical contribution of the model is its ability to foster a proactive cybersecurity culture within SMEs. By defining cybersecurity needs at various maturity levels, the model encourages SME owners and employees to view cybersecurity as a strategic priority rather than an operational burden. The detailed guidance on employee training, threat awareness, and incident response planning empowers SMEs to develop long-term resilience against evolving cyber threats.

Encouraging Ecosystem Collaboration: The model emphasizes the importance of ecosystem collaboration, particularly through partnerships with local universities and Managed Service Providers (MSPs). University partnerships can provide SMEs with access to cutting-edge cybersecurity research, training programs, and skilled interns, creating a cost-effective way to build in-house expertise. Similarly, MSPs offer scalable and specialized services, allowing SMEs to outsource critical cybersecurity functions while focusing on their core business operations.

Implications for Policy and Research

This study provides valuable insights for policymakers and researchers aiming to improve SME cybersecurity. Policymakers can use the proposed maturity model to design targeted initiatives, such as financial incentives for adopting managed service providers (MSPs), grants for regulatory compliance training, and subsidized university partnerships. These measures can address resource and knowledge gaps, enabling SMEs to adopt more robust cybersecurity practices. Moreover, policymakers should consider creating accessible resources, such as simplified regulatory guides, to help SMEs navigate complex compliance requirements like HIPAA and GDPR.

In conclusion, the findings emphasize the importance of developing tailored cybersecurity strategies for SMEs, addressing their unique challenges of limited resources, expertise, and technological capabilities. The proposed model serves as a foundation for advancing both practice and research in this domain. Future research should focus on expanding the model's applicability across diverse geographic and industrial contexts while incorporating emerging technologies such as AI and IoT. By bridging theoretical advancements with practical applications, this research provides a pathway to enhance cybersecurity readiness, ensuring SMEs can thrive in an increasingly digital and threat-laden business environment.

Recommendations and Limitations

This model is useful for multiple purposes. It provides a guide to SMEs that they can use to determine their generic cybersecurity needs as well as to ensure those needs continue to be met as the SME progresses in IS/IT usage. It provides guidance on how much IS/IT resources are needed. It identifies basic risks and threats that the SMEs need to be aware of. Finally, it provides a guide for auditor and SME evaluators as to what they should look for based on the categorization of the SME. Of course, this is a living model and so will continue to evolve as the SME and IS/IT landscape changes. The key recommendation is for lower usage SMEs, levels 1, 2, and 3, is to consider using MSP and contract resources rather than trying to do IS/IT themselves.

One growth area not currently addressed by the model is the application of artificial intelligence (AI). This is an emerging field, and applications are being developed that SMEs may adopt. Currently, most SME AI adoption is through enhanced Internet/Web search and retrieval on browsers. However, this will probably change in the near future.

Another issue not specifically addressed is the Internet of Things (IoT). The model currently addresses this issue as part of packaged solutions or the use of cameras, but this could change as IoT usage evolves.

A potential limitation of this model and area of future work is that the model is based on a relatively modest sample size of 40 SMEs. Auditing more SMEs, especially across different industries, would enhance the model. Further, follow-up visits with previously audited firms could help verify how successful or useful the model is to those businesses.

An opportunity provided by the model is in the area of knowledge resources. To address this challenge, SMEs can explore partnerships with local universities, which offer a wealth of knowledge and resources in the field of cybersecurity. Universities, with their cutting-edge research facilities and highly skilled faculty and students, can provide valuable support to SMEs in strengthening their cybersecurity posture. The cybersecurity audits used to generate this model are the result of the beginnings of such a university partnership. These partnerships can yield the following benefits:

1. Access to Specialized Expertise: By collaborating with university cybersecurity programs, SMEs can tap into the expertise of faculty members and graduate students who specialize in cybersecurity. These experts can conduct comprehensive assessments of the SME's systems and security practices, identify vulnerabilities, and provide recommendations for improvement.
2. Employee Training and Awareness Programs: Universities can assist SMEs in developing and implementing comprehensive cybersecurity training and awareness programs for their employees. These programs can focus on raising awareness about common cyber threats, best practices for password management, and identifying and responding to social engineering attacks.
3. Implementation of Advanced Security Measures: Through collaborative research projects and knowledge-sharing initiatives, SMEs can learn about and implement state-of-the-art security

tools and techniques, such as multi-factor authentication, encryption, and regular system updates. These measures can significantly enhance the SME's cybersecurity posture.

4. Knowledge Transfer and Capacity Building: Partnerships with universities not only provide access to valuable knowledge and resources but also create opportunities for knowledge transfer and capacity building within the SME's workforce. This can help develop in-house cybersecurity expertise and foster a culture of cybersecurity awareness within the organization.

Conclusions

Changing the terminology from SME to Small and Micro Enterprises (SMEs) is a reasonable adjustment for cybersecurity considerations, as extensive support exists for large and medium organizations, but small and micro enterprises remain underserved. These SMEs face significant cybersecurity challenges:

1. Limited Resources and Budget Constraints: SMEs often lack the financial capacity to invest in comprehensive cybersecurity programs, advanced security tools, and dedicated personnel, making it difficult to implement robust protections.
2. Lack of Specialized Cybersecurity Expertise: With no dedicated IT or cybersecurity departments, SMEs rely on employees with multiple roles to manage cybersecurity. This lack of specialized expertise leaves them vulnerable to cyber risks.
3. Insufficient Employee Training and Awareness: Budget constraints and limited expertise hinder SMEs from providing necessary cybersecurity training, making employees susceptible to social engineering and other attacks.
4. Outdated or Inadequate Security Measures: Many SMEs rely on outdated software and practices, which fail to address evolving cyber threats, exposing them to sophisticated attacks.
5. Perception of Being a Low-Priority Target: A false sense of security, driven by the misconception that small businesses are not targeted by cybercriminals, leads to complacency in implementing cybersecurity measures.
6. Resistance to Cybersecurity Policies: Employees at SMEs may view cybersecurity policies as complex or productivity inhibitors, resulting in resistance and non-compliance, which undermines security efforts.

This paper addresses these challenges by proposing a categorization and maturity model tailored to SMEs, focusing on their IS/IT usage. The model provides a structured approach for SMEs to identify their cybersecurity needs, allocate resources effectively, and mitigate risks based on their organizational characteristics. Derived from a detailed analysis of 40 cybersecurity audits conducted by students across the United States, this model represents a robust and practical framework that is scalable and adaptable to various SME contexts. It also serves as a valuable tool for auditors, enabling consistent and actionable assessments of SME cybersecurity maturity.

Additionally, this paper highlights the critical role of university partnerships in supporting SMEs. These collaborations leverage academic expertise to provide training, advanced tools, and practical guidance, addressing SMEs' knowledge gaps and resource limitations. By fostering such partnerships, SMEs can enhance their cybersecurity resilience while gaining access to cutting-edge technologies and best practices.

Future research should focus on several priorities. First, expanding the model’s applicability by incorporating data from SMEs outside the United States will improve its generalizability. Second, integrating emerging technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT) into the model will address their growing adoption and associated security challenges. Finally, additional audits and longitudinal studies will refine the model and ensure its relevance in an ever-changing cybersecurity landscape.

By proposing actionable strategies and fostering collaborative efforts, this paper offers a pathway for SMEs to overcome cybersecurity challenges, strengthen their defenses, and thrive in an increasingly digital economy. The model and recommendations presented contribute to advancing SME cybersecurity readiness and provide a foundation for future policy and research initiatives.

References

Alahmari, A., & Duncan, B. (2020, June). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA) (pp. 1-5). IEEE.

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

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 1(2), 219-238.

Ashley, C., & Preiksaitis, M. (2022). Strategic Cybersecurity Risk Management Practices for Information in Small and Medium Enterprises. Business Management Research and Applications: A Cross-Disciplinary Journal, 1(2), 109-157

Argyris, C., & Schön, D. A. (1997). Organizational learning: A theory of action perspective.

Auyporn, W., Piromsopa, K., & Chaiyawat, T. (2020). Critical factors in cybersecurity for SMEs in technological innovation era. In ISPIM Conference Proceedings (pp. 1-10). The International Society for Professional Innovation Management (ISPIM).

Babb, J., Hoda, R., & Nørbjerg, J. (2014). Embedding reflection and learning into agile software development. IEEE software, 31(4), 51-57.

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security, 27(3), 393-410.

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing maturity models for IT management: A procedure model and its application. Business & Information Systems Engineering, 1, 213-222.

Becker, J., Niehaves, B., Poeppelbuss, J., & Simons, A. (2010). Maturity models in IS research.

Carías, J. F., Borges, M. R., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in SMEs. IEEE access, 8, 174200-174221

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. IEEE Access, 10, 85701-85719.

de Arroyabe, J. C. F., Arroyabe, M. F., Fernandez, I., & Arranz, C. F. (2023). Cybersecurity resilience in SMEs. A machine learning approach. J. Comput. Inf. Syst., 1-17

Dimopoulos, V., Furnell, S., Jennex, M.E., and Kritharas, I., (2004). "Approaches to IT Security in Small and Medium Enterprises," 2nd Australian Information Security Management Conference, November 2004.

Drucker, P. (1989). Sell the mailroom. Wall Street Journal, 25.

Eilts, D. (2020). An empirical assessment of cybersecurity readiness and resilience in small businesses.

Gamma, E., Helm, R., Johnson, R., & Vlissides, J. Design Patterns: Abstraction and Reuse of Object-Oriented Design.

Jennex, M.E., Addo, T.B.A., and Walters, A., (2004). "SMEs and Knowledge Requirements for Operating Hacker and Security Tools" Information Resource Management Association Conference 2004, IRMA2004, Idea Group Publishing, May 2004.

Jennex, M.E. and Babb, J., (2024). "Observations and Learnings From Cybersecurity Audits of SMEs." 23rd Annual Security Conference. April 3, 2024. Retrieved from https://www.google.com/url?q=https://029e2c6.netsolhost.com/II-Proceedings/2024/14.pdf&sa=D&source=editors&ust=1717822517141451&usg=AOvVaw1E6qG7MHOUR2h7wukTDLFs on June 7, 2024.

Kajiyama, T., Jennex, M.E., and Addo, T.A., (2017). "To Cloud or Not To Cloud: How Risks And Threats Are Affecting Cloud Adoption Decisions." Information and Computer Security, 25(5), pp. .634-659.

Kosar, T., Martı, P. E., Barrientos, P. A., & Mernik, M. (2008). A preliminary study on various implementation approaches of domain-specific language. Information and software technology, 50(5), 390-405.

Mettler, T. (2011). Maturity assessment models: a design science research approach. International Journal of Society Systems Science, 3(1-2), 81-98.

Mettler, T., & Ballester, O. (2021). Maturity Models in Information Systems: A Review and Extension of Existing Guidelines. In ICIS.

Nagahawatta, R., Lokuge, S., Warren, M., & Salzman, S. (2021). Cybersecurity Issues and Practices in a Cloud Context: A Comparison Amongst Micro, Small and Medium Enterprises. arXiv preprint arXiv:2111.05993. Presented at the Australasian Conference on Information Systems, Sydney, Australia, 2021.

Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, 2(1), 100080.

Perozzo, H., Ravarini, A., & Zaghloul, F. (2021). Assessing cybersecurity readiness within smes: proposal of a socio-technical based model. Proceedings http://ceur-ws. org. ISSN, 1613, 0073.

Poeppelbuss, J., Niehaves, B., Simons, A., & Becker, J. (2011). Maturity models in information systems research: literature search and analysis. Communications of the Association for Information Systems, 29(1), 27.

Röglinger, M., Pöppelbuß, J., & Becker, J. (2012). Maturity models in business process management. Business process management journal, 18(2), 328-346.

Schön, D. A. (1979). Generative metaphor: A perspective on problem-setting in social policy. Metaphor and thought, 2, 137-163.

Schön, D. A. (2017). The reflective practitioner: How professionals think in action. Routledge.

Shojaifar, A., & Järvinen, H. (2021, August). Classifying SMEs for approaching cybersecurity competence and awareness. In Proceedings of the 16th International Conference on Availability, Reliability and Security (pp. 1-7)

Van Haastrecht, M., Yigit Ozkan, B., Brinkhuis, M., & Spruit, M. (2021). Respite for SMEs: A systematic review of socio-technical cybersecurity metrics. Applied sciences, 11(15), 6909.

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2023). It won't happen to me: Surveying sme attitudes to cyber-security. Journal of Computer Information Systems, 63(2), 397-409.