Observations and Learnings From Cybersecurity Audits of SMEs

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

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

Abstract

This paper uses student conducted cybersecurity audits of SMEs to determine if SME cybersecurity behavior has evolved over the last 20 years. The cybersecurity audits were performed using a core set of audit areas plus other audit items as needed for the audit subject. Findings included observations on the lack of cybersecurity resources, both in terms of personnel and knowledge. Additionally, 10 issues were identified that were common in SMEs, with 5 of those occurring in 50% or more of the subjects. Conclusions include encouraging all SMEs to perform cybersecurity audits, using managed service providers to provide personnel and knowledge resources, and changing SME pricing practices so that they recognize the costs of being cyber secure.

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. Additionally, SMEs tended to have a crisis management culture that focuses on solving the immediate problems of now rather than on planning and management for long term issues (Jennex, et al., 2004; Dimopoulos, et al., 2004). Both papers concluded that SMEs needed simpler and streamlined risk assessment processes, and simplified cybersecurity models such as a knowledge management approach that utilizes best practices, standards, and checklists. Now, twenty years later, this paper raises the question as to whether this knowledge management approach of best practices, standards, and checklists has been effective in reducing SME cybersecurity vulnerability. This paper investigates this question and suggests little has changed.

Dzimiela and Jennex (2023) reviewed responses of small communities in north Texas to a ransomware attack in 2019 and found that the same issues faced in 2004 still existed within the affected communities 15 years later (Dzimiela and Jennex, 2023). A further question is raised as to whether this phenome is unique or common and widespread. To explore these questions, this paper presents the results of 40 cybersecurity audits done on SMEs by the West Texas A&M University Paul and Virginia Engler College of Business's Wellington State Bank Cyber Security Center. An initial analysis suggests there are still significant SME cybersecurity vulnerabilities.

Dzimiela and Jennex endorsed Raghavan, et al. (2020) who proposed the use of cybersecurity audits to aid smaller organizations in preparing for ransomware attacks (Dzimiela and Jennex, 2023). Additionally, the use of cybersecurity audits on SMEs is expanded in this paper to consider overall cybersecurity preparedness and implementation of best practice. The lead author of this paper began using cybersecurity audits of SMEs as a teaching tool and learning experience in his cybersecurity classes in 2014 after conducting research that showed that the knowledge management (KM) discipline did not

include or emphasize cybersecurity knowledge as important aspect of preserving and assuring knowledge assets (Jennex and Durcikova, 2014). This lead to further work at a research center to aid that center to create a security plan and initial accreditation of their security program. This initial accreditation activity was done using a team of graduate cybersecurity students who found the activity to be a useful and popular learning experience. These student-driven accreditation audits continued in subsequent years for the reaccreditation of the research center's security program and to work with other SMEs willing to allow the audit. This audit experience was expanded in the academic year of 2022-23 when the lead author began teaching online graduate cybersecurity courses at West Texas A&M University. As West Texas A&M University has a national online presence and program it resulted in students from all over the United States performing these audits on all sorts of SMEs. The result is a geographically and industry diverse set of SME audits used in the analysis for this paper. It also led to the generation of the following research questions:

RQ1: Are there cybersecurity issues/weaknesses common in SMEs?

RQ2: What are the common cybersecurity issues/weaknesses in SMEs?

The audits were performed using a semi-standard audit scope (see appendix 1). Student auditors were free to add scope to assist the SME in understanding cybersecurity recommendations and to follow up on recommendations arising from observed issues. Each audited SME was provided a report listing the top five identified issues and the top five recommendations to address the issues found. Recommendations were reviewed by the professor to ensure they were achievable (e.g. to ensure the best "bang for the buck" to the SME). To answer these research questions the findings and final reports of the audits were aggregated to determine the nature and frequency of the issues encountered by the SMEs. No SME names or locations were included in the analysis in order to protect the SMEs' privacy. Additionally, any unusual observations were listed to provide richness to the analysis.

The rest of the paper is organized as follows. First, a background review of literature discussing current SME cybersecurity issues. This is followed by a discussion on how the cybersecurity audits were conducted. Then comes the results and a discussions on the findings. The paper concludes with conclusions and recommendations

BACKGROUND ON CURRENT SME CYBERSECURITY

This section examines recent research with respect to SMEs. A common theme found within the literature is that the threats and risks that SMEs encounter are on the rise while, at the same tie, 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 that conducting in this study bring the illumination and attention 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.

Kajiyama, et al. (2017) and Nagahawatta, et al. (2021) found that cyber security concerns within SMEs can influence SME decision-making with respect 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 is limit for many SMEs to leverage 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 exascerbates 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 ignorance of the risks involved in adopting those technologies.

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 (2002) 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 which advocates the use of the least cybersecurity controls necessary to support defense in depth and mission critical assets to meet confidentiality, integrity, and availability (CIA), priorities. Mburu (2023) found similar challenges for SMEs in implementing a machine learning based intrusion detection system.

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. The 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

Methodology

Audits were conducted using a multi-step process. The first step was for the student to find a client. Students were directed to find a small or medium organization that was willing to have a cybersecurity audit performed on them. The students informed the client they weren't experts but would be supervised by their professor. Additionally, the client would get a chance to review the audit plan/scope prior to performance of the audit and that they would receive a report documenting the audit findings and including recommendations for improvement. The second step was the creation of a audit plan. The template in Appendix 1 was tailored by the students to fit their client organization. A basic scope was set in the template but students were free to modify it based on client needs. The third step had the generated audit plan submitted to the professor for review and approval prior to implementing the plan. During this step the professor ensured adequacy of the plan and made changes if needed. Once approved by the professor the fourth step had the student submit the audit plan to the client for approval and scheduling of the audit. The fifth step was performance of the audit with findings documented on the audit plan. The sixth step was analysis by the student on the audit results and generation of an audit report that listed the top five findings and the top five recommendations. The seventh step had the student submit the audit findings and report for the professor's review. In this step the professor ensured the quality of the report and that the recommendations were reasonable for the organization. Once reviewed, the final step was to provide the audit report to the client for their use. No follow-up has been done with the clients as the students finished the course and could follow-up if they wished on their own. No further communication was provided to the professor.

Implementation of the audit plan was guided by the direction included on page one of the audit plan template in Appendix 1. This included direction on how the audit was to begin and allowed for social engineering testing of the client if desired. An introductory meeting was held to ensure that the client and the auditor agreed on how to proceed. After an initial meeting the audit was performed and was followed by a "hot wash" meeting where preliminary results were discussed, and client input received on what was observed.

The audits were analyzed by categorizing the types of organizations audited and the findings into standard issues. The issues were then aggregated by counting how many audits had the categorized finding. Additionally, any unusual observations were noted. Organization categories (with the count in the category) were determined to be:

- 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)

Issues were categorized as follows (with brief description of the issue):

- Weak/reused/no passwords: this issue reflects organizations whose passwords/password policies did not meet best practice.
- Passwords written down: passwords were found on sticky notes on other media around the computers
- Weak access control: this issue reflects lack of access control policies with issues like old accounts not being deactivated, no account/rights review process, shared passwords and accounts among staff, etc.
- Weak physical security: this issue reflects the lack of physical barriers such as locks, doors, etc and public access allowed near computing resources.
- Open/responsive ports: this issue reflects the results of a shields up scan performed on the client network/computer.
- Missing updates: this issue reflects the results of inspecting the update status of client computers

- Weak/partial/no backup/restoration process: this issue reflects findings showing lack of current updates, no update policy, no practiced restoration process.
- No malware protection: this issue reflects findings of no malware protection found on client computers.
- No/weak security systems: this issue reflects findings of no overall security system of firewalls and other security technologies such as regular scans, intrusion detection, password protections/storage, etc.
- Business assets used for non-business purposes: this issue reflects the concurrent presence of business and non-business applications, data, and uses on client computers.
- No security plan: this issue reflects no written or implied security plan and policies.
- Malware found: this issue reflects finding malware during a malware scan of client computers.
- No/weak security training: this issue reflects no or little security awareness, phishing, security issue trainingr

Findings

Audit findings are presented in summary form using the below two lists. The lists are ranked ordered with the most common issues and observations listed first and the number/percent of audit clients having the issue/observation.

Major Findings (finding: number of audits reporting it)

- No security plan: 25 (62.5%)
- Weak/reused/no passwords: 22 (55%)
- Missing updates: 22 (55%)
- Weak physical security: 20 (50%)
- Weak/partial/no backup/restoration process: 20 (50%)
- Open/responsive ports: 14 (35%)
- No/weak security training: 14 (35%)
- Weak access control: 13 (32.5%)
- Business assets used for non-business purposes: 12 (30%)
- No/weak security systems: 9 (22.5%)
- No malware protection: 5 (12.5%)
- Passwords written down: 4 (10%)
- Malware found: 2 (5%)

Other observations: (observation: number of audits reporting it)

- Router in unlocked closet/room: 5 (12.5%)
- Employees share accounts/passwords: 5 (12.5%)
- Fake security cameras: 4 (10%)
- Former employee profiles not deactivated: 4 (10%)
- Router/computer in bedroom: 3 (7.5%)
- Security cameras blocked: 3 (7.5%)
- Old devices/files thrown in dumpster: 3 (7.5%)
- Sensitive material stored in an unlocked box: 3 (7.5%)
- Business/customers share same wifi: 3 (7.5%)
- Router kept behind receptionist desk: 2 (5%)
- Server in manager's office: 2 (5%)
- Wireless extends past business premises: 2 (5%)
- Office in spare bedroom with no special security: 2 (5%)
- No router password: 2 (5%)
- No climate control for router: 2 (5%)
- Original default router password found in use: 2 (5%)
- Weak/shared PINs: 1 (2.5%)
- Unsecured business wifi: 1 (2.5%)
- Security camera on wrong door: 1 (2.5%)

- Messy router room: 1 (2.5%)
- Same password for several years: 1 (2.5%)
- Old devices donated without removing hard drives/sim cards: 1 (2.5%)
- Users using corporate computer usb connections to charge personal phones: 1 (2.5%)
- All computer equipment on front desk next to cash register: 1 (2.5%)
- Admin used as login on all computers: 1 (2.5%)
- Alexa active on business network that can take commands from anyone in a daycare: 1 (2.5%)
- No password on daycare computer: 1 (2.5%)
- Computer/router kept in middle of open floor plan house/daycare: 1 (2.5%)
- Client files not password protected: 1 (2.5%)

Additionally, although we did not specifically ask about how big of an IT/IS staff the organizations had, we 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

Discussion

Looking at the findings through the lens of our literature review, Bada and Nurse (2019) and Ashley and Preiksaitis (2022) cited training as an issue in SMEs. Our audits found this to be an issue in 35% of clients. Pawar and Palivela (2022) observed that SMEs had trouble in selecting and implementing controls. Controls are typically identified during the security planning process and our audits found that 62.5% of the clients did not have security plans, making this the top finding. Wilson, et.al. (2023) found that SMEs 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, but did consider the impact of this if it happened as being high. The audit findings all reflect issues that impact the SMEs' ability to mitigate or prevent a cyber attack. Bada and Nurse (2019), Antunes, et al. (2021), Dzimiela and Jennex (2023), and Alharbi, et al. (2021) support the use of cyber security audits in SMEs. Our findings suggest that SME cyber security audits are a necessary activity given that there are 5 issues that occurred in at least 50% of the audit clients. Finally, all the literature suggests that SMEs have few resources and knowledge necessary to protect themselves from cyber attacks. Our findings strongly support this position as only 7.5% of the audit clients had more than one IT/IS person support staff. The other 92.5% either had one IT/IS support staff, focused primarily on keeping the networks, hardware, and software running; or the owners did their own IT/IS with some contract support, or they had part time IS/IT support.

Additionally, the findings present an interesting picture of SME Cybersecurity. Five issues were observed in at least 50% of the audits. These issues are considered to have occurred often enough for them to be considered endemic in SMEs. Five more issues occurred in more than 20% but less than 50% of the audits. We consider these to be common issues in SMEs. The last three issues occurred infrequently enough that we consider them to be issues unique to those organizations. This means that there are 10 issues that we should consider common enough in SMEs that they should be addressed by a generic SME audit plan and remedial Cybersecurity program. These 10 issues are:

- No security plan: 25 (62.5%)
- Weak/reused/no passwords: 22 (55%)
- Missing updates: 22 (55%)
- Weak physical security: 20 (50%)
- Weak/partial/no backup/restoration process: 20 (50%)
- Open/responsive ports: 14 (35%)
- No/weak security training: 14 (35%)
- Weak access control: 13 (32.5%)
- Business assets used for non-business purposes: 12 (30%)
- No/weak security systems: 9 (22.5%)

Additionally, 60 interesting observations were made. While not generic enough to be classified as generic issues, they do provide a glimpse of findings that show that SMEs are different than larger organizations. Over 20 observations were made relative to server and equipment locations and management. This shows

that SMEs do have issues related to preserving and protecting their unique resources. These issues extend to not only managing their servers and computer equipment but also their workspaces. In acute cases of these observations, it was also observed that the SME either didn't have an office separate from the living quarters of the owner or that the separate office was very small, such as a business suite in a larger office building. This indicates that physical security and router standards typically applied to larger organizations just will not be usable by SMEs and that these standards should be custom developed for SMEs.

CONCLUSIONS/RECOMMENDATIONS

This paper is attempting to answer two research questions: are there cybersecurity issues/weaknesses common in SMEs; and if so, what are they? Our findings answer yes to both the research questions. Also, the research found that SMEs generally have few IS/IT resources and a general lack of cybersecurity knowledge. The common issues are:

- No security plan
- Weak/reused/no passwords
- Missing updates
- Weak physical security
- Weak/partial/no backup/restoration process
- Open/responsive ports
- No/weak security training
- Weak access control
- Business assets used for non-business purposes
- No/weak security systems

So what should be done about the generic issues given the lack of cybersecurity resources? There are three principal trends to inform key takeaways for this work. First, relative to the proportion of SMEs compared to the total number of businesses, the pace of threats and mitigations is such that SMEs have no feasible way to truly keep up. Second, the issue of Cybersecurity awareness and protection has attained such a mass, with ever increasing and complex details to attend to, that SME comprehension of the threat is becoming more abstract in a relative sense. Third, SMEs are not incorporating the true costs of Cybersecurity into their business model and pricing. Each of these assessments are elaborated below.

The first overarching observation is that available resources, affinity, and ability to adequately cope with the steps necessary for Cybersecurity are more elusive than ever for SMEs. It is unlikely that any comprehensive effort for extensive Cybersecurity training will offset this pace and any such efforts must become more condensed such that only the most basic behaviors and measures can be emphasized with any hope of habituated uptake. It is unlikely that any further sounding of alarms will change circumstances for SMEs where other aspects of business survival will take precedent. Another way to reconcile the extent of the challenge is to bear in mind that Cybersecurity compromises and data breaches for large companies remain commonplace despite what are likely far more comprehensive measures taken at those large companies. In short, the pace of the expansion of Cybersecurity issues is likely impossible to maintain for SMEs.

Second, while the pace of the expansion of threats accelerates, the complexity both threats and mitigations suggest that the problem of keeping pace is not simply a matter of volume, but also of expertise. That is, the issue not only a quickening of threats, but a rapid broadening of sophistication and complexity. This makes the problem particularly wicked for the SME as there are a growing number of vectors for attack on each audit finding category identified in this study. The problem is one that be described and more threats, more often, and each other higher resilience against basic protections. In many cases, the SMEs audited has such inadequate basic protection that issues related to pace and extent are moot.

The third overall observations suggests that issues this broad typically develop market responses that more or less follow basic economic principles. In this case, it is likely that broad swathes of the markets created and served by SMEs are simply failing to adequately price Cybersecurity risk mitigation. Should these goods and services price the costs of cybersecurity adequately, then a tertiary ecosystem of managed service providers, or similar intermediaries, would become a normative component of business. To

contextualize this more broadly, it is useful to consider how other segments of trade price in risks. Global commerce relies on an extensive shipping and transit system - whether it be ship, airfreight, rail, or truck – that has long since developed very sensitive and effective mechanisms to ensure that risk is effectively priced into the system. This network of liability pricing has a broad reach where the end-to-end shipping of goods and materials does not commonly escape the structures that account for risk-driven cost.

While it may be true that Cybersecurity threats are so expansive and increasingly complex that reliable mitigation is challenging for SMEs, there are market-driven services and talent available to address the issues. While there is no perfect solution to Cybersecurity threat mitigation as it is a volatile and emergent space, there is nonetheless a reasonable set of solutions available. In the case of SMEs, and in light of this study's results indicating a worsening problem, typical advocacy for more training and awareness, while necessary, may not be the best response it that is all that is done. Rather, it is more likely that the true costs of SME Cybersecurity mitigation are factored into the pricing for the goods and services provided by the SMEs. Market-driven solutions, particularly those that can be validated and audited as being standards-driven, are likely a better approach to addressing SME cybersecurity issues.

The most readily available solution in the case of SMEs is to both assume and pass along the costs of a reputable Managed Service Provider (MSP). Should a more widespread adoption of MSPs arise, the market could expand to allow for reasonable competition in the space with the expected commodification of the market to normalize both cost and reliability. It is largely the case that the very infrastructure most MSPs would rely on has already been commodified. We can re-examine each of the top ten findings from the audits to describe how a reputable MSP would address that issue:

- No security plan: The MSP would likely provide sufficient interfaces and procedures such that only the most important "last mile" issues would be susceptible to customer compliance and habit.
- Weak/reused/no passwords: The MSP would likely insist on several additional controls and policies that would narrow this point of failure and additionally not permit egregious neglect in this area.
- Missing updates: With any reasonable MSP, this would be a non-issue and non-factor.
- Weak physical security: This is conceivably moot with a comprehensive MSP approach.
- Weak/partial/no backup/restoration process: This is conceivably moot with a comprehensive MSP approach.
- Open/responsive ports: This is conceivably moot with a comprehensive MSP approach.
- No/weak security training: Training would become akin to the driver safety on the road – fewer and habitual principles backed up by many additional embedded and environmental protections
- Weak access control: The MSP would likely insist on several additional controls and policies that would narrow this point of failure and additionally not permit egregious neglect in this area.
- Business assets used for non-business purposes: Only explicit efforts to contravene what the MSP provides would raise this issue – all critical infrastructure would not be physically accessible beyond common and control interfaces.
- No/weak security systems: Security weakness would be limited to failures to adhere to the more limited interfaces provided by the MSP. Again, the SME would be actively thwarting the provided protections.

The last step in addressing the SME cybersecurity issue would be a campaign, mostly likely arising from the MSP market, to drive consumer awareness of the importance of who one is doing business with. The UL Enterprise, the Better Business Bureau, and even government monitoring (e.g. the United States Department of Agriculture Economic Research Service) are three examples the potential effectiveness of such an approach. Aside from the government example, there are for-profit monitoring and auditing activities that work to ensure some demarcation of quality "boundaries" and provide some model from which appraisal of MSP use and service delivery could progress. The protections here assume a few dimensions beyond a producer/consumer relationship and extend to appraisals of the quality of the MSP's service and the quality of the SME's compliance with the controls meant to protect them. To borrow from the driver safety metaphor, a faulty seatbelt could be reported as well as faults in effectively using the seatbelt. There are obviously many additional details to attend to for this approach to become

operational, but it is no less feasible than a conclusion that would call upon the SME to take more of the cybersecurity mitigation upon themselves as this study suggests as implausible and infeasible. As a minimum, the research suggests that a special set of SME cybersecurity standards be developed that can be used to certify MSPs and as a knowledge base for those SME organizations that still choose to do their own cybersecurity.

This research has highlighted the results of an audit of SME Cybersecurity practices and had has explored and examined common themes arising form that audit. In general, it can be deduced that Cybersecurity challenges for SMEs are increasing while the ability, or desire, to cope with these challenges is waning. Given the precariousness of this circumstance, we have provided a perspective on the issue that suggests that the marketplace that could support SMEs to adopt secure IT operations very likely lies in approaches that remove direct IT operations entirely. As this will undoubtedly become an unfamiliar and unwanted cost, this cost needs to be prices throughout the information ecosystem that supports the SME. Furthermore, additional 3rd party indicators of authentic services and compliance may adjust consumer expectations with respect to appreciating the full cost of the SME goods and services. While this is more of an aspirational and not operational analysis of the results of the study, it is offered as more prudent than calls for more SME education and training.

References

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. Dimopoulos, V., Furnell, S., Jennex, M.E., and Kritharas, I., "Approaches to IT Security in Small and Medium Enterprises," 2nd Australian Information Security Management Conference, November 2004.
8. Dzimiela, C. and Jennex, M.E., (2023). An Inside View of A Ransomware Attack Response And Recovery. Journal of Information Systems Security, JISSec, 19(2), pp. 97-114. ISSN: 1551-0123, available online at www.jissec.org
9. Jennex, M.E., Addo, T.B.A., and Walters, A., "SMEs and Knowledge Requirements for Operating Hacker and Security Tools" Information Resource Management Association Conference 2004, IRMA2004, Idea Group Publishing, May 2004.
10. Jennex, M.E. and Durcikova, A. (2014). "Integrating IS Security with Knowledge Management: Are We Doing Enough To Thwart The Persistent Threat?." 47th Hawaii International Conference on System Sciences, HICSS47, IEEE Computer Society, January 2014.
11. Jennex, M. E., Durcikova, A., and Ilvonen, I., (2022). Modifying Knowledge Risk Strategy Using Threat Lessons Learned from COVID-19 in 2020-21 in the United States. The Electronic Journal of Knowledge Management, 20(3), pp. 138-151, ISSN 1479-4411, available online at www.ejkm.com
12. 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.
13. Mburu, M. (2023). CYBER SECURITY IN SMALL AND MEDIUM ENTERPRISES. Unpublished thesis, Uppsala University, Sweden, retrieved on February 10, 2024 from file:///C:/Users/murph/OneDrive/Documents/0d85eabd-26cd-45e1-af94-2fd9df9946dd.pdf

14. 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.
15. 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.
16. Raghavan, K., Desai, M., and Rajkumar, P. V. (2020). Multi-step Operations Strategic Framework for Ransomware Protection. SAM Advanced Management Journal, 85(4), 16-2.
17. 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

Appendix 1 – Audit Plan Template

Audit Plan

Purpose

The purpose of this audit is to check the configuration of the computer and router at the Xxxxxxxxx restaurant. Additionally we will review the physical security and security processes of the restaurant.

Outcome

The outcome of this audit will be recommendations for the owner of the restaurant.

Scope

The scope of the audit is the Internet connection, computer, and data processes in the restaurant.

Audit Procedure

Arrival: The auditor/audit team will arrive at the restaurant and contact the owner, Lauar Sellers, for an access code/access/authorization to proceed. Auditor/audit team will then walk into the facility using the code/access/authorization to gauge staff reactions.

Introduction: Once auditor/audit team is satisfied with the entry exercise they will introduce themselves to Xxxxxxxxx.

Audit Meeting: Once introduced, the auditor/audit team will work with Xxxxxxxxx and any members of the staff, as requested by Xxxxxxxxx, to complete the attached audit plan documentation. Items may be added to the audit plan as necessary and as agreed between the auditor/audit team and Xxxxxxxxx. These items will be documented using the blank lines in the audit plan.

Audit Hot Wash: Once the auditor/audit team has completed the attached Audit Plan document the auditor/audit team will inform Xxxxxxxxx that the audit is complete and will then conduct a post audit meeting with Xxxxxxxxx. The purpose of this meeting will be for the auditor/audit team to convey initial findings and for the auditor/audit team and Xxxxxxxxx to generate and agree on any needed action plan/further information needed/potential recommendations/etc..

Audit Commenced (time/date): 1400, 6/30/2022 Audit Complete (time/date):1530, 6/30/2022

Auditor: Murray Jennex, xxxxxxxxx, xxxxxxxx

Xxxxxxxxx xxxxxxxxx:

	Audit Plan: **Items and Observations** **Auditor:** **Date:**			
Item #	**Description**	**Expected Findings/pass criteria**	**Observations**	**Pass (Yes/ No)**
1	Check password strength	Should be strong: no dictionary word	Ok but metro is a dictionary word, some passwords were posted on yellow stickies	no
2	Check ports using shield's up	Ports are in stealth or at least closed	Port 80 is open, most ports reply closed instead of being in stealth	no
3	Check for missing updates	Computer is up to date with auto updates on	Auto updates on, there is a new version of Mac OS available	yes
4	Check for back up	Back up exists	Back up to cloud	yes
5	Computer is kept in a location with controlled access	Access is limited to those with a need	Door is left open, only one account	no
6	Review computer files for possible malware	No malware found	No malware found, but computer has low RAM	yes
7	Check for access control on personal files	Only computer owner can access all files	Only one account so personal files accessible	no
8	Check for malware protections	Malware protection active	Expired webroot	no
9	Check for surge protection on power supply	Surge protection present	Plugged into wall, no surge protection	no
10	Check Router in location with good air flow	Air flow and temperature okay	Ok air flow, room cool	yes
11	Router is kept in a location with controlled access	Access is limited to those with a need	In server room	yes
12	Ensure router is password protected	Password is active	Password active	yes
13	Ensure access controlled on all business systems	Access is controlled	Access controlled	yes
14	Ask about a security plan	Security policies are in place	No formal security plan	no
15	Check for other digital devices	No other devices	Fax/printer, several ipads	Yes, okay
16	If additional devices discovered check for the above on them	Passwords, backups, access control exist	Didn't check	okay