Task, Knowledge, Skill, and Ability: Equipping the Small-Medium Businesses Cybersecurity Workforce

Aadithyan Vijaya Raghavan, Cleveland State University

Aadithyan performed the research described in the paper as part of his Thesis for a Master of Science degree in Electrical Engineering at Cleveland State University. Upon graduation, he currently works at Ford Motor Company as a NetCom Development and Quality Engineer.

Dr. Chansu Yu, Cleveland State University

Chansu Yu received the B.S. and M.S. degrees in electrical engineering from Seoul National University, Korea, in 1982 and 1984, respectively, and the Ph.D. degree in computer engineering from the Pennsylvania State University in 1994. He is currently Chai

Task, Knowledge, Skill, and Ability: Equipping the Small-Medium Businesses Cybersecurity Workforce

Vijaya Raghavan, Aadithyan
Cleveland State University
a.vijayaraghavan@vikes.csuohio.edu

Yu, Chansu
Cleveland State University
c.yu91@csuohio.edu

Abstract

With cyberattacks becoming more frequent and targeted, small-medium businesses (SMBs) are forced to adopt a cybersecurity framework to help secure their cyberspace. While these frameworks are a good starting point for businesses and offer critical information on identifying, preventing, and responding to cyber incidents, they can be hard to navigate and implement. To help with this issue, this paper identifies the most frequent attack vectors to SMBs and proposes a practical model of Knowledge, Skills, Ability, and Tasks (TKSA) from the NICE Framework for those attacks. SMBs can use the model as a guideline to assess, equip their existing workforce, or aid in hiring new employees. Additionally, educational institutions can use the model to develop scenario-based learning modules to adequately equip the emerging cybersecurity workforce for SMBs.

1 Introduction:

Cyberattacks come bearing heavy costs to businesses and they are increasing each year, with 47% of the businesses in the US having experienced a cyberattack in 2022, showcasing a stark increase of 7% from the previous year 2021. Due to these cyberattacks, 22% of the companies suffered a loss of customers as well as found difficulty with attracting new customers [1], and these attacks place immense financial pressure on businesses. The average cost of business being disrupted due to a cyberattack has increased from $1.56 million in 2018 to $1.90 million in the year 2019, a 21% increase [2]. Nonetheless, according to the Hiscox Cyber Readiness Report in the year 2022, 72% of the businesses in the United States are classified as Cyber novices i.e., they have poor strategy and execution in dealing with cyber-attacks [1]. This is especially concerning for small-medium businesses (SMBs) because of their limited resources and their lack of awareness [3],[4].

There are over 32 million SMBs in the US [5], and cyberattacks are a serious threat to them. Cybersecurity awareness and education have played a significant role in improving employee awareness. This paper proposes a comprehensive model of knowledge and skillset that will help SMBs in defending themselves. Our research was steered by three overarching questions.

First. "Where do SMBs stand with respect to cybersecurity?" This question allows us to collect and synthesize existing data, and perform gap analysis to identify a need for bridging the gap between the current SMB workforce and best practices.

Second. "What are the most frequent and impactful attacks faced by SMBs?" This allows us to center the scope of our research on the most frequent and impactful attacks. This is done in order to maximize the area of coverage with as little workforce as possible, due to the limited nature of an SMB. Our research found that, the most frequent attacks are phishing/social engineering, malware/ransomware, and web-based attacks (Section 3.1).

Third. "How can the workforce be equipped with the necessary knowledge, and skills to apply the best practices?" This helps us incorporate the NICE Framework as a bridge between the workforce and the best practices by mapping the TKSA to the most frequent attacks. However, the NICE workforce framework lists a total of 634 knowledges, 377 skills, 1006 tasks, and 177 abilities making it unaffordable for SMB owners. Our research yielded a total of 88 technical TKSA and 54 non-technical TKSA that is required to defend against the three attacks, this is 6.23% of the total TKSAs present in the NICE Framework, and is much more affordable for SMBs (section 3.2 and 3.3).

The rest of the paper is organized as follows, section 2 discusses related works and touches briefly about the cybersecurity frameworks, section 3 discusses the proposed methodology behind our research including the identification of the three frequent attacks and determining the best practices to counter them and map them to the TKSA present in the NICE Framework, and section 4 talks about the results and discusses in depth about the models. And lastly, section 5 talks about the closing remarks.

2 Related Work:

There exist several cybersecurity frameworks, one such framework is The International Organization for Standardization (ISO) 27001, a well-known standard when it comes to information security management systems (ISMS) [6]. The NIST Cyber Security Framework (CSF), consists of three main components; the Framework Core, Implementation Tiers, and Profiles [7]. Factor Analysis of Information Risk (FAIR) Cyber Risk Framework [8], is a model that helps businesses analyze, measure and understand the risks posed by cyber incidents mainly in a two-way classification; loss event frequency, and loss magnitude. Nonetheless, many businesses are still lacking in their understanding of them, particularly SMBs [3],[4],[9],[10]. According to the Organization for Economic Co-operation and Development (OECD), a medium-sized enterprise/business consists of an employee count greater than 50 but below 200 500, with the upper limit varying from country to country, while a small-sized enterprise/business consists of an employee count of less than 50 [11].

To address the gap in the workforce, we propose a TKSA model from the comprehensive NICE Framework published by the National Institute of Standards and Technology (NIST) [12]. The NICE framework defines a set of building blocks named Tasks, Knowledge, Skills, and Abilities (TKSA). These four blocks form the base for building different Competencies, Work Roles, and Teams. Businesses and individuals can use the framework to assess/train themselves, it acts as a bridge between educators, employees, and businesses.

The NICE Framework and the TKSA model has been a foundation of several cybersecurity research work. Kim et al. proposed identifying the commonality and differences among three different sectors; the government, academia, and private, with respect to TKSA [13]. Their research was conducted by performing an ontological qualitative analysis using archival data and this was a limitation of their research, because of their data being archival, their findings might not reflect the current market. Nevertheless, their research provides excellent insight into how TKSA can be related to roles in different sectors. While this research was helpful, it only points out the relationship between the three different sectors and how interconnected they are. But a major takeaway from their work is that it highlights the versatility and the unique application of the NICE Framework.

Bada et al. performed a case study in developing a cybersecurity awareness program for SMBs [14]. They first performed a literature review based on certain keywords and studied the best practices in securing a business' cyber space. Their final program was heavily based on the existing London Digital Security Center (LDSC) program which consists of five primary areas, and changes to the program were performed as per their findings and recommendations. While this is a step in the right direction with spreading awareness about cybersecurity in SMBs and businesses in general, their research did not focus on specific attacks or utilize the NICE Framework which can prove to be an excellent bridge between the workforce and educational institutes.

Tobey et al. studied how applying competency-based learning can help in creating an industry-ready cybersecurity workforce [15]. Their work discusses the difference between the outcome-based approach, which is the current approach followed by most fields of study, and the competency-based approach. The NICE Framework gives us the ability to create our own competencies based on the different TKSA [16]. A competency statement is made up of a combination of different TKS, it is flexible and can be changed as per the needs. They go on to suggest that the NICE Framework is a good starting point for education institutes to start basing their courses [15].

3 Proposed Work:

This section is broken into three subsections. Section 3.1 discusses the attack identification process including the documents and reports used, and the justification behind selecting the attacks discussed in this paper. Section 3.2 discusses the process of identifying the best practices to combat the attacks identified in section 3.1. This section also delves into the keyword extraction program used in this paper, and also talks about the de-duplication of similar keywords, specifically the use of Levenshtein similarity. Section 3.3 wraps up the proposed work portion by talking about how the mapping of keywords to the NICE Framework was performed.

3.1 Identifying The Most Frequent Attacks

To identify the most common attacks, we referred to reports published by Verizon, Hiscox, and Ponemon Institute, and government agencies such as The Cybersecurity and Infrastructure Security Agency (CISA), the European Union Agency for Cyber-security (ENISA). They publish latest trend reports about various cyberattacks, cost of mitigation, and many other valuable

information to help organizations prioritize their resources to defend themselves. The data they collect is usually based on surveys which multiple organizations participate in. Table 1 shows the list of the reports.

According to the Verizon report in 2022, studying 18,419 cyberattacks, over 70% were web-based attacks, 30% were malware-based, and 20% were social engineering attacks [17]. Note that some of the attack vectors may overlap, resulting in the total percentage to be over 100%. The Ponemon report also shows the top three attack vectors faced by SMBs are phishing/social engineering, web-based attacks and malware [2]. The Hiscox Cyber Readiness Report published in 2022 paints a similar picture on the frequent attack variables, it labeled phishing as the most prevalent attack vector, followed by ransomware [1].

Table 1: List of documents used to identify the attack vectors

Publisher	Document
Verizon	Data Breach Investigation Report (DBIR) 2022 [17]
Ponemon Institute	Ponemon Institute 2019 Global State of Cybersecurity in Small to Medium-sized Businesses [2]
Cybersecurity and Infrastructure Security Agency (CISA)	CISA Insights [18]
Hiscox Group	Hiscox Cyber Readiness Report 2022 [1]
European Union Agency for Cybersecurity (ENISA)	Cybersecurity for SMEs – Challenges and Recommendations [19] ENISA Threat Landscape: List of top 15 threats [20]

CISA labeled ransomware as the most visible cyberattack faced by businesses in the US [18]. A report published by the ENISA states that phishing and malware attacks are the most common attacks faced by SMBs [19], and another report published by ENISA titled "List of top 15 threats" declare Malware, Web-based attacks, and Phishing to be the top three attacks [20].

Based on the aforementioned reports, we decided to narrow the scope of our research to phishing/social engineering, malware, and web-based attacks. First, the three at-tacks would cover a significant percentage of the attacks SMBs face. Second, SMBs do not have a significant workforce or budget to deal with all the possible types of cyberattacks.

3.2 Identifying Best Practices and Extracting Keywords

In order to obtain the desired set of TKSA for the defense against the three attack vectors, this paper uses a well-known keyword extractor, Yet Another Keyword Ex-tractor! (YAKE!) [31], on the documents published by government agencies and standardization institutions/organizations as shown in Table 2 and Table 3.

First. Keyword extraction has been widely used to derive knowledge maps [32, 33, 34]. YAKE! allows us to achieve better results compared to other state-of-the-art keyword extraction methods such as Rake, TextRank [31]. The n-gram parameter which stands for the size of a sequence of terms in a keyword, was suggested to be set at 3 for best results [31].

Second. To ensure the credibility and quality of the best practices, we restricted our pool of

Table 2: List of documents categorized by publisher and attacks

Publisher	Document	Attack Vector
Cybersecurity and Infrastructure Security Agency (CISA)	Capacity Enhancement Guide: Counter-phishing recommendations for Non-Federal Organizations [21] Capacity Enhancement Guide: Counter-phishing recommendations for Federal Organizations [22] CISA Website Security [23] CISA Ransomware Guide [24]	Phishing/Social Engineering Web-based Attacks Malware/Ransomware
Australian Cybersecurity Centre (ACSC)	ACSC Ransomware Prevention and Protection Guide [25]	Malware/Ransomware
National Cyber Security Centre (NCSC)	NCSC Mitigating malware and ransomware attacks [26]	Malware/Ransomware
National Institute of Standards and Technology (NIST)	NIST SP 800-83r1: Guide to Malware Incident Prevention and Handling for Desktops and Laptops [27]	Malware/Ransomware
European Union Agency for Cybersecurity (ENISA)	ENISA Threat Landscape 2020 – Web-based Attacks [28]	Web-based Attacks

Table 3: List of documents specific to SMBs

Publisher	Document	Attack Vector
Federal Trade Commission (FTC)	Cybersecurity for Small Businesses: Phishing [29]	Phishing/Social Engineering
Cybersecurity and Infrastructure Security Agency (CISA)	CISA Insights: Mitigations and hardening guidance from MSPs and Small and Mid-Sized Businesses [30]	Malware/Ransomware

documents to limited but highly credible and well-established ones from organizations such as NIST, CISA, Federal Trade Commissions (FTC), as well as ENISA, National Cyber Security Centre (NCSC), and Australian Cybersecurity Centre (ACSC) as in Table 2. We included documents that were specific to SMBs as shown in Table 3. Table 4 shows the snippet of keywords extracted from a document [21], along with their score (S). Score (S) is based on keyword features (term casing, term position, term frequency normalization, term relatedness to context, term different sentence) and is computed by the YAKE! Algorithm [31]. Lower the value of S, the more significant the keyword [31].

Third. To eliminate similar keywords, we employed a de-duplication process based on similarity algorithms such as Levenshtein similarity [35], Jaro-Winkler [36], and Hamming Distance [37, 38, 39]. We used Levenshtein similarity because it works on the principle of the minimum number of single-character edits required to change one word into the other [38].

For example, take a group of similar keywords like “Secure Gateway Capabilities, Gateway

Table 4: Snippet of keywords extracted from [21]

Keywords	Score (S)	After De-duplication
Secure Gateway Capabilities	0.0023	
Stop Phishing Emails	0.0090	Removed
Secure email gateways	0.0102	
Gateway Capabilities	0.0132	Removed
Secure Gateway	0.0345	Removed
Gateways	0.1013	
Email filter solution	0.1434	
Signatures and blocklists	0.1481	Removed
Host Level Protections	0.1710	

Capabilities, Secure Gateway", all of which are similar and can be considered as just one keyword "Secure Gateway Capabilities". Table 4 shows a snippet of keywords after the de-duplication process is applied, the "After De-duplication" column shows if the keyword was removed after the de-duplication process.

3.3 Mapping Keywords To The NICE Framework

The last step in the research was mapping the NICE framework with the help of the keywords and deriving the model for the three attack vectors. The NICE Framework consists of Task, Knowledge, Skill, and Abilities. We used the keywords extracted from the previous step to perform a search in the NICE Framework using the keyword search tool [40], and mapped the TKSA pertaining to them.

4 Results:

For convenience, we divided the result of the mapping exercise into two models, technical and non-technical models. The technical model consists of all the TKSA that involve a certain level of proficiency in the technical aspect of cybersecurity, whereas the non-technical model consists of TKSA that are related to general cyber awareness, legal, and managerial proficiencies. Most of the non-technical TKSA can be applied to all the employees in an SMB. Sections 4.1 and 4.2 explain the technical and non-technical model respectively, while sections 4.3 and 4.4 talk about the competency that was derived from the TKSA discussed in this paper.

4.1 Technical Model

We mapped 49 technical knowledges covering 7.57% of all the knowledges in the NICE Framework, 23 technical skills covering 6.10% of all the skills in the NICE Framework, 6 technical abilities covering 3.38% of all the abilities in the NICE Framework, and 10 technical tasks covering 1.02% of all the Tasks in the NICE Framework, totaling 88 technical TKSA. These TKSA all address a different aspect of dealing with the three attack vectors. Table 5 depicts the technical Knowledges mapped to the three different attack vectors. Take K0002 for example, the knowledge statement is so broad that it can be used in all three attack cases, whereas K0105 and K0188 are specific to an attack.

Table 5: Snippet of technical knowledge mapped to the three attack vectors (7.8% of all the knowledge in the NICE Framework)

TKSA Number	TKSA Description	Phishing/Social Engineering	Malware	Web-Based Attacks
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.			*
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	*	*	*
K0004	Knowledge of cybersecurity and privacy principles.	*	*	*
K0007	Knowledge of authentication, authorization, and access control methods.	*	*	*
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).			*

56.26% of the technical knowledges we mapped are applicable to just one specific attack vector, i.e., they cannot be applied to a different attack than the ones they are mapped to. 16.66% of the technical knowledges are mapped to two attacks, i.e., it can vary based on the description of the knowledge, they can be used in 2 specific attacks out of the three. E.g., K0202 is applicable to phishing/social engineering attacks, and malware/ransomware attacks but is not applicable to web-based attacks. And for the remaining 27.08% of the knowledge, they are applicable to all three attack vectors.

The technical skills and technical abilities seem to be the least versatile among the different TKSA, with 56.53% of the technical skills and 83.33% of the technical abilities being applicable to only 1 specific attack vector. The technical tasks seem to be the most versatile among the TKSA with 50% of them being applicable to all three attack vectors, and 40% being applicable to at least 2 specific attack vectors.

4.2 Non-Technical Model

The non-technical model consists of 28 non-technical knowledges covering 4.41% of all the knowledge in the NICE Framework, 8 non-technical skills covering 2.12% of all the skills in the NICE Framework, 7 non-technical abilities covering 3.95% of all the abilities in the NICE Framework, and 11 non-technical tasks covering 1.12% of all the tasks in the NICE Framework, adding up to a total of 54 non-technical TKSA. They paint a different picture when compared to the technical model due to most of the general TKSA being applicable to all the 3 attack vectors. Table 6 depicts how non-technical Knowledges are mapped to the three attack vectors. 93% of the non-technical knowledges are applicable to all 3 attack vectors with only 7% of the non-technical knowledges being applicable to one specific attack. 85% of the non-technical abilities and 87.5%

Table 6: Snippet of non-technical knowledge mapped to the three attack vectors (4.4% of all the knowledge in the NICE Framework)

TKSA Number	TKSA Description	Phishing/Social Engineering	Malware	Web-Based Attacks
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	*	*	*
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	*	*	*
K0066	Knowledge of Privacy Impact Assessments.	*	*	*
K0126	Knowledge of Supply Chain Risk Management Practices (NIST SP 800-161)		*	
K0267	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.	*	*	*

of the non-technical skills are applicable to all 3 attack vectors while 91% of the non-technical tasks are applicable to all 3 attack vectors.

4.3 Competency

We derived a competency based on the guidelines provided by NIST [16], based on the results of our mapping exercise. A competency according to NIST is defined as measurable cluster of related TKSA in a particular domain. Competencies consists of a name, description of the area, and group of associated TKSA [16]. Table 7 shows our derived competency, the competency encompasses all the 142 TKSA derived from the mapping exercise.

Table 7: Competency derived from all the TKSA discussed in this paper.

Competency Title	Competency Description
Mitigation, prevention and response to Phishing/social Engineering, Malware, and Web-based attacks	This competency describes a learner's capabilities related to the prevention, mitigation, and response to phishing/social engineering, malware, and web-based attacks in a SMB. Includes understanding on technical knowledge such as network analysis, malware analysis as well as non-technical knowledge such as rules and regulations pertaining to cyber incident response, local laws related to cyber operations of a business.

4.4 Competency To Education

To provide further insights on how the results of our work can be used, we show an example of how coursework at Cleveland State University [41] covers, if not aims to cover the 13 knowledges

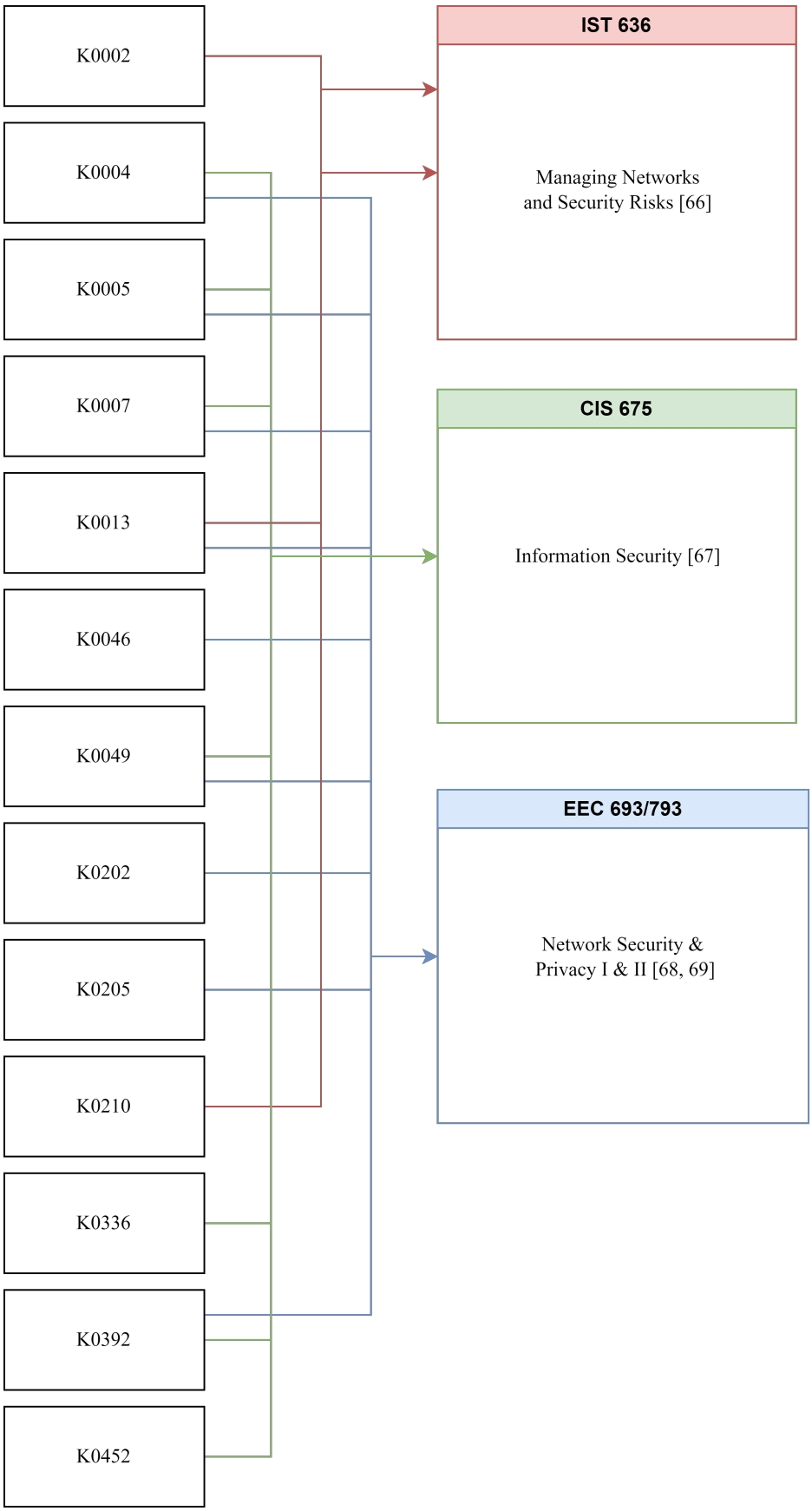

Figure 1: Cleveland State University coursework encompassing various technical knowledges The figure shows how various Knowledge that pertain to one or more attack are covered in various coursework from Cleveland State University

from our technical model. The four courses [42],[43],[44],[45] shown in Fig. 1. encapsulate the 13 technical knowledges that are common to all three attack vectors.

While we're not attempting to develop a curriculum, we simply wish to show a use case scenario of the outcomes presented in this research, which is institutions using the two models to create new/modify existing course works to better incorporate the TKSA from the NICE Framework.

5 Conclusion And Future Work:

We wanted to create a model based on the NICE Framework, that helps bridge the gap between the workforce and cybersecurity best practices, particularly for SMBs.

Our findings led to a model that serves as a sound reference for SMBs to equip themselves with and defend against the attacks discussed in this paper. With the TKSA acting as a bridge between the implementation of the best practices and the Knowledge, Skill, and Ability required, SMBs can focus on the model and create evaluation, and training activities for their existing workforce. SMBs can further extend the work presented in this paper by building their own competencies, and work roles based on the TKSA presented here and NIST guidelines. This opens up a path for SMBs to collaborate with educational institutions to build new coursework based on real-world scenarios.

Educational institutions can design new competencies based on the TKSA presented in this paper and build a fully modular multidisciplinary course with a scenario-based learning [46] module to help equip the upcoming cyber-workforce.

With cybersecurity being an ever-growing and ever-changing field, TKSA can be derived for more than just the three attacks discussed in this research. In the future, we aim to determine a list of TKSA for cybersecurity best practices related to the Internet of Things (IoT) domain. Businesses and individuals are adopting smart technologies, and many are not aware of the threats they expose themselves to. With very little literature available in the field, we aim to touch upon these topics and expand our current work to include them in the future.

6 Acknowledgment:

This work was supported in part by the U.S. National Science Foundation under Grant 2028397.

References

[1] H. Group, "Hiscox cyber readiness report." https://www.hiscoxgroup.com/cyber-readiness, 2022.

[2] P. Institute, "Global state of cybersecurity in small to medium-sized businesses." https://www.cisco.com/c/dam/en/us/products/collateral/security/ponemon-report-smb.pdf, 2019.

[3] S. Dojkovski, S. Lichtenstein, and M. J. Warren, "Fostering information security culture in small and medium size enterprises: An interpretive study in australia," *ECIS 2007 Proceedings*, 2007. [Available]: http://aisel.aisnet.org/ecis2007/120.

[4] C. Paulsen, "Cybersecuring small businesses," *Computer*, vol. 49, p. 92–97, Aug. 2016. doi: 10.1109/mc.2016.223.

[5] S. B. Adminstration, "Frequently asked questions about small businesses.." https://cdn.advocacy.sba.gov/wp-content/uploads/2021/12/06095731/Small-Business-FAQ-Revised-December-2021.pdf, 2021.

[6] ISO, "ISO/IEC 27001." https://www.iso.org/standard/27001, Oct. 2022.

[7] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*. Apr. 2018. doi: 10.6028/nist.cswp.04162018.

[8] J. Freund and J. Jones, *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann, Sept. 2015.

[9] E. Osborn and A. Simpson, "Risk and the small-scale cyber security decision making dialogue—a UK case study," *The Computer Journal*, vol. 61, p. 472–495, Sept. 2017. doi: 10.1093/comjnl/bxx093.

[10] A. Chidukwani, S. Zander, and P. Koutsakis, "A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations," *IEEE Access*, vol. 10, p. 85701–85719, Aug. 2022. doi: 10.1109/ACCESS.2022.3197899.

[11] O. S. Directorate, "Oecd glossary of statistical terms - small and medium-sized enterprises (smes) definition," 2005.

[12] R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel, and G. Witte, *Workforce Framework for Cybersecurity (NICE Framework)*. Nov. 2020. doi: 10.6028/nist.sp.800-181r1.

[13] K. Kim, J. Smith, T. A. Yang, and D. J. Kim", "An exploratory analysis on cybersecurity ecosystem utilizing the NICE framework," *National Cyber Summit (NCS)*, June 2018. doi: 10.1109/ncs.2018.00006.

[14] M. Bada and J. R. C. Nurse, "Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (smes)," *Information and Computer Security*, vol. 27, no. 3, p. 393–410, 2019. doi: 10.1108/ics-07-2018-0080.

[15] D. H. Tobey, A. B. Watkins, and C. W. O'Brien, "Applying competency-based learning methodologies to cybersecurity education and training: Creating a job-ready cybersecurity workforce.," *Infragard Journal*, pp. 1–14, June 2018.

[16] K. A. Wetzel, *NICE Framework Competencies: Assessing Learners for Cybersecurity Work*. NIST, Dec. 2021. doi: 10.6028/nist.ir.8355-draft2.

[17] Verizon, "Data breach investigation report 2022." https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/, 2022.

[18] CISA, "CISA insights ransomware outbreak." https://www.cisa.gov/uscert/sites/default/files/2019-08/CISA_Insights-Ransomware_Outbreak_S508C.pdf, 2019.

[19] ENISA, "Cybersecurity for SMEs - challenges and recommendations." https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes, June 2021.

[20] ENISA, "List of top 15 threats ENISA Threat Landscape." https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-enisas-list-of-top-15-threats, 2020.

[21] CISA, "Capacity enhancement guide: Counter phishing recommendations for non-federal agencies." https://www.cisa.gov/sites/default/files/publications/Capacity_Enhancement_Guide-Counter-Phishing-Recommendations_for_Non-Federal_Organizations_0.pdf.

[22] CISA, "Capacity enhancement guide: Counter phishing recommendations for federal agencies." https://www.cisa.gov/sites/default/files/publications/Capacity_Enhancement_Guide-Counter-Phishing_Recommendations_for_Federal_Agencies_1_0.pdf.

[23] CISA, "Website security," Nov. 2018.

[24] CISA, "Ransomware guide." https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf, Sept. 2020.

[25] ACSC, "Ransomware prevention and protection guide." https://www.cyber.gov.au/sites/default/files/2023-03/ACSC_Ransomware_Prevention_Guide_05082022_0.pdf.

[26] NCSC, "Mitigating malware and ransomware attacks." https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks, Feb. 2020.

[27] M. Souppaya and K. Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*. NIST, 2013. doi: 10.6028/nist.sp.800-83r1.

[28] ENISA, "ENISA threat landscape 2020 - web-based attacks." https://www.enisa.europa.eu/publications/web-based-attacks, Oct. 2020.

[29] FTC, "Cybersecurity for small business: Phishing." https://www.ftc.gov/system/files/attachments/phishing/cybersecurity_sb_phishing.pdf.

[30] CISA, "CISA insights: Mitigations and hardening guidance for MSPs and small- and mid-sized businesses." https://www.cisa.gov/sites/default/files/publications/CISA%20Insights_Guidance-for-MSPs-and-Small-and-Mid-sized-Businesses_S508C.pdf, July 2021.

[31] R. Campos, V. Mangaravite, A. Pasquali, A. Jorge, C. Nunes, and A. Jatowt, "YAKE! keyword extraction from single documents using multiple local features," *Information Sciences*, vol. 509, p. 257–289, Jan. 2020. doi: 10.1016/j.ins.2019.09.013.

[32] C. Chen, "Science mapping: A systematic review of the literature," *Journal of Data and Information Science*, vol. 2, p. 1–40, Mar. 2017. doi: 10.1515/jdis-2017-0006.

[33] B. Yoon, S. Lee, and G. Lee, "Development and application of a keyword-based knowledge map for effective RD planning," *Scientometrics*, vol. 85, p. 803–820, Sept. 2010. doi: 10.1007/s11192-010-0294-5.

[34] M. F. Manesh, M. M. Pellegrini, G. Marzi, and M. Dabic, "Knowledge management in the fourth industrial revolution: Mapping the literature and scoping future avenues," *IEEE Transactions on Engineering Management*, vol. 68, p. 1–12, Jan. 2020. doi: 10.1109/tem.2019.2963489.

[35] V. I. Levenshtein *et al.*, "Binary codes capable of correcting deletions, insertions, and reversals," in *Soviet physics doklady*, vol. 10, pp. 707–710, Soviet Union, 1966.

[36] W. E. Winkler, *String comparator metrics and enhanced decision rules in the Fellegi-Sunter model of record linkage.* ERIC, 1990. [Available]: https://eric.ed.gov/?id=ED325505.

[37] SeatGeek, "Thefuzz." https://github.com/seatgeek/thefuzz.

[38] D. D. Prasetya, A. P. Wibawa, and T. Hirashima, "The performance of text similarity algorithms," *International Journal of Advances in Intelligent Informatics*, vol. 4, p. 63, Mar. 2018. doi: 10.26555/ijain.v4i1.152.

[39] R. W. Hamming, "Error detecting and error correcting codes," *The Bell system technical journal*, vol. 29, no. 2, pp. 147–160, 1950. doi: 10.1002/j.1538-7305.1950.tb00463.x.

[40] NIST, "NICE framework keyword search." https://niccs.cisa.gov/workforce-development/nice-framework/tasks.

[41] C. S. U. Ohio, "Cleveland state university." https://www.csuohio.edu/.

[42] C. S. U. Ohio, *IST 636 - MANAGING NETWORKS AND SECURITY RISKS*. https://catalog.csuohio.edu/preview_course_nopop.php?catoid=40&coid=185307.

[43] C. S. U. Ohio, *CIS 675 - Information Security*. https://engineering.csuohio.edu/sites/csuohio.edu.engineering/files/CIS-675.pdf.

[44] C. S. U. Ohio, *EEC 693/793 Network Security Privacy I*. https://engineering.csuohio.edu/sites/csuohio.edu.engineering/files/EEC-693%2C793_5.pdf.

[45] C. S. U. Ohio, *EEC 693/793 Network Security Privacy II*. https://engineering.csuohio.edu/sites/csuohio.edu.engineering/files/EEC-693%2C793_6.pdf.

[46] T. Ghosh and G. Francia, "Assessing competencies using scenario-based learning in cybersecurity," *Journal of Cybersecurity and Privacy*, vol. 1, p. 539–552, Sept. 2021. doi: 10.3390/jcp1040027.