ISSN: 2473-4901
v10 n6115

Importance of Soft Skills Comparative Study with Cybersecurity Professionals in the Manufacturing and Finance Critical Sectors

Stanley J. Mierzwa
smierzwa55724@ucumberlands.edu

Mary Lind
mary.lind@ucumberlands.edu

School of Computer and Information Sciences
University of the Cumberlands
Williamsburg, KY 40769, USA

Abstract

Cybersecurity professionals require and will benefit from having strong and competent technical and soft skills, knowledge, and abilities. Cyber-attacks continue to plague our organizations and businesses, and finding the individuals with the skills needed for industry teams to contend with these broad and varying types of breaches is essential. This research article will outline the results of a comparative quantitative study that compares the importance of soft skills or nontechnical competencies by information security and cybersecurity professionals in the finance and manufacturing critical infrastructure sectors. This research study used a validated survey instrument from a previous seminal study to capture results from cybersecurity and information security professionals from the United States focused on management, business, and interpersonal soft skills. The survey population from the finance and manufacturing critical sectors used resulted in (N = 185) usable records from which analysis using the Mann-Whitney U test calculations occurred. This study provided evidence that the soft skills within the business functional construct were perceived as more critical to the finance sector than to the manufacturing sector. Understanding what soft skills and abilities are considered essential and what differences exist between the critical sectors of the United States economy can be valuable to both industry professionals and the academic community, from which many cybersecurity graduates will exit and join work roles in the field. Many studies include content related to the technical skill needs of cybersecurity professionals, but this study emphasizes nontechnical and soft skills. The results of this study will contribute to those academic institutions planning to create, modify, or enhance their cybersecurity and information security programs and offerings.

Keywords: Cybersecurity; Information Security; Soft Skills; Nontechnical Skills; Manufacturing Sector; Finance Sector

1. INTRODUCTION

Cybersecurity or information security programs may reside in different academic discipline homes ranging from computer science, information technology, and even criminal justice majors. These programs, which can be considered under the broad spectrum of information systems and technology, require that students possess the proper balance of technical skills (hard skills) as well as soft skills to prepare them to enter work roles with success after completing their education (Bohler et al., 2020). This research study emphasized and focused on the perceived

©2024 ISCAP (Information Systems and Computing Academic Professionals)

importance of soft skills of cybersecurity professionals in the manufacturing and finance sectors. Including soft skills combined with technical or complex skills will only be further valuable for organizations given the more advanced and emerging types of cyber threats, attacks, and breaches that continue to grow in volume (Brilingaitė et al., 2020). The creation of updated job descriptions in cybersecurity and information security will benefit from greater inclusion of soft skills (Booker & Munmun, 2023).

This study will detail the critical components of the research activity, including the theories and frameworks adopted, validated survey instrument utilized, abbreviated literature review, research questions, and results. Finally, a discussion, conclusion, and limitations are provided.

2. THEORETICAL MODEL AND FRAMEWORK

Several frameworks common to information technology, information systems, and security were utilized as a theoretical guide to this research effort. The leading theory used was the technology-organization-environment (TOE) model, along with support from the socio-technical systems (STS) and the holistic competency model. The TOE framework, created by Depietro et al. (1990), provides good alignment with an understanding of the many aspects of implementing, building, and integrating information technology products and solutions, including cybersecurity, in organizations.

The TOE with extended attributes for cybersecurity was previously utilized by Wallace et al. (2020), studying the intersection of cybersecurity adoption decisions. Because the TOE is considered very broad, this study pursued supporting theories with a specific aim toward social and soft skills. Bostrom and Heinen (1977a, 1977b) initiated and developed the STS, which provides the framing with information systems, cybersecurity, and other solution integrations that were the element of two correlative systems, the social and technical constructs. The social construct parallels well with this current research effort emphasizing soft skills, as Bostrom and Heinen (1977a, 1977b) iterated the importance of the human effect and aspects as foundational to the field of information systems. The demonstrated model in this research combines the models in Figures 1 and 2. The STS and holistic competency model feed the construct variables into the TOE. The holistic competency model provides a far-reaching view, variable, and social dimensional vision of technological innovations and implementations when introducing the concepts of required technical knowledge, skills, and abilities (Le Deist & Winterton, 2005; Persaud, 2020). Pursuing a more holistic development of student education in academic programs will help to increase the potential for employability and meet industry sector needs and gaps (Dubey et al., 2022).

The combination of the TOE with support from the STS and the holistic competency model provides a unified structure that permits the intersections of soft skills and technical skills that are part of this research investigation. Including the SDLC framework allows cybersecurity technologies, solutions, and practices to be introduced into different lifecycle parts. Figure 1 depicts the theoretical model and includes the facets of technical skills and competencies funneling into the technology pillar of the TOE as well as the technical component subsystem of the socio-technical system. The organization prong of the TOE was fed the elements of the socio-subsystem components of the socio-technical framework and the technology management skills and interpersonal skills constructs. It yielded research questions 1 and 3. The role of business functional knowledge and skills will vary depending on the sector and the variables of this construct funnel and align with the holistic competency model, which connects to the environment pillar of the TOE and yielded research question 2.

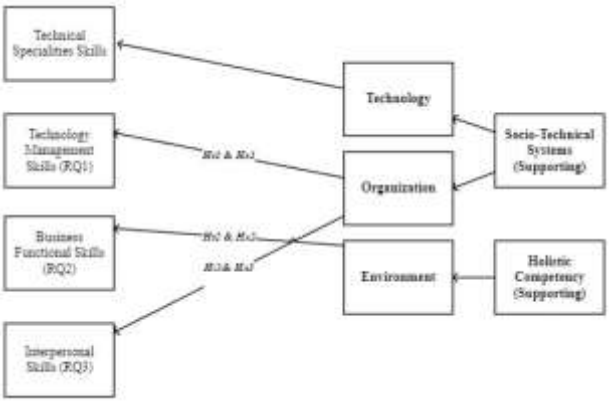

Figure 1: Theoretical Model Tested

Note: Figure 1 was generated for this study to outline the primary and supporting theories.

ISSN: 2473-4901
v10 n6115

Figure 2: Construct Variables and Sectors Research Questions

Three research questions, in alignment with the components of Figure 2, pursuing soft skills were approached in this comparative study and are as follows:

RQ1. To what extent do cybersecurity professionals' technology management skills differ in the finance and manufacturing sectors?

RQ2. To what extent do cybersecurity professionals' business functional skills differ in the finance and manufacturing sectors?

RQ3. To what extent do cybersecurity professionals' interpersonal skills differ in the finance and manufacturing sectors?

3. LITERATURE REVIEW

Constructs Background

The soft skills and complex technical skill constructs selected for this research activity emanate from the seminal work by Lee et al. (1995) that surrounded information systems professionals' critical skills and knowledge requirements. The study included facets that remain critically important today to information technology professionals but are similar to those focused on information security or the cybersecurity discipline realm. Overall, the study by Lee et al. (1995) suggested that information technology professionals will require knowledge of technology hard skills, business skills, management skills, and interpersonal qualities to lead organizations successfully. The previous research study presents four constructs of knowledge and skills, including technical specialties, management, business, and interpersonal variables. Participants were asked to rate how important the specific variables in the four constructs are in supporting the needs of their companies, both in the timeframe of now and in three years. The technical variables adopted from the Lee et al. (1995) study include such skills as networking, operating systems, systems integration, programming, data management, and expert systems. The management construct variables comprised of recognizing and understanding trends, focusing on technology as a means, and learning new technologies. The technical specialties skills variables were captured as part of the complete validated survey instrument. Business skills and knowledge include understanding business functions, the business environment of the sector, the ability to learn about business functions, interpreting business problems, and creating solutions. Interpersonal skills encompassed such variables as dealing with ambiguity, working collaboratively, teaching others, planning and organizing, writing and communicating clearly, and being in tune with culture and sensitivity to organizational politics. The constructs of business, management, and interpersonal were the main component areas of the survey included in this research report because of their alignment with soft skills.

Soft Skills or Nontechnical Skills

Soft skills in cybersecurity and information systems and technology security roles vary, and this paper focused on management, interpersonal, and business nontechnical skills. Such skills will contribute to a more holistic and broadly based set of individual competencies. Vess et al. (2023) noted through the Society for Information Management (SIM) Issues and Trends study the priority items and most hard-to-discover soft skills. These included critical thinking, collaboration, business knowledge, leadership, solving problems, being innovative, relationship management, and demonstrating empathy and emotional intelligence. The realm of soft skills can become more critical when professionals take on roles with greater authority, as was outlined by Akdur (2021) in finding that for those in the software industry, greater importance was given to soft skills by experienced professionals and those who have worked in a management role. This finding aids this current research, which aims to determine if academic programs need to be modified in the cybersecurity discipline to meet industry needs.

Cybersecurity Workforce

As information technology and systems continue to advance and develop, there will be times when a skill set shortage or gap exists in newly emerging innovative solutions (Furnell, 2021). Take, for example, the recent expansion and growth of artificial intelligence. This newer technology strategy and solution draws attention

ISSN: 2473-4901
v10 n6115

to the need for such skills. The realm of cybersecurity continues to be an area that continues to experience a significant shortage of skills, especially in critical infrastructure sectors, which is causing potential harm and risks to organizations (Coulson et al., 2018; Furnell, 2021; Jones et al., 2018). There remains a significant need to produce qualified cybersecurity professionals with the proper technical and soft skills and abilities in order for digital solutions to remain available (Jones et al., 2018).

Cybersecurity Degree Frameworks

There continue to be available and developing cybersecurity degree frameworks that may provide overlap between them and varied components. The National Security Agency (NSA) sponsors the Centers of Academic Excellence (CAE) in Cybersecurity. This program focuses on cyber defense, cyber operations, or research. The CAE programs guide academic institutions in pursuing approval or designation after demonstrating knowledge unit alignment, formidable outreach, experiential learning, and a host of other substantial requirements (DoD Cyber Exchange, 2020). The National Initiative for Cybersecurity Education (NICE) Workforce Framework lists and provides the knowledge, skills, and abilities to outline the large variety of cyber work roles in cybersecurity. The NICE framework includes categories for soft skills in addition to technical components. The Association of Computing Machinery (ACM) contributes toward the creation of curriculum recommendations (Brown et al., 2024). As part of the ACM effort to create information technology curriculum guides, one focused on cybersecurity through the CSEC2017 framework has been developed and includes the many holistic components of security and cybersecurity (AlDaajeh et al., 2022; Joint Task Force on Cybersecurity Education, 2017).

Critical Sectors

The areas or categories defined as critical sectors of a nation are critical infrastructures essential for the proper ongoing societal functioning and could harm national security, health, and general wellness (Makrakis et al., 2021). With increasing cyberattacks, the potential exists to disrupt critical infrastructure sectors with security and cybersecurity breaches and attacks. The Department of Homeland Security (DHS) outlines the general classification of 16 critical infrastructure sectors in the United States. Various vital sectors include many, such as transportation, public health, telecommunications, and energy (Plachkinova & Vo, 2023).

The two critical sectors selected for this investigative study included the areas of finance and manufacturing. These two areas may share similar functional staffing departments, as would be expected in any enterprise, but are distinctively different in their core business products. Regarding the nation's economy and resilience, finance is critically important in providing loans, savings, investing, and the ability to deposit and secure financial assets (Raval et al., 2024). Akdur (2021) studied the essential skills of the software industry from various factors, and the results demonstrated that hard and soft skills are directly related to such qualities as work roles, experience, software type, and actual sector. This concept aligns with this current research seeking to determine if a difference in the importance of soft skills exists between the manufacturing and finance sectors.

4. METHODS

This comparative quantitative study was completed by identifying a validated survey instrument that could be adopted and used, creating a secure web-based self-report survey, and analyzing the results. The identified questionnaire was from the seminal work of D. M. S. Lee et al. (1995) and remains relevant even in our current technological state. For this current study, the original questionnaire was modified in only one variable or component: to replace the knowledge or skill of COBOL with Java—approval to utilize the validated instrument was obtained by Lee et al. (1995). In this current research study, the independent variable was the sector (Finance or Manufacturing), and the dependent variables included the constructs of technology management skills, business functional skills, or interpersonal skills.

Data Collection

The web-based survey tool SurveyMonkey allowed for the creation and hosting of the instrument. Using the SurveyMonkey Audience feature permitted the selection of potential survey respondents to those ages 18-99, located in the United States, and from the finance and manufacturing sectors. The data was anonymous, and no personally identifiable information was collected during the effort. The power analysis was performed using G*Power 3.1.97. With the test family set to T-Tests, the statistical test set to means to determine a difference between two independent groups, the sample size pursued was set to at least 74 for each group. The resulting data was analyzed, and all incomplete surveys in

ISSN: 2473-4901
v10 n6115

any field were removed prior to analysis. The total sample size obtained for analysis was *N* = 185; the sector breakdown can be found in Table 2.

Analysis Measurements

The analysis tests performed on the resulting data included T-Tests or Mann-Whitney if the data was nonparametric. From the survey results, all records that were incomplete in any field, either demographic data or Likert-scale questionnaire results, were removed before analysis. The independent sample tests included a comparison being made between the finance and manufacturing sectors with statistical significance measured to reject the null hypothesis with a *p*-value < .05. The statistical test software tool utilized was the IBM Statistical Package for the Social Sciences (SPSS) version 28.0.1.1(15). All analyses were performed on a secured Windows-based laptop with up-to-date security updates and endpoint protection. All analyzed data was kept in duplicate as a backup in a secured cloud location.

Demographics

Several characteristics were captured as part of the demographic information requested in the self-report online survey before the start of the Likert-based questions. The demographic questions obtained as part of the descriptive statistics included survey participant gender, sector, company size in budget and personnel, cybersecurity or information security leadership role, and expected staffing changes. The *N* = 185 completed surveys included those who identified as 94 males, 90 females, and one participant who preferred not to respond, as detailed in Table 1. The sector breakdown included *N* = 110 from the finance sector and *N* = 75 from the manufacturing sector, as demonstrated in Table 2. Of the respondents, *N* = 96 reported having responsibility for cybersecurity or information security in their organizations, as detailed in Table 3. To provide a sense of the organization or company size, the annual budget of the survey respondents is provided in Table 4.

Gender	*N*	%
Female	90	48.6
Male	94	50.8
Prefer not to respond	1	.5
Total	185	100

Table 1: Participants' Gender

Sector	*N*	%
Finance	110	59.5
Manufacturing	75	40.5
Total	185	100

Table 2: Organization or Company Sector

Cybersecurity Responsibility	*N*	%
Yes	96	51.9
No	89	48.1
Total	185	100

Table 3: Responsibility for Cybersecurity or Information Security in an Organization

Size in Annual Budget	*N*	%
Small (less than $250 million)	63	34.1
Medium ($250 million - $1 million)	69	37.3
Large (More than $1 billion)	53	28.6
Total	185	100

Table 4: Company size in annual budget

Reliability and Normality Testing

The validated survey instrument used for this study was adopted from D. M. S. Lee et al. (1995) and created with the input and expertise of 50 individuals in various professional roles and from colleges and universities to outline critical issues to be addressed. The survey underwent a pilot test of 20 relevant professionals before being used in this study.

In this current research effort, the 5-point Likert-scaled survey instrument assessment of the construct variable results ranged from 1 = (Not important) to 5 = (Extremely important). Normality tests were performed using the Kolmogorov-Smirnov and Shapiro-Wilk tests on the survey result data. Respondents were asked to rate the variables in the timeframe of now and three years. The Kolmogorov-Smirnov test results of the construct analysis are found in Table 5. The results indicated that the data did

©2024 ISCAP (Information Systems and Computing Academic Professionals)

ISSN: 2473-4901
v10 n6115

not follow a normal distribution, thus requiring the independent sample tests to use nonparametric strategies. The Mann-Whitney U test was selected based on the results of the non-normal data. The reliability of the survey instrument was tested using Cronbach's Alpha, and the results are outlined in Table 6. The results of optimal value to demonstrate the reliability range from .7 and .9 (Creswell & Creswell, 2018). All four construct survey question results were grouped and analyzed with Cronbach's alpha, and the output was over the .70 range to represent reliability.

Construct	*Kolmogorov-Smirnov Z*	Sig.
Technical Specialties Skills	.197	.000
Technology Management Skills	.279	< .001
Business Functional Skills	.241	< .001
Interpersonal Skills	.246	.000

Table 5: Kolmogorov-Smirnov Test of Normality

Construct	Cronbach's α
Technical Specialties Skills	.971
Technology Management Skills	.889
Business Functional Skills	.928
Interpersonal Skills	.956

Table 6: Cronbach's Alpha analysis

5. RESULTS

The results from pursuing this research in determining the differences between the finance and manufacturing sector technology management, business functional, and interpersonal soft skills are outlined in this section and summarized in Table 7. For the first research question, which approached the importance of technology management skills between the sectors, it was found that no statistical difference existed, via the Mann-Whitney U test, between the finance and manufacturing areas (Z = -1.41, p = .157). This research question statistical test results failed to reject the null hypothesis.

The second research question dove into the importance of business functional skills of cybersecurity professionals and whether there is a perceived difference between the finance and manufacturing sectors. The result of the Mann-Whitney U test discovered that a statistical difference did exist (Z = -3.51, p < .001). The null hypothesis was rejected, and the results demonstrated that a relationship existed in terms of the importance of business functional skills between the finance and manufacturing sectors.

The third research question posed whether a difference is determined between the sectors in the importance of interpersonal skills of cybersecurity professionals. The results of the Mann-Whitney U test outlined that a statistical difference did not exist between the sectors, and the null hypothesis was retained (Z = -1.47, p = .140). This research question statistical test results failed to reject the null hypothesis.

Construct	*Mann-Whitney U*	*Z*	*p*-value
Technical Specialties Skills	4644848.50	-9.466	<.001
Technology Management Skills	141629.00	-1.414	.157
Business Functional Skills	237380.50	-3.513	< 001
Interpersonal Skills	1945325.00	-1.474	.140

Table 7: Mann-Whitney U of Constructs Between Sectors

Table 8 provides the construct means analysis and comparison between the manufacturing and finance sectors. The composite mean demonstrated that the soft skills constructs of technology management, business functional, and interpersonal skills were more important than technical skills.

ISSN: 2473-4901
v10 n6115

	Manufacturing		*Finance*	
Construct	***Now***	***3 Yrs.***	***Now***	***3 Yrs.***
Technical Specialties Skills	3.48	3.62	3.73	3.95
Technology Management Skills	3.98	4.23	4.06	4.36
Business Functional Skills	3.88	4.00	4.04	4.34
Interpersonal Skills	3.93	4.01	3.95	4.20

Table 8: Construct Means Analysis Among Sectors

6. DISCUSSION AND IMPLICATIONS

For cybersecurity academic programs to remain viable and sustainable with benefits to both students and industry needs, continuous improvement can keep their programs fresh and meet expectations. This study aimed to understand if particular soft skills should be further considered in cybersecurity programs and if different sectors may expect different soft skill sets. Several critical questions were asked of information security and cybersecurity professionals about the importance of soft skills aligned with technology management, business functional skills, and interpersonal qualities. As cybersecurity and information technology professionals enter security work roles, introducing business skills will contribute toward more holistic and broad interdisciplinary academic programs (Payne et al., 2021). This research effort further contributes to the previous work by Payne et al. (2021) that introduced the concept of a general cybersecurity education course with varying components stemming from information technology, engineering, business, criminal justice, and philosophy. There is no complete agreement on what set of standard soft skills should be part of cybersecurity academic programs (Lee & Fang, 2008; S. Lee et al., 2002). With the current favor of cybersecurity certifications, it is not completely clear whether companies hiring employees for work roles in cybersecurity are getting the expected soft skill competencies. Additional research into this topic will benefit the cybersecurity discipline, and this study did shine a light on the importance of business functional skills. A broader study, perhaps comparing all the DHS CISA critical sectors evaluating soft skills, will benefit the cybersecurity academic and industry community.

7. CONCLUSION

Cybersecurity academic programs follow several notable frameworks that are made available for institutions to align with. These include the highly regarded and rigorous NSA CAE-CD program and the CSEC 2017. These guidelines and frameworks offer terrific technical abilities from which academic programs can follow and even apply for designation status, as in the case of the NSA CAE program. The problem remains that these frameworks still lack adequate content related to soft skills. The CSEC2017 guidance recommends that cybersecurity professionals benefit from strong technical and soft skills. However, it does not include a specific knowledge area focus in the same light as data security or software security in this realm. This study demonstrated that excellent business functional soft skills were perceived as more critical to the finance sector than to the manufacturing sector. This finding can have implications for consideration when updating cybersecurity academic programs. Although existing frameworks, such as the CSEC2017 and CAE-CD, do mention business knowledge as an individual contributor in such areas as the organizational topic perspective, there does not exist a dedicated business or business function top-level topic area in cybersecurity curriculums. Considering or evaluating whether instituting a new topic area surrounding business acumen soft skills can be a valuable addition for cybersecurity professionals entering the workforce.

8. LIMITATIONS

Several limitations of this research are outlined and could allow for potential future exploration into the topic of soft skills of cybersecurity professionals. Related to the theories approached, the TOE, supported by the STS, and holistic competency models were chosen to provide a paradigm. Other potential theories exist, such as activity theory, that could align with the effort. In addition, a review of cybersecurity curriculums from various higher education institutions was not invoked, which could provide an excellent background into what program learning outcomes include soft skills. In addition, this study pursued the critical infrastructure sectors of finance and manufacturing, and other critical sectors could potentially be compared, perhaps a comparison of all the DHS CISA sixteen critical sectors. Finally, another limitation is via the specific individual survey population, which

©2024 ISCAP (Information Systems and Computing Academic Professionals)

ISSN: 2473-4901
v10 n6115

included information security and cybersecurity professionals. Students were not included in the research activity. They could also shine more excellent knowledge into their perception of the importance of soft skills and what they may consider most important.

9. REFERENCES

Akdur, D. (2021). Skills gaps in the industry: Opinions of embedded software practitioners. *ACM Transactions on Embedded Computing Systems, 20*(5), 1–39. https://doi.org/10.1145/3463340

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security, 119*, 1-12. https://doi.org/10.1016/j.cose.2022.102754

Bohler, J. A., Larson, B., & Shehane, R. F. (2020). Evaluation of information systems curricula. *Journal of Information Systems Education, 31*(3), 232–243. http://jise.org/Volume31/n3/JISEv31n3p232.html

Booker, Q. E., & Munmun, M. (2023). Comparing cybersecurity skills and cybersecurity curricula: a pre and post COVID analysis. *Issues in Information Systems, 24*(2), 320-333. https://doi.org/10.48009/2_iis_2023_128

Bostrom, R. P., & Heinen, J. S. (1977a). MIS problems and failures: A socio-technical perspective. Part 1: The causes. *MIS Quarterly, 1*(3), 17–32. https://doi.org/10.2307/248710

Bostrom, R. P., & Heinen, J. S. (1977b). MIS problems and failures: A socio-technical perspective. Part II: The application of socio-technical theory. *MIS Quarterly, 1*(4), 11–28. https://doi.org/10.2307/249019

Brilingaitė, A., Bukauskas, L., & Juozapavicius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security, 88,* Article 101607. http://dx.doi.org/10.1016/j.cose.2019.101607

Brown, N., Xie, B., Sarder, E., Fiesler, C., & Wiese, E. S. (2024). Teaching ethics in computing: A systematic literature review of ACM computer science education publications. *ACM Transactions on Computing Education, 24*(1), 1-36. https://doi.org/10.1145/3634685

Coulson, T., Mason, M., & Nestler, V. (2018). Cyber capability planning and the need for an expanded cybersecurity workforce. *Communications of the IIMA, 16*(2), 1-13. https://doi.org/10.58729/1941-6687.1401

Creswell, J. W., & Creswell, J. D. (2018). *Research design* (5th ed.). Sage.

Depietro, R., Wiarda, E., & Fleischer, M. (1990). The context for change: Organization, technology and environment. In L. G. Tornatzky & M. Fleischer (Eds.), *The processes of technological innovation* (pp. 151–175). Lexington Books.

DoD Cyber Exchange. (2020). *CAE documents library CAE-CD knowledge units,* 1–102. https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf

Dubey, R. S., Paul, J., & Tewari, V. (2022). The soft skills gap: A bottleneck in the talent supply in emerging economies. *The International Journal of Human Resource Management, 33*(13), 2630–2661. https://doi.org/10.1080/09585192.2020.1871399

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers Security, 100,* Article 102080. https://doi.org/10.1016/j.cose.2020.102080

Joint Task Force on Cybersecurity Education. (2017). Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity. *Technical Report. ACM/IEEE/AIS-SIGSEC/IFIP. WG 11.8*. New York, NY, USA. 1–123. https://dl.acm.org/doi/pdf/10.1145/3184594

Jones, K. S., Namin, A. S., & Armstrong, M. E. (2018). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Transactions on Computing Education, 18*(3), Article 11. https://doi.org/10.1145/3152893

Le Deist, F. D., & Winterton, J. (2005). What is competence? *Human Resource Development International, 8*(1), 27–46. https://doi.org/10.1080/1367886042000338227

ISSN: 2473-4901
v10 n6115

Lee, D. M. S., Trauth, E. M., & Farwell, D. (1995). Critical skills and knowledge requirements of IS professionals: A joint academic/industry investigation. *MIS Quarterly, 19*(3), 313–340. http://dx.doi.org/10.2307/249598

Lee, S., & Fang, X. (2008). Perception gaps about skills requirement for entry-level IS professionals between recruiters and students: An exploratory study. Information Resources Management Journal, 21(3), 1-26.

Lee, S., Koh, S., Yen, D., & Tiang, H. L. (2002). Perception gaps between IS academic and IS practitioners: An exploratory study. *Information & Management, 40*(1), 51-61.

Makrakis, G. M., Kolias, C., Kambourakis, G., Reiger, C., & Benjamin, J. (2021). Industrial and critical infrastructure security: Technical analysis of real-life security incidents. *IEEE Access, 9,* 165295-165325. https://doi.org/10.1109/access.2021.3133348

Payne, B. K., He, W., Wang, C., Wittkower, D. E., & Wu, H. (2021). Cybersecurity, technology, and society: Developing an interdisciplinary, open, general education cybersecurity course. Journal of Information Systems Education, 32(2), 134-149. https://aisel.aisnet.org/jise/vol32/iss2/6

Persaud, A. (2020). Key competencies for big data analytics professions: A multimethod study. *Information Technology & People, 34*(1), 178–203. https://doi.org/10.1108/ITP-06-2019-0290

Plachkinova, M., & Vo, A. (2023). A taxonomy for risk assessment of cyberattacks on critical infrastructure (TRACI). *Communications of the Association for Information Systems, 52*, Digital Design Science Article 1. https://doi.org/10.17705/1CAIS.05202

Raval, K. J., Jadav, N. K., Rathod, T., Tanwar, S., Vimal, V., & Yamsani, N. (2024). A survey on safeguarding critical infrastructures: Attacks, AI security, and future directions. *International Journal of Critical Infrastructure Protection, 44*, 1-18. https://doi.org/10.1016/j.ijcip.2023.100647

Vess, J., Torres, R., Maurer, C., Guerra, K., & Srivastava, S. (2023). The 2022 SIM IT Issues and Trends Study. *MIS Quarterly Executive, 22*(1), Article 6. https://aisel.aisnet.org/misqe/vol22/iss1/6

Wallace, S., Green, K. Y., Johnson, C., Cooper, J., & Gilstrap, C. (2020). An extended TOE framework for cybersecurity-adoption decisions. *Communications of the Association for Information Systems, 47*(51), Article 16. https://aisel.aisnet.org/cais/vol4

©2024 ISCAP (Information Systems and Computing Academic Professionals)

ISSN: 2473-4901
v10 n6115

©2024 ISCAP (Information Systems and Computing Academic Professionals)