Towards Assessing Cybersecurity Posture of Manufacturing Companies: Review and Recommendations

John Del Vecchio
jd2940@mynsu.nova.edu

Yair Levy
Nova Southeastern University

Ling Wang
Nova Southeastern University

Ajoy Kumar
Nova Southeastern University

Abstract

With the continued changes in the way businesses work, cyber-attack targets are in a constant state of flux between organizations, individuals, as well as various aspects of the supply chain of interconnected goods and services. As one of the 16 critical infrastructure sectors, the manufacturing sector is known for complex integrated Information Systems (ISs) that are incorporated heavily into production operations. Many of these ISs are procured and supported by third parties, also referred to as interconnected entities in the supply chain. Disruptions to manufacturing companies would not only have significant financial losses but would also have economic and safety impacts on society. The vulnerabilities of interconnected companies created inherited exploitations in other interconnected companies. Cybersecurity practices need to be further enhanced to understand supply chain cybersecurity posture and manage the risks from lower-tier interconnected entities up to the top-level dependent organization. This paper will provide an overview of the Theory of Cybersecurity Footprint to emphasize the relationship among interconnected entities and the cybersecurity effects one organization can have on another regardless of size. This paper provides a literature review on the manufacturing industry with a recommendation for future developmental research using the Delphi method with a panel of experts to develop an index to measure cybersecurity posture based on interconnected entities from lower tiers and establish index weights specifically for the manufacturing industry.

Disciplines

Information Security | Management Information Systems | Technology and Innovation

Comments

Keywords—interconnected entities, supply chain cybersecurity, third-party cyber-risk, Delphi method, SMEs, cybersecurity footprint, index model.

Towards Assessing Cybersecurity Posture of Manufacturing Companies: Review and Recommendations

John Del Vecchio
College of Computing and Engineering
Nova Southeastern University
Ft. Lauderdale, FL, USA
jd2940@mynsu.nova.edu
0009-0007-2996-2958

Yair Levy
College of Computing and Engineering
Nova Southeastern University
Ft. Lauderdale, FL, USA
levyy@nova.edu
0000-0002-8994-6497

Ling Wang
College of Computing and Engineering
Nova Southeastern University
Ft. Lauderdale, FL, USA
lingwang@nova.edu
0000-0002-9202-6501

Ajoy Kumar
College of Computing and Engineering
Nova Southeastern University
Ft. Lauderdale, FL, USA
akumar@nova.edu
0000-0001-6450-7730

***Abstract*—With the continued changes in the way businesses work, cyber-attack targets are in a constant state of flux between organizations, individuals, as well as various aspects of the supply chain of interconnected goods and services. As one of the 16 critical infrastructure sectors, the manufacturing sector is known for complex integrated Information Systems (ISs) that are incorporated heavily into production operations. Many of these ISs are procured and supported by third parties, also referred to as interconnected entities in the supply chain. Disruptions to manufacturing companies would not only have significant financial losses but would also have economic and safety impacts on society. The vulnerabilities of interconnected companies created inherited exploitations in other interconnected companies. Cybersecurity practices need to be further enhanced to understand supply chain cybersecurity posture and manage the risks from lower-tier interconnected entities up to the top-level dependent organization. This paper will provide an overview of the Theory of Cybersecurity Footprint to emphasize the relationship among interconnected entities and the cybersecurity effects one organization can have on another regardless of size. This paper provides a literature review on the manufacturing industry with a recommendation for future developmental research using the Delphi method with a panel of experts to develop an index to measure cybersecurity posture based on interconnected entities from lower tiers and establish index weights specifically for the manufacturing industry.**

Keywords—interconnected entities, supply chain cybersecurity, third-party cyber-risk, Delphi method, SMEs, cybersecurity footprint, index model

I. INTRODUCTION

The United States (U.S.) government has deemed manufacturing as one of the 16 critical infrastructure sectors requiring protection from cyber threats, which if impacted would debilitate society and the economy [9], [37]. Prior research [17] asserted, "manufacturing companies are not fully protected from risk of cyber-attacks as long as some object (human or machine) communicates and shares information and data" (p. 2). In recent decades, the manufacturing industry has been transformed into what is commonly known as Industry 4.0 (I4.0), with technology embedded into processes and operations to improve the use of manufacturing resources [18]. I4.0 consists of Information Technology (IT) and Operational Technology (OT) systems connecting cloud resources with industrial Internet to various technologies such as sensors, embedded applications, and industrial hardware for real-time data. Prior literature [29] acknowledged the precise operation of such equipment and systems is important, and in the case of malfunction, vendors (e.g., partners or suppliers) may have quick access through backdoor methods to systems that are normally protected. Generally, partners and suppliers are not considered threat actors, however, a partner that is compromised could be exploited for their trusted network access they have to a protected network of another organization, which could lead to the propagation of a cyber incident to other connected partners [1], [38]. In response to the growing number of interconnected entities, ease of system hacking, and increased number of exploits, Levy and Gafni [23] proposed the Theory of Cybersecurity Footprint, which defined Cybersecurity Footprint as "the potential malicious impact to an entity and/or its cascading effects on interconnected entities, which may result from a cybersecurity incident from exploits" (p. 725). The intent of this review paper is to establish an argument for the criticality of the Cybersecurity Footprint to manufacturing companies as well as the impact they continue to experience from data theft, data leaks, operational disruptions, and monetary loss due to extortion [20]. Ciano et al. [6] claimed very few companies have mastered tools to protect against unlawful access by attackers seeking to disrupt operations, obtain intellectual property, or achieve financial gain. Thus, recommendations will be provided for assessing the cybersecurity posture of manufacturing companies by determining the risk exposure from interconnected entities within their supply chain.

II. LITERATURE REVIEW

A. Targeting the Manufacturing Industry

Companies in the manufacturing industry are attractive targets to cyber threats for several reasons, such as the critical nature of production operations, proprietary information, dependencies on integrated supply chains, and diverse use of

technologies. According to [12] Deloitte [12], the manufacturing industry is targeted for financial gain and intellectual property theft, while at the same time is highly vulnerable because of a fragmented approach to managing cyber-related risks. Prior research [15] and [27] suggested manufacturers are prime targets because of the transition toward I4.0 technologies for automation and information exchange. Such I4.0 integrations appear to increase system complexities, vulnerabilities, and security challenges that traditional IT security is insufficient to protect. Sailio et al. [38] contended collaboration, network connectivity, intelligence (e.g., machine learning), and flexible automation from I4.0 technologies, along with the premise of the "factory of the future" (p. 2), had created new opportunities for threat actors. In 2022, the manufacturing sector represented 58% of cyber incidents remediated by X-Force [20], with 28% of the incidents involving backdoor deployments and 14% involving external remote services [20]. A variety of technologies, such as Internet of Things (IoT), Industrial Control Systems (ICS), Human Machine Interface (HMI) devices, and Programmable Logic Controllers (PLC) used in manufacturing environments are known to have longer replacement lifecycles. As a result, the ease of accessibility and exploitation in open connected systems across the enterprise has been exacerbated by unsupported software, which in turn extended vulnerabilities beyond normal time periods [2], [33]. Moreover, the combination of weak security for industrial networks, highly specialized equipment requiring constant Internet access to cloud resources, and an expanded attack surface using partners to manage the infrastructure has created a highly attractive environment for threat actors [38]. Pandey et al. [35] claimed the manufacturing industry is unprepared to address new cyber threats stemming from connected devices, I4.0 digital capabilities, and integration with partners as companies are required to protect a wide array of technologies, while attackers only need to focus on the weakest link.

B. Threats and Impacts to Manufacturing

Prior to the technology convergence in manufacturing, the primary issues of concern were performance, reliability, and safety of production operations [2]. However today, manufacturing is one of the most frequently compromised industries due to I4.0 technologies, which include Industrial Internet of Things (IIoT) machines as well as cloud-based control and sensing systems [41]. In a study conducted by Makhdoom et al. [28], a set of IoT security deficiencies were composed that presented several vulnerabilities for threats and exploitation. Culot et al. [8] observed company controls and practices had become ineffective in addressing the increased connectivity of IT and OT networks as workloads shifted to public clouds. Prior research [16] and [30] identified key categories of cyber threats to I4.0 technologies to include direct external attacks, indirect attacks through trusted service providers who have been granted access, compromise through interconnected networks, malicious software to impair functionality, and zero-day attacks. Makhdoom et al. [28] provided a list of generalized IoT threats, including several specific to the physical, application, and network layers. Masum [27] identified threats associated with network configurations, informational databases, production machines accessed by smart devices, and connectivity of cloud resources for distributed manufacturing.

While cyber-attacks on manufacturing systems could result in stopped production, altered production, physical damage, or injury to workers. Additionally, prior research[7] also contended, "there are several areas of impact as a result of cyber-attack: financial theft/fraud, theft of intellectual property or strategic plans, business disruption, destruction of critical infrastructure, reputation damage, threats to life/safety, and regulations" (p. 4). Similarly, Bhamare et al. [3] stressed the high costs of cybersecurity breaches to industrial systems translate into lost revenues, financial impacts, and environmental impacts. Ani et al. [2] qualified impacts in perspective of time, such that daily activities of the business or individual end users are unable to access systems or receive information in the short-term, while impacts could come from a data breach or loss of intellectual property affecting competitiveness and public confidence over a long-term horizon. The economic and social impacts that result from a cybersecurity attack on manufacturing and its supply chains could result in significant harm to the entire industry. Moreover, such attacks may have a greater scale impact on human life relying heavily on products to meet essential needs [2].

C. Third Party Compromise

The maturity of the Information and Communications Technology (ICT) sector has created a dependency on a converged infrastructure in manufacturing that has resulted in a growing concern about cyber threats due to introduced vulnerabilities and exploits [2]. Research conducted by Deloitte and The Manufacturers Alliance for Productivity and Innovation (MAPI) emphasized the need to evaluate third-party cyber risks [12]. In 2017, there were 620 separate data breaches in the manufacturing industry out of 1,579 breaches reported (nearly 40%) for all sectors in the U.S. [10]. The Sikich Report found 54% of 310 manufacturing companies surveyed were confident in their ability to withstand the effects of a data breach. However, the survey found 38% of 245 smaller companies (revenue less than $500M) performed cyber audits [39]. A report conducted by the Ponemon Institute in 2017 found 263 (nearly 42% of 625) respondents indicated cyber-attacks against third parties resulted in misuse of their sensitive or confidential information, while 350 (nearly 56% of 625) respondents confirmed a data breach was caused by one of their vendors [36].

D. The Theory of Cybersecurity Footprint

Levy and Gafni [23] argued the need to identify risks that organizations are unaware of downstream in their supply chain, and thus, proposed the Theory of Cybersecurity Footprint as a means to prevent the "domino effect" (p. 725) by improving risk assessments. The Theory of Cybersecurity Footprint is based on the premise that vast data from digital activities and organization size are not the only factors contributing to the impact of data breaches, but also the

cascading effect cyber-attacks can have on interconnected entities. In likeness, the rationale for understanding the importance of the "ripple effect" caused by supply chain disruption impacting partners and other areas of the supply chain has been well established in prior research [13], [19], [21]. Based on a literature review, Levy and Gafni [24] proposed the quantification of the Cybersecurity Footprint Index (CFI) based on six domains from Level 1 of the Cybersecurity Maturity Model Certification 2.0 (CMMC 2.0) and 26 associated elements for universal perspective, not specific for manufacturing or any other industry. Moreover, they [24] derived the CFI elements from the 17 practices associated with CMMC 2.0 Level 1. The CMMC 2.0 is a framework published by the Department of Defense (DoD) to protect national security by providing defense contractors as well as sub-contractors with a set of cybersecurity practices, standards, and processes to manage information in their possession. The CMMC 2.0 Level 1 domains which are designated as foundational while being used for self-assessment consist of Access Control (AC), Identification and Authentication (IA), Media Protection (MP), Physical Protection (PE), System and Communications Protections (SC), as well as System and Information Integrity (SI).

III. PROPOSED RESEARCH

It appears that additional research is warranted to go beyond traditional cyber risk assessments and to measure the cascading effects of interconnected entities to accurately quantify an organizational cybersecurity posture [23]. Keskin et al. [22] stated many assessment methods exist; however, they focus on the organization's risk to devise mitigation plans and employ security controls rather than assessing the third-party vendors the organization is dependent upon that are interconnected to their network. Levy and Gafni [24] suggested the use of the Delphi method, comprised of an expert panel to validate the proposed domains and elements, establish weights, and develop a validated index for quantifying the Cybersecurity Footprint. Moreover, Strohmier et al. [40] stated, "use of a maturity model with built-in accountability is a way to reduce vulnerabilities from the use of interdependent systems" (p. 18). Levy and Gafni [23] claimed, "the size of the organization is not the main factor to measure Cybersecurity Footprint" (p. 732). In that capacity, the digital interaction (e.g., software, hardware, and communications networks) between customers, suppliers, and partners are responsible for the transformation as well as increased complexities of the supply chain cybersecurity [4], [31].

The recommendation is to develop a measurement index by engaging Subject Matter Experts (SMEs) to identify and validate weights for tiers of interconnected entities, weights for the CMMC 2.0 domains, as well as weights for the Cybersecurity Footprint elements to aggregate and quantify an organizational cybersecurity posture for manufacturing companies, referred to as Cybersecurity Footprint Index for Manufacturing (CFI-Mfg) [34], [24]. Levy and Gafni [24] asserted a self-assessment method that is easy to comprehend and allows for industry benchmarking will be an important contribution. Additionally, an innovative contribution of this research will be the confirmation and validation of weights specific to manufacturing companies for the selected CMMC 2.0 – Level 1 domains, proposed Cybersecurity Footprint elements, interconnected tiers, and the introduction of the CFI-Mfg. Keskin et al. [22] concluded that data-driven empirical tools provide organizations with the means to better understand their cybersecurity landscape. As such, the quantification of a CFI-Mfg score is relevant to addressing cyber-attacks on companies and interconnected entities in the supply chain by having the ability to measure areas of risk, recognize threats, and reduce uncertainty [24].

IV. PROPOSED METHODOLOGY

To achieve the recommended goal to design, develop, and validate a CFI-Mfg, a proposed developmental research approach with multiple phases is shown in Fig. 1. The proposed method starts with SMEs in the field of cybersecurity and the Delphi method in an effort to answer the following questions:

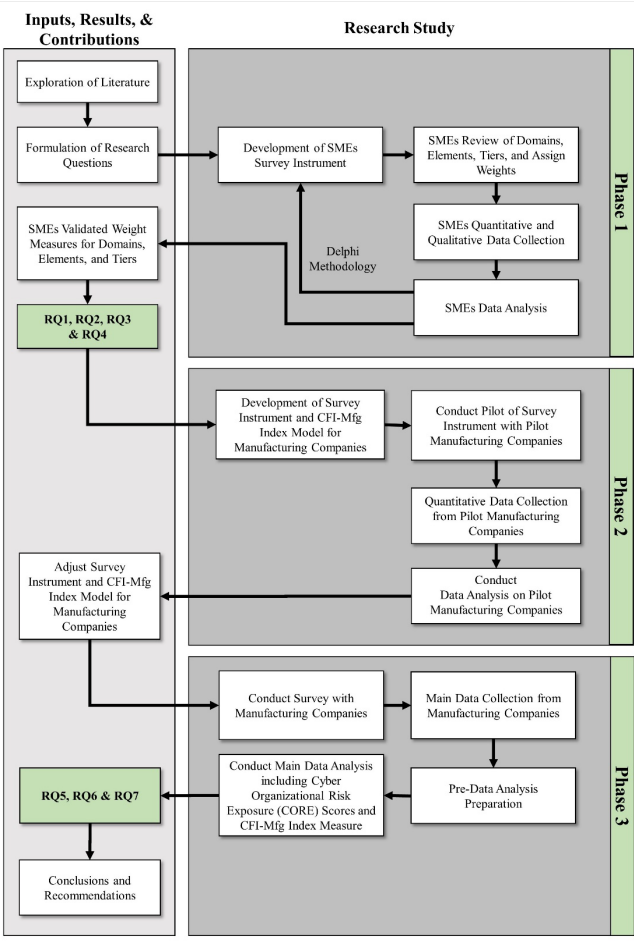

Fig. 1. Proposed Research Design Process

RQ1: What are the specific SMEs identified set of weights for the domains and elements of the CFI-Mfg?

RQ2: What are the specific SMEs identified number of tiers of interconnected vendors/suppliers of the CFI-Mfg?

RQ3: What are the specific SMEs identified weights for the tiers of interconnected vendors/suppliers of the CFI-Mfg?

RQ4: What is the specific CFI-Mfg that provides a measurable organizational cybersecurity posture for companies and their interconnected vendors/suppliers?

RQ5: Are there any statistically significant mean differences to the CFI-Mfg based on the number of interconnected suppliers/vendors?

RQ6: Are there any statistically significant mean differences to the CFI-Mfg based on the number of tiers of interconnected suppliers/vendors?

RQ7: Are there any statistically significant mean differences to CFI-Mfg based on attack surfaces, to name a few: (a) number of workstations and laptops, (b) number of network file servers, (c) number of application servers, (d) number of public cloud instances, I number of firewalls and switches, (f) number of multi-function printers, (g) number of mobile devices, (h) number of IoT devices, and (i) number of employees.

Phase 1 will consist primarily of executing the Delphi method to achieve SME consensus on the number of tiers of the CFI-Mfg, and the weights of the tiers, domains, and elements. Once consensus is reached in Phase 1, questions RQ1, RQ2, and RQ3 will be answered and a proposed CFI-Mfg measurement index will be developed. Phase 2 will focus on conducting a pilot with a controlled group of manufacturing companies to validate the CFI-Mfg measurement index and a survey instrument consisting of 26 questions proposed by Levy and Gafni [23] representing the 26 elements and six domains from CMMC 2.0 Level 1. Both quantitative and qualitative data will be captured from the pilot for further analysis and refinement of both instruments. Lastly, Phase 3 will collect data from interconnected entities of manufacturing companies using the survey instrument. The collected data from each interconnected entity will have the weights confirmed in the Delphi method for the elements and domains applied to the survey responses to calculate a Cyber Organizational Risk Exposure (CORE) score for each organization, as shown in Fig. 2. The CORE score of each interconnected entity will serve as input into the measurement index to calculate a CFI-Mfg score for each top-tier company. Following, RQ4 will be answered and provide a basis for the research conclusions and recommendations, as well as address RQ5, RQ6, and RQ7 concerning statistically significant mean differences between manufacturing companies' CFI-Mfg score, as well as several other variables.

V. DISCUSSION AND CONCLUSIONS

Németh et al. [32] referred to Multi-criteria Decision Analysis (MCDA), also known as Multiple Criteria Decision Making (MCDM), as "the collective name of formal approaches that support decision making by taking into account multiple criteria in an explicit and transparent way" (p. 195). As presented by Dean [11], the key elements of MCDA are options, objectives, criteria, criterion weights, and performance scores. The application of MCDA is a justified approach to satisfy the objective to calculate a CORE score based on the criterion of CMMC 2.0 – Level 1 domains, the proposed Cybersecurity Footprint elements, and their associated weights. Németh et al. [32] asserted the problem can be described visually, where the objective, criteria, and sub-criteria are arranged in a hierarchy, as shown in Fig. 2.

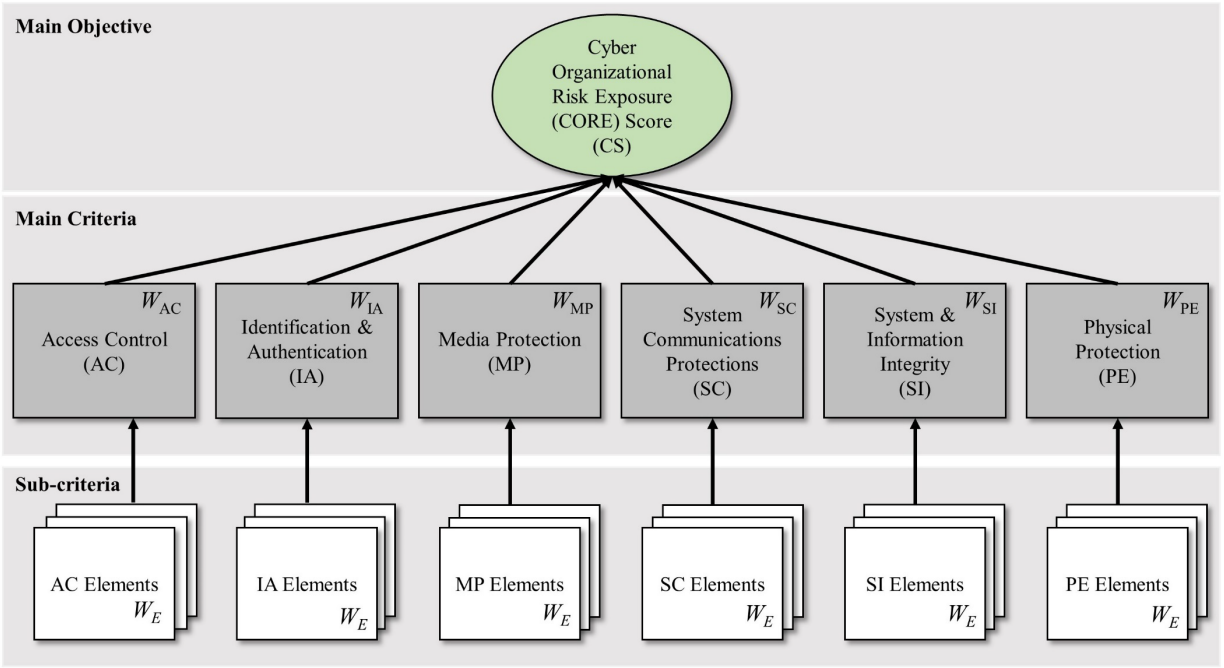

Fig. 2. Association of Elements, Domains, and Weights Toward a CORE Score For a Given Organization

The anticipated CORE Score of an interconnected entity is the sum of the weighted domains (WD) multiplied by the sum of the weighted elements (WE) multiplied by a coefficient (CE) applied to the values of each of the elements (E):

$$COREOrg = \Sigma\ (WD * \Sigma\ (WE * (CE * E1..n)))$$

A normalized CORE Score is calculated for each tier based on the following:

$$Normalized\_CORETier.n = (1 / ((Num\_EntitiesTier.n) * MAX(COREOrgA.1..A.n))*100) * \Sigma\ (COREOrgA.1..A.n)$$

A contribution CORE Score is calculated based on the weight of the tier (WT) and the calculated "Entity Impact Weight" (WE) applied to the normalized CORE Score of the given tier:

$$Contr\_CORETier.n = Normalized\_CORETier.n * (WTier.n * (Num\_EntitiesTier.n / Total\_Num\_Entities)) / \Sigma\ ((WTier.1 * (Num\_EntitiesTier.1 / Total\_Num\_Entities)) + \cdots\ (((WTier.n * (Num\_EntitiesTier.n / Total\_Num\_Entities))$$

The CFI-Mfg score of the originating manufacturing company (Tier 0) is determined by the sum of the contribution CORE Scores of each of the tiers:

$$CFI\text{-}MfgOrgA = \Sigma\ (Contr\_CORETier.1) + (Contr\_CORETier.2) \cdots\ (Contr\_CORETier.n)$$

The calculation of the CFI-Mfg score for the originating (Tier 0) manufacturing company is quantified to indicate a risk posture on a scale from 0 being "Low" to 100 being "High", as [24] indicated to aid companies in the effort to self-assess and communicate easy-to-understand information (See Fig. 3 for an example).

Tier	Tier Weights (W_T)	Num in Tier	Entity Impact Weight (W_E)	Tier Contrib %	Tier Contrib CORE Score	Normalized CORE Score	Cyber Organizational Risk Exposure (CORE) Scores										
Tier 1	75.0%	30	20.1%	67.7%	**50.17**	74.13	93	57	85	82	80	49	51	49	95	68	100
Tier 2	15.0%	48	32.2%	21.7%	**11.62**	53.64	40	55	93	35	65	86	12	80	16	50	83
Tier 3	5.0%	18	12.1%	2.7%	**2.28**	84.34	84	54	97	79	54	84	78	60	84	99	91
Tier 4	5.0%	53	35.6%	8.0%	**3.33**	41.72	45	22	70	13	83	51	97	71	98	59	40
	100%	149	100%	100%													
				CFI-Mfg Score --->	**67.4**		**Low Risk Posture**										**High Risk Posture**

Fig. 3. An Example of CORE Scores and CFI-Mfg Score

Burke et al. [5] noted indexes are used for evaluation based on a series of questions weighted by importance to determine an overall score. Prior studies [14], [25], and [26] determined the "influence weight" of distinct factors enabling the measurement of risk, safety, and performance respectively. In conclusion, the recommendation to establish weights for the domains, elements, and tiers specifically for the manufacturing industry will be key findings essential to the determination of a CFI-Mfg score. As shown in Fig. 4, the conceptual CFI-Mfg hierarchical index model is anticipated to provide a clearer understanding of the interconnected entities' influence on cyber posture at different levels and the roles of the domains and elements.

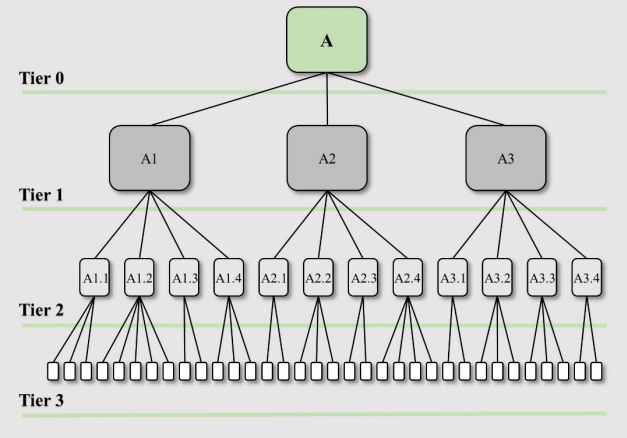

Fig. 4. Conceptual CFI-Mfg Hierarchy Index Model

Lastly, the combination of descriptive statistics and one-way Analysis of Variance (ANOVA) will address the outlined research questions, including determining whether there are significant mean differences to the CFI-Mfg based on the number of interconnected entities and the number of tiers of interconnected entities.

ACKNOWLEDGEMENTS

This publication was supported by the U.S. Department of Defense (DoD) managed by the National Security Agency (NSA) award number H98230-22-1-0262.

REFERENCES

[1] Accenture (2019). Cyber threatscape report. Available online: https://www.accenture.com/_acnmedia/pdf-107/accenturesecurity-cyber.pdf (Last accessed on May 2022).

[2] Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. Journal of Cyber Security Technology, 1(1), 32-74. https://doi.org/10.1080/23742917.2016.1252211

[3] Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. computers & security, 89, 101677. https://doi.org/10.1016/j.cose.2019.101677

[4] Bhargava, B., Ranchal, R., & Othmane, L. B. (2013, February). Secure information sharing in digital supply chains. In 2013 3rd IEEE International Advance Computing Conference (IACC) (pp. 1636-1640). IEEE. https://doi.org/10.1109/IAdCC.2013.6514473

[5] Burke, W., Oseni, T., Jolfaei, A., & Gondal, I. (2019). Cybersecurity indexes for eHealth. In Proceedings of the Australasian Computer Science Week Multiconference (pp. 1-8). https://doi.org/10.1145/3290688.3290721

[6] Ciano, M. P., Ardolino, M., & Müller, J. M. (2022). Digital Supply Chain: Conceptualisation of the Research Domain. Proceedings of the 5th European International Conference on Industrial Engineering and Operations Management Rome, Italy, July 26-28, 2022.

[7] Corallo, A., Lazoi, M., Lezzi, M., & Pontrandolfo, P. (2021). Cybersecurity challenges for manufacturing systems 4.0: Assessment of the business impact level. IEEE Transactions on Engineering Management. https://doi.org/10.1109/TEM.2021.3084687

[8] Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing industry 4.0 cybersecurity challenges. IEEE Engineering Management Review, 47(3), 79-86. https://doi.org/10.1109/EMR.2019.2927559

[9] Cybersecurity and Infrastructure Security Agency (CISA). (2020, October 21). Critical infrastructure sectors. https://www.cisa.gov/critical-infrastructure-sectors

[10] de Groot, J. (2020). Biggest manufacturing data breaches of the 21st Century. Digital Guardian. https://digitalguardian.com/blog/biggest-manufacturing-data-breaches-of-the-21-century

[11] Dean, M. (2022). A practical guide to multi-criteria analysis. UCL: London, UK.

[12] Deloitte. (n.d.). Cyber risk in advanced manufacturing. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manufacturing-cyber-risk-in-advanced-manufacturing-executive-summary.pdf

[13] Dolgui, A., Ivanov, D., & Sokolov, B. (2018). Ripple effect in the supply chain: an analysis and recent literature. International Journal of Production Research, 56(1-2), 414-430. https://doi.org/10.1080/00207543.2017.1387680

[14] Duo, Z., Chen, Z., Liang, Y., Dai, M., & Guo, H. (2021). Risk Rating Framework of Power Grid Business Entities Based on AHP. In ACM Turing Award Celebration Conference-China (ACM TURC 2021) (pp. 273-277). https://doi.org/10.1145/3472634.3474084

[15] Elhabashy, A. E., Wells, L. J., & Camelio, J. A. (2020). Cyber-physical attack vulnerabilities in manufacturing quality control tools. Quality Engineering, 32(4), 676-692. https://doi.org/10.1080/08982112.2020.1737115

[16] Flatt, H., Schriegel, S., Jasperneite, J., Trsek, H., & Adamczyk, H. (2016, September). Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements. In 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA) (pp. 1-4). IEEE.

[17] Hemilä, J., Mikkola, M., & Salonen, J. (2019, December). Management of cyber security threats in the factories of the future supply chains. Proceedings of the 9th International Conference on Operations and Supply Chain Management, OSCM 2019. Institut Teknologi Sepuluh Nopember.

[18] Ho, W. R., Tsolakis, N., Dawes, T., Dora, M., & Kumar, M. (2022). A digital strategy development framework for supply chains. IEEE Transactions on Engineering Management, 1-14. https://doi.org/10.1109/TEM.2021.3131605

[19] Hsu, C. H., Zeng, J. Y., Chang, A. Y., & Cai, S. Q. (2022). Deploying industry 4.0 enablers to strengthen supply chain resilience to mitigate ripple effects: An empirical study of top relay manufacturer in China. IEEE Access, 10, 114829-114855. https://doi.org/10.1109/ACCESS.2022.3215620

[20] IBM Security's 2023 X-Force Threat Intelligence Index. Retrieved from https://www.ibm.com/reports/threat-intelligence

[21] Ivanov, D., Sokolov, B., & Dolgui, A. (2014). The ripple effect in supply chains: Trade-off 'efficiency-flexibility-resilience in disruption management. International Journal of Production Research, 52(7), 2154-2172. https://doi.org/10.1080/00207543.2013.858836

[22] Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. Electronics, 10(10), 1168-1187. https://doi.org/10.3390/electronics10101168

[23] Levy, Y., & Gafni, R. (2021). Introducing the concept of cybersecurity footprint. Information & Computer Security, 29(5), 724-736. https://doi.org/10.1108/ICS-04-2020-0054

[24] Levy, Y., & Gafni, R. (2022). Towards the quantification of cybersecurity footprint for SMBs using the CMMC 2.0. Online Journal of Applied Knowledge Management (OJAKM), 10(1), 43-61. https://doi.org/10.36965/OJAKM.2022.10(1)43-61

[25] Li, M., & Chen, H. (2021, September). Road Safety Evaluation Based on Analytic Hierarchy Process and Entropy Weight Method. In The 2021 7th International Conference on Industrial and Business Engineering (pp. 345-350). https://doi.org/10.1145/3494583.3494586

[26] Liang, Z., & Anni, Y. (2021). Design of performance evaluation system for transformation of patent achievements in colleges and universities based on AHP. In 2021 2nd International Conference on Computers, Information Processing and Advanced Education (pp. 1070-1076). https://doi.org/10.1145/3456887.3457463

[27] Masum, R. (2023). Cyber Security in Smart Manufacturing (Threats, Landscapes Challenges). arXiv preprint arXiv:2304.10180. https://doi.org/10.48550/arXiv.2304.10180

[28] Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of threats to the internet of things. IEEE communications surveys & tutorials, 21(2), 1636-1675. https://doi.org/10.1109/COMST.2018.2874978

[29] Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: Cybersecurity across the supply chain. International Journal of Production Research, 60(1), 162-183. https://doi.org/10.1080/00207543.2021.1984606

[30] Mullet, V., Sondi, P., & Ramat, E. (2021). A review of cybersecurity guidelines for manufacturing factories in industry 4.0. IEEE Access, 9, 23235-23263. https://doi.org/10.1109/ACCESS.2021.3056650

[31] Nasiri, M., Ukko, J., Saunila, M., & Rantala, T. (2020). Managing the digital supply chain: The role of smart technologies.

Technovation, 96, 102121. https://doi.org/10.1016/j.technovation.2020.102121

[32] Németh, B., Molnár, A., Bozóki, S., Wijaya, K., Inotai, A., Campbell, J. D., & Kaló, Z. (2019). Comparison of weighting methods used in multicriteria decision analysis frameworks in healthcare with focus on low-and middle-income countries. Journal of Comparative Effectiveness Research, 8(4), 195-204. https://doi.org/10.2217/cer-2018-0102

[33] Ouellette, M. (2023). Operational technology vulnerabilities combined with low tolerance for downtime to put manufacturers in cyber-attackers' crosshairs. Engineering.com. https://www.engineering.com/story/manufacturing-was-the-most-targeted-sector-for-ransomware-attacks-in-2022-says-ibm

[34] O. U. S. D. A. S. (n.d.). *Securing the defense industrial base. OUSD A&S - Cybersecurity Maturity Model Certification (CMMC)*. Retrieved from https://www.acq.osd.mil/cmmc/ (Last accessed on August 2023).

[35] Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. Journal of Global Operations and Strategic Sourcing. https://doi.org/10.1108/JGOSS-05-2019-0042

[36] Ponemon Institute. (2017) Data risk in the third-party ecosystem - Second annual study. https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/sep2017/cs2017_0340.pdf

[37] Robles, R. J., Choi, M. K., Cho, E. S., Kim, S. S., Park, G., & Lee, J. (2008). Common threats and vulnerabilities of critical infrastructures. International Journal of Control and Automation, 1(1), 17-22. Retrieved from: https://www.earticle.net/Article/A147480

[38] Sailio, M., Latvala, O. M., & Szanto, A. (2020). Cyber threat actors for the factory of the future. Applied Sciences, 10(12), 4334. https://doi.org/10.3390/app10124334

[39] Sikich LLP. (2019). Transforming for tomorrow. https://sikich.com/wp-content/uploads/2019/06/SKCH-MD-Report-2019-1.pdf

[40] Strohmier, H., Stoker, G., Vanajakumari, M., Clark, U., Cummings, J., & Modaresnezhad, M. (2022). Cybersecurity maturity model certification initial impact on the defense industrial base. Journal of Information Systems Applied Research, 17-29.

[41] Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X., & Terpenny, J. (2018). Cybersecurity for digital manufacturing. Journal of manufacturing systems, 48, 3-12. https://doi.org/10.1016/j.jmsy.2018.03.006