

TOWARDS ASSESSING CYBERSECURITY POSTURE OF MANUFACTURING COMPANIES: REVIEW AND RECOMMENDATIONS

John Del Vecchio,

Dr. Yair Levy,

Dr. Ling Wang,

Dr. Ajoy Kumar

November 1, 2023



Contents

➤ Introduction

➤ Literature Review

- Targeting the Manufacturing Industry
- Threats and Impacts to Manufacturing
- Third Party Compromise
- The Theory of Cybersecurity Footprint

➤ Proposed Research

➤ Proposed Methodology

➤ Discussion and Conclusions

Introduction

- Manufacturing is one of the 16 critical infrastructure sectors.
- Recent decades of transformation toward Industry 4.0.
- Cloud connected resources (e.g., sensors, applications, real-time data from industrial hardware).
- 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 (Melnik et al., 2022).
- A partner that is compromised could be exploited for their trusted network access - lead to the propagation of a cyber incident to other connected

Introduction

- Levy and Gafni (2021) proposed the Theory of Cybersecurity Footprint; defined 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).
- Manufacturing companies continue to experience data theft, data leaks, operational disruptions, and monetary loss due to extortion (IBM, 2023).
- Argue the criticality of the Cybersecurity Footprint.
- Provide recommendations for assessing cybersecurity posture of manufacturing companies by determining the risk exposure from interconnected entities within their supply chain.

Literature Review

- Targeting the Manufacturing Industry

- Reasons include critical nature of production operations, proprietary information, dependencies on integrated supply chains, and diverse use of technologies.
- I4.0 Technologies for automation and information integration/exchange appear to increase system complexities, vulnerabilities, and security challenges that traditional IT security is insufficient to protect (Elhabashy, 2020; Masum, 2023).
- In 2022, the manufacturing sector represented 58% of cyber incidents remediated by X-Force, with 28% of the incidents involving backdoor deployments and 14% involving external remote services (IBM, 2023).
- 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 (Ani et al., 2017; Ouellette, 2023).
- 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 (Sailig et al., 2020).

Literature Review

- Threats to Manufacturing

- Prior to the technology convergence in manufacturing, the primary issues of concern were performance, reliability, and safety of production operations (Ani et al., 2017).
- 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 (Wu et al., 2018).
- Culot et al. (2019) observed company controls and practices had become ineffective in addressing the increased connectivity of IT and OT networks as workloads shifted to public clouds.
- Key categories of cyber threats to I4.0 technologies 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 (Flatt et al., 2016; Mullet et al., 2021).

Literature Review

- Impacts to Manufacturing
 - Cyber-attacks on manufacturing systems could result in stopped production, altered production, physical damage, or injury to workers.
 - Corallo et al. (2021) 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).
 - Bhamare et al. (2020) stressed the high costs of cybersecurity breaches to industrial systems translate into lost revenues, financial impacts, and environmental impacts.
 - Ani et al. (2017) conveyed 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. Attacks may have a greater scale impact on human life relying heavily on products to meet essential needs.

Literature Review

• Third Party Compromise

- Dependency on converged infrastructure in manufacturing has resulted in a growing concern about cyber threats due to introduced vulnerabilities and exploits (Ani et al., 2017).
- Research conducted by Deloitte and The Manufacturers Alliance for Productivity and Innovation (MAPI) emphasized the need to evaluate third-party cyber risks (Deloitte, n.d.).
- 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. (de Groot, 2020).
- The Sikich Report (2019) 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 (Sikich, 2019).
- Ponemon Institute (2017) in 2017 found:

- Nearly 56% (350 of 625) respondents confirmed a data breach was caused by one of their vendors.

- Nearly 42% (263 of 625) respondents indicated cyber-attacks against third parties resulted in misuse of their sensitive or confidential information.

Literature Review

• The Theory of Cybersecurity Footprint

- Levy and Gafni (2021) argued the need to identify risks that organizations are unaware of downstream in their supply chain; proposed the Theory of Cybersecurity Footprint to prevent the “domino effect” (p. 725) by improving risk assessments.
- 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 (Levy & Gafni, 2021).
- 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 (Dolgui et al., 2018; Hsu et al., 2022; Ivanov et al., 2014).
- Levy and Gafni (2022) 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.

Proposed Research

- Many assessment methods 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 (Keskin et al., 2021).
- Measure the cascading effects of interconnected entities to accurately quantify an organizational cybersecurity posture (Levy & Gafni, 2021).
- Levy and Gafni (2022) asserted a self-assessment method that is easy to comprehend and allows for industry benchmarking will be an important contribution.
- Keskin et al. (2021) concluded that data-driven empirical tools provide organizations with the means to better understand their cybersecurity landscape.
- 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-

Proposed Methodology

- 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.
- 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 (2021) representing the 26 elements and six domains from CMMC 2.0 Level 1.
- 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.
- 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.

Proposed Methodology

- 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,
 (e) number of firewalls and switches,
 (f) number of multi-function printers,
 (g) number of

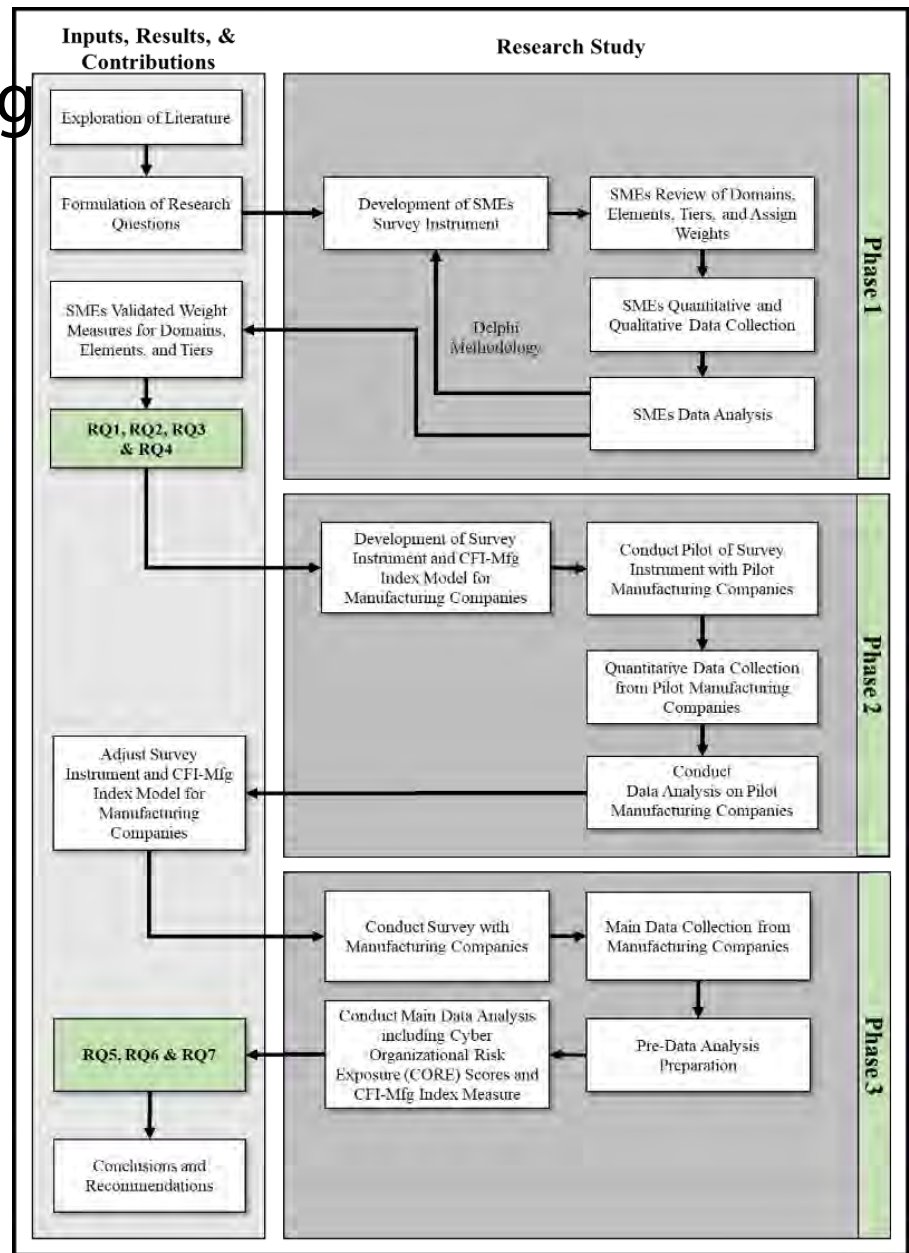


Fig. 1. Proposed Research Design Process

Discussion and Conclusions

- Németh et al. (2019) 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 (2022), 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. (2019) asserted the problem can be described visually, where the objective, criteria, and sub-criteria are arranged in a hierarchy.
- 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

Discussion and Conclusions

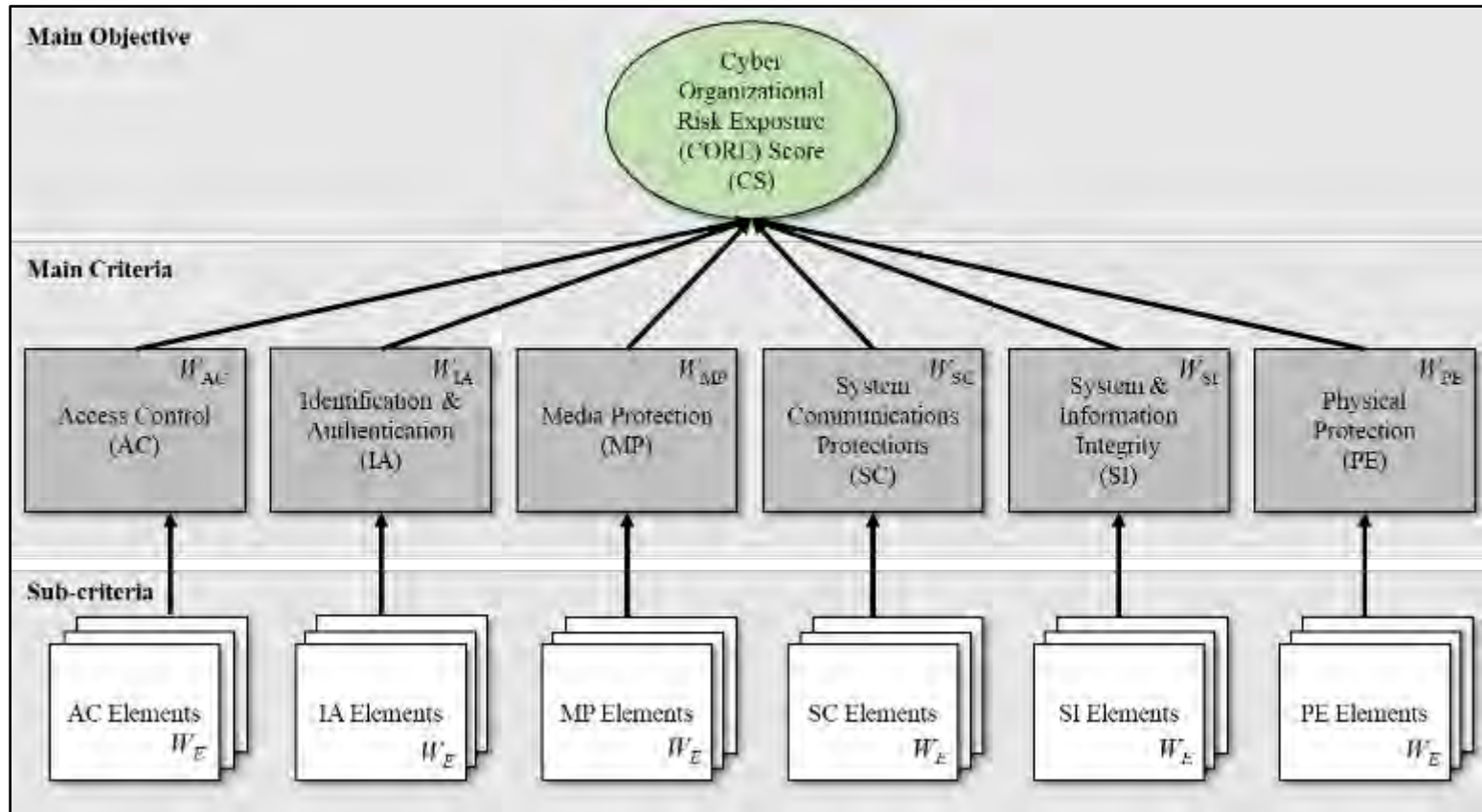


Fig. 2. Association of Elements, Domains, and Weights Toward a CORE Score For a Given Organization

Discussion and Conclusions

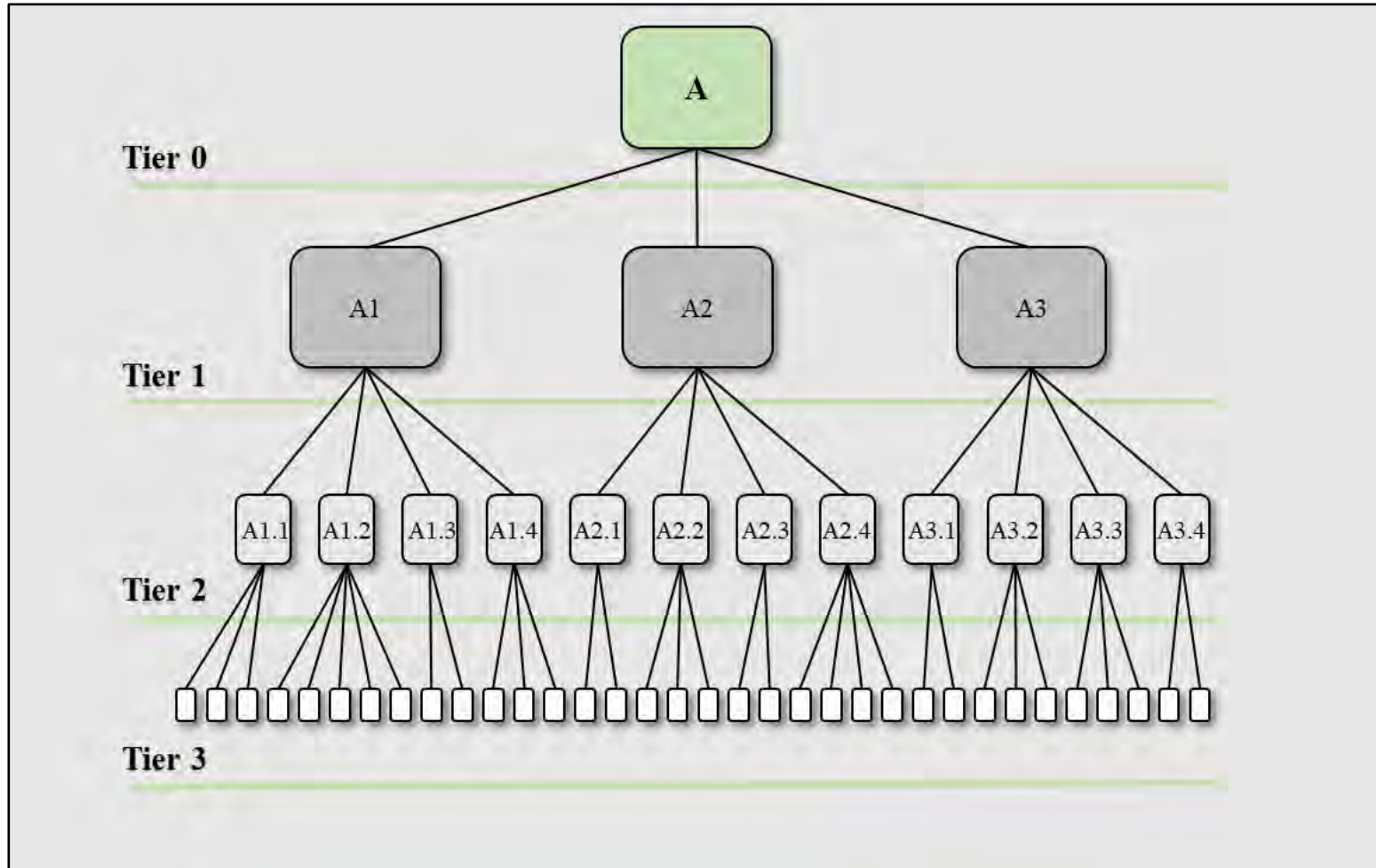


Fig. 3. Conceptual CFI-Mfg Hierarchy Index Model

Discussion and Conclusions

- 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”.
- Levy and Gafni (2022) indicated to aid companies in the effort to self-assess and communicate easy-to-understand information.
- Burke et al. (2019) noted indexes are used for evaluation based on a series of questions weighted by importance to determine an overall score.
- Prior studies of Duo (2021), Li and Chen (2021), as well as Liang and Anni (2021) determined the “influence weight” of distinct factors enabling the measurement of risk, safety, and performance, respectively.
- 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.

Discussion and Conclusions


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%	46.39	68.56	42 78 96 40 58 99 88 45 48 47 57	
Tier 2	15.0%	48	32.2%	21.7%	11.45	52.89	12 73 36 10 76 64 48 64 37 65 83	
Tier 3	5.0%	18	12.1%	2.7%	2.20	81.23	96 51 85 80 54 70 82 74 92 93 94	
Tier 4	5.0%	53	35.6%	8.0%	3.30	41.40	12 87 39 14 21 54 50 84 19 85 66	
					100%	149	100%	
					CFI-Mfg Score -->	63.3	Low Risk Posture  High Risk Posture	

Fig. 4. An Example of CORE Scores and CFI-Mfg Score

THANK
YOU

QUESTION
S?

