

2024

Development of Cybersecurity Footprint Index for Manufacturing Companies to Assess Organizational Cyber Posture

John A. Del Vecchio

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd



Part of the [Computer Sciences Commons](#)

Share Feedback About This Item

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

Development of Cybersecurity Footprint Index for Manufacturing
Companies to Assess Organizational Cyber Posture

by

John A. Del Vecchio

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Cybersecurity Management

College of Computing and Engineering
Nova Southeastern University

August 2024

We hereby certify that this dissertation, submitted by John A. Del Vecchio conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.



Yair Levy, Ph.D.
Chairperson of Dissertation Committee

8/27/24
Date



Ling Wang, Ph.D.
Dissertation Committee Member


8/27/24
Date



Ajoy Kumar, Ph.D.
Dissertation Committee Member

8/27/24
Date

Approved:



Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

8/27/24
Date

College of Computing and Engineering
Nova Southeastern University

2024

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Development of Cybersecurity Footprint Index for Manufacturing Companies to Assess Organizational Cyber Posture

by
John A. Del Vecchio
August 2024

With the continued changes in how businesses work, cyber-attack targets are constantly in flux between organizations, individuals, and various aspects of the supply chain of interconnected companies delivering goods and services. As one of the 16 critical infrastructure sectors, manufacturing is known for complex integrated Information Systems (ISs) incorporated heavily into production operations. Many of these ISs are procured and supported by third parties, also called 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 create inherited exploitations in other interconnected companies. Cybersecurity practices must be enhanced to understand supply chain cybersecurity posture and manage the risks from lower-tier interconnected entities to the top-level dependent organization. The Theory of Cybersecurity Footprint is at the core of this study, emphasizing the relationship among interconnected entities and the effects one organization can have on another regardless of size.

The goal of this research study was to develop an index to measure the cyber posture of manufacturing organizations based on their interconnected entities. Prior research regarding CMMC 2.0 Level 1 and the referenced domains and elements were leveraged to establish the constructs of an index. A multi-phase developmental research approach was conducted. In Phase 1, 30 cybersecurity Subject Matter Experts (SMEs) were engaged to establish aspects of the index. A pre-analysis data screening was performed with descriptive statistics to address the first three research questions for the importance of domains, elements, and tiers, as well as the number of tiers to establish weight measures. The level of agreement among the SMEs confirmed all domains were important, while 18 of 26 elements were considered important and included in the development of the index. Additionally, the SMEs provided input to questions to determine the response scale options used in a subsequent survey tool called the Cyber Organizational Risk Exposure (CORE) Survey.

In Phase 2, there were significant challenges in recruiting manufacturing companies willing to engage suppliers and vendors in their supply chain. A repeated number of communication methods overcame the lack of interest and commitment to recruit key manufacturing contacts to participate in a pilot group. A pilot group of six manufacturing companies reviewed the CORE Survey questions and provided insightful feedback to refine a final version of the survey. The pilot group's responses to the 18 questions were used to validate the calculation of CORE scores using the weights of the domains and the elements, as well as the Cybersecurity Footprint Index for Manufacturing (CFI-Mfg). A

web-based application prototype was developed to verify the resulting CORE scores as an additional testing method. Immediately following the submission of the web-based application, a CORE score was calculated and displayed on a scale of 0 to 100. The CORE scores for each of the pilot group manufacturing companies were used to calculate three different CFI-Mfg scores based on one, two, and three tiers and a different number of entities in the tiers. The calculated CFI-Mfg Scores were 66.33, 51.26, and 60.26 respectively.

In Phase 3, several manufacturing associations and the FBI-affiliated InfraGard were contacted in an attempt to recruit manufacturing companies for participation in this phase. This effort was also met with a lack of interest and resistance. The initial communication with key contacts was promising, and they expressed a willingness through emails and phone calls; however, as the information was shared with members, there was either no follow-through or no continued interest from the manufacturing associations. To gain participation, companies having Business-to-Business (B2B) relationships supporting manufacturing companies were targeted. With the dedicated support of key consulting contacts and strong relationships with their clients, over 70 B2B companies participated in Phase 3.

The resulting CORE scores were used to calculate 60 CFI-Mfg scores based on a different number of tiers, as well as a different number of entities in the tiers. A combination of descriptive statistics and one-way analysis of variance (ANOVA) was used to determine the significance of CFI-Mfg based on the number of interconnected entities, the number of tiers of interconnected entities, and a set of attack surface variables. The attack surface variables included (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 mobile devices, (h) number of IoT devices, and (i) number of employees. Each of the variables did not appear to be significant in the determination of a CFI-Mfg score. However, the combination of the CORE Survey to gather data from interconnected entities in the supply chain can be used to determine the CFI-Mfg as a single tier of all entities and to assess an organization's cyber posture on a measurable scale. Discussions, implications, and future research recommendations are provided.

Acknowledgment

First and foremost, I give all glory and honor to God for the countless blessings in my life and for the opportunity to pursue a doctorate degree. It is only through His grace, peace, and strength that I have reached this milestone.

This accomplishment is dedicated to my parents, Barbara and Tony. The values of hard work and striving to reach my goals you both instilled in me have been the foundation of my life. Mom, thank you for your unconditional love and constant encouragement. Losing my father on July 5, 2022, left an irreplaceable void. Dad, your tireless work ethic and dedication shaped me from boyhood to adulthood. The lessons of perseverance and resilience you taught through your example are ones I carry with me every day. Until we meet again, rest in peace.

To my children, Justin and Kayla, you are constant inspiration. I am incredibly proud of the people you have become. Never stop learning, exploring, and contributing to the world around you. You are the greatest blessing of my life.

To my wife, Karen, words cannot fully capture my gratitude. Your love, unwavering support, and countless sacrifices made this journey possible. I am truly blessed to have you by my side, and I love you more than words can express.

I extend my heartfelt thanks to my professors and mentors, whose guidance and insight were critical in shaping my work. Special thanks to Dr. Wang, Dr. Kumar, and especially Dr. Levy, whose support, encouragement, and mentorship pushed me forward and created doors to be opened. You have been instrumental, thank you.

I am deeply grateful to everyone who supported me throughout this journey—those who consulted with me, provided feedback, read drafts, participated in surveys, responded to emails, or simply checked in. Your encouragement and support have been invaluable.

To everyone who has touched my life in meaningful ways, whether briefly or enduringly, thank you. Each of you has shaped the person I am today, and your collective impact is immeasurable.

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

Table of Contents

Abstract	iv
List of Tables	ix
List of Figures	xii

Chapters

1. Introduction	1
Background	1
Problem Statement	2
Research Goals	4
Relevance and Significance	7
Barriers and Issues	9
Limitations	10
Definition of Terms	11
Summary	14
2. Review of Literature	16
Introduction	16
The Theory of Cybersecurity Footprint	17
Supply Chains	22
Industry 4.0	28
Cyber-Physical Systems	34
Supply Chain, I4.0, and CPS Risks	37
Supply Chain Risks	37
Industry 4.0 Risks	42
Cyber-Physical Systems Risks	47
Data Breaches	53
Data Breaches Defined	53
Data Breach Causes, Impacts, and Consequences	54
Data Breach Incidents	58
Targeting the Manufacturing Industry	66
Threats to Manufacturing and Impacts	69
Cybersecurity Frameworks	77
Cybersecurity Maturity Model Certification (CMMC)	79
CMMC 2.0 Level 1	80
CFI Domains and Elements	82
Multi-Criteria Decision Analysis (MCDA)	91
Pairwise Complexity and Alternatives	101
AHP and Delphi Method	107
Summary of What is Known and Unknown	113

3. Methodology	116
Overview	116
Research Measures	120
Research Method	120
Research Phases	126
Phase 1	127
Phase 2	128
Phase 3	128
Instrument Development	129
Phase 1 Instruments	129
Weight Measure	129
Phase 2 Instruments	135
Proposed Samples	138
Phase 1	138
Phases 2 and 3	138
Data Analysis	139
Research Validity and Reliability	140
Validity	140
Reliability	141
Presenting Results	142
Summary	143
4. Results	145
Overview	145
Phase 1 – Subject Matter Expert (SME) Survey	146
Demographic Analysis	146
Phase 1 Pre-Analysis Data Screening	149
Phase 1 Data Analysis of Tiers, Domains, and Elements	151
Phase 2 – Pilot Survey	165
CORE Score Calculation Assumptions	166
Validation of CORE Scores	167
Example Calculation for Pilot Company 1	167
Pilot Companies’ CFI-Mfg Score Calculation Assumptions	169
Calculating CFI-Mfg Score based on One, Two, and Three Tiers	170
Example Calculation of CFI-Mfg Score with Pilot Companies in Two Tiers	171
Phase 3 - Quantitative Research	175
Quantitative Analysis of the Number of Interconnected Suppliers/Vendors	183
Quantitative Analysis of the Number of Tiers of Suppliers/Vendors	184
Quantitative Analysis of the Attack Surfaces	185
Summary	188
5. Conclusions, Implications, Recommendations, and Summary	190
Conclusions	190
Implications	192

Recommendations and Future Research	194
Summary	195

Appendices

A. CMMC 2.0 – Level Domains and Cybersecurity Footprint Elements	203
B. Phase 1 SME Survey	206
C. Phase 2 Pilot Group – CORE Score Survey	218
D. Phase 3 CORE Score Survey	232
E. Participation Email to Experts	242
F. Participation Email to Pilot Group	244
G. Participation Email to Manufacturing Companies	245
H. Web-Based Prototype of CORE Score Survey and Results	246
I. The IRB Approval	247

References	249
-------------------	------------

List of Tables

Tables

1. Literature Summary of Cybersecurity Footprint and RDT 19
2. Literature Summary of Supply Chain 24
3. Literature Summary of Industry 4.0 31
4. Literature Summary of Cyber-Physical Systems 36
5. Literature Summary of Supply Chain Risks 40
6. Literature Summary of Industry 4.0 Risks 44
7. Literature Summary of Cyber-Physical Systems Risks 49
8. Literature Summary of Data Breach Consequences 56
9. Literature Summary of Manufacturing Company Breaches 61
10. Literature Summary of Data Breaches 63
11. Literature Summary of Manufacturing Industry 73
12. Example of Access Control Domain 80
13. Literature Summary of Cybersecurity Framework 86
14. Example of Pairwise Comparison 93
15. Literature Summary of MCDA and AHP 95
16. Literature Summary of Pairwise Complexity and Alternatives 105
17. Example Index for Information System Cybersecurity Risk 109
18. Literature Summary of AHP and Delphi Method 111
19. Literature Summary of Delphi Method Studies 124

20. Proposed Measures for Phase 1	130
21. Descriptive Statistics of SMEs' Demographics (N=30)	147
22. Pre-Analysis Data Screening of High-end Number Survey Question Responses (N = 30)	150
23. Descriptive Statistics of Number of Tiers (N=30)	151
24. Means of SME Weights Percentage for each Tier (N=30)	153
25. Weight Distribution Based on # of SMEs (N=25)	153
26. Calculated Weights for Two Tiers and Three Tiers (N=25)	154
27. Importance Level of Domains (N=30)	155
28. Importance Level of Elements (N=30)	157
29. Association of Domain Weights and Element Weights (N=30)	162
30. Determination of Element Scale Intervals (N=30)	163
31. Example of Survey Selection Options and Values (N=30)	165
32. Pilot Companies' CORE Score Survey Results (N=6)	166
33. Pilot Companies' Summed Weighted Element Scores by Domain (N=6)	168
34. Pilot Companies' Weighted Domain Scores and CORE Score (N=6)	169
35. CFI-Mfg Score with Pilot Companies in One Tier (N=6)	172
36. CFI-Mfg Score with Pilot Companies in Two Tiers (N=6)	173
37. CFI-Mfg Score with Pilot Companies in Three Tiers (N=6)	173
38. Summary of Phase 2 Pilot Group Qualitative Results (N=6)	174
39. Calculated Core Scores (N = 71)	176
40. Descriptive Statistics of Calculated CORE Scores (N=71)	178
41. Summary of Tiers, Entities, and CFI-Mfg by Org No. (N=60)	180

42. Descriptive Statistics of CFI-Mfg Scores (N=60)	181
43. ANOVA Results for the Number of Entities (N=60)	183
44. ANOVA Results for Two Tiers and Three Tiers of CFI-Mfg Scores (N=60)	184
45. Descriptive Statistics of Attack Surface Survey Responses (N=71)	186
46. ANOVA Results for CFI-Mfg and Individual Attack Surface Variables (N=60)	187

List of Figures

Figures

1. An Example of Increasing Number of Pairwise Comparisons (n) 102
2. Research Design 118
3. Association of Elements, Domains, and Weights Toward a CORE Score for a Given Organization 119
4. Conceptual CFI-Mfg Hierarchy Model 119
5. An Example of a Participant Survey Question 136
6. An Example of CORE Scores and CFI-Mfg Score 137
7. Mean and Standard Deviation of SMEs' Number of Tiers 152
8. Mean and Standard Deviation of SMEs' Level of Domain Importance 156
9. Mean and Standard Deviation of SMEs' Level of Element Importance (N=30) 160
10. Proportion [in%] Agreement of Elements' Importance on the Cyber Posture of an Organization Toward the Potential Risk Exposure from Interconnected Entities (N=30) 161
11. Scatter Plot of CORE Scores (N=71) 178
12. Mean and Standard Deviations of CORE Scores by Type of Entity (N=71) 179
13. Mean and Standard Deviations of CFI-Mfg Scores (N=60) 182
14. Mean and Standard Deviation of Attack Surface Survey Responses (N=71) 187

Chapter 1

Introduction

Background

The digital transformation of business processes and systems, initially designed as silos, has allowed business partners in the supply chain to integrate and interact globally as distributed organizations (Ciano et al., 2022). Asghar et al. (2019) indicated that corporate networks have become highly interconnected with the public network (e.g., Internet and Cloud Computing) supported by standardized open architectures, alleviating organizations of proprietary and isolated systems. Over 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 (Ho et al., 2022). 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 (Ani et al., 2017).

In response to the growing number of interconnected entities, ease of system hacking, and increased number of exploits, Levy and Gafni (2021) presented the Cybersecurity Footprint concept, 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). 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.). The U.S. government has deemed manufacturing as one of the 16 critical infrastructure sectors requiring protection from threats, which, if impacted, would debilitate society and the economy (CISA, 2020; Robles et al., 2008). Hemilä et al. (2019) 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). Culot et al. (2019) indicated that in traditional manufacturing companies’ cybersecurity is seen as a pure cost and technical issue; the approach is typically reactive rather than planned and only comes up on executives’ radars after a major crisis occurs.

Problem Statement

This research study addressed the loss manufacturing companies encounter from degradation of product/production qualities, damaged brand reputations, impacted sales revenues, and jeopardized health and safety of human lives caused by successful cybersecurity attacks (Ani et al., 2017). A thorough understanding of assets and resources is required for effective cybersecurity management to prevent business impacts, such as data leakage, disruption of business operations, loss of intellectual property, and loss of financial assets (Syed et al., 2022).

Strohmier et al. (2022) indicated that the cybersecurity posture of an entire supply chain is weakened by any vulnerability introduced by the least cybersecurity-capable

company. Moreover, Strohmier et al. (2022) claimed, “use of a maturity model with built-in accountability is a way to reduce vulnerabilities from the use of interdependent systems” (p. 18). The Cybersecurity Maturity Model Certification (CMMC) is a framework of controls and practices that builds upon regulations, best practices, and cybersecurity standards to protect an interconnected supply chain (DoD, 2021). CMMC 2.0 consists of three levels: foundational, expert, and advanced. Each level is representative of practices across 14 domains. Level 1 is for self-assessment and consists of 17 practices, while Levels 2 and 3 are significantly more complex, with 110 practices each. The United States (U.S.) Department of Defense (DoD) mandated more than 350,000 contractors in the Defense Industrial Base (DIB) providing services to it must comply with CMMC 2.0 and establish compliance checks, as well as self-assessments (Ajayi et al., 2022). While CMMC compliance is a requirement for the DIB Sector, the recent events of Solar Winds, Colonial Pipeline, and JBS, to name a few, will likely become a standard for all U.S. businesses (Strohmier et al., 2022). Keskin et al. (2021) stated that 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 on which the organization is dependent.

Levy and Gafni (2021) indicated that the Cybersecurity Footprint of an organization is not determined by the organization’s size but based on the number of business linkages, the number of customers, types of stored data, cybersecurity mitigation controls, and attack surfaces, to name a few. A key point of the Theory of Cybersecurity Footprint is the damage an organization can have on another organization regardless of

size. 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 found that 54% of 310 manufacturing companies surveyed were confident in their ability to withstand the effects of a data breach. However, their survey found that 38% of 245 smaller companies (revenue less than \$500M) performed cyber audits (Sikich LLP, 2019). 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 (almost 56% of 625) respondents confirmed a data breach caused by one of their vendors (Ponemon Institute, 2017).

To compete in today's marketplace, manufacturing companies must increase technology use and effectively participate in I4.0 (Immerman, 2021). The use of interconnected technologies, such as the Internet of Things (IoT) and Industrial Control Systems (ICS), supported by third-party service providers, create layers of cybersecurity vulnerabilities that manufacturing companies may be unaware of (İlhan & Karaköse, 2019). Hence, additional research is warranted to go beyond traditional cyber risk assessments and measure interconnected entities' cascading effects to accurately conceptualize an organizational cybersecurity posture (Levy & Gafni, 2021).

Research Goals

The main goal of this research study was to design, develop, and validate a Cybersecurity Footprint Index for Manufacturing (CFI-Mfg) to measure an organization's cybersecurity posture with input from interconnected multi-tiered vendors/suppliers. This

research study attempted to aggregate and quantify an organizational cybersecurity posture by utilizing a set of CMMC 2.0 domains and proposed Cybersecurity Footprint elements (see Appendix A) to construct the CFI-Mfg (Levy & Gafni, 2022; O.U.S.D.A.S., n.d.). The seven specific goals of this study were as follows.

The first specific goal of this study was to identify, using Subject Matter Experts (SMEs), a set of weights for the domains and elements that are valid for the development of the CFI-Mfg. As noted by Chowdhury and Squire (2006), more weight may be given to categories that are deemed to be more important, as “equal weight is considered to be universally wrong” (p. 762). The second specific goal of this study was to determine whether using SMEs-specific interconnected vendors/suppliers’ tiers beyond the originating manufacturing organization is valid for the development of the CFI-Mfg. Wang (2021) demonstrated the use of the Analytic Hierarchy Process (AHP) method to calculate importance layer by layer and quantitatively described the value. The third specific goal of this study was to identify using SME weights for the tiers of the originating manufacturing organization and the interconnected vendors/suppliers that are valid for the development of the CFI-Mfg. The fourth specific goal of this study was to determine the specific CFI-Mfg that provides a measurable cybersecurity posture for at least 30 manufacturing companies and their interconnected vendors/suppliers. Whereby cybersecurity posture defined by National Institute of Standards and Technology (NIST) Special Publication 800-128 was “the security status of an enterprise’s networks, information, and systems based on information security resources (e.g., people, hardware,

software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes” (Johnson et al., 2011, Appendix B-7).

This study's last three specific goals determined if there are statistically significant mean differences among the CFI-Mfg and other variables. Gallo (2016) referred to Tom Redman’s definition of statistical significance as confidence in a real finding, not by chance. The testing of statistical significance does not indicate the reliability, replicability, magnitude, or importance of a result but whether it will occur under the null hypothesis (Shaver, 1993). As such, the fifth specific goal was to determine if there are statistically significant mean differences to the CFI-Mfg based on the number of interconnected suppliers/vendors. The sixth specific goal was to determine if there are statistically significant mean differences to the CFI-Mfg based on the number of interconnected suppliers/vendors tiers. The last specific goal of this study was to determine if there are statistically significant mean differences to CFI-Mfg based on various attack surfaces.

The main Research Question (RQ) this study addressed was: What is the role of the elements of the CFI-Mfg in providing a measurable cybersecurity posture for manufacturing companies and their interconnected vendors/suppliers? Furthermore, RQs were addressed to support the development of a CFI-Mfg specifically for manufacturing companies and their multi-tiered interconnected entities. This study had seven additional specific RQs as follows:

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 mobile devices, (h) number of IoT devices, and (i) number of employees.

Relevance and Significance

Keskin et al. (2021) expressed, “every vendor or partner organization poses a potential security risk” (p. 1183). The major security breaches that have occurred, such as in Target, Home Depot, and the U.S. Office of Personnel Management, were due to a

weakness in the supply chain; a 2017 KPMG report indicated the most significant gap in managing cyber risk was from the vulnerabilities of supply chain partners (Melnyk et al., 2022). Bowman (2013) claimed criminals have realized the susceptibility of the supply chain, whereby more than 40% of data breaches originate from an attack on a supplier.

For manufacturing companies, I4.0 consists of Information Technology (IT) and Operational Technology (OT) systems connecting cloud resources and industrial Internet to various technologies such as sensors, embedded applications, and industrial hardware for real-time data (Melnyk et al., 2022). Additionally, Melnyk et al. (2022) acknowledged the precise operation of such equipment and systems is important. In the case of malfunction, vendors (e.g., partners or suppliers) may have quick access through backdoor methods to systems that are usually secure. 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 secure network of an organization, which could lead to the propagation of a cyber incident to other connected partners (Accenture, 2019; Sailio et al., 2020).

There remains a lack of solutions from an academic and practitioner perspective to address supply chain cybersecurity issues, even though the problems have become clearer and more defined (Melnyk et al., 2022). However, Keskin et al. (2021) concluded that data-driven empirical tools provide organizations with the means to understand their cybersecurity landscape better. As such, quantifying a CFI-Mfg score is relevant to addressing cyber-attacks on companies and interconnected entities in the supply chain by

being able to measure areas of risk, recognize threats, and reduce uncertainty (Levy & Gafni, 2022).

This study contributed to the cybersecurity management body of knowledge by extending the Theory of Cybersecurity Footprint through the development of a measurable cyber posture index for manufacturing companies. Levy and Gafni (2022) asserted a self-assessment method that is easy to comprehend and allows for industry benchmarking would be an important contribution. An innovative contribution of this research was the confirmation and validation of weights specific to manufacturing companies for the selected CMMC 2.0 – Level 1 domains, proposed Cybersecurity Footprint elements, and interconnected tiers that construct the CFI-Mfg.

Barriers and Issues

The research approach had several barriers and issues to contend with, which could have impacted the validity and reliability of this study. The use of the Delphi method required a minimum number of SMEs who were recognized as domain experts to participate through Phase 1. Although a standard number of participants is not clearly defined, fewer than ten and no more than 100 are most ordinary (Avella, 2016). The length of the first SME survey required an extended amount of time beyond what participants may have been willing to provide to submit their responses for weights of the tiers, domains, and CFI-Mfg elements. Although the questions were developed from a prior literature review, without requesting approval or critique of the domains or elements, the SMEs may have felt overwhelmed by asking for written justification for

their responses. A low survey response rate or SME attrition may have occurred if the time to complete the initial survey exceeded the SME's expectations. To address SME-related issues, communication with the SMEs was necessitated upfront with explanations and periodic check-ins to ensure progress and to meet targeted completion dates. Subsequently, arriving at a consensus with the SMEs was challenging, as differing opinions impacted the progress of the research to Phase 2 quickly and efficiently.

Finally, managing the cascading requests from the originating manufacturing companies to the interconnected entities was a barrier for a few reasons. The first issue arose due to a lack of follow-through when the originating company identified and communicated with their suppliers/partners, who in turn were required to identify and communicate with their suppliers/partners. A lack of participation from manufacturing companies and their supplier/partners was addressed by the recruitment of companies with Business-to-Business (B2B) relationships.

Limitations

Limitations of this study included the recruitment of SMEs, their relevant experiences, and their objectivity in participation. To address this, Chalmers and Armour (2019) indicated a lack of guidelines for researchers for the Delphi method and encouraged them to make priori decisions to reduce bias and improve the technique's validity. A preceding literary review confirmed the primary constructs toward the development of the CFI-Mfg index. Similarly, the criteria of the SMEs were defined before selection based on academic achievement, certifications, and professional

experience in cybersecurity. Finally, the sample size of manufacturing companies that participated in the quantitative phase of this study presented limitations in achieving validation and generalizability of the results, especially due to the variability of the number of tiers and the number of entities at each tier.

Definition of Terms

The following represent terms and definitions.

Attack surface – the exposed, reachable, and exploitable vulnerabilities in which an adversary can enter a system and potentially cause damage (Howard, 2003; Lipner, 2004).

Cyber-attack – a malicious activity coordinated by one or more adversarial parties exploiting an operational vulnerability or weakness to infect a computer system without the consent or knowledge of its users, administrators, or vendors with the intent to obtain or manipulate sensitive information (Huang et al., 2018; Cornish, 2021; Udofot & Topchyan, 2020).

Cybersecurity – “is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights” (Craig et al., 2014, p. 17).

Cybersecurity footprint – Levy and Gafni (2021) described Cybersecurity footprint as:

The potential malicious impact to an entity (organizational or individual) and/or its cascading effects on interconnected entities, which may result from a cybersecurity incident from exploits to their set of traceable digital footprints

including movements, transactions, and records that are performed via digital networks or the internet. (p. 2)

Cybersecurity Maturity Model Certification (CMMC) – is a cybersecurity framework initiated by the DoD in 2019 intended to require all contractors and subcontractors doing business with the DoD to obtain verification and certification of adherence to the unified set of cybersecurity standards (Peters, 2020).

Cybersecurity incident – “Any event or activity that misaligns actual (de facto) property rights from perceived (de jure) property rights, whether by intention or accident, whether known or unknown, is a cybersecurity incident” (Craig et al., 2014, p. 17).

Cyber posture – is the maturity of an organization to significantly decrease the probability or likelihood (or frequency) of success of a cyber incident (Battaglioni et al., 2022).

Data breach – “is a security incident in which sensitive, protected, or confidential data are copied, transmitted, viewed, stolen, or used by an unauthorized individual” (Khan et al., 2019, p. 2).

The Delphi methodology – is an iterative process technique developed by Dalkey and Helmer in the early 1960s for the RAND Corporation to develop and rank solutions to a problem typically by soliciting experts anonymously (Irvine, 2021).

Index model – a tool devised to measure a particular subject based on variables or dimensions, for example, the American Customer Satisfaction Index (ACSI) measures fashion companies' sustainable performance in retailing and supply chains based on consumer evaluation (Wang et al., 2019).

Internet of Things (IoT) – “a well-known paradigm that defines a dynamic environment of interrelated computing devices with different components for seamless connectivity and data transfer” (Stoyanova et al., 2020, p. 1191).

Industrial Control Systems (ICS) – the various connected electronic equipment (e.g., robots, computers, machine tools, sensors, actuators, and measuring instruments) used via communication networks in factories, process plants, and automated facilities to monitor and control manufacturing and applications (Kim & Tran-Dang, 2019).

Subject Matter Expert (SME) – a person who possesses depth and breadth of technical knowledge and can articulate and communicate effectively (Mattoon, 2005).

Third-party cyber risk – “Third-party cyber risk is the likelihood that your organization will experience an adverse event (e.g., data breach, operational disruption, reputational damage) when you choose to outsource certain services or use software built by third parties to accomplish certain tasks” (Hyperproof Team, 2022, para. 6).

Threat actor – “is an entity responsible for an incident that impacts or has potential to impact an organization’s security” (Sailio et al., 2020, p. 4335). A compromised business partner could be a threat actor (Accenture, 2019).

Vulnerability – “weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source” (Furlani, 2009, p. 9).

Summary

This research study developed a measurement index by engaging SMEs to identify and validate the weights for tiers, domains, and elements to determine the cyber posture of manufacturing companies. Six domains and 26 proposed elements from CMMC 2.0 Level 1 identified by Levy and Gafni (2022) in support of the Theory of Cybersecurity Footprint were foundational input to this study. Quynh (2014) claimed that the preparation of elements and indicators for first-round questions with experts could be based on literature analysis. Moreover, while determining weights was a key contribution to developing the index, the SMEs were asked for their expert opinion on the number of interconnected tiers to include beyond the originating organization.

Levy and Gafni (2021) argued the need to identify risks that organizations are unaware of downstream and, thus, proposed Cybersecurity Footprint to prevent the “domino effect” (p. 725) by improving risk assessments and prioritization. They claimed, “the size of the organization is not the main factor to measure Cybersecurity Footprint” (p. 732). In that capacity, the interaction between customers, suppliers, and partners through digital integration (e.g., software, hardware, and communications networks) has transformed and increased the complexities of the supply chain (Bhargava et al., 2013; Nasiri et al., 2020).

The manufacturing sector is an attractive target due to its dependencies on operational technologies and low tolerance for downtime. In 2022, the manufacturing sector represented 58% of cyber incidents remediated by X-Force (IBM, 2023), with 28% of the incidents involving backdoor deployments and 14% involving external remote services

(IBM, 2023). Various technologies, such as IoT, 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 and extended vulnerabilities beyond regular time periods (Ani et al., 2017; Ouellette, 2023).

This research study addressed the impact manufacturing companies experience from data theft, data leaks, operational disruptions, and monetary loss due to extortion (IBM, 2023). Ciano et al. (2022) claimed that very few companies have mastered tools to protect against unlawful access by attackers seeking to disrupt operations, obtain intellectual property, or achieve financial gain. With that, this research devised a measurable index to aggregate and calculate CFI-Mfg scores for companies and to determine risk exposure from associated entities within their supply chain.

Chapter 2

Review of Literature

Introduction

This chapter presents a literature review to provide a theoretical basis for this study to develop an index to evaluate the cyber posture of manufacturing companies. Levy and Ellis (2006) claimed an effective and quality literature review is based on a concept-centered approach; therefore, by exploring the Theory of Cybersecurity Footprint and related subjects such as supply chains, Industry 4.0 (I4.0), Cyber-Physical Systems (CPS), and data breaches provided a deeper understanding, an awareness of risks, as well as the potential effects from interconnected entities. Literary evidence demonstrated that the manufacturing industry is a target for cyber-attacks, whereby potential impacts and consequences were synthesized, such that the research problem is confirmed.

Levy and Gafni (2023) established the Universal Cybersecurity Footprint Index (UCFI) as a generic calculation and encouraged researchers to adjust or define new indices for specific industries. Therefore, a review of the Delphi method and previous studies demonstrated the applicability of an iterative approach with SMEs to establish key measures and index weights specific to the manufacturing industry. From this literature review, MCDA and modified approaches to AHP were observed, and their combination with the Delphi method in prior research was demonstrated to be effective.

In addition, the literature presented adaptations of Cybersecurity Frameworks (CSFs) as widely accepted. The use of CMMC 2.0 Level 1 domains and the practices proved to be an effective and viable option for the CFI-Mfg.

The Theory of Cybersecurity Footprint

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, Levy and Gafni (2021) termed the concept of Cybersecurity Footprint to illustrate the cascading effect cyber-attacks can have on interconnected entities. Digital technologies such as mobile, social media, embedded devices, and analytics enable the creation of new business models and improve business processes (Fitzgerald et al., 2014). However, these very same technologies can be used by cybercriminals to significantly impact a company's Cybersecurity Footprint (Levy & Gafni, 2021). As such, while digital technologies create value from a positive perspective, the reliance on them to remain business competitive can also have unintended negative consequences, such as disseminating information publicly that makes a system vulnerable (Srinivas & Liang, 2022; Vial, 2019).

From a theoretical perspective, Srinivas and Liang (2022) suggested a paradoxical view can assist with identifying the negative aspects of dual concepts, with examples such as innovation and change, cooperation and competition, and stability and change, to name a few. Levy and Gafni (2021) stated, "the organizational cybersecurity footprint is dependent upon the volume of their supply chain digital connectivity" (p. 726) and expressed, "cybersecurity footprint has only negative implications" (p. 725). Paradox

Theory can explain this phenomenon, such that new technologies and digital integrations create complex interactions that contribute to business success. However, this could lead to vulnerabilities, further digitization, and ultimately, the company's demise (Srinivas & Liang, 2022).

Schroeder et al. (2019) indicated, "Resource Dependence Theory (RDT) deals with a firm's dependence on another firm's resources and the consequences and strategies for managing this dependence" (p. 1307). In likeness to RDT, Levy and Gafni (2022) described the dependency between organizations in supply chains and proposed the Theory of Cybersecurity Footprint as a means for understanding, assessing, and managing their cybersecurity posture influenced by the decisions of others. Furthermore, the parallel between RDT and Cybersecurity Footprint is supported by the focus on external resources, mutual dependence, as well as intent to minimize the uncertainty of the external dependency and impact (Levy & Gafni, 2021; Schroeder et al., 2019).

Levy and Gafni (2021) stated, "it is important to note that the notion of trust and the potential for breaking that trust appear to be inherent to the concept of Cybersecurity Footprint" (p. 725). Xiao et al. (2019) asserted that RDT theorizes that parties in the supply chain make every effort to develop alternative relationships to avoid becoming interdependent. However, as knowledge and information sharing becomes easier, partners' confidence, reliability, security, and trust develop within their relationships (Kim et al., 2020). Lastly, from an RDT perspective, Wang and Liu (2021) indicated the depth (e.g., number of tiers) and the width (e.g., number of suppliers in the tier) are two factors of the supply chain that influence behavior, as well as introduce risk and

uncertainty as resource needs increase. Based on the Theory of Cybersecurity Footprint, Levy and Gafni (2023) claimed an organization should be able to track its cybersecurity posture by understanding how the decisions and actions of interconnected entities, as well as their own, impact the supply chain. Furthermore, Levy and Gafni (2021) alluded that risks and impacts to interconnected entities may be mitigated by reducing their Cybersecurity Footprint. A summary of the prior research regarding the Theory of Cybersecurity Footprint, Paradox Theory, and RDT is listed in Table 1.

Table 1

Literature Summary of Cybersecurity Footprint and RDT

Study	Description of the Problem or Theory	Methodology	Sample	Instrument or Constructs	Main Finding or Contribution
Fitzgerald et al., 2014	Challenges of digital technologies, business adoption, and transformation	Empirical study	1,559 people in 106 counties	Survey	Achieving digital transformation (DT) is critical, organization's pace of changing is too slow, minority of CEOs have DT on their agenda, high percentage of employees support CEO's shared vision
Kim et al., 2020	Impact of key factors on logistics	Empirical study	250 manufacturers	Survey	Trust, satisfaction, and

Study	Description of the Problem or Theory	Methodology	Sample	Instrument or Constructs	Main Finding or Contribution
	integration and supply chain performance related in outsourcing situations				commitment are positively correlated with logistics integration between the client firm and the logistics service providers
Levy & Gafni, 2021	Proliferation of data breaches and implications between interconnected entities	Conceptual paper	None	Digital footprint versus active and passive cybersecurity footprint and interconnected “domino effect”	Illustrated cases in support of the cybersecurity footprint conceptual definition
Levy & Gafni, 2022	Implications to small businesses with trying to secure systems and lack of knowledge in conducting self-assessments	Literature review	None	CMMC 2.0 – Level 1 domains and practices	Translation of 17 practices from CMMC 2.0 Level 1 into 26 elements for cybersecurity footprint index
Levy & Gafni, 2023	Small business organizations have less resilience to	Quantitative research	27 Subject Matter Experts	Survey	Provided an equation for a Universal Cybersecurity Footprint

Study	Description of the Problem or Theory	Methodology	Sample	Instrument or Constructs	Main Finding or Contribution
	reduce their chances against cyber incidents				Index (UCFI) based on 20 validated elements and associated weights
Schroeder et al., 2019	Key barriers to product use data impacts or influences benefit opportunities for business network capabilities	Qualitative research (interviews, focus group, Delphi-based inquiry)	21 SMEs	Product-use data	Provided recommendations for management operating in context I4.0 from a resource theory dependency
Srinivas & Liang, 2022	Theorize digital transformation efforts increase the likelihood and severity of data breaches	Literature review and empirical research	3604 data breaches over a 10-year timespan (2011-2020)	Digital IQ, innovativeness, data breach risk, data breach severity, revenue, good will, and acquisitions	Mobile and digital marketing are most vulnerable and significantly increase the likelihood and severity of a data breach event
Vial, 2019	Lack of comprehension and implication of digital transformation	Literature review	282 published works	Building blocks of digital transformation process	Framework to ethically study digital transformation
Wang & Liu, 2021	Uncertainty in buyer and	Empirical study	1,075 observatio	Firm innovation,	Highlighted actions to

Study	Description of the Problem or Theory	Methodology	Sample	Instrument or Constructs	Main Finding or Contribution
	supplier relationships		ns from 502 firms	supplier depth, supplier width, institutional distance, and market competition	reduce uncertainty and need for supplier heterogeneity
Xiao et al., 2019	Lack of understanding concerning resource dependence for supplier involvement and technology uncertainty	Empirical study	125 manufacturers	Survey	Proven set of hypothesis regarding buyer dependency, supplier dependency, and technology uncertainty

Supply Chains

Sobb et al. (2020) depicted a supply chain to “consist of a network of systems, processes and organizations that produce valuable goods and services, and their delivery to their end user” (p. 1866). Furthering the definition, supply chains provide more than the transport of goods; they are comprised of services facilitated by the flow of information within and between organizations, resulting in financial exchange (Hassija et al., 2020; Sobb et al., 2020). Hassija et al. (2020) indicated supply chains have become complicated from an ever-increasing and growing number of variables. Therefore, the goals and objectives among suppliers, customers, and partners must be aligned from origination to consumption to deliver value at the lowest cost for the overall supply chain

(Pandey et al., 2020). Boiko et al. (2019) declared “the chains of manufacturers, suppliers, contractors, transport, and trading companies are intertwined in the most intimate way” (p. 67). Garay-Rondero et al. (2020) claimed to leverage the power of the “network”, the integration should go beyond internal and functional to include the supplier’s supplier and the customer’s customer (p. 908).

The supply chain can also be described as a third-party ecosystem based on a Nth number of companies with direct and indirect relationships (Ponemon Institute, 2017). To put into perspective, a survey conducted by the Ponemon Institute (2017) found that 57% of 471 (roughly 269) companies indicated they had more than 100 third parties, which represented a 24.6% increase in companies (up by 93 from 378) over the prior year. Supply chains foster a dependency on third parties, evident in all industries, such as the pharmaceutical industry, electronics industry, agriculture-food industry, retail industry, and oil and gas industry, to name a few (Hassija et al., 2020). To provide further evidence, Heinbockel et al. (2017) indicated the U.S. DoD has distinct supply chains for various purposes, as demonstrated by their global commercial supply chain to source microelectronics, acquisition supply chain to source prime contractors, and sustainment supply chain to source from aftermarket suppliers. Lastly, in the context of Cybersecurity Footprint, Levy and Gafni (2021) referred to the supply chain as interconnected entities and their associated volume of digital connectivity.

Supply Chain Management (SCM) is the practical organization and effective management of business relationships across all stages of the supply chain (Sobb et al., 2020). More elaborately defined, Ivanov et al. (2017) stated SCM is “cross-department

and cross-enterprise integration and coordination of material, information, and financial flows to transform and use the SC resources in the most rational way along the entire value chain, from raw material suppliers to customers” (p. 5). Supply chain managers have relied on IT to gain a competitive advantage across different geographic and socioeconomic boundaries from organizational systems and infrastructures (Hassija et al., 2020; Norman et al., 2020). This has been demonstrated by electronic commerce conducted via the Internet, such that information is distributed quickly for visibility of demand, procurement, production planning, inventory management, and the management of customer orders, billings, and payments (Warren et al., 2000). Sobb et al. (2020) and Turnball (2018) agreed that the goals of SCM are to remove constraints and drive high-quality value stream levels by accessing information that strengthens connectivity between supply chain parties. A summary of the prior research regarding supply chains is listed in Table 2.

Table 2

Literature Summary of Supply Chains

Study	Description of the Problem or Theory	Methodology	Sample	Instrument or Constructs	Main Finding or Contribution
Boiko et al., 2019	Direction of information systems use for SCM for companies with multi-	Qualitative Research	None	Uncertainties, risks, and cybersecurity aspects	Developed an approach to identify and predict supply chain risks with uncertainty conditions; and

Study	Description of the Problem or Theory	Methodology	Sample	Instrument or Constructs	Main Finding or Contribution
	component production				secure data in information systems for SCM
Garay-Rondero et al., 2020	Lack of a conceptual model of SCM that integrates components and elements into a digitalized SCs	Systematic literature review	Literature (1989 – 2019)	Interconnected dimensions of SCM processes, components, flows, and structures	Developed a framework for adoption and incorporation of Industry 4.0 technology into current SCM to evolve into a digitalized SC
Hassija et al., 2020	Lack of reference model for implementation of complex supply chains	Literature review	None	Sources of threats, security challenges, security critical application areas of the SC	Identified and addressed security threats, security and privacy issues in SCM; recommended technologies for secure communication in SC
Heinbockel et al., 2017	Mitigate supply chain attacks	Technical report	41 supply chain attacks	Supply chain attacks against mission systems consisting of information and comm technologies	Identified phases to apply cyber resiliency mitigations / techniques during the acquisition lifecycle

Study	Description of the Problem or Theory	Methodology	Sample	Instrument or Constructs	Main Finding or Contribution
Norman et al., 2020	Lack of a framework for logistics and SC cybersecurity	Literature review and content analysis	None	Cybersecurity risk reduction for systems and data	Developed concepts to describe the dynamics of cyber-supply chain and logistics management data security vulnerabilities and opportunities for process improvements
Pandey et al., 2020	Limited research identifying cybersecurity risks in the globalized SC and risk mitigation strategies	Literature review and case study research with 11 SC professionals	Several selected case studies	Focus group discussions	Identified and categorized 16 cybersecurity risks as supply, operational, and demand risks
Ponemon Institute, 2017	Limited progress has been made to improve overall effectiveness of third-party risk management programs	Empirical study via survey	625 participants	Third-party data risks	Provided trends and challenges companies face to protect sensitive and confidential information shared third parties and their third parties (Nth party risk)

Study	Description of the Problem or Theory	Methodology	Sample	Instrument or Constructs	Main Finding or Contribution
Sobb et al., 2020	Limited awareness of how SCs are built and the fundamental technologies	Literature review	None	Military SC	Explained the nature of the military SCs compared to commercial SCs to indicate strengths, weaknesses, and dependencies to understand the effect of new technologies on military SCs
Turnbull, 2018	Australian Army to face threats to the Defense supply chain by malicious actors in cyberspace	Conceptual paper	None	Challenges of the Future Operating Environment (FOE) of the Australian Army and the relationship between digitized supply chains, cyber-resilience, and mission assurance	Provided identification and classification of vulnerabilities to be addressed based on risk management, centralized architecture and data, education and research, system and software obsolescence, IT supply chain, and supply chain design

Study	Description of the Problem or Theory	Methodology	Sample	Instrument or Constructs	Main Finding or Contribution
Warren et al., 2000	Risk and impacts involved with electronic commerce and SCM via the Internet	Conceptual paper	Four common attack methods	Cybersecurity risks	Outlined technical, organizational, and human aspects to improve against system risks

Industry 4.0

Industry 4.0 (I4.0) is a term used in the manufacturing industry to define the use of digital technologies, such as cloud systems, data analytics, and machine learning that have been applied to the physical world (Hemilä et al., 2019). In 2011 at the Hanover Fair in Germany, a group of officials termed the concept I4.0 by referring to the fourth industrial revolution and the technologies expected to improve supply chain resilience and performance (Dastbaz, 2019; Madsen, 2019). As evidenced, Qader et al. (2020) found I4.0 improved supply chain visibility, which as a result, strengthened supply chain resilience and subsequently increased supply chain performance. Hsu et al. (2022) indicated I4.0 has increased speed, improved quality, and lowered costs by automating supply chain processes between companies and reducing the dependency on people.

Rad et al. (2022) specified I4.0 as the application of digital technologies toward the realization of digitalization that “affords fundamental changes in intra- and inter-organizational processes, with potential value creation estimated to exceed 100 trillion USD by 2025” (p. 268). From a theoretical perspective, I4.0 design principles are based

on decentralization, interoperability, and modularity to enable vertical integration of an organization's systems, horizontal integration of networks, and end-to-end integration of the supply chain (Zheng et al., 2021). Hofmann and Rüsç (2017) outlined a collection of I4.0 technologies to improve the automation and availability of real-time information, such as Cyber-Physical Systems (CPS), IoT, Industrial IoT (IIoT), Artificial Intelligence (AI), Block Chain (BC), Additive Manufacturing (AM), Machine Learning (ML), and Robotics (RO). Similarly, Rad et al. (2022) referred to Boston Consulting Group's "nine pillars" (p. 269) as a basis of I4.0, which overlapped many of the same technologies and proposed an additional two for a total of 11 core technologies.

Companies are being driven toward I4.0 due to the demands of globalization, customization, and competition (Zheng et al., 2021). Pandey et al. (2020) asserted that I4.0 technologies have enabled a world of customized products and services through connected and smart environments. Benotsmane et al. (2019) claimed without the implementation of smart machines and smart devices (e.g., sensors), which communicate and collaborate continuously, companies would be unable to maintain or increase their competitiveness. Ghobakhloo (2018) stated, "smart factories as the heart of Industry 4.0 cannot work on a standalone basis, and vertical networking of smart factories, smart products and other smart production systems is indeed a necessity" (p. 923). A smart factory is a dynamic manufacturing environment of physical resources connected through smart devices that communicate with each other and human resources to optimize and automate processes to minimize waste, defects, and downtime (Ghobakhloo, 2018).

While many of the concepts appear widely addressed, Garay-Rondero et al. (2020) indicated through a review of the literature on I4.0, Barata et al. (2018), Ben-Daya et al. (2017), as well as Bibby and Dehe (2018), claimed there was a lack of frameworks to address supply chains with the concepts, features, and technologies in an I4.0 environment. However, Garay-Rondero et al. (2020) proposed an interconnected framework to transform traditional supply chains into integrated Digital Supply Chains (DSC) with I4.0 technologies and features. The proposed DSC model addressed the transition from internal to external integration and toward collaborative and interconnected DSC networks. Zheng et al. (2021) referred to other frameworks based on maturity and sustainability, which outlined the relationship between the supply chain and I4.0 and focused on technical aspects of machine-to-machine and human-to-machine integration, respectively.

With manufacturing as the most significant area impacted by I4.0, Zheng et al. (2021) posited which manufacturing business processes were most affected by investigating supply chain planning, operational performance, product development, and production processes. Furthermore, with a focus on manufacturing, Zheng et al. (2021) posed CPS as more than a technology but a working environment to build applications with effective systems integration for production activities. Jirkovský et al. (2016) concluded CPS was the foundation for I4.0, as it could capture physical data, affect physical processes, interact between the physical and virtual world, and be connected (wired or wireless) with the local and global network. A summary of the prior research regarding Industry 4.0 is listed in Table 3.

Table 3*Literature Summary of Industry 4.0*

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Barata et al., 2018	Mobile SCM (mSCM) was understudied and lacked future research direction	Literature review	53 total papers	mSCM classifications	mSCM lacked impact on Industry 4.0; suggested direction for future studies to include innovative technologies, produce mSCM cases, study regulatory compliance, develop maturity model, and explore social aspects
Ben-Daya et al., 2017	Unclear questions regarding research of IoT impact on SCM	Systematic Literature Network Analysis (SLNA)	166 studies	SCOR processes (source, make, deliver, and return)	Identified potential areas of IoT addressing supply chain management challenges
Benotsmane et al., 2019	Implement Smart Factory concept in practice otherwise companies will be unable to maintain or increase competitiveness	Literature review and quantitative with case study	One case study for robotic simulation	Smart Factory	Smart devices, such as collaborating robots, are essential to be competitive, flexible, and efficient for optimal operation of

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
					production processes
Bibby & Dehe, 2018	Companies' lack of understanding or capability to assess I4.0 maturity level without definitions, consensus, or measurement tools	Empirical study with semi-structured interviews and case-study	One company and 14 experts	Eight attributes of Factory of the future	Industry 4.0 framework was developed and tested to forecast objectives, operationalize, benchmark, and assess current position
Ghobakhl oo, 2018	Lack of framework or roadmap to transition from traditional manufacturing to I4.0	Literature review	178 documents	Technology trends of I4.0	Devised a strategic roadmap for the transition to Industry 4.0 for manufacturers
Hemilä et al., 2019	Limitation on economic investment for technology and human aspects relative to cyber threats in SCs	Conceptual paper	Sole case study	Measures and capabilities	Proposed a cyber threat management framework (SoS Management Model)
Hofmann & Rüs ch, 2017	Implications in the field of logistics management due to I4.0	Conceptual paper	None	Fully automated cross-organizational implementations	No commonly agreed-upon definition of I4.0; there is potential in logistics management with implications on

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
					the operative level and cross-organizational logistics as a critical barrier
Hsu et al., 2022	Need to enhance SC resilience to address SC risk from the ripple effect that will disrupt normal operations	Empirical study, with literature review on proposed model, and expert questionnaire	Six Experts	I4.0 enablers (I4Es), ripple effect risk factors (RERFs), supply chain resilience indicators (SCRIs)	Proposed a method based on integration of several frameworks to enhance I4Es, strengthen SCRIs, and mitigate RERFs
Jirkovský et al., 2016	CPS integration challenges caused by semantic heterogeneity	Conceptual paper	None	Heterogeneity classification	Clarified the semantic heterogeneity reduction process and facilitated usage of the process with a real application
Madsen, 2019	Understanding the factors and influences contributing to the emergence and rise of I4.0	Literature review	None	Supply and demand side forces	Examined I4.0 from the perspective of management fashion theory
Qader et al., 2020	Association and effects between I4.0, SC performance (SCP), SC resilience	Partial Least Squares Structural Equation Modeling (PLS-SEM)	458 respondents	Questionnaire	Confirmed impact of Industry4.0 on SCP, SCR as a mediating role between I4.0 and SCP,

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	(SCR), and SC visibility (SCV)				SCV as a moderating role between I4.0 and SCR.
Rad et al., 2022	Fragmentation in review of I4.0 technologies, implications on SC performance, and critical success factors	Literature review	221 articles	Key technology characteristics in I4.0 and SCs	Provided a framework of Industry 4.0 supply chain performance and developed suggested areas of research
Zheng et al., 2021	Lack of research on I4.0 enabling technologies can be applied to support manufacturing life cycle processes	Literature review	186 articles	Enabling technologies and business processes	Provided a framework outlining the potential applications of I4.0 technologies in manufacturing

Cyber-Physical Systems

CPSs are seen in several areas of the supply chain, predominantly within manufacturing, to provide the ability to control physical devices through computer devices (Sobb et al., 2020). Moreover, Yeboah-Ofori and Islam (2019) specified CPS as “the integration of computation and physical process that make a complete system, such as physical components, network systems, embedded computers, software, and the linking together of devices and sensors for information sharing” (p. 63). In the

manufacturing industry, CPSs are sourced from external suppliers to include the likes of such systems as robotic automation, Machine-to-Machine (M2M) communication devices, Supervisory Control and Data Acquisition (SCADA) systems, Enterprise Resource Planning (ERP), and supply chain systems (Hemilä et al., 2019).

NIST described industrial CPS as “fully integrated, collaborative manufacturing systems that respond in real time to meet changing demands and conditions in the factory, in the supply network, and in customer needs” (Canizo et al., 2019, p. 52456). Trappey et al. (2016) expressed the difficulty in developing a single standard due to variability in communication technologies worldwide and the voluminous amount of data collection required. Numerous studies presented different and advanced architectures that were either based on three, four, five, or six layers (e.g., physical, network, processing, and application) or based on a service-oriented architecture with sensors and actuators, network modules, and service modules (Yao et al., 2019). For example, Lee et al. (2015) described the 5Cs of a CPS architecture model as consisting of “connection,” “conversion,” “computation,” “cognition,” and “configuration.” In simpler terms, the model indicated the need for integration so that algorithms could analyze information regarding the current situations to transform gained intelligence into action. Amid many examples of CPS in a Computer-Integrated Manufacturing (CIM) environment, Yao et al. (2019) stated, “RFID (radio-frequency identification) and sensor networks offer advanced monitoring and control of real-world processes at an unprecedented scale, which makes a big difference to CIMS” (p. 2806). A summary of the prior research regarding Cyber-Physical Systems is listed in Table 4.

Table 4*Literature Summary of Cyber-Physical Systems*

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Canizo et al., 2019	Increased amount of data produced by IoT/CPS devices requires innovative method to manage the volumes of data	Quantitative research	None	Evaluation metrics	Demonstrated effectiveness of proposed solution and scalability for future demand
Lee et al., 2015	At the early development stage of CPS requires clear structure and methodology for implementation in industry	Conceptual paper	None	5C architecture	Presented a CPS guideline based on 5C architecture for manufacturing industry to implement for better product quality and system reliability
Trappey et al., 2016	Limited evaluation and research of standards and intellectual property in CPS patents	Literature, standards, and patents review	None	CPS ontology	Provided findings of the latest trends in I4.0 technical standards and patents; guided further research to achieve globally inter-

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
					operable of CPS manufacturing
Yao et al., 2019	A lack of systemic and comprehensive research on the linkages and relationships among models within I4.0	Conceptual paper	None	CPS architectures	Provided a framework for emerging manufacturing integrations
Yeboah-Ofori & Islam, 2019	Risks in the cyber supply chain cause disruption and financial impacts	Conceptual paper	None	Cyber supply chain risk mitigation process	Described how to address cyber supply chain risks, determined probable risks and likelihood of an attack, and identified infrastructure vulnerabilities

Supply Chain, I4.0, and CPS Risks

Supply Chain Risks

Supply chains rely heavily on the Internet, the interconnection of networks, and the interrelationships among interconnected entities. The relationships among companies in the supply chain are conceptually labeled as “upstream and downstream” where linkages and flow of information are multi-directional leading to potential supply chain risk

(Pandey et al., 2020). In likeness to the “domino effect” described by Levy and Gafni (2021), 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 (Dolgui et al., 2018; Hsu et al., 2022; Ivanov et al., 2014).

The act of collaborating and sharing information between supply chain partners can be threatened by terrorism, malware, or data theft leading to interruption, corruption, and discreditation (Pandey et al., 2020). Complex supply chains are entry points for cyber attackers, as each interconnected entity in the supply chain, be that a vendor, supplier, partner, or customer, could be compromised and consequently become a threat to systems and processes. Keskin et al. (2021) suggested that companies inherently increase their risk due to third parties by engaging in third-party relationships to leverage specialized skills and knowledge.

Compared to cyber-attacks, supply chain attacks can be embedded in a component at the start or delivered as a change through a trusted or approved source that goes undetected (Heinbockel et al., 2017). With trusted connections between supply chain partners and the potential spread of cyber incidents, Sailio et al. (2020) expressed that partners find it more difficult than insiders to adopt cybersecurity measures in a timely manner due to partner agreements, legal reviews, and associated expenses. Sailio et al. (2020) acknowledged while partners are rarely identified as threat actors, they are trusted sources that can unintentionally compromise systems or be exploited by third parties.

Theoretically, connected relationships among business partners in a non-hierarchical network are suggested as weakly manageable (Schroeder et al., 2019). Ponemon Institute

(2017) found only 18% (roughly 112 of 625) of the organizations claimed they had visibility into third-party and Nth party data handling procedures, while 75 of the same organizations (approximately 67% of the 112) relied on contractual agreements and 24 organizations (roughly 21% of 112) conducted third-party audits and assessments for visibility. Yeboah-Ofori and Islam (2019) alleged that supply chain issues have occurred due to a lack of cybersecurity controls, lack of risk management, and failure to conduct third-party audits.

Vulnerabilities arise from third-party service providers that do not have the same cybersecurity standards as others in the supply chain. Thus, the susceptibility to security threats increases as the complexity of the supply chain increases (Alladi et al., 2020). Supply chain cyber-attacks can originate through intentional methods, such as network penetration, embedded malicious software, vulnerable websites, or email phishing. Unintentional cyber risks can arise from an underperforming cybersecurity system or an accidental human error (Ghadge et al., 2020). While external intrusions are commonly discussed, Boyson (2014) pointed to supply chain compromise originating from hardware counterfeits, hardware tampering, and insider threats as consequences of the dispersion and reliance on IT systems.

Yeboah-Ofori and Islam (2019) described island hopping as a method attackers use to target their victims through another company engaged in outsourced services to gain access to valuable information to commit a larger-scale attack elsewhere. Hassija et al. (2020) indicated that the cybersecurity of the overall supply chain can be measured by the weakest link, as there are cybersecurity challenges and risks in all phases from malicious

parties targeting vulnerabilities in software and hardware from remote locations. This was exemplified by historic cyber-attacks on the electric power grids of Saudi Aramco and Ukraine, which occurred due to vulnerabilities in other supply chain partner systems (Yeboah-Ofori & Islam, 2019). A summary of the prior research regarding supply chain risks is listed in Table 5.

Table 5

Literature Summary of Supply Chain Risks

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Alladi et al., 2020	ICSs have common cybersecurity vulnerabilities that need to be addressed to prevent significant impacts	Analyze case studies	Seven ICS attacks	Cyber-attack characterization	ICS systems are compromised by phishing and malware; provided protection measures to combat ICS attacks
Boyson, 2014	Globalization and dispersion of the IT supply chain increased the attack surface and ease of penetration by cyber attack	Effectiveness study	Two case studies and prior survey of 200 companies	Categorical assessments	Defined a capability/maturity model to assess cyber risk management practices addressing SC risks
Dolgui et al., 2018	Impact of ripple effect	Literature review and	None	Literary classification	Provided mitigation strategies

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	(disruption propagation) on SC performance	quantitative evaluation			ripple effect for SCs in a controlled framework
Ghadge et al., 2020	Inherent and potential threats and risks to SCs based on the integration and connectedness of information technology infrastructures	Literature review	41 articles	Theme based typology	A conceptual model establishing the link between information technology (direct or indirect attacks), organizational (insider threats), and supply chain security systems (physical threats)
Ivanov et al., 2014	Lack of business models and processes for SC control, as well as a lack of education and research activities	Literature review	None	SC disruption attributes	Highlighted a research agenda on SC dynamics, control, continuity and disruption management to make SCs more robust, adaptable and profitable
Keskin et al., 2021	Need efficient and effective methods to assess the cybersecurity	Literature review and exploratory analysis	Four vendors and a pilot company	Assessment criteria	Various variations exist among cyber risk scoring companies due

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	risks of third-party business partners				to different evaluation methodologies, proprietary datasets, and other risk factors. Standardization is needed from data collection to risk score calculation for reliability and consistency

Industry 4.0 Risks

By 2025, the estimated number of IoT devices connected to the Internet worldwide will be roughly 75 billion (Statista, 2018). The scale of I4.0 and IoT devices makes an industrial environment an attractive target for threat actors as the number of entry points and attack surfaces continues to increase (Avdibasic et al., 2022; Barbosa et al., 2021). Ghobakhloo (2018) asserted that any device connected to the Internet is at risk. As new devices are added, new forms of network communication between devices will lead to more vulnerabilities and increased threat vectors to the organization (Naanani, 2021). Some representative examples that create protection challenges include connecting IoT devices to intercepted Wi-Fi networks (Pilloni, 2018) and communications to the public cloud (Barbosa et al., 2021). Moreover, Prinsloo (2019) specifically pointed to network eavesdropping as a method to access confidential or sensitive information through

insecure channels, such as wireless communication or connectivity to the public cloud for collaborative sharing.

Barbosa et al. (2021) noted that external developers typically use Application Program Interfaces (APIs) to manage the flow of information and remote access to devices. However, they have become entry points for threat actors and architectural vulnerabilities. Avdibasic et al. (2022) contended that the magnitude of I4.0 has caused traditional cybersecurity measures to be inadequate, consequently unable to address unique I4.0 cybersecurity and privacy risks. This is highlighted by a broad list of risks in I4.0 by Avdibasic et al. (2022), which included the lack of trained and knowledgeable cybersecurity resources, the deployment of shadow devices, unchanged default device passwords, outdated software, and weak data encryption.

From a historical perspective, the manufacturing systems in traditional OT environments were siloed and disconnected from other systems, and the operator was the most significant vulnerability. As IoT devices have evolved and expanded into the industrial environment, the IT and OT domains have converged because devices are controlled over the Internet and connected through IT network routers and switches (Prinsloo, 2019). There is no straightforward way to apply IT cybersecurity controls to the OT environment, as cybersecurity has not been a primary design concern of IoT devices, and whose primary focus has been on device availability and support the need to achieve higher plant production yields (Prinsloo, 2019).

Soltovski et al. (2019) attributed cybersecurity risks in I4.0 to a high level of environment heterogeneity and lack of interoperability, while Prinsloo (2019) offered a

review of several cyber-attacks that I4.0 and IoT environments are not benign, that included zero-day attacks, Denial of Service (DoS) attacks, false data injections, and ransomware. Matsuda et al. (2021) conducted direct and indirect attack scenarios against I4.0 technologies, proving the ability to manipulate datasets, steal secret keys, decrypt encrypted communication, and establish unauthorized connections to devices to infect with ransomware. The implications of attacks could lead to the manipulation, exposure, or destruction of data; as Prinsloo (2019) claimed, “one of the most commented risks in the literature is related to data security” (p. 8). Müller and Voigt (2018) also conveyed that data compromise risks in I4.0 may be internal data and connected partners' data. Other aspects concerning data compromise in I4.0 could lead to industrial espionage or industrial sabotage, where manufacturing defects are introduced, causing mechanical failures and catastrophic consequences (Prinsloo, 2019). A summary of the prior research regarding Industry 4.0 risks is listed in Table 6.

Table 6

Literature Summary of Industry 4.0 Risks

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Avdibasic et al., 2022	Cybersecurity trends, threats, and challenges toward I4.0	Literature review	70 articles	Challenges and responses	Identified cyber threats to I4.0 and offered viable solutions

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Barbosa et al., 2021	Cyber threats the industrial sector faces due to the growth of I4.0 and the number of connected devices	Qualitative approach in the evaluation of risk analysis methodology	Industrial plant	Assets, vulnerabilities, and cybersecurity controls	Validated and improved the risk analysis methodology as adapted to the industry sector and I4.0
Matsuda et al., 2021	I4.0 technologies introduced cyber risks to ICS with a lack of cybersecurity considerations	Conceptual paper	None	Attack scenarios	Proved examples of cyber risks associated with specific technology of I4.0, such as AI, IoT, and cloud through penetration testing
Müller & Voigt, 2018	Dimensions of sustainable industrial value creation had not been studied collectively or comparatively	Empirical study	329 Small and Medium Enterprises	Questionnaire	The concept of sustainability is quantitatively assessed in the context of IIoT for SMEs in Germany and China
Naanani, 2021	Reliance on computer networks for I4.0 in factory environments is vulnerable to attacks	Literature review	None	Cyber-attacks and solutions	In addition to technical solutions to protect against cyber-attacks, employees' naivety or neglect should

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
					be addressed with awareness to avoid impact on continuity of production
Pilloni, 2018	The use of technologies related to IIoT and CPS enhances industrial processes	Exploratory research	None	Application domains in I4.0	Presented the technologies to enable I4.0; specifically, crowdsourcing and crowdsensing are beneficial toward I4.0
Prinsloo, 2019	Cybersecurity concerns for I4.0 in manufacturing could have profound consequences	Exploratory research	None	Attacks, cybersecurity problems, and solutions	Highlighted cyber-attacks in the I4.0 environment to create awareness concerning cybersecurity risks that could impact adoption and proposed a few counter measure solutions
Soltovski et al., 2019	Limited support for a sustainability approach to I4.0 to address conceptual	Literature review	66 articles	Risk dimensions	Devised a theoretical framework of relationships among dimensions of social risks,

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	negative impacts				technological risks, environmental risks, economic risks, and regulatory

Cyber-Physical Systems Risks

CPSs are observed and controlled across virtual networks within environments that need to be safe, secure, and reliable to sense and manipulate physical processes in real-time (Monostori et al., 2016). The complexity of CPS has created an environment vulnerable to cyber, physical, and hybrid attacks (Yaacoub et al., 2020). Canizo et al. (2019) asserted to avoid production impacts and financial losses, the operation of CPS devices and networks in industrial environments must be uninterrupted. Zografopoulos et al. (2021) alleged the exploitation of CPS has increased due to vulnerabilities caused by the combined use of off-the-shelf commercial hardware components, software packages, and communication devices.

Yaacoub et al. (2020) suggested several CPS cybersecurity risks are related to big data, IoT storage, and operating system vulnerabilities. Like IoT, CPS components are often without cybersecurity services, leaving large-scale complex environments of Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), and Intelligent Electronic Devices (IEDs) vulnerable to attacks (Zografopoulos et al., 2021). Jbair et al.

(2022) indicated that CPS could be compromised by common attacks, such as DoS, Man-in-the-Middle (MITM), replay attacks, ransomware attacks, and zero-day attacks. Gupta et al. (2020) stated, “the CPS threats and risks go well beyond traditional cybersecurity risks” (p. 47327). For example, Jbair et al. (2022) portrayed a threat actor who gained network access with lateral movement to launch a CPS firmware attack, enumerated network connections, intercepted network traffic, and changed program states.

Other contributing factors to CPS vulnerabilities are poor system requirements, software errors, and system misconfigurations due to CPS implementations adapting to an ever-changing threat landscape (Yeboah-Ofori et al., 2019). Alguliyev et al. (2018) expressed concern for CPS cybersecurity, specifically for ensuring the trust of data from sensors, the control of dynamic permissions required of actuators, the protection of stored data, and the integrity of communication methods and routing. Yeboah-Ofori et al. (2019) noted the integrated nature of CPS, when exploited, will cause significant disruptions and considerable damage to organizations. As such, the Stuxnet computer worm is a historical example of an attack on industrial infrastructures, which was designed to cause significant damage by changing the operations of ICS through the modification of PLC code (Collins & McCombie, 2012; Karnouskos, 2011).

CPS cybersecurity challenges center around two key aspects: preventing retrieval of physical system information and limiting the modification of physical system functions (Alguliyev et al., 2018). In this vein, Yeboah-Ofori et al. (2019) reiterated risks and impacts on CPS operations, including attacker control of equipment, falsified measurements, affected data integrity, and disrupted operations. Simply put, based on the

CPS risks identified in manufacturing, attacks are categorized as technical data theft, system and data alteration, as well as impairment of system communication, processes, and performance (NDIA, 2014; Vincent et al., 2015). A summary of the prior research regarding CPS risks is listed in Table 7.

Table 7

Literature Summary of Cyber-Physical Systems Risks

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Alguliyev et al., 2018	Rapid growth of CPS presents a complex situation leading to problems with cybersecurity and information confidentiality	Literature review and exploratory research	None	Operational and philosophical aspects of CPS	Provided an approach to cyber-attack consequences estimation, modeling of CPS attacks, CPS attacks detection, and CPS cybersecurity architecture
Collins & McCombie, 2012	Significant threats to critical infrastructure due to Internet connectivity of legacy systems (e.g., SCADA, PLC, ICS)	Exploratory research	None	Malware	Awareness of sophisticated malware causing serious implications for the cybersecurity of critical infrastructure worldwide

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Gupta et al., 2020	Traditional cybersecurity methods are inadequate to address new attack vectors of additive manufacturing SC	Conceptual paper	Three novel supply chain models	Attack and risk classifications	Classification of threats into categories for AM SC based on the level of interaction of the attacker, skill implementing the attack, and defending against the attack
Jbair et al., 2022	Cyber-attacks on CPS pose severe business risks to smart manufacturing	Conceptual paper	None	Asset classification and digital twin tool	Framework and tool to generate software code and configurations to be deployed as countermeasures for CPS assets
Karnouskos, 2011	Risks to future SCADA systems are increasing rapidly	Conceptual paper	None	-	The capability of Stuxnet can be modified as a tool for advanced persistent threats tailored for other systems and platforms (e.g., automobile and power plants) as well as modern

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
					distributed SCADA and PLC
Monostori et al., 2016	Further investigation into the research and development, economic, and socio-ethical challenges faced by CPS are needed to realize the expectations in manufacturing systems	Exploratory research	10 Case Studies	-	CPS is considered extremely important for the development of future manufacturing systems
NDIA, 2014	Need for the DIB to protect unclassified technical information to avoid damage to national cybersecurity	Literature review and interviews	None	Gaps, solutions, best practices, and actions	Manufacturing companies are targets, the factory floor is not secure to safeguard technical information, and manufacturers are not well equipped to manage risks
Vincent et al., 2015	Quality control system weaknesses to detect real-time attacks increase	Exploratory research	None	CPS manufacturing systems vulnerabilities	Demonstrated the need for cybersecurity in the product/process design stage

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	manufacturing security and safety concerns that could alter systems and products				and adapted the method to detect Trojans in integrated circuits and methods to detect change in manufactured part's behavior without disrupting the flow
Yaacoub et al., 2020	Large-scale heterogeneous deployments of CPS are susceptible to cyber threats and attacks, resulting in catastrophic effects	Exploratory research and qualitative risk assessment	None	CPS vulnerabilities, threats, attacks and failures	Security services can be applied to CPS without impacting performance and quality of service to ensure the resilience of the systems
Zografopoulos et al., 2021	Compromise of mission-critical Cyber-Physical Energy Systems (CPES) could lead to disastrous consequences	Literature review and exploratory research	Four cyber-attack scenarios	Threat modeling	Framework is provided to characterize CPS and establish the threat model, attack setup, and risk assessment for various scenarios and other industry sectors

Data Breaches

Data Breaches Defined

A data breach is an unauthorized access to confidential or sensitive information, such as personal information, Personal Health Information (PHI), Personally Identifiable Information (PII), intellectual property or trade secrets, and financial data, which has been “copied, transmitted, viewed, stolen, or used by an unauthorized individual” (Khan et al., 2021, p. 1). Goode et al. (2017) indicated research has described data breaches as breaches of cybersecurity, information, and privacy while also considering intentional or accidental service failures related to electronic activities of an organization with customers, trading partners, or internal systems. Additionally, Goode et al. (2017) suggested scientific literature referred to a data breach specifically when there is a violation of confidentiality.

Schlackl et al. (2022) indicated a data breach is when data has suffered from an incident affecting confidentiality, availability, or integrity. More recently, Levy and Gafni (2023) referenced the McCumber Cube, which identified a data breach as a compromise to the confidentiality and/or integrity of information during the various stages of processing, storage, and transmission. Moreover, Privacy Rights Clearinghouse (PRC) described data breaches by type, such as information disclosed unintentionally, information compromised by hacking or malware, credit or debit card fraud, insider access to data, lost or stolen portable device (e.g., laptop or smartphone), or lost or stolen stationary device (e.g., desktop computer or server) (Holtfreter & Harrington, 2015).

Every industry has experienced a data breach, including healthcare, hospitality, education, financial, government/military, manufacturing, retail, non-profit, and others (Holtfreter & Harrington, 2015; Khan et al., 2021). Goode et al. (2017) expressed concern regarding the growth and magnitude of data breaches caused by the increased reliance on confidential information shared between organizations. To the extent an organization is breached, they do not know the content of the breached data until after the incident has been detected and investigated. Schlackl et al. (2022) stated, “among cyber threats, data breaches are rated as the most important issue for security managers” (p. 1).

Data Breach Causes, Impacts, and Consequences

Schlackl et al. (2022) outlined human factors, management factors, technology factors, and organizational size as contributors to data breaches. Although there are many circumstances for data breaches, Caston et al. (2021) claimed about 50% of the root causes of data breaches are human error. Of these incidents, roughly 35% are attributed to an individual. Information security policies are described as antecedents to data breaches; however, when violated, such as unnecessarily clicking a link in a phishing email or traveling with sensitive information, will increase the risk of data breaches (Schlackl et al., 2022). Likewise, Srinivas and Liang (2022) conveyed that the information available from social media contributed to data breaches as attackers gained authorized access from insiders by using impersonation and social engineering. Furthermore, business decisions concerning partner relationships and integrations, such as mergers and acquisitions, increase the risk of data breaches by sharing confidential information or creating complex IT cybersecurity environments (Schlackl et al., 2022). McLeod and Dolezel (2018), as

well as Tanriverdi et al. (2020), agreed that while the size of an organization directly influences the use and number of digital technologies and IT equipment, the diverse and heterogeneous nature of technology plays a more significant role in leading to more data breaches.

President Joe Biden signed an executive order on May 12, 2021, after a series of cyber-attacks, particularly the one on Colonial Pipeline, impacting gas delivery nationwide. Schlackl et al. (2022) and Srinivas and Liang (2022) asserted that data breaches have become increasingly common and normal as businesses have become more digital and connected to the Internet. A PRC report for Q4 2020 quantified the average ransomware payout as \$233,000, indicating more than three hundred million individuals had been affected by a data breach (Srinivas & Liang, 2022), while the average data breach cost increased over 140% between 2008 and 2022 to \$8.64 million (Schlackl et al., 2022). Brandao and Rezende (2020) indicated that regulations and laws have been established to ensure compliance with the use and protection of personal data, which holds parties accountable for preventing significant financial impacts on customers and businesses. In their study, Srinivas and Liang (2022) chose to use the “number of records” breached as a measure of severity, equating to the number of people impacted. A summary of data breach consequences and referenced study are listed in Table 8.

Table 8*Literature Summary of Data Breach Consequences*

Categories	Consequences	Study
Operational	Business disruption and productivity decreases	Gallagher et al., 2016; Martin et al., 2014
	Increased media scrutiny	Agrafiotis et al., 2018
	Loss of business opportunity	Algarni & Malaiya, 2016
	Customer churn	Choong et al., 2017; Tanimura & Wehrly, 2009
Workforce	Decrease of staff morale and retention	Agrafiotis et al., 2018; Gallagher et al., 2016; Wang et al., 2019
	Dismissal of leadership and management	Say & Vasudeva, 2020; Banker & Feng, 2019
Legal	Face fines if victims are not notified in the required timeframe	Agrafiotis et al., 2018; Song et al., 2017; Tanimura & Wehrly, 2009
	Class-action or liability lawsuits for damages	Algarni & Malaiya, 2016; Hovav & Gray, 2014; Kolevski et al., 2021
Financial	Reduced sales growth	Kamiya et al., 2021; Wang et al., 2019;
	Company's stock market value	Campbell et al., 2003; Richardson et al., 2019; Spanos and & Angelis, 2016
	Cost of identity protection services	Meisner, 2017; Tanimura & Wehrly, 2009; Wang et al., 2019;
	Inability to access capital possibly leading to bankruptcy	Dinger & Wade, 2019

Categories	Consequences	Study
For Customers	Feeling violated	Choi et al., 2016
	Worry about time, financial, and material losses	Karwatzki et al., 2017
	Decrease their trust and perception about reliability and credibility	Afroz et al., 2013; Berezina et al., 2012; Hovav & Gray, 2014; Muzatko & Bansal, 2020
	Social media complaints	Ivaturi & Bhagwatwar, 2020; Syed, 2019
	Reduced purchases at retailers	Janakiraman et al., 2018
	Fraudulent credit card charges and identity theft	Agrafiotis et al., 2018; Hovav & Gray, 2014;
For Competitors	Effects entire industry	Kamiya et al., 2021; Kashmiri et al., 2017
	If seen as entire industry, the stock market impact	Haislip et al., 2019; Martin et al., 2017; Zafar et al., 2012
	If seen as isolated, a positive stock market impact	Martin et al., 2017
	Possible customer switch from breached firm to competitor	Choong et al., 2016
For Supply Chain Partners	Partner is perceived to have risk	Choong et al., 2016; Choong et al., 2017; Gwebu et al., 2014
	Decrease in sales demand	Hovav & Gray, 2014
	Investments may decline and the chance of partner relationship termination increases	He et al., 2020

Categories	Consequences	Study
Other Entities	For credit card breaches, re-issuance costs for merchants, banks, credit card issuers	Hovav & Gray, 2014
	Cyber insurance providers may have to cover costs	Khan et al., 2021; Romanosky, 2016
	Increase in auditor expenditures, causing an increase in audit fees	Haislip et al., 2019, He et al., 2020
	Positive cumulative abnormal return for security vendors	Cavusoglu et al., 2004; Garg et al., 2003

Note. Data breach consequences adapted from Schlackl et al. (2022, p. 6-7).

Data Breach Incidents

The 2022 Verizon Data Breach Investigations Report (DBIR) indicated of the 23,896 total cybersecurity incidents reported in 2021, roughly 22% (5,212) were data breaches. Additionally, the report highlighted significant breaches that occurred throughout the year, which included a compromised processing chemical at a freshwater plant in Florida, a ransomware attack on Colonial Pipeline that caused a 6-day closure and \$5 million ransom payment, a ransomware attack on Kaseya's Virtual Systems Administrator (VSA) caused millions of endpoints to be encrypted, a PII data breach of 40 million T-Mobile customers, and a data breach of seven million customers of Robinhood Markets (Verizon DBIR, 2022). Furthermore, the Identity Threat Resource Center (ITRC) has tracked and provided information based on publicly reported data breaches in the U.S. for the past 17 years, which has accumulated information on more than 15 thousand data compromises, more than 11 billion victims, and more than 19 billion exposed records. The ITRC 2022 Data Breach Report reported over 1,800 compromises, of which 1,774 (roughly 98.5%)

were data breaches, 18 were data exposures, and 10 were unknown compromises. There were more than 422 million total victims, and 40% more supply chain attacks than malware attacks based on 1,700 entities targeted (ITRC, 2022). For the first quarter of 2023, ITRC reported 445 total compromises, of which 436 (roughly 98%) were data breaches, seven were data exposures, and two were unknown compromises. There were more than 89 million victims, with approximately 87% of the data breaches related to cyber-attacks and 13% by system and human errors (ITRC, 2023).

Reviewing prior research studies, known data breaches are analyzed to identify steps conducted by threat actors, highlight contributing deficiencies or issues, and recommend countermeasures that could have prevented the compromises. For instance, a case study by Radichel (2014) focused on Target Corporation's data breach of 40 million credit cards in 2013, which started with the compromise of a Heating, Ventilation, and Air Conditioning (HVAC) provider and had characteristics of reconnaissance, use of malware, exploitation of vulnerabilities, access through a supplier portal, lateral movement in the environment, and lack of response by Target Corporation. Likewise, studies by Hassija et al. (2020), Keskin et al. (2021), and Shu et al. (2017) also conveyed Target's data compromise as a significant example of a smaller third party with lesser cybersecurity and technology misuse. Furthermore, many studies have documented and described Target's data breach, such that an argument could be made about the difficulty in understanding how the incident went undetected (Caston et al., 2021).

Caston et al. (2021) asserted the most dangerous consequence of a breach is the exposure of data to the public, and in the case of Target, stated "the attack should not

have happened for a variety of reasons” (p. 3). Shu et al. (2017) claimed the Target data breach demonstrated the cybersecurity challenges of credit cards and personal information. They attributed the compromise to the extensive connected systems required for a large retailer. Conversely, research has indicated that while Target invested in sophisticated software to detect intrusions, the support processes were inadequately defined, and staff were insufficiently trained (Radichel, 2014). Moreover, Target had not conducted oversight or regularly audited their vendors and did not appropriately control access for third-party providers (Brandao & Rezende, 2020; Caston et al., 2021). Radichel (2014) contended there is a need to consider all assets within an environment instead of solely following compliance guidelines such as Payment Card Industry (PCI) compliance, as Target had followed, but it was not suitable to avoid massive data loss.

Shu et al. (2017) noted before the Target data breach, the most significant breach was TJX in 2007, which consisted of 45.6 million credit card numbers and Personal Identification Numbers (PINs), which was conducted by the same threat actor using the same methods to previously breach BJ’s Wholesale Club, Boston Market, Barnes & Noble, Sports Authority, Forever 21, DSW and OfficeMax. Other retail and consumer-related breach examples include Home Depot, which suffered 56 million credit and debit card information stolen in 2014 (Hoehle et al., 2021; Shu et al., 2017), and Sony PlayStation Network, which experienced a hack of 77 million customers’ personal and financial information in 2011 respectively (Goode et al., 2017; Hoehle et al., 2021). Within the financial industry, examples include Capital One, with a data breach of bank account numbers and social security numbers from 100 million U.S. citizens and six

million Canadians (Caston et al., 2021), as well as over 145 million customers impacted by sensitive information stolen from Equifax in 2017, which consequently carried breach-related costs of roughly \$90 million (Khan et al., 2021; Srinivas & Liang, 2022) and lastly in 2014, J.P. Morgan Chase experienced a compromise of accounts for 76 million households and seven million small businesses (Brandao & Rezende, 2020). In a review of the manufacturing industry, several high-profile and well-known companies have experienced data breaches, as shown in Table 9.

Table 9

Literature Summary of Manufacturing Company Breaches

Company	Type of Manufacturer	Exposure / Loss / Impact	How Compromised
LC Industries	Tactical products for the Military	3,700 customer records	Malicious code to gather personal information
FA-CC	Airplane components	Estimated loss of \$61 million	CEO impersonation attack via an email exchange
Hanes Brands	Clothing	Over 900,000 customer phone numbers	Guest account on a public website
JBS	Meatpacking	\$11 million in ransom and 5-day plant closure	Remote hijack and ransomware attack
Boeing	Airplanes	Information on 36,000 Boeing employees	Email sent outside of the corporate network to spouse
Dupont	Scientific research and products	20,000 - 40,000 sensitive files	Employee downloaded before leaving for a competitor

Company	Type of Manufacturer	Exposure / Loss / Impact	How Compromised
		(\$400 million in value of Intellectual Property accessed)	
Norsk Hydro	Aluminum	\$75 million and impacted three other companies	Ransomware attack
Royal Dutch Shell	Oil and gas	176,000 records of employee sensitive information	Emailed externally by a disgruntled employee
Apple	Technology	Sensitive information for 225,000 iPhone users	Compromise of jailbroken iPhones by malware with unauthorized purchases and ransom
Mondelez	Food and beverage	Permanent damage to 1,700 servers and 24,000 laptops, \$100 million in costs	Encrypting malware attack

Note. Notable manufacturing data breaches adapted from Arctic Wolf (2023) and de Groot (2020).

Morgan (2021) predicted the cost of damages from cybercrime would grow from \$3 trillion in 2015 to \$10.5 trillion globally in 2025 due to expanding attack surfaces and increased hacking activities by aggressive nation-states and gangs. The compounding rate of 15% year over year is exemplified by Farrelly (2023), who profiled the most recent data breaches of 2023, which include Norton Life Lock (January), MailChimp (January), Google Fi (February), Activision (February), Chik-Fil-A (March), ChatGPT (March), Yum Brands (April), and T-Mobile (January and May). A summary of the prior research regarding data breaches is listed in Table 10.

Table 10*Literature Summary of Data Breaches*

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Brandao & Rezende, 2020	Data breach growth continues as total costs associated rise along with the global cybersecurity market	Exploratory research	None	Data breach threats and consequences	Specified approaches to cybersecurity, including Zero Trust Security (ZTS) and Artificial Intelligence (AI), however, emphasized user security awareness training and the need for a combination of correctly implemented and maintained technologies
Caston et al., 2021	Corporations fail to take the necessary steps to defend and protect the data they collect	Exploratory research	None	Cyber-attacks	Human error is significantly responsible for data breaches
Goode et al., 2017	Companies face the loss of customers after a data breach occurs	Field study	144 customers	Two-stage longitudinal online survey (Mechanical Turk)	After a data breach, customer compensation has a positive effect on perceived

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
					service quality, continuance intention, and repurchase intention
Hoehle et al., 2021	Successful replication of a study in a new context allows for generalization	Replication study	901 participants	Two-stage longitudinal online survey	After a data breach, compensation is suitable to restore sentiment, compensation is driven by customer expectations, and demographic or geographic characteristics do not impact customer response to compensation
Holtfreter & Harrington, 2015	The number of data breaches and trends not improving	Classification research	2,280 data breaches	Data breach categories	Provided data breach model to create workable strategies to improve data protection and reduce identity theft. Over six years, the trend has increased, however not consistently

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Khan et al., 2021	Theorized organizations can manage data breach incidents based on risk item profiles and resolution methods	Literature review	103 articles	Data breach cause, locus, impact, prevention, containment, and recovery	Risk model for data breach management, specifically for data breach risks, resolutions, and heuristics
McLeod & Dolezel, 2018	Healthcare data breaches impact patient data, resulting in significant costs, litigation, and penalties	Literature review and quantitative research	6600 healthcare facilities	Organizational factors, level of exposure, and level of security	Quantity and quality of users, size, and complexity of organizations, sophistication, and interconnectedness mean more vulnerabilities and greater risks
Schlackl et al., 2022	A wide breadth of literature on data breaches across various disciplines leaves practitioners/researchers with an incomplete understanding	Literature review and quantitative research	122 articles	Categories for data breach antecedents and consequences	Reviewed and structured literature on data breach antecedents and consequences ; confirmed a relationship between policy compliance and data breach

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
					occurrences and that antecedents can be used to uncover root causes of data breaches
Tanriverdi et al., 2020	In the context of multi-hospital systems (MHS), theorized organizational complexity, IT complexity, and enterprise standardization of cybersecurity solutions affect data breaches of the MHS	Empirical research	446 MHS, 3,823 MHS-yearly observations (2009 – 2017), and 491 data breaches	Data breach types, control weakness types, organizational complexity, IT complexity, and standard cybersecurity solutions	Organizational complexity and IT complexity in MHS lead to weaknesses in technical, process, and people controls, which increase data breaches. However, enterprise-wide standard cybersecurity solutions improve controls and reduce data breaches

Targeting the Manufacturing Industry

Companies in the manufacturing industry are attractive targets for 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.

Deloitte (n.d.) claimed the manufacturing industry is targeted for financial gain and intellectual property theft and is highly vulnerable because of a fragmented approach to managing cyber-related risks. According to X-Force (IBM, 2023), manufacturing was the most targeted industry in 2021 and 2022 for extortion and data theft due to spear phishing, as well as the exploitation of public applications. However, in a broader sense, Brandao (2019) stated, “the aggressor's motivations cover a wide range, including intellectual property robbery as well as of trade secrets, sabotage of processes, extortion and malicious damage to networks and information systems” (p. 33). As motivations differ, the type of attackers varies from nation-states to hobbyist hackers to organized crime, as well as those inside the company with malicious intent to introduce vulnerabilities or damage, steal, or change the flow of information (Corallo et al., 2021).

Elhabashy et al. (2020) and Masum (2023) suggested manufacturers are prime targets because of the transition toward I4.0 technologies for automation and information exchange, which has increased complexities, vulnerabilities, and cybersecurity challenges that traditional IT cybersecurity is insufficient to protect. For instance, Makhdoom et al. (2018) predicted a sizable number of enterprises worldwide would deploy IoT devices by 2020 with a substantial lack of confidence in cybersecurity, which would lead to almost a quarter of corporate attacks originating from IoT devices. Sailio et al. (2020) contended collaboration, network connectivity, business intelligence (e.g., machine learning), and flexible automation from I4.0 technologies and the premise of the “factory of the future” (p. 2) had created new opportunities for threat actors. Moreover, the combination of weak cybersecurity for industrial networks, highly specialized equipment requiring constant

Internet to cloud resources, and an expanded attack surface using partners to manage the infrastructure has created a highly attractive environment to threat actors (Sailio et al., 2020). Pandey et al. (2020) 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 must protect a wide array of technologies, while attackers only need to focus on the weakest link.

In particular, Corallo et al. (2021) noted ICS is considered the most critical asset in terms of cybersecurity in an industrial environment. Ani et al. (2017) provided further insight into the attractiveness of the manufacturing industry based on the combination of ICS and a human element. This understanding highlighted the lack of skills and technical preparedness to manage and defend against cyber-attacks. The unawareness of ICS risks and the contention between IT and industrial experts contributed to a lack of trust and understanding. In contrast, Hemsley and Fisher (2018) stated, “the skill level of sophisticated threat actors is increasing, as are the frequency of attacks targeting critical infrastructures and the systems that control them. Many threat actors targeting ICSs have advanced skills and knowledge” (p. 25).

Ani et al. (2017) expressed that the wide range of vulnerabilities in ICS has made manufacturing systems and the associated networks attractive targets for cyber-attacks. Attackers know ICS vulnerabilities tend to be older, have less-supported software, and extend well beyond the physical lifespan of traditional IT equipment (IBM, 2023). Yaacoub et al. (2020) suggested the lack of physical security for ICS is also a vulnerability, which could lead to physical tampering, alteration, modification, sabotage,

or destruction. While vulnerabilities are not intentional, those that are not fixed immediately lead to improved ease of attack and raise the interest of cyber actors to target manufacturing companies (Ani et al., 2017). The transformation of ICS from a proprietary isolated system to an open platform with remote access and interconnections between corporate and public networks has exposed significant vulnerabilities (Asghar et al., 2019; Savin, 2021). McLaughlin et al. (2016) found that, by studying ICS vulnerabilities, security was reliant on obscurity. ICS system patches were at least a year behind, and there was a false sense of cybersecurity from deploying firewalls, cryptography, and antivirus software.

Threats to Manufacturing and Impacts

Based on NIST's Risk Management Guide for Information Technology Systems, Wu et al. (2018) declared a threat is "the potential for a particular threat source to successfully exercise a particular vulnerability," and a threat source refers to "any circumstance or event with the potential to cause harm to an IT system" (p. 5). Mullet et al. (2021) clarified a cyber threat as "any circumstance impacting organizational operations, assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information" (p. 23240). Khalid et al. (2020) indicated people or nature are the sources of threats, as people can be internal users or external to an organization with malicious intent to disrupt system operations. Tuptuk and Hailes (2018) found insider attacks are mainly unauthorized access to sensitive or private information that is stolen or, at times, unintentionally exposed. Makhdoom et al. (2018) noted insider attacks are challenging to

prevent with methods designed to protect the perimeter, such as firewalls, Intrusion Prevention Systems (IPS), and Intrusion Detection Systems (IDS). Threats can be unstructured with the use of tools by inexperienced people or structured with the use of scripts or code to exploit known system vulnerabilities (Khalid et al., 2020). Moreover, regardless of whether a threat is malicious or accidental, Barbosa et al. (2021) insisted destruction, modification, or leakage would result in the same.

Another reason manufacturing is one of the most frequently compromised industries is due to I4.0 technologies, including IIoT machines and cloud-based control and sensing systems (Wu et al., 2018). Before the technology convergence in manufacturing, the primary issues of concern were performance, reliability, and safety of production operations (Ani et al., 2017). Makhdoom et al. (2018) composed a set of IoT cybersecurity deficiencies that presented vulnerabilities for threats and exploitation. 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. Flatt et al. (2016) and Mullet et al. (2021) 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. (2018) provided a list of generalized IoT threats, including several specific to the physical, application, and network layers. Masum (2023) identified threats associated with network configurations, informational databases, production

machines accessed by smart devices, and connectivity of cloud resources for distributed manufacturing.

Additionally, manufacturing companies have experienced attacks affecting access, escalated privileges, process controls, Human-Machine Interface (HMI) systems, service delays, and data manipulation (Corallo et al., 2021; Wu et al., 2018). Ani et al. (2017) identified several attack methods resulting from vulnerability scans conducted on a manufacturing system testbed to defend the position where numerous vulnerabilities had become apparent. Due to publicly well-known configuration details, ICSs have experienced insider attacks, external targeted attacks, Advanced Persistent Threats (APTs), and Distributed Denial of Service (DDoS), to name a few (Bhamare et al., 2020; McLaughlin et al., 2016). Bhamare et al. (2020) claimed that the transition of ICS to the cloud and the lack of cybersecurity standards have led to data breach threats, including loss, theft, manipulation, and exploitation. Manufacturing companies have a wealth of information that would be extremely valuable to competitors, which consists of intangible assets, including trademarks, patents, copyrights, trade secrets, and designs, to name a few (Prinsloo et al., 2019).

Makrakis et al. (2021) indicated the goals of threat actors toward industrial environments are to cause loss of view, loss of control, and potential loss of safety. In contrast, Wu et al. (2018) stated, “the most important security goal is protecting confidentiality, integrity, and availability (also known as CIA triad) of data” (p. 4). Several studies identified threats to I4.0 manufacturing and categorized them in the context of CIA. For instance, theft of industrial secrets and cyber espionage are

considered confidentiality attacks intended to compromise the intellectual property of a company, affecting its competitiveness, reputation, and customer trust (Corallo et al., 2021; JBair et al., 2022; Masum, 2023; Wu et al., 2018). Sabotage on critical infrastructure or equipment was identified as integrity attacks leading to altered information, designs, or configurations causing degradation of performance and product quality (Corallo et al., 2021; JBair et al., 2022; Masum, 2023; Wu et al., 2018). DoS attacks are an example of availability attacks, which affect production machines, slow down processes, or cause production downtime (Corallo et al., 2021; JBair et al., 2022; Masum, 2023; Wu et al., 2018).

While cyber-attacks on manufacturing systems could result in stopped production, altered production, physical damage, or injury to workers, Corallo et al. (2021) 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. (2020) stressed that the high costs of cybersecurity breaches to industrial systems translate into lost revenues and financial and environmental impacts. Ani et al. (2017) 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 an attack on manufacturing and supply chains could significantly harm entire industries and, on a

greater scale, human life, relying heavily on products to meet essential needs (Ani et al., 2017). A summary of the prior research regarding the manufacturing industry is listed in Table 11.

Table 11

Literature Summary of the Manufacturing Industry

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Asghar et al., 2019	Rising number of cyber-attacks on ICS systems	Literature review	None	Solution categories	No single risk assessment can be applied to any environment
Bhamare et al., 2020	ICS exposure to cyber-attacks leads to significant physical damage and danger to human lives	Literature review / case study analysis	Four case studies	Cybersecurity approach for ISC/SCADA	Confirmed need for ICS security test bed to study attack effects
Brandao, 2019	Cybersecurity challenges for I4.0	Conceptual paper	None	Cybersecurity risks and cyber-attacks	Commonly used cyber-attacks and methods for defense
Corallo et al., 2021	Lack of understanding of impacts on networked manufacturing systems (machines and	Theoretical study (impact assessment method)	Sole case study	Confidentiality, integrity, and availability (CIA triad)	Identified and assessed business impacts using the impact assessment methodology

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	3-D printers) by cyber-attacks				
Elhabashy et al., 2020	Lack of understanding where Quality Control (QC) tools can be exploited	Empirical study	Various (attack samples)	Exploitation classes	Categorization of QC vulnerabilities, negative effects of exploiting QC tools, and identified guidelines for cyber-physical security
Hemsley & Fisher, 2018	ICS are lesser known, unique to OT, and differ from IT	Literature review	23 cyber incidents	ICS threat types, vulnerabilities, and incidents	Enhanced awareness that nation-states are actively developing capabilities to attack critical infrastructure, threat actors perform reconnaissance, and it is importance to detect and recover from an attack
JBair et al., 2022	Increasing trend of reported cyber-attacks targeting industrial systems	Developmental research	None	Characterization, taxonomies, methodologies, models, and security	Proposed a structured end-to-end threat modeling approach and simulation of

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
				counter measures	ICPS to include cybersecurity
Makhdoom et al., 2018	Lack of an overall understanding of IoT cybersecurity	Literature review	None	Threats, exploited vulnerabilities, and cybersecurity measures	Developed an attack methodology for most common attacks, a specific strategy for DDoS, and assessed lessons and pitfalls
Makrakis et al., 2021	Lack of cybersecurity knowledge concerning ICS leading to economic, privacy, and safety loss	Literature review	None	Cybersecurity incidents, attacker methods, vulnerabilities, outcomes, mitigation strategies	Identified common factors and vulnerabilities for key incidents and offered mitigation measures for prevention
Masum, 2023	Challenges in the detection of cyber-attacks in smart manufacturing (context of data-over-net)	Literature review	None	Confidentiality, Integrity, and Availability (CIA); and dimensions for design, production, and operations	Maintain secure operations by adhering to CIA
McLaughlin et al., 2016	The rate of attacks on ICS is substantial	Literature review	None	Vulnerability assessments	Demonstrated all levels of the ICS

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	for both governments and industries			and attacks on ICS	architecture can be targeted by cyber-attacks and disturb the control processes
Sailio et al., 2020	Lack of standard definitions of Cyber Threat Actors (CTAs) and associated cybersecurity challenges in Factory of the Future (FoF)	Literature review	22 cyber security expert organizations	Aspects of FoF	Nation-state actors were highly identified as CTA, while cybercrime had high incidents but was not classified as CTA. Competitors and partners ranked extremely low
Savin, 2021	Cyber vulnerabilities associated with new ICS capabilities	Literature review / analysis	None	ICS targeted components and vulnerabilities	Identified key elements needing protection, and encouraged ICS administrators to take continuous security measures
Wu et al., 2018	Financial impacts	Literature review	None	Threats, vulnerabilities,	Presented challenges to

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	associated with cyber-attacks on the manufacturing sector			control methods, and risks	manufacturers to address retrofitted equipment and detect/prevent embedded defects

Cybersecurity Frameworks

The term “cybersecurity framework” has been described as a collection of many components or domains that are considered guidelines for organizations to adopt and adapt to address cyber threats and mitigate cybersecurity issues. Gourisetti et al. (2021) contended that Cybersecurity Frameworks (CSFs) were initially created to identify cybersecurity vulnerabilities in critical infrastructure. In contrast, evidence in the literature has shown further development and use of CSFs by government agencies, international organizations, academic institutions, and corporations. Schiliro (2023) purported there is no universal approach, and thus, companies will adopt CSFs differently depending on their strengths and weaknesses in addressing threats and risks. Syafrizal et al. (2020) asserted that CSFs are flexible, while Taherdoost (2022) expounded further by suggesting organizations have the freedom to undertake some or all of the CSF’s methods or practices. Furthermore, Taherdoost (2022) claimed that CSFs are effective against cyber threats because they are based on cybersecurity standards, implementations, and best practices.

A cybersecurity standard differs from a CSF in that there is an expected set of steps or methods defined by the standard to be performed. Nevertheless, the successful implementation of a cybersecurity standard depends on a CSF to align the organization's business, technology, and policies to mitigate cybersecurity issues and address cyber risks (Taherdoost, 2022). An example of a CSF intended to improve an organization's cybersecurity posture is NIST's Cybersecurity Framework, a set of best practices, standards, and recommendations. The distinguishing factor of NIST's CSF is how the framework is organized and categorized by a list of terms: *Identify, Protect, Detect, Respond, and Recover*. Syafrizal et al. (2020) highlighted components such as access control, incident management, and governance, to name a few, which were found to be shared between cybersecurity standards and frameworks.

Strohmier et al. (2022) conducted a study with an open-ended questionnaire to understand which CSFs or cybersecurity standards organizations had adopted, which revealed a wide variety of CSFs and standards had been in use. The frameworks and standards confirmed by the participants included NIST Risk Management Framework (RMF), ISO 27001, NIST 800-171, Capability Maturity Model Integration (CMMI), Payment Card Industry Data Security Standard (PCI DSS), Federal Risk and Authorization Management Program (FedRAMP), Health Insurance Portability and Accountability Act (HIPAA) provisions, Health Information Technology for Economic and Clinical Health (HITECH), and CMMC. Contrary to known CSFs and standards, a study conducted by Schiliro (2023) devised a new framework called the Cybersecurity Resilience and Law Enforcement Collaboration (CyRLEC) Framework, which

emphasized the importance of a strong relationship with law enforcement and aspects to strengthen cybersecurity through the cooperation among entities sharing threat information, response coordination, and training. Additionally, Strohmer et al. (2022) contended that researchers have attempted to align cybersecurity maturity models with analytic models, such that inputting a quantitative framework with associated quantitative analytics could potentially lead to the development of cyber risk mitigation approaches. Along these lines, Levy and Gafni (2022) focused on CFI as a method of self-assessment based on the CMMC framework for quantification, leading to recognizing and mitigating cybersecurity threats from the supply chain or interconnected entities.

Cybersecurity Maturity Model Certification (CMMC)

The U.S. DoD established the first version of CMMC in 2019 to replace the Defense Federal Acquisition Regulation Supplement (DFARS) with the addition of a certification requirement for defense contractors and sub-contractors to manage information in their possession based on a set of cybersecurity practices, standards, and processes (Levy & Gafni, 2022, 2023; Peters, 2020; Syafrizal et al., 2020). Peters (2020) confirmed the CMMC framework was built upon NIST requirements to provide a “unified cybersecurity standard” for defense acquisitions (p. 5). The structure of the CMMC 1.0 was based on five levels. Each level built upon the former, establishing a maturity level with the intent to measure maturity progression with increasing tiers of cybersecurity requirements, practices, and methods (Peters, 2020; Stokes & Childress, 2020). By the end of 2021, CMMC 1.0 had been revised and updated to CMMC 2.0, which reduced the levels from five to three (Level 1 – Foundational, Level 2 – Advanced, and Level 3 –

Expert), comprised of 14 domains from NIST and three additional domains for a total of 17, while Level 1 remained the same with six of the domains and 17 practices. DoD (2021) claimed the changes from CMMC 1.0 to CMMC 2.0 simplify and clarify requirements, minimize barriers to compliance, and increase the ease of implementation.

CMMC 2.0 Level 1

Strohmier et al. (2022) stated, “many attacks can be prevented by companies adopting CMMC 1.0 Level 1 (basic cyber hygiene) which is also the same in CMMC 2.0” (p. 25). Stokes and Childress (2020) disclosed in simple terms, the requirements of Level 1 are “basic cyber hygiene” practices, such as changing passwords or having anti-virus software to protect information. Gardner (2021) documented the practices and processes for the 17 CMMC domains using brief and straightforward explanations to improve the interpretation and understanding of the framework. This is shown in Table 12 for the practices of Access Control in CMMC 2.0 Level 1.

Table 12

Example of Access Control Domain

Level 1 – Access Control (AC) Practices		
Practice ID	CMMC Description	Gardner’s Description
AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Manage permissions to get on a system or to connect your system to the network.

Level 1 – Access Control (AC) Practices

Practice ID	CMMC Description	Gardner’s Description
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Manage permissions to do specific things, limited by your role in the company.
AC.1.003	Verify and control/limit connections to and use of external information systems.	Demonstrate ways to trust systems that you do not own and cannot control directly.
AC.1.004	Control information posted or processed on publicly accessible information systems.	Make sure you do not accidentally post sensitive information on your websites or social media.

Note. Adapted from Gardner (2021, p. 5).

CMMC 2.0 Level 1 consists of six domains of the 14 total domains for the framework, which is represented by Access Control (AC), Identification and Authentication (IA), Media Protection (MP), Physical Protection (PE), System and Communications Protections (SC), and System and Information Integrity (SI). Levy and Gafni (2022) proposed the quantification of the CFI will be satisfied by utilizing CMMC 2.0 Level 1 domains and associated practices. Subsequently, each of the practices of CMMC 2.0 Level 1 was restated and prefaced with statements such as “number of”, “average number of”, or “volume of” to propose measurable elements for CFI (Levy & Gafni, 2022).

CFI Domains and Elements

The original 17 practices of CMMC 2.0 Level 1 were translated into 26 CFI elements (shown in Appendix A), as several of the practices had been consolidated or expanded based on the literature review of 144 articles conducted by Levy and Gafni (2022). In support of this research, an additional literature review was conducted to understand further the nature of CMMC 2.0 Level 1 domains and practices and their applicability toward the quantification of cyber posture. Starting with the AC domain, the associated practices for Level 1 are concerned with authorized users, authorized devices, and control of access to external systems. Mohamed et al. (2022) distinguished the differences between authorization and access control and asserted access rights are based on specific authorizations to determine who can perform what actions on what devices or systems. Nahar et al. (2021) declared AC is required to mitigate the risks of unauthorized access, regardless of modifications or adjustments based on the organization's structure, technology, and capabilities. Almeahmadi and El-Khatib (2013) stated, "authentication is a main access control method that is based on the recognition of an identity where the legitimate users whose identities have been identified/verified are only those who are granted access to the protected resources" (p. 363). As an example, companies have encountered information cybersecurity incidents originating from employees accessing organizational networks and resources remotely from personal workstations due to a lack of access controls (Khando et al., 2021).

Moreover, both AC and PE domains are affected by the use of personal devices in the workplace, known as Bring Your Own Device (BYOD). The Level 1 practices for the PE

domain are concerned with physical devices, accessibility of devices by non-authorized individuals, and the monitoring of visitors' access to facilities. Bello et al. (2017) studied the use and management of BYOD and found through three distinct case studies a significant lack of cybersecurity controls by organizations and a considerable lack of cybersecurity awareness by employees. While BYOD presents many benefits for business and personal use, Palanisamy et al. (2020) claimed BYOD has increased the organization's cybersecurity perimeter, and thus, the cybersecurity of BYOD is literally in the hands of the employees. If BYODs are not being lost or stolen, leading to data loss or leakage, they are targets of malware attacks and exploitation of vulnerabilities by hackers to gain access to corporate networks. Bada and Nurse (2019) described the comprehensive approach a not-for-profit organization used to assess and improve the cyber posture of companies. However, their efforts turned to employee education to secure BYODs and social media to defend themselves specifically against social engineering and phishing attempts.

As depicted, BYODs extend beyond organizational communication methods, and with the associated risks of social media applications and mobile payment applications, the practices of the SC domain are highlighted by Palanisamy et al. (2020), which is concerned with communication with external systems and the boundaries needed with internal systems, both physically and logically. Furthermore, concerning the PE domain, Diesch et al. (2020) expressed the lack of literature mentioning the physical protection of assets and the importance of countermeasures to limit physical entry and access to buildings, offices, servers, and hardware. Adesemowo (2021) argued a coherent

definition of “IT assets” is required to identify assets [tangible and intangible] for effective risk assessments. Accordingly, the Level 1 practice of MP is concerned with the removal of information before the destruction or re-use of devices. Neigel et al. (2020) advocated for cyber hygiene and considered the protection, handling, and disposal of removable media, as well as the deletion of sensitive or personal information, to be a determinant factor. Similarly, Bada and Nurse (2019) expressed concern for cyber posture and noted an organization’s enhanced awareness of cybersecurity issues improved their adoption and practice of secure disposal of IT assets.

The Level 1 practices for the IA domain are concerned with the authentication and verification of the identities of users, processes, or devices accessing information systems. Still et al. (2017) stated, “it is essential that systems housing valuable data be able to correctly verify users’ identities” (p. 437). Fischer-Hübner et al. (2021) indicated the use of cryptography would achieve identity protection and secure access to devices throughout the value chain. Meanwhile, Lal et al. (2016) stressed the importance of identity authentication for information systems and proposed various methods, including passwords [something you know], smart cards [something you have], and biometrics or digital certificates [something you are] (Almehmadi & El-Khatib, 2013; Zviran & Erlich, 2006). However, Idrus et al. (2013) asserted biometrics is the only method that should be used for the authentication of users; even though enrollment requires more operation, the verification step afterward is much more convenient.

Levy and Gafni (2023) revised the practice for the IA domain to read “number of individuals sharing the same user credentials, and/or devices” (p. 6) as a proposed CFI

element. While passwords are the most common and widely used method of authentication (Zviran & Erlich, 2006), people struggle to remember passwords and tend to use the same password across many different accounts (Wash & Rader, 2021). A study conducted by Song et al. (2019) found credentials (e.g., account and password) sharing in the workplace was considered a normal activity rather than a workaround, having been justified with reasons such as centralized collaboration, convenience (temporary or emergency), cost savings, and trust among co-workers. Lastly, the SI domain is concerned with protecting data from malicious software, using tools for patching systems, and performing scans on information systems and files received from external sources. Integrity is an aspect of quality, and in the case of information use, cybersecurity experts have conveyed integrity as a significant determinant, as any alteration can compromise the physical well-being of humans as a worst case (Harley & Cooper, 2021). Ahmad et al. (2021) discussed various controls, including formal, informal, technological (e.g., firewalls, intrusion detection systems, anti-virus software, layers of encryption), physical, and administrative to protect the integrity of sensitive information, such as customer data, intellectual property, and trade secrets. Fischer-Hübner et al. (2021) stressed cybersecurity services should be implemented by default to ensure the confidentiality, integrity, and availability of products and services, mainly through safe connections of devices in the value chain. A summary of the prior research regarding the cybersecurity framework is listed in Table 13.

Table 13*Literature Summary of Cybersecurity Framework*

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Adesemo wo, 2021	Continued cybersecurity breaches due to a lack of understanding and definition of IT assets	Exploratory scoping, internet-based research, interviews, and logical reasoning and argumentation	30 interviewees	Survey	Improve risk assessments with the conceptual definition of IT/digital assets toward a uniform process of asset identification
Ahmad et al., 2021	Lack of understanding of how organizations practice situational awareness in incident response	Qualitative research	Sole case study	Semi-structured interviews	Provided an incident response process model to practice situational awareness of the cyber-threat landscape
Almehma di & El-Khatib, 2013	The functionality of an access control system is limited if only relying on the identity correlating to the possible means of access	Conceptual paper	None	Authorized and unauthorized user, emotion detection, and decision-making	Confirmed the used/proposed algorithm was not robust enough for 100% emotion detection

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Bada & Nurse, 2019	Cybersecurity challenges faced by small-medium enterprises	Literature review and exploratory research	36 articles and sole case study	Survey with 27 small-medium enterprises	Provided an outlined program for cybersecurity education and awareness for small-medium enterprises
Bello et al., 2017	Lack of understanding of information cybersecurity risks and privacy issues with BYOD	Qualitative research	Three case studies and 62 participants	Surveys and interviews	Demonstrated the integration of policies, standards, procedures, and technical controls to manage BYOD
Diesch et al., 2020	Lack of decision makers' understanding of information cybersecurity	Literature review	136 articles	Interviews of 19 experts	Provided 12 management success factors (MSFs) for information cybersecurity decision-makers
Harley & Cooper, 2021	Theorized information integrity is crucial, necessitating a literary understanding	Literature review	None	Information flow, data modification, quality, mechanisms, and trustworthiness	Identified integrity protection challenges and expressed the importance of standardization, definitions, and applications of information integrity

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Idrus et al., 2013	An increasing amount of damage from cyber-attacks from access to online information	Exploratory research	None	Authentication methods	Recommended biometrics as the only method to authenticate users
Khando et al., 2021	Limited gathered knowledge about methods and factors to enhance employees' information security awareness	Literature review	64 articles	Methods and factors in ISA development	Distinguished methods and factors for the public and private sectors concerning ISA
Mohamed et al., 2022	Difficulty in selecting the appropriate access control model for cybersecurity needs due to numerous amount of models available	Literature review	None	Criteria and access control models	Provided classification of access control models, implementations, and extended categories
Neigel et al., 2020	Lack of understanding of the latent individual differences associated with attitudes, behavior, and	Quantitative research	173 university participants	Surveys	Disclosed why humans may be the weakest link in cybersecurity breaches and where they are most vulnerable

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	knowledge of cyber hygiene				
Palanisamy et al., 2020	Lack of understanding of the features of BYOD that impact the threat landscape and factors for policy-compliant behaviors	Literature review	21 articles	BYOD features and cybersecurity policy compliance factors	Proposed to improve cybersecurity compliance with training, policy development, and social factors.
Schiliro, 2023	Lack of emphasized collaboration with law enforcement agencies in cybersecurity frameworks	Literature review / qualitative research	Sole healthcare organization	Semi-structured interviews	Developed the CyRLEC framework as an effective architecture to partner with police agencies to manage and control hospital risks
Song et al., 2019	Single-user design models create account challenges in workplace collaboration with account sharing as the primary option as opposed to a workaround	Quantitative and qualitative research	98 responses from Amazon Mechanical Turk (MTurk)	Two surveys	Guided researchers and designers to support usable and secure ways for password sharing among multiple users

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Strohmer et al., 2022	Poor organizational cybersecurity habits and posture contribute to data breaches and theft (assess DoD contractors)	Qualitative research	Ten defense contractors	Interviews	Indicated contractors had full awareness of compliance. However, readiness varied depending on the size and nature of the business
Syafrizal et al., 2020	Organizations' lack of experience in cybersecurity causes difficulty in choosing and adopting standards or frameworks	Literature review	Over 1,000 articles	Cybersecurity frameworks, standards, and regulations	Indicated standards, frameworks, and regulations are either general or very specific to their purpose
Taherdoost, 2022	Businesses are challenged to adopt standards to address their cybersecurity requirements	Literature review	17 papers	Features and applications of cybersecurity standards and frameworks	Presented a summary of standards and applications as some are mandatory, while others may not fulfill the needs and may require a combination of standards
Wash & Rader, 2021	Increased vulnerabilities occur from the reuse of user	Literature review and quantitative research	134 participants	Survey and web browser data collection tool	Identified the influences and users' decisions for

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	passwords across accounts				password creation and use
Zviran & Erlich, 2006	Authentication is expressed as the most problematic component of access control in information systems	Comparative analysis	None	Authentication types and methods	Outlined the pros and cons of authentication methods and indicated selection criteria to be considered

Multi-Criteria Decision Analysis (MCDA)

Németh et al. (2019) referred to 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). Dean (2022) described multi-criteria analysis (MCA) as overarching, not as a single or specific method, but as a means for multiple objectives and decision criteria included to examine a problem. Moreover, Dean (2022) indicated MCA has been influenced directly or indirectly by several theories, such as utility and value theories, social choice theory, revealed preference theory, and game theory. MCDA methods are popular in solving management-related issues; as the main goal is predefined, and criteria are broken down into smaller pieces, which allows for group decision-making to be an easier process (Baylan, 2020; Bouayad, et al., 2018; Németh et al., 2019).

As presented by Dean (2022), the key elements of MCA are options, objectives, criteria, criterion weight, and performance score. The performance score is a calculated number, which is identified on a scale, for example, as a 0 to 1 scale, a 1 to 100 scale, or a -5 to +5 scale to establish the performance of an option relative to the objective and criterion. As such, the application of MCA toward developing an index is supported by the objective to calculate a CFI-Mfg value based on the criterion of CMMC 2.0 – Level 1 domains, the proposed Cybersecurity Footprint elements, the interconnected tiers, and their associated weights.

One of the most popular MCDA methods is the Analytical Hierarchy Process (AHP), developed by Thomas Saaty in the 1970s as a framework to solve complex problems by quantifying decision-making elements within a hierarchical structure (Tavana et al., 2021). AHP has been used to solve problems across many areas, such as political, economic, social, and management sciences, to name a few (Lee et al., 2008). Sipahi and Timor (2010) found based on literature review and categorization of articles, AHP was one of the most preferred techniques used in the manufacturing industry for cases such as supplier selection, supply chain evaluation, location selection, system selection or evaluation, and strategy.

The basic steps of AHP are to define the problem, establish the hierarchy, formulate a paired comparison matrix (e.g., pairwise table), calculate the weights, check for consistency, and determine the results (Dash & Sar, 2020; Duo et al., 2021). Using a hierarchy, subjectivity exists in the decision process structured by criteria, sub-criteria, and weighted factors (Jakupovic et al., 2010; Önder & Hepsen, 2013). Németh et al.

(2019) asserted the problem can be described visually, where the criteria and sub-criteria are in the middle of the hierarchy. This was demonstrated by a study conducted by Duo et al. (2021), as abnormal events were used to quantify the risk level of a power grid system to provide decision support for cybersecurity personnel.

In multi-criteria and multifactor problems, Sutrisno (2022) claimed measurement theory applies to AHP in determining ratio scales, such as pairwise comparisons. Pairwise comparisons are used to establish the criterion weights at each level and the priorities of the hierarchy (Harker & Vargas, 1987; Németh et al., 2019). The number of pairwise comparisons is determined by $n = m * (m - 1) / 2$, where m is the number of criteria and n is the resulting number of pairwise comparisons. Table 14 illustrates a pairwise comparison of $m = 3$ criteria and $n = 3$ comparisons.

Table 14

Example of Pairwise Comparison

	Criteria A	Criteria B	Criteria C
Criteria A	1	9	5
Criteria B	1/9	1	7
Criteria C	1/5	1/7	1

AHP's widespread use and popularity are due to ease of usage, ability to compare qualitative and quantitative factors, and flexibility in the hierarchy model to adjust the size of the decision-making problems while maintaining transparency in the approach

(Awang et al., 2022; Ziburko & Szulżyk-Cieplak, 2019). In a risk management study, Sharma (2014) claimed that AHP provided a way to think through the decision problem and quantified risks based on project managers' feelings, resulting in a risk map showing the level of risk criticality. Wang (2021) applied AHP to develop a network security risk assessment to evaluate assets, threats, and vulnerabilities, whereby they had identified hardware and software failure as a highly weighted threat, necessitating the need to increase maintenance and replace damaged network equipment timely to reduce risks. Comparable to the proposed CFI-Mfg, Alora and Barua (2022) claimed the need for supply chain risk management systems “as the complexity of manufacturing supply chains, which could reach up to 25 tiers, with hundreds of suppliers, buyers, bankers and logistics service providers” (p. 497). Their study identified, classified, and prioritized five categories and 26 associated supply chain risks that contributed to developing a supply chain disruption risk index based on AHP.

The literature review identified a broad set of studies where an AHP-based approach was applied, as in the case of a performance evaluation system for university patient achievement (Liang & Anni, 2021), the establishment of a highway traffic evaluation system to measure safety (Li & Chen, 2021), as well as a case study involving an IT project selection process in a large oil and gas company, leading to consensus and improved criteria for the prioritization of portfolio projects (da Silva Neves & Camanho, 2015). Petrova (2021) produced a cybersecurity risk ranking method to prioritize the components of a system in terms of their importance to successful operation based on criteria that included attacks, vulnerabilities, penetration testing, threats, assets,

cybersecurity measures, unauthorized access, and cybersecurity alerts. Xinlan et al. (2010) gathered data for key assets, threats, and vulnerabilities and, based on AHP and group decision-making, calculated associated risk values and the prioritization of risk incidents. With the use and combination of AHP and Capability Maturity Model Integration (CMMI), Raghuram et al. (2021) developed a Supply Chain Risk Management Index (SCRMI) to measure the manufacturer's preparedness in mitigating the risks based on CMMI levels (initial, managed, defined, quantitatively managed, and optimizing) along with dozens of risks identified from the literature. Lastly, Ziburko and Szulzyk-Cieplak (2019) used the experience and knowledge of employees to determine the risks associated with the loss of information as an example, calculated that 48.23% occur due to human factors, 42% occur due to technical hazards, and 9.77% occur as random events. A summary of the prior research regarding the MCDA and AHP is listed in Table 15.

Table 15

Literature Summary of MCDA and AHP

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Alora & Barua, 2022	Financial performance and loss from interruptions, delays, and production issues in supply chains	Literature review and hybrid AHP and fuzzy TOPSIS	354 small-medium enterprises	Financial supply chain risks, demand-side risks, supply-side risks, process risks, and	Developed supply chain risk index and conveyed the importance of supply-side and financial-side risks of

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
				environmental risks	manufacturing supply chains
Awang et al., 2022	University networks are exposed to cyber threats and risks	AHP	Nine experts	Threat prevention and criteria (technical, human resource, and logistics)	Established decision guidance to prioritize and optimize solutions to overcome threats and risks
Baylan, 2020	Impacts from poorly assessed project risks	AHP- Stochastic TOPSIS Hybrid method	None	Cost, time, output quality, project work package, project activities, and weights	Determined impact of activity risks on quality, cost, and time
Bouayad, et al., 2018	Lack of a definition of IT Governance (ITG) and difficulty in selection from a multitude of frameworks	AHP method	Sole case study	Alignment, architecture, infrastructure, applications, project /portfolio management, framework complexity, and ITG maturity	Proposed a framework based on AHP for the selection of the most suitable ITG framework
da Silva Neves & Camanho, 2015	IT project selection is challenged by the increasing complexity	Exploratory	Sole case study	Decision-making variables	AHP provided a transparent, rational, and quality

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	and dynamics of markets				decision-making approach
Dash & Sar, 2020	Floods are devastating threats to human lives and socio-economic conditions	MCDA	Sole case study	Flood hazard mapping criteria	Prepared and confirmed the credibility of MCDA-based index to identify flood hazard areas
Duo et al., 2021	Difficulty to detect and evaluate cybersecurity risk level of power grid systems	AHP method	501 business entities	Data outputs from processing module and abnormal discovery module	Developed risk assessment framework for power grid systems to provide decision support for security personnel
Harker & Vargas, 1987	Criticisms and misunderstandings of the theoretical basis of AHP leading to slow acceptance	Literature review	None	Criticisms and controversial areas	Proved from literature and day-to-day operations that AHP has a theoretical foundation and is a viable decision-making tool
Jakupovic et al., 2010	No metrics to determine whether a business sector is more	AHP method	None	Complexity classes and indicators	Demonstrated a model which measured the level of

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	complex than the business software				complexity business software brings or removes to understand the positive effects
Lee et al., 2008	Measuring and evaluating IT based on financial measures is not sufficient	Fuzzy-AHP method	Sole case study	Goal, perspectives (criteria), and performance indicators (sub-criteria)	Proposed a performance evaluation model to guide IT performance evaluation
Li & Chen, 2021	Increasing demand for road transportation has created more traffic accidents and road safety issues	AHP and entropy weight method	Sole case study	Objective, criterion, and index	Proved a developed index model is a practical and effective method for solving highway traffic safety evaluation
Németh et al., 2019	Healthcare decision-making is complex, and it is difficult to reach healthcare policy objectives	Narrative review	None	Resource requirement, software requirement, chance of bias, and general complexity	Evaluation of weight elicitation methods and proposed selection criteria

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Petrova, 2021	Reliability concerns of cyber risk exposure models	Literature review and AHP method	393 studies	Attacks, vulnerabilities, assets, and threats	As an alternative in the structured hierarchy, confidentiality was more advantageous than availability and integrity
Raghuram et al., 2021	Proper risk assessments and risk management capabilities reduce the impact of supply chain disruptions	Literature review and order of magnitude AHP (OM-AHP)	None	Questionnaire	Developed a supply chain risk management index for companies to assess their maturity level concerning risks
Sharma, 2014	Excessive cost overruns and losses encountered due to delayed construction projects	AHP and risk map method	None	Questionnaire	Developed a risk framework for project risk management in construction
Sipahi & Timor, 2010	The use of AHP will continue to increase	Literature review	232 articles published 2005-2009	Integrated methods used	Confirmed exponential growth, emphasized the benefit of AHP, guided future work and advancement of the method

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Sutrisno, 2022	Employee discipline issues in a company heavily relying on human resources	AHP method	None	Questionnaire	Developed the Human Resource Performance Measurement (scorecard), which determined compensation was the most important alternative
Tavana et al., 2021	Complexity of pairwise comparison process and inconsistency in AHP	Literature review and comparative analysis	None	AHP features, strengths, and weaknesses	Proved five other AHP methods with the same ranking required fewer judgments and effort
Wang, 2021	Increasing network cybersecurity incidents and impacts on society and the economy	Quantitative research	Single local network and five network cybersecurity experts	Assets, threats, and vulnerabilities	Employed fuzzy operator to AHP in network cybersecurity risk assessment and identified key areas of importance
Xinlan et al., 2010	Difficulty in gathering risk probability and risk	Group Decision Making	Single test case	Assets, threats, and vulnerabilities	The proposed method established risk incidents

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	impact creates challenges for information systems risk assessments	(GDM) and AHP			priority and confirmed improved risk management support
Zaburko & Szulżyk-Cieplak, 2019	Challenges to maintaining computer system security and safety of users at a national and international level	Literature review and AHP	Eight employees	Survey	Subjective assessment of employees confirmed the need to increase training frequency and verify knowledge obtained on the importance of cyberspace

Pairwise Complexity and Alternatives

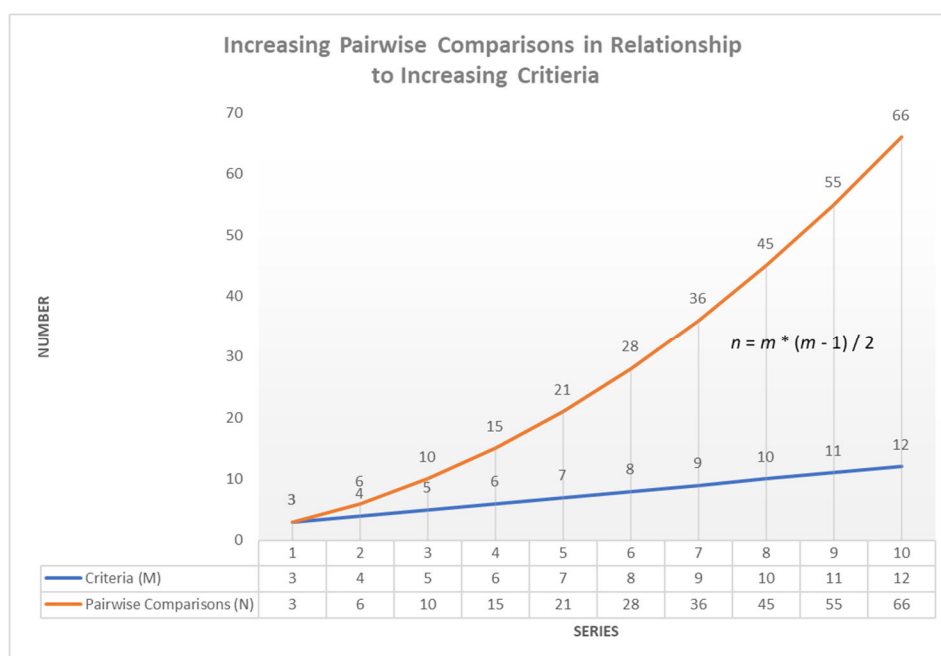
As the literature suggested, AHP requires pairwise comparison to be performed within a set of elements and across the system so that as the number of elements increases, the task of performing the pairwise comparison becomes difficult (Tavana et al., 2021). The complexity of pairwise comparison can be reasoned by the scenario described by Li and Chen (2021), where the importance of the weights is determined at the same level for all the factors, as well as the next level and the subsequent level above, until all are determined for comparison. Odu (2019) claimed as the number of criteria increases, the number of pairwise comparisons increases rapidly, thus making the effort

burdensome. Equally, Ma et al. (2022) expressed that research with many criteria for pairwise comparisons is consuming, extends the processing time, and reduces efficiency.

Figure 1 illustrates the increase in pairwise comparisons (n) because the number of criteria (m) increases.

Figure 1

An Example of Increasing Number of Pairwise Comparisons (n)



Note. Chart developed with Microsoft Excel. (Created by John Del Vecchio, 2024).

Dean (2022) indicated that applying MCA involves a lot of time, which people do not have, nor the resources or knowledge to perform many pairwise comparisons to solve complex problems. Raghuram et al. (2021) stated, “the major limitation of AHP is that it prioritizes only homogenous variables, and the accuracy of pairwise comparison is lost as

the number of variables increases beyond seven variables” (p. 619). Wei et al. (2005) expressed that when selecting an ERP system with several layers in the hierarchy, pairwise comparisons are impractical as the process becomes inefficient when too many attributes are identified. Harker and Vargas (1987) advocated for simple pairwise comparison to support the smaller rational broken-down components of a problem.

Odu (2019) indicated several types of elicitation methods to determine the weights for factors categorized as subjective, objective, integrated, or a combined weighting approach. Roszkowska (2013) had described:

The subjective approaches select weights based on preference information of criteria, subjective intuitions or judgments based on their knowledge given by the decision maker, the objective methods determine the weights of criteria through a mathematical calculation using objective information in a decision matrix. (p. 17)

Some of the most common subjective weighting methods, in addition to AHP, include point allocation, direct rating, and ranking method (Odu, 2019). Dean (2022) and Roszkowska (2013) described point allocation as a method that requires tradeoffs, such that more points are assigned to criteria with higher importance, which then requires subtracting points from other criteria to maintain a total of 100 points. Bottomley et al. (2000) indicated that the allocation scale varies as the decision maker proceeds; therefore, balancing the allocation of points is necessary to avoid running out too soon or having points remaining. Odu (2019) critiqued the approach by stating, “the weights obtained from the use of point allocation method are not very precise, and the method becomes more difficult as the number of criteria increases to 6 or more” (p. 1451). In contrast, the

direct rating method is performed by assigning number values to the different criteria with no trade-offs (Roszkowska, 2013) as this technique does not require comparisons; this method is straightforward for decision-makers as they are subjected only to the number of questions (Németh et al., 2019).

In test-retest situations, Bottomley et al. (2000) found that the same alternative was chosen 88% of the time using the direct rating method, as opposed to 74% using the point allocation method. In another study conducted by Bottomley and Doyle (2001), the direct rating method was modified with a Max100 and Min10 approach, where subsequent criteria were rated against criteria after they were assigned 100 for most important or 10 for least important, respectively. In this case of a test-retest scenario, with both internal consistency and convergent validity evaluated, the same alternative would have been chosen 91% of the time using Max100, 87% of the time using direct rating, and 75% of the time using Min10.

The ranking method has been noted in the literature as one of the simplest methods to assign weights, which include rank sum, rank exponent, and rank reciprocal. Wu et al. (2023) outlined the ranking methods as criteria weighting methods used in the design of experiments, asserting rank exponent and rank reciprocal are like rank sum; however, for rank exponent, the value is raised to an exponential of a parameter, and rank reciprocal is a normalized reciprocal of the criterion rank. Odu (2019) cautioned the use of ranking methods due to the difficulty of attempting to straight rank many criteria and considering these methods for estimating weights. However, a study conducted by Pamidimukkala et al. (2023) overcame this issue by calculating effect size, which was used to rank criteria

for various categories and gave weights to various stakeholders. Roszkowska (2013) conveyed aspects for consideration toward the use of rank-order decision-making as experts and decision-makers

- may not be able to reach agreement on a set of exact weights,
- are more confident about the ranks of some criteria than their weights,
- can agree on ranks more easily,
- can easily understand and use the method (Roszkowska, 2013).

A summary of the prior research regarding pairwise complexity and alternatives is listed in Table 16.

Table 16

Literature Summary of Pairwise Complexity and Alternatives

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Bottomley et al., 2000	The selection of weight elicitation methods yields different results	Theoretical and empirical study	113 business students	Survey	Identified several reasons why the direct rating method is preferred over the point allocation method
Bottomley & Doyle, 2001	Lack of information concerning the reliability and validity of numerous	Empirical study	108 post-graduate students	Survey	The confirmed weighting method Max100 is superior to

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	weighting methods				DR, which is superior to Min10
Ma et al., 2022	An increase in cloud services options makes selection challenging	AHP and Fuzzy AHP (FAHP) methods	Sole case study	Categories and attributes of service measurement index	Demonstrated efficiencies of pre-decision fuzzy Delphi (PFDR) compared to other existing methods
Odu, 2019	Difficulty selecting the appropriate weighting method due to the influence and significance of the criteria weight on the outcome	Case study	None	Subjective, objective, and integrated weighting methods	Reviewed and discussed weighting methods to make it easier to understand the differences and the performance toward a selection process
Pamidimukkala et al., 2023	The impact of effective project-based communication indicators is not known for construction projects	Literature review	40 case studies	Questionnaire	Determined impact on quality communication is caused by availability of financial resources, labor turnover, transparency of owner's objectives, number of approvals required, and complexity of

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution additional requirements
Roszkowska (2013)	Lack of understanding of the significant role the weights of criteria play in MCDM moles	Literature review and comparative analysis	None	-	Proposed various reasons to use ranking methods due to ease and confidence by decision-makers
Wei et al., 2005	Selection of an ERP system is important as it is tedious, time-consuming, requires significant financial investment, and potential risks involved	AHP method	Sole case study	System and vendor factors	Presented a comprehensive framework for ERP system selection

AHP and Delphi Method

Levy and Gafni (2022) suggested using the Delphi method, which comprises an expert panel to validate the proposed elements, establish weights for the elements, and develop a validated index for Cybersecurity Footprint. For this proposed study, the Delphi method and a modified AHP will be used, evidenced by several studies that have employed the combination of the techniques to identify criteria and sub-criteria, construct

hierarchies, and establish weights. For example, Khorramshahgol and Moustakis (1988) simply screened unimportant objectives by expert evaluation and prioritized only the remaining objectives for developing a highway. Kharat et al. (2016) utilized the Delphi method and AHP to establish a solution to select the best alternative for municipal solid waste treatment and disposal by determining the degree of importance of each criterion to construct measures. Likewise, Shen et al. (2019) used the Delphi method and AHP to develop an index to evaluate the quality of nursing simulation education, and they claimed the method and resulting weight assignments were scientific and reliable. Furthermore, based on a body of literature, Hsu et al. (2013) developed a survey for experts to evaluate and select criteria for selecting a Customer Relationship Management (CRM) solution. After that, the weights of five criteria and 15 sub-criteria were established based on AHP, which provided the ability to quantify decision-maker judgments and calculate vendor scores. Similarly, Teng et al. (2020) determined the main factors that contribute to the development of the Taiwan Cruise Tourism Industry based on the Delphi method and AHP, which highlighted key factors such as the promotion of safety measures, premium service quality, simplified visa processes, and the promotion of increasing cruise passengers.

Numerous studies have been performed within the cybersecurity discipline using the Delphi method and AHP to develop measurement indexes. For instance, a study by Meng (2013) structured a hierarchy of cybersecurity risk evaluation factors for a company based on information obtained from the Delphi method. The factors (criterion layer) consisted of physical security, platform security, operation security, backup security, and

management security. In addition, the evaluation model included a secondary set of more specific factors (index layer), which aligned with the factors. AHP was performed to devise weights, which for the factors were 0.3191 (C3), 0.2928 (C4), 0.1784 (C2), 0.1169 (C5), and 0.0928 (C1) in that order. Based on indicators from cybersecurity standards (e.g., ISO/IEC 27002), Peisheng et al. (2020) used the Delphi method to establish five factors as the main criterion layer toward the development of an information system cybersecurity risk assessment model, which included a subsequent level of 21 indicators and weights from conducting an AHP method, as shown in Table 17.

Table 17

Example Index for Information System Cybersecurity Risk

Target Layer	Criteria Layer	Weights	Indicator Layer	Weights
Information System Security Risk (U)	Information Security (U1)	.140	Identification (U11)	.130
			Access control (U12)	.050
			Information encryption (U13)	.400
			Non-repudiation (U14)	.020
			Information integrity (U15)	.400
	Software Security (U2)	.200	Database security (U21)	.120
			Operating system security (U22)	.070
			Application software security (U23)	.130
			Disaster recovery security (U24)	.180
			Trojan Virus Prevention (U25)	.200
			Patch repair (U26)	.150

Target Layer	Criteria Layer	Weights	Indicator Layer	Weights
			System log (U27)	.150
	Hardware Security (U3)	.240	Firewall (U31)	.380
			Fault tolerant backup (U32)	.270
			Intrusion detection (U33)	.350
			Management system (41)	.320
	Management Security (U4)	.170	Internal management (U42)	.230
			Management agency (U43)	.450
			Equipment safety (U51)	.480
	Environment Security (U5)	.250	Physical protection (U52)	.250
			Safe power supply (U53)	.270

Note. Adapted from Peisheng et al. (2020).

Agyepong et al. (2023) developed a model to measure the performance of Security Operations Center (SOC) Analysts to address problems and inadequacies faced by SOC managers to be fair and systematic with evaluations. The key criteria in the hierarchy were analyst functions (at the 2nd level) and Key Performance Indicators (KPIs) (at the 3rd level). In addition to the model, Agyepong et al. (2023) claimed that the consensus of the proposed weights was a main contribution from the study, as the SOC managers could determine the performance score of analysts without having to repeat the approach and intense pairwise comparison that had been conducted previously. A summary of the prior research regarding the AHP and Delphi Methods is listed in Table 18.

Table 18*Literature Summary of AHP and Delphi Method*

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
Agyepong, et al., 2023	Lack of a systematic approach to evaluating cybersecurity analyst performance	Delphi method, AHP, and empirical evaluation	Eight Security Operations Center (SOC) experts	Questionnaire	Proposed a model that enables SOC managers to aggregate, quantify, and evaluate the performance of analysts
Hsu et al., 2013	Lack of solutions to support the creation of a new business model for the medical tourism industry in Taiwan	Literature review, Delphi method, and AHP	Nine experts	Questionnaire	Developed a decision model to evaluate CRM systems for the medical tourism industry
Kharat et al., 2016	Major challenges for developing countries to address Municipal Solid Waste (MSW) management	Delphi method and AHP	None	Questionnaire	Developed a model that addresses complex and diverse issues to prioritize the optimal treatment and disposal for MSW
Khorrarnshahgol & Moustakis, 1988	Inappropriate objectives lead to improper	Delphi method and AHP	Two university student classes	Questionnaire	Proposed the Delphic Hierarchy Process

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	planning and eventual problems				(DHP) to determine objectives and priorities
Meng, 2013	Claimed technology and security devices will not solve all the problems with information security	AHP and empirical study	Single company	Questionnaire	Proposed a method that is effectively applied to information security risk evaluation and management
Peisheng et al., 2020	Increased attention toward information systems leads to increased security risks and losses	Delphi method, AHP, and empirical analysis	Single information system in a university	The criteria layer and indicator layer	The proposed model is effective, accurate, and saves time by reducing to a three-scale AHP method
Shen et al., 2019	Lack of ability to evaluate training simulations for nursing students	Delphi method and AHP	27 nursing education experts	Questionnaire	Developed a tool to evaluate the quality of the teaching simulation in nursing
Teng et al., 2020	Increasing demand for cruise tourism in Taiwan requires an understanding of key factors for the	Delphi method and AHP	Six experts and 70 questionnaires	Questionnaire	Determined key factors such as the promotion of safety measures, premium service quality,

Study	Description of the Problem or Theory	Methodology	Sample	Instruments or Constructs	Main Finding or Contribution
	sustainable development of the industry				simplified visa processes, and the promotion of increasing cruise passengers

Summary of What is Known and Unknown

A review of various literature was conducted to provide the foundation for this proposed research study. Based on this review, a summary explanation and understanding are provided to convey what is known and unknown toward developing a measurement index to assess organizational cyber posture for manufacturing companies. The literature exposed various reasons the manufacturing industry is a target of cyber-attacks (Masum, 2023) and depicted several significant impacts that could occur from cyber incidents (Corrallo et al., 2021). For instance, the manufacturing industry was portrayed as deficient in protecting against vulnerabilities associated with outdated technology (IBM, 2023), the increased use of complex I4.0 technologies (Elhabashy et al., 2020), and integrated third parties (Pandy et al., 2020). Additionally, the literature described the supply chain as a series of trusted connections between parties and as a source of potential cyber incidents from compromised partners (Keskin et al., 2021; Sailio et al., 2020). The Ponemon Institute (2017) and Yeboah-Oforis and Islam (2019) demonstrated a lack of visibility into third-party data handling procedures and security controls, as well as failures by companies to conduct third-party audits.

The Target Corporation data breach of 40 million compromised credit and debit cards has been well covered in the literature (Lynch, 2017; Levy & Gafni, 2021). However, upon further review and analysis, the literature noted the compromise originated from a third-party HVAC company and confirmed Target's lack of oversight, lack of access control by third parties, and lack of audits were contributing factors (Brandao & Rezende, 2020; Caston et al., 2021). The increased reliance on confidential information shared between organizations and the connected systems required has been highlighted as a significant concern toward data breaches (Goode et al., 2017; Schlacki et al., 2022). A large number of industries have experienced data compromise incidents exposing billions of records and impacting billions of victims, as demonstrated by a subset of noteworthy cases (ITRC, 2022; Verizon DBIR, 2022) and several identified explicitly in the manufacturing industry (Arctic Wolf, 2023; de Groot, 2020).

Levy and Gafni (2021, 2022, 2023) introduced the Theory of Cybersecurity Footprint and proposed the development of measurable indices for specific industries, laying the groundwork for this research. To understand the methods used to address problems or achieve objectives, this study reviewed measurement indices across various disciplines, including tourism, waste treatment, healthcare education, and cybersecurity risk. However, a measurement index to aggregate and calculate the cyber posture, specifically in the context of manufacturing companies based on their interconnected entities, as suggested by the Theory of Cybersecurity Footprint, is notably absent from the literature.

Peisheng et al. (2020) presented a measurable index consisting of a criteria layer and a sub-criteria layer with associated weights. This study provided a comprehensive

understanding of the hierarchical decision model, the AHP method, and the structuring and arrangement of criteria in a hierarchy. The criteria and sub-criteria proposed by Levy and Gafni (2022) based on the CMMC 2.0 Level 1 domains and practices suggested a hierarchical approach. However, specific weights for the manufacturing industry are not available in the literature. Importantly, the use of the Delphi method, as demonstrated by Khorramshahgol and Moustakis (1988), Hsu et al. (2013), and Agyepong et al. (2023), is particularly suitable for gaining insight from SMEs and determining the weights of the domains and elements for the manufacturing industry.

Chapter 3

Methodology

Overview

The methodology for this study was based on a developmental research approach. Richey and Klein (2005) described developmental research as providing reliable and valuable information to practitioners and theorists through a systematic approach to evaluate tools, processes, and models. From a traditional perspective, developmental research includes planning, conducting, and reporting a research project (Richey & Klein, 2005). As shown in Figure 2, this proposed research started with 30 SMEs in the field of cybersecurity utilizing the Delphi method to identify the number of tiers, as well as confirm the weights of the tiers, domains, and proposed elements of the Cybersecurity Footprint (Levy & Gafni, 2022; Pei et al., 2019; Shi et al., 2020).

Based on the literature review of Levy and Gafni (2022), a list of six domains from CMMC 2.0 Level 1 and 26 proposed Cybersecurity Footprint elements was used as initial input to this research. The set of domains consisted of Access Control (AC), Identification and Authentication (IA), Media Protection (MP), Physical Protection (PE), System and Communications Protections (SC), and System and Information Integrity (SI). During Phase 1, survey instruments were administered to a panel of SMEs for review, assessment, and validation of the domains, elements, tiers, and associated

weights. Phase 1 utilized the Delphi method as an iterative process to gather anonymous feedback. Kermanshachi et al. (2020) noted that when the best information available is the judgment of knowledgeable individuals, it is more advantageous to have a controlled and systematic process to gather individual judgment rather than a discussion. As such, the collected data was analyzed to provide statistical measures, such as central tendencies with dispersion, percentages, and frequency of distribution, to gather feedback and generate a reliable consensus opinion of the SMEs (Ameyaw et al., 2016; Nasa et al., 2021).

After Phase 1, the SMEs validated the survey instrument to collect a company's Cyber Organizational Risk Exposure (CORE) Score contributing to the Cybersecurity Footprint hierarchical index (Figure 3). Subsequently, Phase 2 consisted of a pilot with six manufacturing companies to review and make final adjustments to the CORE Score survey instrument and index model. Phase 3 used the developed and validated CORE Score survey instrument to conduct a quantitative empirical study with more than 70 B2B companies. The scores were calculated in association with the index measurement (shown in Figure 4) by collecting, calculating, and documenting the results of the CORE Score survey instrument. To conclude this study, data analysis determined the statistically significant mean differences among the companies' CFI-Mfg based on the number of interconnected entities, the number of interconnected tiers, and aspects of the attack surface. Research findings were provided, along with recommendations for future research.

Figure 2

Research Design

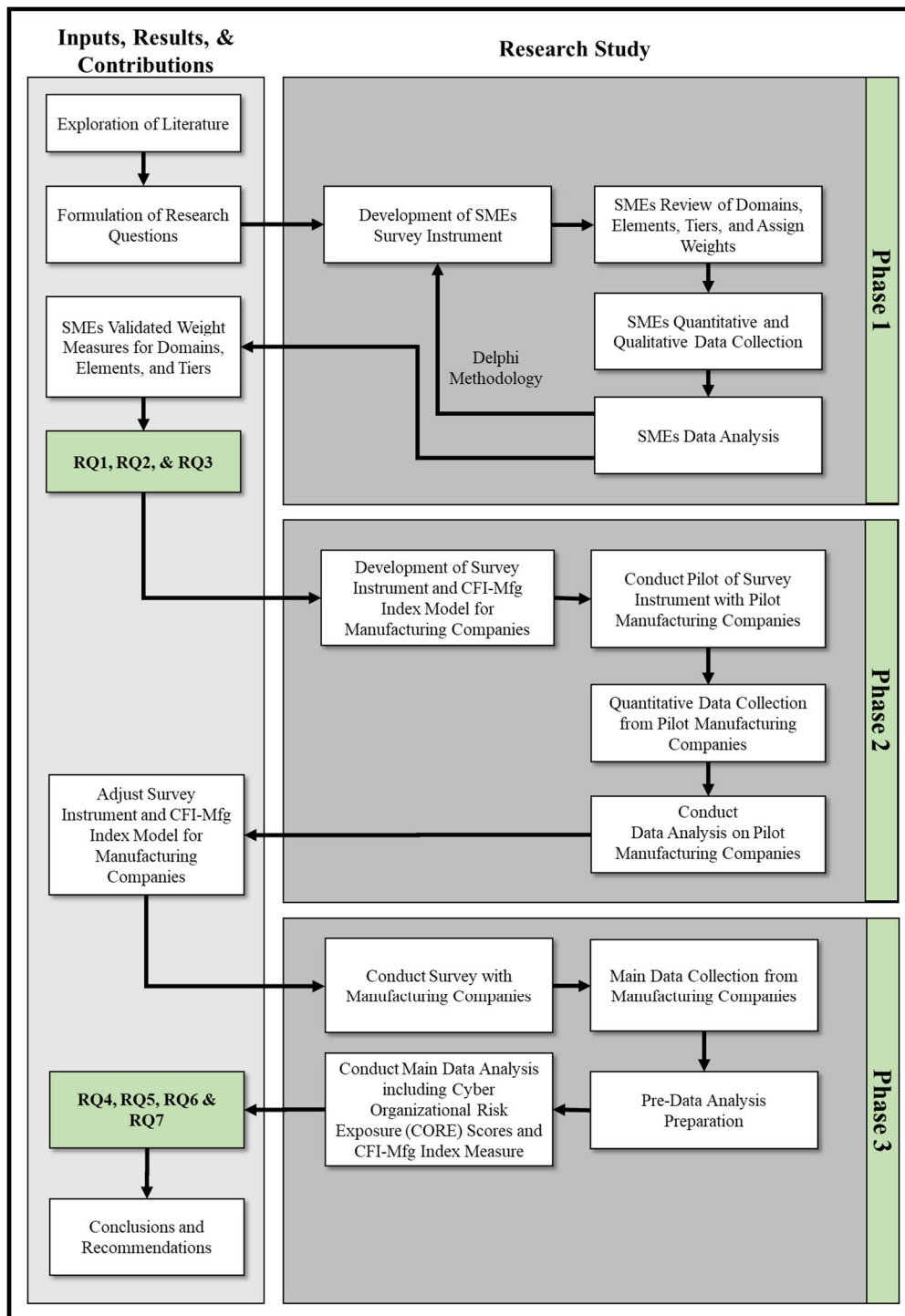


Figure 3

Association of Elements, Domains, and Weights Toward a CORE Score for a Given Organization

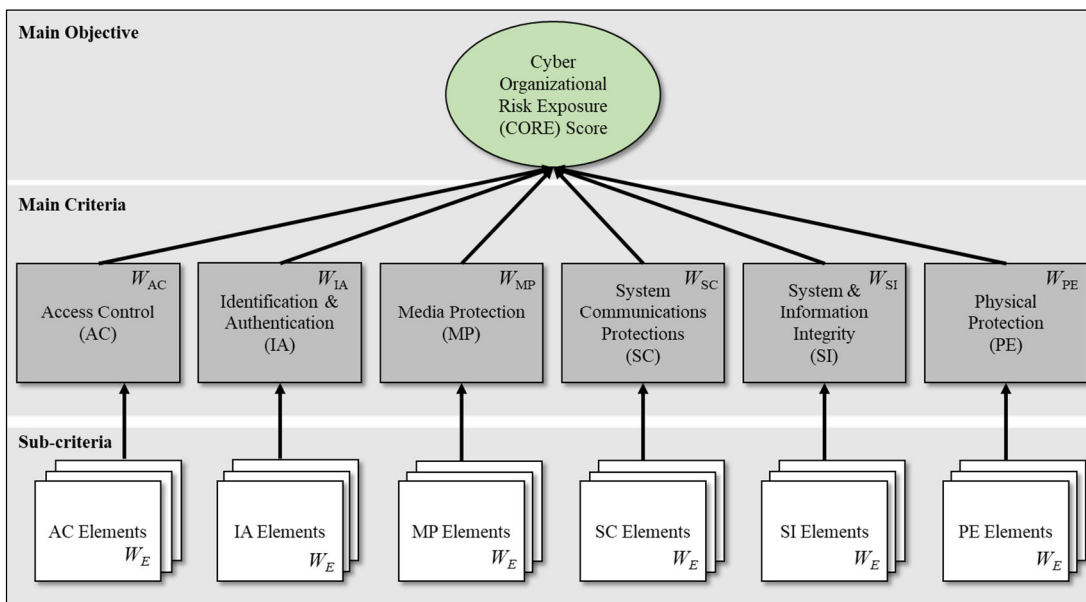
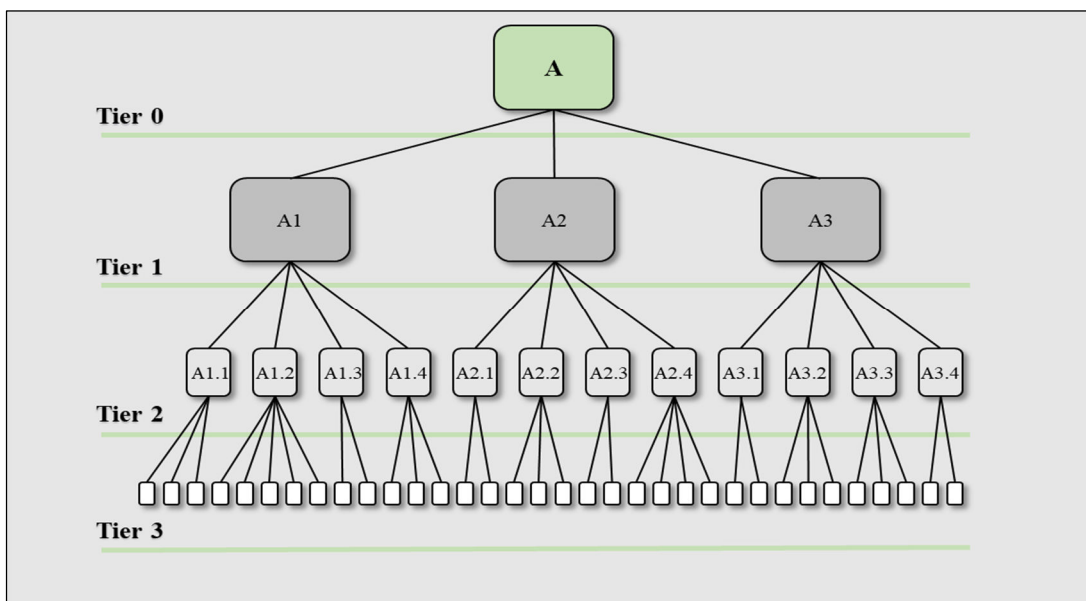


Figure 4

Conceptual CFI-Mfg Hierarchy Model



Research Measures

This research was comprised of independent and dependent variables. The independent variables are those that are varied; the dependent variables are those with no control, resulting in measurable change caused by independent variables (Leatham, 2012). Moreover, the independent variables of this study were the CORE Score survey elements measured on an ordinal scale with specific category values for each. Suparji et al. (2021) asserted that ordinal scale data have more than two categories and differences in degrees between the categories. In cases where respondents reduce the categories to two, the data would be dichotomy and, thus, nominal scale data (Suparji et al., 2021).

For the originating manufacturing organization (Tier 0), the CFI-Mfg score is a dependent variable, while the CORE Scores for the interconnected entities (Tier 1 – Tier n) are independent variables. Song et al. (2020) contended that the AHP divides indexes into distinct levels with weights of indexes at the criterion level and sub-criterion levels influencing the objective issue. The originating manufacturing organization's CFI-Mfg score depended upon the hierarchical formula of the collected CORE Scores of the interconnected entities, which were calculated by the weighted scores of the elements for each domain and the weights of the domains.

Research Method

The Delphi method is a well-structured, rigorous process developed in the early 1960s by the Rand Corporation during the Cold War and used for military defense projects to study technology impacts on warfare (Alarabiat & Ramos, 2019; Setiadi et al.,

2018; Taylor, 2020). McKay et al. (2022) asserted Delphi as a structured and iterative method involving independent experts to gain consensus of opinions to deal with and solve complex problems. Generally, with the Delphi method, a panel of experts is subjected to a questionnaire (Levy & Gafni, 2023). However, focus groups, individual interviews, workshops, meetings, or seminars can also be used (Alarabiat & Ramos, 2019; McKay et al., 2022; Ramim & Lichvar, 2014). The Delphi method empowers the researcher to provide controlled feedback to the SMEs after each iteration through an interactive process to decrease variability and achieve the most reliable consensus of the expert panel's opinion (Keeney et al., 2001; von der Gracht, 2012).

Beiderbeck et al. (2021) stated, "Delphi has been frequently used in various scientific disciplines ranging from healthcare, medicine, education, business, engineering and technology, social sciences to information management, and environmental studies" (p. 2). Through a combination of accumulating, assimilating, and assessing human judgment, the Delphi method has been widely used in cases where there is a lack of information, disagreement, or irregularity (Fisher et al., 2020). Additionally, several variants of the Delphi method have been developed over time to satisfy differing needs. For instance, Griffey et al. (2020) noted that a Modified Delphi approach was valuable, with in-person group discussions at the end of the process to address disagreements and resolve uncertainties. Di Zio (2018) proposed that Spatial Delphi could solve three distinct problems, such as choosing an optimal location (e.g., for goods or services), predicting where an event has a probability of occurring (e.g., an earthquake), and finding things not visible (e.g., archaeology) by using maps in the process. Paraskevas and Saunders (2012)

indicated that Policy Delphi is a tool used for analysis and decision-making based on the pros and cons of differing expert opinions instead of expert consensus. Lastly, Linstone and Turoff (2011) described Problem-Solving Delphi as a system used to compare and rank participants' judgment and to resolve major disagreements through discussions. Regardless of which method is used, expert participation, anonymity, controlled feedback, statistical response, and iteration exemplify the core characteristics of Delphi to ensure consistency (Fisher et al., 2020). Goluchowicz and Blind (2011) purported that the output of Delphi is determined entirely by the opinions of the experts selected. Delphi allows for broad access to knowledge and experience of people with different qualifications, various exposures to the topic of investigation, and dependency that they are proven decision-makers with the capacity, willingness, and communication skills to convey their opinions and thoughts (Hsu & Sandford, 2007; Paraskevas & Saunders, 2012; Romano, 2010).

Participants' anonymity is essential to minimize or eliminate the effect of dominant individuals and avoid influence that creates bias; the equality of responses is critical to the process (Hallowell & Gambatese, 2010; Taylor, 2020). The interaction between participants can be eliminated by using electronic methods such as an online platform, web-based survey, or e-mail, concealing which comments are from whom (Barrios et al., 2021; Hsu & Sandford, 2007; Linstone & Turoff, 2011). Anonymity contributes to achieving the goal of consensus by converging opinions as the experts evaluate additional information and can reconsider their initial judgment (Barrios et al., 2021; Linstone & Turoff, 1975). Anonymity also enables participants to add further insight by changing

their opinion or original viewpoint without fear of losing credibility (Belton et al., 2019; Liao & Lai, 2017).

Skulmoski et al. (2007) referred to controlled feedback as “informs the participants of the other participant’s perspectives and provides the opportunity for Delphi participants to clarify or change their views” (p. 3). Likewise, Taylor (2020) indicated that a summary of results reported to participants in each round is controlled feedback. Hallowell and Gambatese (2010) suggested that expert panelists should be requested to provide justifications for their ratings to be shared as part of controlled feedback in subsequent rounds, as this has been found to significantly improve the accuracy of a research study. There is a possibility of shifting the expert panelist’s opinion between Delphi rounds depending on the type of feedback provided (Turnbull et al., 2018). Barrios et al. (2021) reported that the level of consensus in subsequent rounds is affected by shared feedback of the consensus level in the previous round, which results in participant opinion tending to change toward the majority opinion.

The most common feedback for participants in subsequent rounds is statistical summaries, such as median, mean, or quartile ranges (Hallowell & Gambatese, 2010). Goluchowicz and Blind (2011) suggested that statistical summaries and, more specifically, standard deviation should be provided as a measure of dispersion. Boulkedid et al. (2011) recommended providing the percentages of participant agreement. In Delphi, iteration involves a redistribution of surveys and controlled feedback to improve the precision of the results and reach consensus (Hallowell & Gambatese, 2010). Hsu and Sanford (2007) asserted that the participants present thoughtful opinions and become

problem solvers due to multiple iterations. A typical number of Delphi rounds is two or three. However, a single round could suffice (Day & Bobeva, 2005), while up to 10 could occur depending on the circumstances (Goluchowicz & Blind, 2011). Day and Bobeva (2005) indicated that a broader gap in time between rounds can affect the situation's circumstances, knowledge, and context. A round or iteration is concluded when sufficient information has been provided, a research question is answered, responses are stable and have a level of accuracy, or consensus is reached (Skulmoski et al., 2007). A summary of literature in which the Delphi method was used in research to solve complex problems is shown in Table 19.

Table 19

Literature Summary of Delphi Method Studies

Study	Description of the Problem or Theory	Industry or Discipline	Sample	Instruments or Constructs	Main Finding or Contribution
Almaiah et al., 2022	Increased development costs due to poor selection of technical requirements for mobile applications	Information Systems	30 experts (24 experts in software engineering and information systems, as well as six experts in mobile learning)	Six quality dimensions and 21 associated technical requirement items	Identification of 19 technical quality requirements as guidelines to enhance applications meeting users' requirements
Setiadi et al., 2018	Develop a directed and integrated manner to	Cyber Security	Six experts in the field of	National Cyber Security 12 components	Improved accuracy of the NCS Framework

Study	Description of the Problem or Theory	Industry or Discipline	Sample	Instruments or Constructs	Main Finding or Contribution
	protect assets from cyber loss based on initial components from National Cyber Security		cybersecurity	and 57 sub-components	based on extracted sub-components from the initial set of components
McKay et al., 2022	Lack of guidelines for Australian clinicians to address women experiencing hunger and food insecurity during pregnancies	Human Healthcare	12 experts engaged in round one, and 11 experts involved in round two	Online surveys were used to capture item rankings and open-ended questions. Subsequently, experts provided feedback and used a 5-point Likert scale to rank suggested priorities	The study identified several suggestions to be implemented at the institutional, community, and government levels to support food insecurity during pregnancy
Hohmann et al., 2020	Limitations and difficulties with random clinical trials to determine a practical approach toward the treatment of degenerative meniscus tears	Surgical Healthcare	20 panel experts participated who had been published on the topic or were members of a specific committee	A survey with ten initial open-ended questions expanded by four iterations with experts to devise a series of questions using Likert-style questions	The established consensus that tears are part of aging, should initially be treated non-operatively, repairable tears should be repaired, and outcomes are dependent on several

Study	Description of the Problem or Theory	Industry or Discipline	Sample	Instruments or Constructs	Main Finding or Contribution specific factors
Beiderbeck et al., 2023	A deficient understanding of the need for emerging technology innovation within the global football (soccer) ecosystem	Sports	85 technical directors (TDs) out of 211 TDs from FIFA member associations representing 200 countries worldwide	Ten future projections related to Players, Coaches, and TDs concerning technology in football (soccer)	Desire to improve game-related aspects with technology focused on communications, training, or scouting. However, reservations about technology impact players

Research Phases

This research was conducted in three phases to address the research questions outlined in Chapter 1 and illustrated in Figure 2. Phase 1 consisted primarily of executing the Delphi method to achieve SME consensus on the number of tiers and the weights of the tiers, domains, and elements of the CFI-Mfg. Once consensus was reached in Phase 1, questions RQ1, RQ2, and RQ3 were answered, and a proposed CFI-Mfg measurement index was developed. Phase 2 focused on piloting the CORE Score survey instrument and the measurement index with a controlled group of manufacturing companies. Quantitative and qualitative data were captured for further analysis and refinement of both instruments. Lastly, Phase 3 collected data from B2B companies using the CORE

Score survey to serve as input to the CFI-Mfg measurement index to answer RQ4 and provide a basis for the research conclusions and recommendations, as well as to address RQ5, RQ6, and RQ7 concerning statistically significant mean differences to the CFI-Mfg and several variables.

Phase 1

Phase 1 started with a survey to collect input from the SMEs concerning the number of tiers and a percentage based on the importance associated with each Tier from the Originating Organization. The sum of the percentages provided equaled 100%. SMEs were asked to provide the level of importance for each of the domains and elements on a scale from 1, indicating ‘Not at all important’ to 7, indicating ‘Very important’. To develop an ordinal scale for the CORE Score survey, the SMEs were asked to select a number provided or propose a number for the high-end of the scale for each of the elements. Finally, for the attack surface variables, SMEs were asked to select a number provided or propose a number for the high-end of the scale for each of the attack surface questions.

The survey was designed to eliminate the need for additional Delphi rounds. Green (1982) claimed that the Delphi subjects’ 70% score on a Likert-type scale should be required for consensus. Barrios et al. (2021) found that providing controlled feedback regarding the consensus percentage to Delphi participants in subsequent rounds would strengthen or weaken consensus; therefore, they recommended a target threshold of 75% for consensus since responses differed on either side of this level. This study deemed consensus when 70% of the Likert scale selections were measured within two points on

the seven-point scale and refrained from using simple percentages as a measure, which was deemed a concern (Linstone & Turoff, 1975; Ulschak, 1983).

Phase 2

The CORE Score survey instrument and the measurement index were inputs to Phase 2. Six manufacturing companies participated in a pilot of the CORE Score survey instrument to collect data input for the CFI-Mfg index and feedback concerning the CORE Score survey. The survey included each element and its associated ordinal scale for input. The data gathered during this phase was input into the index model to validate the calculations and refine the CORE Score survey instrument as needed.

Phase 3

71 B2B companies completed the CORE Score survey instrument in Phase 3. Upon receipt of the supplied data, CORE Scores were calculated for each company. To answer RQ4, RQ5, RQ6, and RQ7, the resulting CORE Scores were used to calculate the originating organizations' index model CFI-Mfg score. As in the case for RQ5, the CFI-Mfg score of index models was used to determine any statistically significant mean differences to the CFI-Mfg based on the number of interconnected suppliers. Likewise, for RQ6, the CFI-Mfg score of index models was used to determine any statistically significant mean differences to the CFI-Mfg based on the number of tiers of interconnected suppliers/vendors. Lastly, for RQ7, the CFI-Mfg score of index models was used to determine any statistically significant mean differences to the CFI-Mfg based on attack surfaces. To conclude Phase 3, a thorough data analysis was performed, along

with a reflection on this research summarizing the results and the findings and offering recommendations for further research.

Instrument Development

Phase 1 Instruments

This research developed and provided a survey instrument for SMEs to initiate Phase 1 based on constructs from a literature review conducted by Levy and Gafni (2022). The constructs comprised six domains from CMMC 2.0 Level 1 and 26 proposed elements forming the Cybersecurity Footprint index. The SME survey (Appendix B) gathered data for various measures, including the tiers, domains, elements, and attack surface variables (Table 20). The questions of this survey employed scales consisting of ‘Not at all important’ to ‘Very important’ to capture the importance of the domains and elements, as well as scales of numeric options for the elements and the attack surface variables.

Weight Measure

Phase 1 of this research identified and gained consensus on the weights for the CFI-Mfg tiers, domains, and elements. The process required the SMEs to indicate the number of tiers to be included in CFI-Mfg and the importance of each tier by providing percentages that sum to 100%. Additionally, SMEs provided feedback on the importance of domains and elements in establishing weights. Kermanshachi and Safapour (2019) used the Delphi method to devise weights associated with complexity indicators for construction projects, such as cost overruns, schedule delays, and poor project performance. Equal weights indicate equal importance, while unequal weights specify

greater or lesser importance and influence the final index value (Sutadian et al., 2016). Burke et al. (2019) noted that indexes are used for evaluation based on questions weighted by importance to determine an overall score. Studies by Duo et al. (2021), Li and Chen (2021), as well as Liang and Anni (2021), demonstrated the use of AHP to determine the “influence weight” of distinct factors, enabling the measurement of risk, safety, and performance respectively. For this research, the SME-defined weights were critical findings in determining a CFI-Mfg score.

Table 20

Proposed Measures for Phase 1

Measure	Value	Description
Tiers	Number	Number of Tiers
Tier Weight	Percent	Weight of Tier(s)
Domain Weight	Percent	Weight for Access Control (AC) Weight for Identification & Authentication (IA) Weight for Media Protection (MP) Weight for Physical Protection (PE) Weight for Systems & Communications Protections (SC) Weight for System and Information Integrity (SI)
AC Element Weight	Percent	Number of authorized users.

Measure	Value	Description
		Number of authorized devices.
		Number of information system access to the types of transactions and functions that authorized users are permitted to execute.
		Number of transactions and functions that authorized users are permitted to execute for each type of information classification level.
		Number of connections to external information systems.
		Volume of transactions using external information systems connections (per month).
		Volume of information posted or processed on publicly accessible information systems (per month).
		Number of employees.
		Number of Bring Your Own Device (BYOD) devices connected to the organizational network.
		Average number of BYOD device applications per employee.
IA Element Weight	Percent	Number of individuals sharing the same user credentials and/or devices.
MP Element Weight	Percent	Number of unsensitized or non-destroyed information systems media containing Organizational Information before disposal or release for reuse.
		Volume of data in the information systems (# of records).
		Average number of non-licensed applications per employee on work assigned device.

Measure	Value	Description
		Average number of social media accounts per employee.
PE Element Weight	Percent	<p>Number of devices (organizational information systems, equipment, and the respective operating environments) with physical access to non-authorized individuals.</p> <p>Number of escorted visitors (per month).</p> <p>Number of non-escorted visitors (per month).</p> <p>Volume of logs of physical access (per month).</p> <p>Number of physical access devices (CCTV, IP Cameras, NVRs, etc.)</p>
SC Element Weight	Percent	<p>Volume of organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.</p> <p>Number of subnetworks for publicly accessible system components that are physically or logically separated from internal networks.</p>
SI Element Weight	Percent	<p>Number of provided tools to protect from malicious code at appropriate locations within the organizational information systems.</p> <p>Number of up-to-date malicious code protection patched systems.</p> <p>Number of periodic scans of information systems per month.</p> <p>Volume of scanned files from external sources as files are downloaded, opened, or executed.</p>

Measure	Value	Description
AC Element Scale	Number	<p>Number of authorized users.</p> <p>Number of authorized devices.</p> <p>Number of information system access to the types of transactions and functions that authorized users are permitted to execute.</p> <p>Number of transactions and functions that authorized users are permitted to execute for each type of information classification level.</p> <p>Number of connections to external information systems.</p> <p>Volume of using external information systems connections.</p> <p>Number of employees.</p> <p>Number of Bring Your Own Device (BYOD) devices connected to the organizational network.</p> <p>Average number of BYOD device applications per employee.</p>
IA Element Scale	Number	Number of individuals sharing the same user credentials, and/or devices.
MP Element Scale	Number	<p>Number of unsensitized or non-destroyed information systems media containing Organizational Information before disposal or release for reuse.</p> <p>Volume of data in the information systems (# of records).</p> <p>Average number of non-licensed applications per employee on work assigned device.</p>

Measure	Value	Description
		Average number of social media accounts per employee.
PE Element Scale	Number	<p>Number of devices (organizational information systems, equipment, and the respective operating environments) with physical access to non-authorized individuals.</p> <p>Number of escorted visitors (per month).</p> <p>Number of non-escorted visitors (per month).</p> <p>Volume of logs of physical access (per month).</p> <p>Number of physical access devices (CCTV, IP Cameras, NVRs, etc.)</p>
SC Element Scale	Number	<p>Volume of organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.</p> <p>Number of subnetworks for publicly accessible system components that are physically or logically separated from internal networks.</p>
SI Element Scale	Number	<p>Number of provided TOOLS to protect from malicious code at appropriate locations within the organizational information systems.</p> <p>Number of up-to-date malicious code protection patched systems.</p> <p>Number of periodic scans of information systems per month.</p> <p>Volume of scanned files from external sources as files are downloaded, opened, or executed.</p>

Measure	Value	Description
Attack Surface	Number	<p>How many workstations and laptops does your company have deployed and in use?</p> <p>How many network file servers does your company have deployed and in use?</p> <p>How many application servers does your company have deployed and in use?</p> <p>How many public cloud instances does your company have deployed and in use?</p> <p>How many firewalls and switches does your company have deployed and in use?</p> <p>How many multi-function printers does your company have deployed and in use?</p> <p>How many mobile devices does your company have deployed and in use?</p> <p>How many IoT devices does your company have deployed and in use?</p> <p>How many employees does your company have?</p>

Phase 2 Instruments

A pilot group of six manufacturing companies participated in Phase 2 by responding to a CORE Score survey instrument (Appendix C) comprised of 26 questions grouped by the six domains (AC, IA, MP, PE, SC, and SI). Each survey question included “number of,” “average number of,” or “volume of,” along with a corresponding scale of numeric choices. As shown in Figure 5, the categorical scale had a precise order with a corresponding ranking from 1 to 10 to translate the selection into a numeric value

(Mishra et al., 2018). Following the completion of CORE Score survey submissions, the associated value for each selection was multiplied by a coefficient of 10 (e.g., $7 * 10 = 70$) to normalize the element value on a scale of 10 to 100 and be input to calculate the CORE Score of the organization. Cinelli et al. (2021) noted, “normalization consists in making all the indicators comparable on the same scale” (p. 83).

Figure 5

An Example of a Participant Survey Question

Number of authorized users (select a choice that most applies):

Selection	1-5 <input type="radio"/>	6-10 <input type="radio"/>	11-15 <input type="radio"/>	16-20 <input type="radio"/>	21-25 <input type="radio"/>	26-30 <input type="radio"/>	31-35 <input type="radio"/>	36-40 <input type="radio"/>	41-45 <input type="radio"/>	> 45 <input type="radio"/>
Value	1	2	3	4	5	6	7	8	9	10

The CORE Score of an interconnected entity was calculated by the sum of the weighted domains (W_D) multiplied by the sum of the weighted elements (W_E) multiplied by a coefficient (C_E) applied to the values of each of the elements (E):

$$CORE_{Org} = \sum (W_D * \sum (W_E * (C_E * E_{l..n})))$$

A Normalized Value (NV) was calculated as an average for each tier based on the following:

$$NV_{Tier.n} = \sum_{(l-n)} ((CORE_{Org.l-n} - \text{Min}(CORE_{Org.l-n})) / (\text{Max}(CORE_{Org.l-n}) - \text{Min}(CORE_{Org.l-n}))) / n$$

A contribution CORE Score was calculated based on the weight of the tier (W_T) and the calculated “Entity Impact Weight” (W_E) applied to the normalized value of the given tier ($NV_{Tier.n}$):

$$\text{Contr_CORE}_{Tier.n} = NV_{Tier.n} * (W_{Tier.n} * (\text{Num_Entities}_{Tier.n} / \text{Total_Num_Entities})) / \sum ((W_{Tier.1} * (\text{Num_Entities}_{Tier.1} / \text{Total_Num_Entities})) + \dots + ((W_{Tier.n} * (\text{Num_Entities}_{Tier.n} / \text{Total_Num_Entities})))$$

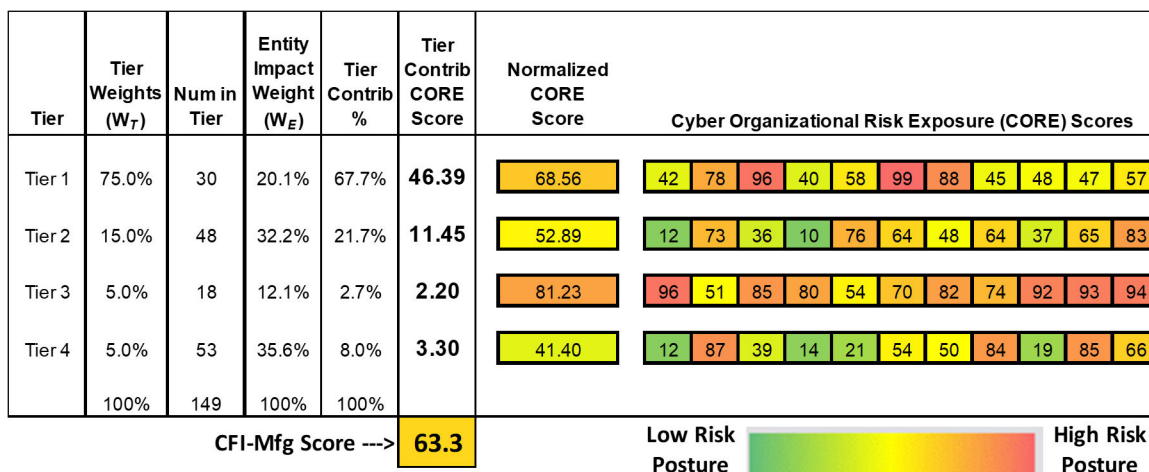
The CFI-Mfg score of the originating manufacturing company (Tier 0) was determined by the sum of the contribution CORE Scores of each of the tiers:

$$\text{CFI-Mfg}_{OrgA} = \sum (\text{Contr_CORE}_{Tier.1}) + (\text{Contr_CORE}_{Tier.2}) \dots (\text{Contr_CORE}_{Tier.n})$$

The calculation of the CFI-Mfg score for the originating (Tier 0) manufacturing company was quantified to indicate a risk posture on a scale from 10 being “Low” to 100 being “High,” as Levy and Gafni (2022) suggested to aid companies in the effort to self-assess and communicate easy-to-understand information (See Figure 6 for an example).

Figure 6

An Example of CORE Scores and CFI-Mfg Score



Proposed Samples

Phase 1

Brady et al. (2015) noted, “the Delphi method is not concerned with having a generalizable sample but instead seeks input from a purposive sample of individuals with specific expertise on a topic” (p. 61). A purposive sample has relevant characteristics to the study (Andrade, 2021). Goode et al. (2018) emphasized a homogeneous group of SMEs as a best practice; however, they suggested the importance of varying attributes such as ages, education, and backgrounds. As such, this research selected SMEs based on the level of expertise demonstrated by academic degrees, certifications, and professional experience in cybersecurity.

Phases 2 and 3

The manufacturing companies participating in this research were based on the number of employees. Likewise, the Small Business Act (SBA) indicates that manufacturing firms' size is based on the number of employees. Before the SBA's inception, the 500-employee manufacturing size standard defined the size of a small business (SBA, 2019). Isaac and Michael (1995) asserted that a sample size of between 10 and 30 participants would provide pragmatic advantages of simplicity and easy calculations toward developing a measurement instrument. Hertzog (2008) indicated that sample sizes as small as 10 to 15 could be sufficient, but depending on the pilot study's purpose, Hertzog recommended a sample size of 25 to 40 for instrument development. For Phase 2 and Phase 3 of this study, participation of manufacturing companies was solicited from organizations such as the National Association of Manufacturers

(<https://www.nam.org/>), the Manufacturers Association (<https://mascpa.org/>), and the FBI-affiliated organization InfraGard (<https://infragard.org>). For Phase 2, the initial response to solicitation requests was ineffective. However, persistent communication with key contacts from six manufacturing organizations resulted in a pilot group. Meanwhile, for Phase 3, to address the challenge of soliciting manufacturing companies and their interconnected entities, more than 70 B2B companies participated in this research study as an alternative by responding to the CORE Survey.

Data Analysis

This study's primary goal was to determine the role the elements of the CFI-Mfg serve in providing a measurable cybersecurity posture for manufacturing companies and their interconnected vendors/suppliers. This research used a combination of descriptive statistics and one-way Analysis of Variance (ANOVA) to assess the collected data and address several research questions, including determining whether there were significant mean differences to the CFI-Mfg based on the number of interconnected entities and the number of tiers.

At this study's onset, central tendency measures were determined after each round of the Delphi method. The means of the weights provided by the SMEs were calculated for the domains and elements. The standard deviation of the weights was calculated to assess the dispersion from the average weight value, and the median was identified to describe the data further. Sekaran and Bougie (2016) indicated that getting a feel for the data is a necessary first step, as these statistics can be easily obtained and provide an

understanding of whether variance can be explained. The ANOVA evaluates the significance of group differences between two or more means while analyzing the variation between and within groups (Mertler et al., 2021). The number of interconnected suppliers/vendors and tiers of interconnected suppliers/vendors are the representative groups whose numbers varied in determining the significant differences with the result of the CFI-Mfg. Finally, the attack surface and demographic data were analyzed to provide frequency and percentages of the sample population. In addition, the CFI-Mfg calculated means and standard deviations were compared by attack surface.

Research Validity and Reliability

Validity

Sekaran and Bougie (2016) indicated, “validity is the extent to which observations accurately record behavior; and reliability is the consistency of observations, usually of two (or more) observers on separate occasions, observing the same event attain the same results” (p. 137). In the case of the CFI-Mfg, the elements are a crucial component to record observations from the interconnected entities, and such that a failure of SMEs to identify, confirm, and validate all the required elements would threaten internal validity. To address this, the panel of SMEs was asked to provide feedback on all the proposed elements, precisely the wording and the measures, to confirm that there was no evidence of a problem (Ramim & Lichvar, 2014).

Reliability

While this study used the Delphi method, Ameyaw et al. (2016) and Hallowell and Gambatese (2010) claimed that at least eight participants are required to preserve reliability. Powell (2003) argued that the reliability of the Delphi method increases as the panel of SMEs increases. This study attempted to identify and select at least eight SMEs while balancing the threat of maturation and the potential of participants to refuse continued participation in the iterative process.

Keeney (2001) conveyed that the results of the Delphi method could be unreliable due to weak selection of the experts and issues controlling bias. To address this, Chalmers and Armour (2019) indicated a need for more guidelines for researchers for the Delphi method. However, researchers were encouraged to make preset decisions to reduce bias and improve the technique's validity. Andrade (2021) claimed that generalization to the population will only be possible by the defined selection criteria. Hallowell and Gambatese (2010) suggested that the level of expertise is the most crucial factor. To create a knowledgeable and qualified panel of experts for this study, the selection criteria of the SMEs was based on the SME's relevant experience and objectivity.

Consensus among the SMEs is a critical issue. Barrios et al. (2021) advised that the results could be meaningless or invalid if the Delphi method were stopped after a specific number of rounds. For this study, a seven-point Likert scale captured feedback on the domains, elements, tiers, and weights to confirm consensus among the SMEs. Cicchetti et al. (1985) claimed, "results indicate that reliability increases steadily up to a 7 scale, with

no substantial increase when the number of scale points is increased to as many as 100” (p. 31).

Presenting Results

The results of this research convey whether the research questions and goals have been addressed. Analysis of the data collected in each research phase contributed to such findings. With the potential for multiple Delphi rounds, measures of central tendency, also known as descriptive statistics (Ali & Bhaskar, 2016), were presented, including the mean, median, and standard deviation for each weight of the domains, elements, and tiers. Ali and Bhaskar (2016) stated, “basic statistical methods will help a researcher conduct an appropriately well-designed study leading to valid and reliable results. Inappropriate use of statistical techniques may lead to faulty conclusions, inducing errors and undermining the significance” (p. 668). Moreover, the similarities and non-similarities of scores were distinguished by measures of dispersion such as the range, interquartile range, variation ratio, and standard deviation (Cumberbatch, 2004).

Where appropriate, the numeric results were presented in table format with descriptive headings for rows and columns, where data values will be compared. Other methods, such as charts for visual aids, were used to present more convincing results. Additional commentary presented observations, illustrated the research findings, and answered the RQs. This research supplied quantitative and qualitative data analysis results to support its validity. For example, the consensus of the SMEs was aided by the detailed analysis of the number of tiers and weights for the domains, elements, and tiers.

The results of the data collected from the pilot group were examined, and the validity of the CFI-Mfg survey instrument and index model was confirmed. Finally, Cumberbatch (2004) indicated that the justification of the selected tests for statistical significance should be discussed, whereby the use of ANOVA indicated the results of whether statistically significant differences existed among the companies' CFI-Mfg based on the number of tiers, number of interconnected entities, and attack surfaces.

Summary

This chapter provided an overview of the multi-phase methodology for this research study. The phases of this study have been described in detail, starting with the Delphi method to engage SMEs in Phase 1 to validate a CORE Score survey instrument and measurement index, conducting a pilot Phase 2, and concluding with calculated CFI-Mfg scores, and findings and recommendations in Phase 3. Detailed aspects of the Delphi method, such as expert participation, anonymity, controlled feedback, statistical response, and consensus, have been provided to convey the importance of each and how they will be managed in the research approach.

While the input to this study was based on a prior literature review, as described in Chapter 3, the constructs of this study are the domains and elements from CMMC 2.0 – Level 1 to identify and validate their respective weights. The instruments for this research have been described in detail in this chapter, which facilitated the gathering of data from the SMEs, the pilot group, and participating B2B companies. Consequently, the results of the data analysis in each phase are conveyed in both tabular and graphic formats. The

supporting details were provided to answer the RQs associated with each phase. Besides a review of the research design, research method, and research instruments, this chapter also discussed the proposed sample of participants and the study's validity and reliability.

Chapter 4

Results

Overview

This study employed a three-phased approach involving SMEs, a pilot group, and individual companies. Each phase builds upon the previous one by collecting data, performing data analysis, and addressing the outlined research questions. Distinct surveys were used, necessitating data validation and cleansing in each phase. Ahuja et al. (2024) expressed the need for data validation and cleansing to ensure the quality, accuracy, reliability, and consistency of the data, especially in the case of data analytics.

In Phase 1, based on input from SMEs, weight measures specifically for the manufacturing industry were validated and established for the domains, elements, and tiers. This phase also removed several elements from subsequent survey instruments and the CFI-Mfg index model. Additionally, Phase 1 set the scales for the CORE Survey questions used in Phases 2 and 3 (Appendix C and Appendix D). Phase 2 involved collecting survey responses and feedback from a pilot group of manufacturers, which were used to refine the survey instrument and validate the CFI-Mfg index model.

In Phase 3, participation was broadened due to challenges experienced with recruiting manufacturing companies to coordinate the involvement with their suppliers and vendors (also referred to as interconnected entities or third-party providers). This phase included

small and medium-sized companies that provide products or services to manufacturing companies and other companies in B2B relationships. Over several weeks, survey responses were collected from 71 companies in B2B relationships. Using the CFI-Mfg index, CFI-Mfg Scores were calculated to represent 60 originating organizations based on varying entities and two or three tiers. Through one-way ANOVA, the data analysis seemed to indicate no statistical significance on the CFI-Mfg Score based on the number of entities or tiers in the CFI-Mfg index. Additionally, the results seemed to indicate no statistical significance on the entities' CFI-Mfg Score-based attack surface variables.

Phase 1 – Subject Matter Expert (SME) Survey

At the onset of Phase 1, an SME survey was developed based on a list of domains and elements originating from CMMC 2.0 Level 1 and refined by Levy and Gafni (2022). Subsequently, targeted invitation emails and LinkedIn connection requests were sent to prospective participants based on academics, certifications, and professional experience. Over about four weeks, 30 SMEs responded to a web-based survey for Phase 1 of this research study. Issues related to SMEs were addressed as needed with upfront introductions to the web-based survey and periodic check-ins to ensure progress. The goal of at least 25 survey responses was achieved for Phase 1.

Demographic Analysis

The collected demographic data, shown in Table 21, indicated that 80% of the respondents (24 of 30) have more than 16 years of experience in IT/Cybersecurity. Over 60% have at least one or more certifications, and over 93% have a bachelor's degree or

higher. In addition, Table 21 shows that 100% of the respondents are familiar with CMMC, with almost 50% being “Very familiar” to “Extremely familiar” with the framework. Selecting the appropriate SMEs is critical, as their capabilities are confirmed by their understanding of the topic area and their application of practice in the workplace (Mattoon, 2005).

Table 21

Descriptive Statistics of SMEs’ Demographics (N=30)

Demographic Item	Frequency	Percentage
<i>How long have you been working in the field of IT/Cybersecurity?</i>		
5 or less years	1	3.3%
6 - 10 years	4	13.3%
11 - 15 years	1	3.3%
16 - 20 years	5	16.7%
More than 20 years	19	63.3%
<i>What is your highest level of education achieved?</i>		
High school diploma	1	3.3%
2-year college (associate degree)	1	3.3%
4-year college (bachelor’s degree)	5	16.7%
Master’s degree	19	63.3%
Doctorate degree	4	13.3%
<i>What is your current job function?</i>		
Administrative/executive	9	30.0%
Cybersecurity/IT staff	6	20.0%
Manager	5	16.7%
Engineer	3	10.0%
Other		
- CISO		
- Consultant	3	10.0%
- Global Head of Security		
Professional staff	2	6.7%
Academics/professor/faculty member	2	6.7%

Demographic Item	Frequency	Percentage
<i>How many years have you been in your current role?</i>		
5 or less years	12	40.0%
6 - 10 years	12	40.0%
11 - 15 years	2	6.7%
16 - 20 years	1	3.3%
More than 20 years	3	10.0%
<i>How many years have you been in the Manufacturing Industry?</i>		
5 or less years	7	23.33%
6 - 10 years	6	20.00%
11 - 15 years	4	13.33%
16 - 20 years	3	10.00%
More than 20 years	2	6.67%
No prior experience in Manufacturing	8	26.67%
<i>What information security certificates do you hold?</i>		
CISSP	7	63.3% with 1 or more certifications
CompTIA Security+	5	
CISM	4	
CISA	3	
CIRSC	1	
Other(s)	13	
None	11	
<i>How familiar are you with (Cybersecurity Maturity Model Certification) CMMC 2.0?</i>		
Not at all familiar	0	0.0%
Slightly familiar	7	23.3%
Moderately familiar	9	30.0%
Very familiar	9	30.0%
Extremely familiar	5	16.7%
<i>What is the size of your company based on Annual Revenue?</i>		
< \$10M	6	20.0%
\$10M < \$50M	2	6.7%
\$50M < \$200M	1	3.3%
\$200M < \$500M	1	3.3%
\$500M < \$1B	9	30.0%
\$1B or Greater	11	36.7%
<i>What is the size of your company based on the number of Employees?</i>		
< 500	9	30.0%
500 < 1,000	2	6.7%

Demographic Item	Frequency	Percentage
1,000 < 1,500	1	3.3%
1,500 < 2,000	2	6.7%
2,000 < 2,500	2	6.7%
2,500 or Greater	14	46.7%

Phase 1 Pre-Analysis Data Screening

In Phase 1, pre-analysis data screening identified several SME responses that required removal. Although all of the questions in the SME survey were marked as 'required,' several responses to the question, “What should the [Highest End Number] be for the maximum tolerated risk exposure scale?” were not provided in the numerical format as per the instructions. Rather than choosing one of the seven selections (shown in Appendix B), SMEs chose “Other” and were instructed to provide a number. Based on the SME responses, Table 22 shows the selection frequency for each question, including “Other keep” and “Other removed.” “Other keep” were valid numerical values used to develop an average [Highest End Number] for each element within a 67% - 90% contribution range. The responses for “Other removed” included commentary, such as “Depends on the organization,” “Minimum as possible,” “Unable to provide,” and “No limit,” and thus were not numerical and were removed from the calculation. For the remaining SME survey responses, no incomplete or erroneous data was submitted for the number of tiers and the importance of tiers, domains, and elements.

Table 22*Pre-Analysis Data Screening of High-end Number Survey Question Responses (N = 30)*

	Selection Frequency							“Other” keep	“Other” removed	N keep	% N keep
	1	2	3	4	5	6	7				
AC1	10	1	1	3	0	0	4	1	10	20	67%
AC2	6	5	1	1	2	1	4	4	6	24	80%
AC3	2	4	4	4	3	2	1	3	7	23	77%
AC4	0	1	2	13	1	0	4	2	7	23	77%
AC5	6	5	3	2	1	1	1	4	7	23	77%
AC6	4	4	1	2	0	2	5	5	7	23	77%
AC7	9	2	0	1	0	4	3	4	7	23	77%
AC8	7	0	4	3	0	1	3	4	8	22	73%
AC9	6	1	1	1	3	2	4	6	6	24	80%
AC10	9	2	1	3	0	0	3	6	6	24	80%
IA1	9	2	1	1	2	0	1	9	5	24	80%
MP1	6	1	3	4	1	0	5	6	4	26	87%
MP2	6	1	2	0	1	2	9	3	6	24	80%
MP3	11	0	0	4	1	0	4	7	3	27	90%
MP4	4	10	0	6	0	0	3	2	5	25	83%
PE1	11	1	0	5	1	1	2	6	3	27	90%
PE2	6	0	2	2	3	0	9	3	5	25	83%
PE3	7	2	0	4	0	0	4	7	6	24	80%
PE4	3	2	1	2	5	1	6	4	6	24	80%
PE5	6	1	1	3	1	1	6	5	6	24	80%
SC1	7	2	3	0	2	2	4	4	6	24	80%
SC2	4	9	1	4	0	1	4	2	5	25	83%
SI1	4	4	1	7	2	1	5	1	5	25	83%
SI2	9	0	0	3	1	1	7	5	4	26	87%
SI3	4	4	2	3	1	0	7	5	4	26	87%
SI4	7	2	2	0	3	1	5	5	5	25	83%
AS1	7	1	3	4	0	1	4	3	7	23	77%
AS2	9	2	1	3	2	3	4	1	5	25	83%
AS3	5	2	4	4	3	1	5	1	5	25	83%
AS4	4	6	1	7	0	1	6	1	4	26	87%
AS5	9	2	5	0	0	0	5	5	4	26	87%
AS6	8	2	2	4	1	1	4	3	5	25	83%

Selection Frequency											
	1	2	3	4	5	6	7	“Other” keep	“Other” removed	N keep	% N keep
AS7	7	4	1	1	0	1	8	3	5	25	83%
AS8	8	3	2	0	2	0	6	4	5	25	83%
AS9	10	2	2	3	1	0	3	4	5	25	83%

Phase I Data Analysis of Tiers, Domains, and Elements

Table 23 and Table 24 reflect the results of the SME data establishing the frequency and associated percentage for the number of tiers proposed by the SMEs to include in the CFI-Mfg, whereby answering RQ2. The average number of tiers was 3.0, with a standard deviation 2.22. In the case of excluding the respective outliers (proposed tiers 10 and 11), the average number of tiers to be included would be 2.46, with a standard deviation of 0.98.

Table 23

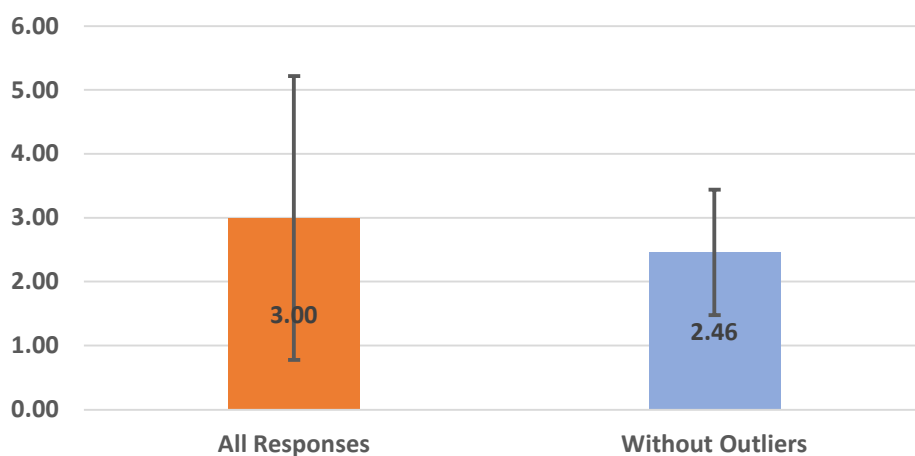
Descriptive Statistics of Number of Tiers (N=30)

Number of Tiers	Frequency	Percentage
1	5	16.67%
2	9	30.00%
3	11	36.67%
4	2	6.67%
5	1	3.33%
10	1	3.33%
11	1	3.33%

As shown in Table 23, 46.67% of the respondents indicated two tiers or less, while 83.34% indicated three tiers or less. Ahuja et al. (2024) indicated outliers can distort the statistical analysis, where outlier values are much smaller or larger than other values in the dataset. Figure 7 illustrates a comparison of the mean and standard deviation of the SMEs' number of tiers.

Figure 7

Mean and Standard Deviation of SMEs' Number of Tiers (N=30)



As a result of the SME survey, each SME indicated the number of tiers and the associated weights of the tiers to include in the index. Table 24 reflects the average weight percentage by tier.

Table 24

Means of SME Weights Percentage for each Tier (N=30)

Number of Tiers	Weight Percentage by Tier				
	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
1	100.00	-	-	-	-
2	63.56	36.44	-	-	-
3	54.54	27.73	17.72	-	-
4	50.00	22.50	17.50	10.00	-
5	50.00	25.00	15.00	5.00	5.00

Table 25 reflects the weight distribution for tiers one, two, and three based on the number of SMEs that proposed each tier. The calculation for each tier is:

$$W_t = \sum_{(1-t)} (\% \text{ of SMEs} * W\%_t)$$

$$\text{Tier 1} = (20\% * 100) + (36\% * 63.56) + (44\% * 54.54) = 66.88$$

$$\text{Tier 2} = (36\% * 36.44) + (44\% * 27.73) = 25.32$$

$$\text{Tier 3} = (44\% * 17.72) = 7.80$$

Table 25

Weight Distribution Based on # of SMEs (N=25)

	Tier 1	Tier 2	Tier 3	Total
Number of SMEs	5	9	11	25
% of SMEs	20%	36%	44%	100%
Tier 1 Weight	20.00	22.88	24.00	66.88
Tier 2 Weight	-	13.12	12.20	25.32
Tier 3 Weight	-	-	7.80	7.80
				100.00

Table 26 reflects the results of the SME's proposed weights for two and three tiers, answering RQ3. In the case of two tiers, 0.078 was distributed to tier 1 and tier 2 based on the respective ratio percentages of 0.669 and 0.253, respectively 0.725 and 0.275.

Table 26

Calculated Weights for Two Tiers and Three Tiers (N=25)

Tiers	Weights for 2 Tiers	Weights for 3 Tiers
1	0.725	0.669
2	0.275	0.253
3	-	0.078

To determine the importance level for the domain measures, SMEs responded on a scale from 1 – ‘Not at all important’ to 7 - ‘Very important’. Based on the average score from all SMEs, Table 27 reflects the results of the SME, whereby answering RQ1. Access Control (AC) and Identification and Authentication (IA) were identified as the top two domains contributing to the importance of cyber posture, with Media Protection (MP) being the least important. Access Control (AC) had the highest importance level mean at 6.87 with a standard deviation of 0.43, and it is given the highest weight of 0.181. Access Control was considered the most important security domain with relatively low variability in its importance ratings. Identification and Authentication (IA) had a mean of 6.70 and a standard deviation of 0.53, with a weight of 0.177. This domain was also considered highly important but with slightly more variability in its ratings compared to Access Control. System and Information Integrity (SI) had a mean of 6.50, standard

deviation of 0.73, and a weight of 0.172. SI was an important domain but had higher variability in importance ratings. System and Communications Protections (SC) had a mean of 6.43, standard deviation of 0.90, and a weight of 0.170. The higher standard deviation indicated variability in how respondents viewed its importance. Physical Protection (PE) had a lower mean importance level of 5.73 and a standard deviation of 1.17, with a weight of 0.151. Physical Protection was less important than the domains listed prior and had high variability in ratings. Media Protection (MP) had the lowest mean importance level at 5.63, the highest standard deviation of 1.43, and the lowest weight of 0.149. This indicated that Media Protection was considered the least important and had the most variability in its importance ratings. Figure 8 illustrates a comparison of the mean and standard deviation of SMEs' level of domain importance.

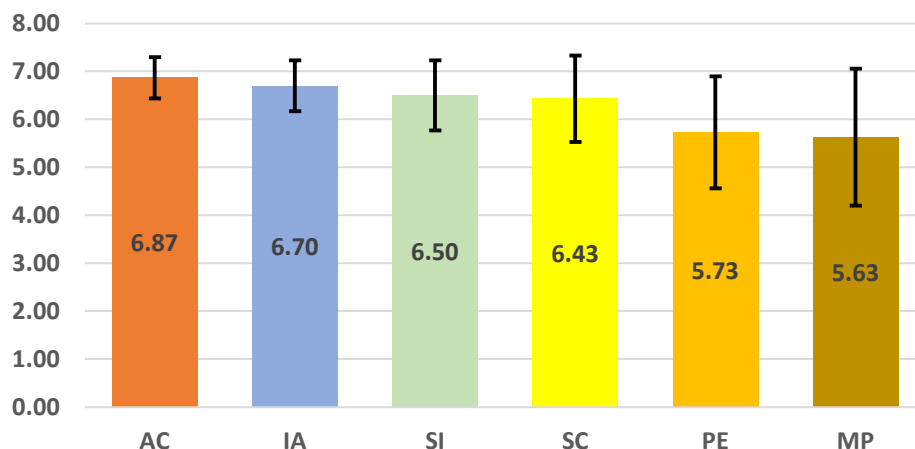
Table 27

Importance Level of Domains (N=30)

Domain	Domain Description	Importance Level (Mean)	Std. Deviation	Weight
AC	Access Control	6.87	0.43	0.181
IA	Identification and Authentication	6.70	0.53	0.177
SI	System and Information Integrity	6.50	0.73	0.172
SC	System and Communications Protections	6.43	0.90	0.170
PE	Physical Protection	5.73	1.17	0.151
MP	Media Protection	5.63	1.43	0.149

Figure 8

Mean and Standard Deviation of SMEs' Level of Domain Importance (N=30)



Likewise, to determine the importance level for the element measures, SMEs responded on a scale from 1 – ‘Not at all important’ to 7 - ‘Very important’. Based on the average score from all SMEs, Table 28 reflects the SME data results, further answering RQ1. Elements such as IA1 “Number of individuals sharing the same user credentials and/or devices,” SI2 “Volume of up-to-date malicious code protection patched systems,” AC5 “Number of connections to external information systems,” and SI3 “Number of periodic scans of the information systems per month,” was identified as the top contributors to the importance for cyber posture. In contrast, MP4 “Average number of social media accounts per employee” and PE2 “Number of escorted visitors per month” were the least important. The comparison of means and standard deviations is illustrated in Figure 9.

Table 28*Importance Level of Elements (N=30)*

ID	Element	Importance Level (Mean)	Std. Deviation	Weight
IA1	Number of individuals sharing the same user credentials, and/or devices.	6.73	0.83	1.000
SI2	Volume of up-to-date malicious code protection patched systems.	6.37	1.33	0.222
AC5	Number of connections to external information systems.	6.23	0.86	0.118
SI3	Number of periodic scans of the information systems per month.	6.20	0.92	0.172
SI4	Volume of scanned files from external sources as files are downloaded, opened, or executed.	5.97	1.59	0.250
AC3	Number of information system access to the types of transactions and functions that authorized users are permitted to execute.	5.87	1.14	0.111
PE1	Number of devices with physical access to non-authorized individuals.	5.77	1.57	0.241
AC9	Number of Bring Your Own Device (BYOD) devices connected to the organizational network.	5.77	1.63	0.109
MP1	Number of unsensitized or non-destroyed information system	5.63	1.50	0.295

ID	Element	Importance Level (Mean)	Std. Deviation	Weight
	media containing organizational information before disposal or release for reuse.			
MP3	Average number of non-licensed applications per employee on work assigned devices.	5.50	1.76	0.288
SC2	Number of subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	5.47	1.79	0.507
AC2	Number of authorized devices.	5.40	1.35	0.102
AC4	Number of transactions and functions that authorized users are permitted to execute for each type of information classification level.	5.37	1.47	0.102
SC1	Volume of organizational communications at the external boundaries of the information systems.	5.31	1.81	0.493
SI1	Number of provided tools to protect from malicious code at appropriate locations with organizational information systems.	5.30	1.68	0.222
PE3	Number of non-escorted visitors per month.	5.27	1.80	0.221

ID	Element	Importance Level (Mean)	Std. Deviation	Weight
AC1	Number of authorized users.	5.27	1.57	0.100
AC7	Volume of information posted or processed on publicly accessible information systems.	5.00	1.62	0.095
PE5	Number of physical access devices (CCTV, IP cameras, NVRs, etc.).	4.90	1.60	0.205
AC10	Average number of BYOD device applications per employee.	4.83	1.58	0.092
AC6	Volume of using external information systems connections.	4.80	1.54	0.091
PE4	Volume of logs of physical access per month.	4.43	1.91	0.185
MP2	Volume of data in the information systems.	4.17	1.68	0.218
AC8	Number of employees.	4.17	1.64	0.079
MP4	Average number of social media accounts per employee.	3.80	1.69	0.199
PE2	Number of escorted visitors per month.	3.53	1.68	0.148

Note. Weights have been calculated before the exclusion of Elements.

Figure 9

Mean and Standard Deviation of SMEs' Level of Element Importance (N=30)

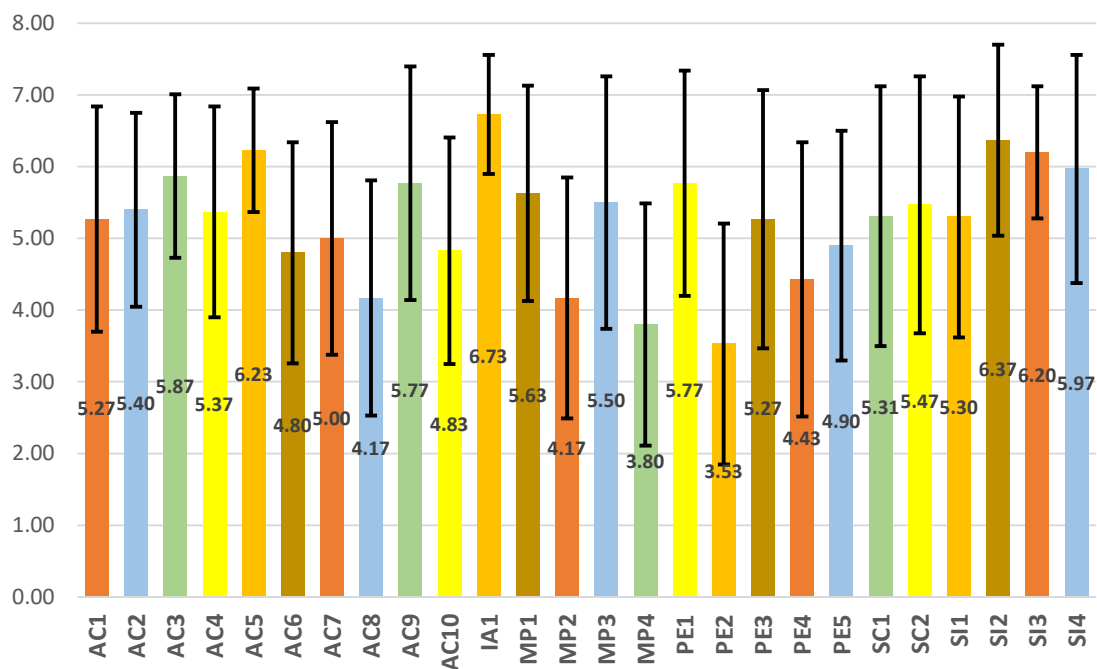
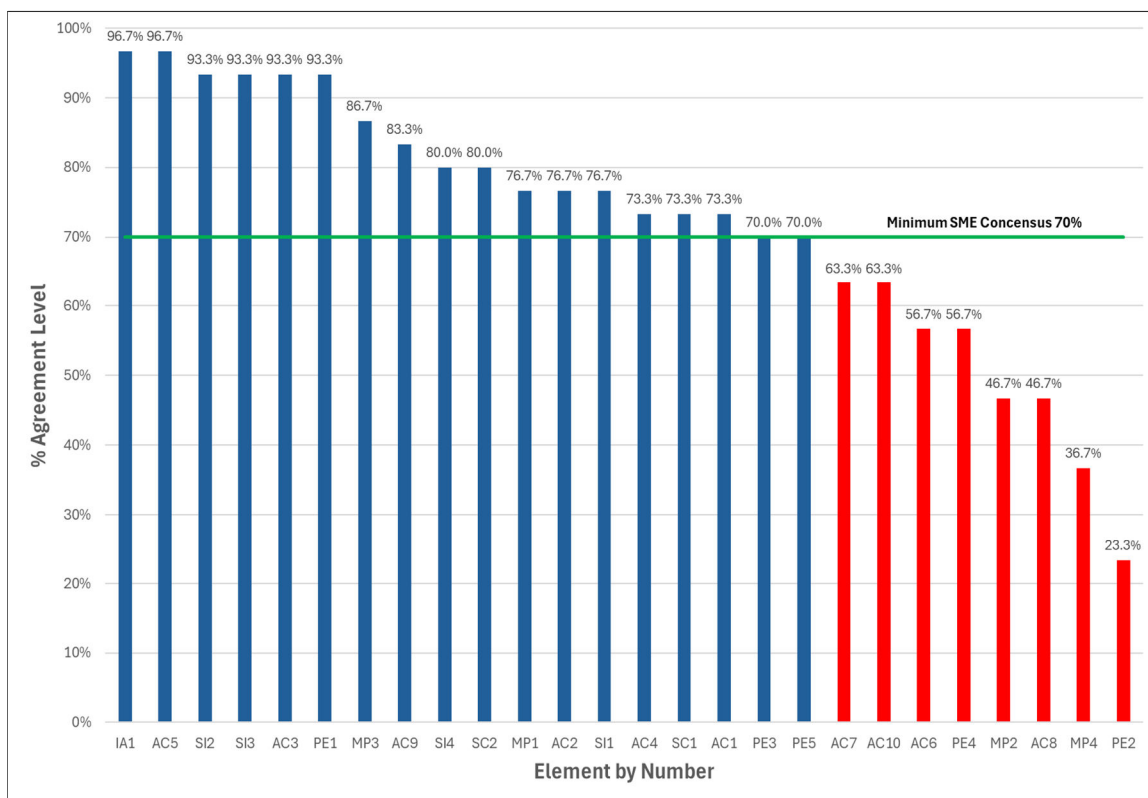


Figure 10 illustrates the percentage agreement for each of the elements based on responses of importance (ratings of 5, 6, or 7) from 30 SMEs, shown by element number. The minimum level of SME consensus was identified as 70%, resulting in 18 of 26 elements being agreed upon.

Figure 10

Proportion [in%] Agreement of Elements' Importance on the Cyber Posture of an Organization Toward the Potential Risk Exposure from Interconnected Entities (N=30)



The weights for each domain and element were calculated based on the SMEs' resulting importance levels. Table 29 outlines each element's association with a domain in a hierarchical structure and the weights. The elements below the minimum SME consensus of 70% were removed (AC6, AC7, AC8, AC10, MP2, MP4, PE2, and PE4) from the index and excluded from the weight calculations.

Table 29*Association of Domain Weights and Element Weights (N=30)*

Domain	Weight	ID	Weight
AC	0.181	AC1	0.155
		AC2	0.159
		AC3	0.173
		AC4	0.158
		AC5	0.184
		AC9	0.170
IA	0.177	IA1	1.000
MP	0.149	MP1	0.506
		MP3	0.494
PE	0.151	PE1	0.362
		PE3	0.331
		PE5	0.307
SC	0.170	SC1	0.493
		SC2	0.507
SI	0.172	SI1	0.222
		SI2	0.267
		SI3	0.260
		SI4	0.250

Note. Weights have been calculated after the exclusion of Elements.

Subsequently, in Phase 1, SMEs provided input for a proposed number for the high-end of the scale for each of the elements and attack surface variables (See Appendix B, questions E1.1 through F9.1). Table 30 depicts the standard deviation, median, mean, and

rounded value to establish the scales and options. SME responses for SC1 and SI4 revealed high selection variability, with high values indicating wide disparities and inconsistent selections. The MP1, PE1, and PE3 responses had very low variability, indicating consistent selections close to the median and mean values. Furthermore, AC3 had low variability and a close mean and median, indicating a balanced distribution with slightly more selections on the higher end. AC1 had a high standard deviation and a mean (2,429) higher than the median (1,500), suggesting a more comprehensive set of selections. Conversely, AC3 had a lower mean (24) and a low standard deviation (25), indicating a more stable and less variable set of selections. These insights allowed for understanding the selection distributions across the different elements, highlighting areas of consistency, variability, and central tendencies.

Table 30

Determination of Element Scale Intervals (N=30)

Element	Std. Dev.	Median	Mean (\bar{X})	Rounded \bar{X}	Interval
AC1	2,212	1,500	2,429	2,400	240
AC2	1,201	625	1,165	1,200	120
AC3	25	20	24	30	3
AC4	19	10	15	20	2
AC5	37	20	37	40	4
AC9	371	150	374	400	40
IA1	13	5	9	10	1
MP1	11	7	9	10	1
MP3	7	1	5	10	1

Element	Std. Dev.	Median	Mean (\bar{X})	Rounded \bar{X}	Interval
PE1	7	1	5	10	1
PE3	7	1	6	10	1
PE5	95	125	127	130	13
SC1	711,292	600,000	793,450	800,000	80,000
SC2	7	4	7	10	1
SI1	7	10	10	10	1
SI2	1,918	2,500	2,466	2,500	250
SI3	10	10	13	20	2
SI4	29,631	25,000	38,584	40,000	4,000
AS1	1,399	2,000	2,131	2,200	220
AS2	25	30	34	30	3
AS3	23	40	37	40	4
AS4	7	10	9	10	1
AS5	153	150	201	200	20
AS6	25	20	27	30	3
AS7	408	250	480	500	50
AS8	322	125	235	250	25
AS9	2,039	1,000	1,984	2,000	200

The Rounded \bar{X} values are divisible by 10 to establish an interval. For example, based on the values for AC1, the mean of 2,429 was rounded to 2,400, such that each selection option would be an interval of 240 with an attribute value in increments of 10. This is shown in Table 31.

Table 31

Example of Survey Selection Options and Values (N=30)

AC1 - Number of authorized users	
Selection Options	Values
1 – 240	10
241 – 480	20
481 – 720	30
721 – 960	40
961 – 1,200	50
1,201 – 1,440	60
1,441 – 1,680	70
1,681 – 1,920	80
1,921 – 2,160	90
2,161 or Greater	100

Phase 2 – Pilot Survey

The intent of Phase 2 was to engage manufacturing companies to solicit participation from interconnected entities in their supply chain to validate the CORE survey and the CFI-Mfg index model. Due to manufacturers' lack of interest and unwillingness to coordinate with their vendors and suppliers, six manufacturing companies participated in this phase, submitting survey responses on their behalf. The complete responses from the pilot group are gathered in Table 32. CORE Scores (66.9, 63.2, 32.3, 36.7, 66.4, and 66.0) for each pilot company have been calculated based on the association of the weights of the domains and the weight of the elements from Phase 1.

Table 32

Pilot Companies' CORE Score Survey Results (N=6)

Domains	Domain Weights	Elements	Element Weights	Pilot Company					
				1	2	3	4	5	6
AC	0.181	AC1	0.155	100	70	40	60	100	100
		AC2	0.159	100	100	90	100	100	100
		AC3	0.173	40	40	20	20	70	70
		AC4	0.158	50	60	20	20	20	80
		AC5	0.184	20	30	30	50	30	60
		AC9	0.170	100	100	10	30	100	10
IA	0.177	IA1	1.000	100	100	10	10	100	100
MP	0.149	MP1	0.506	100	100	10	10	10	10
		MP3	0.494	30	10	10	10	10	10
PE	0.151	PE1	0.362	10	10	10	10	100	10
		PE3	0.331	100	10	10	10	100	10
		PE5	0.307	50	60	20	80	40	100
SC	0.170	SC1	0.493	100	70	100	70	100	100
		SC2	0.507	20	10	10	10	50	100
SI	0.172	SI1	0.222	90	60	70	100	10	60
		SI2	0.267	100	80	40	60	100	100
		SI3	0.260	10	100	100	100	10	10
		SI4	0.250	20	100	60	60	100	100
			CORE Scores	66.9	63.2	32.3	36.7	66.4	66.0

CORE Score Calculation Assumptions

The CORE Scores are calculated based on the following assumptions:

- Each domain has a weight.

- Each domain consists of elements, and each element within a domain has its weight.
- The values provided for each company in the pilot group are multiplied by the element weights and then aggregated within each domain.
- The domain scores are then weighted by the domain weights to arrive at the CORE Score for each company.

Validation of CORE Scores

The CORE Score for each company in the pilot group was calculated with data provided from the surveys by repeatedly following detailed steps:

Step 1: Calculate Weighted Scores for Each Element

- For each element, multiply the element weight by the value for each company in the pilot group.

Step 2: Aggregate Weighted Scores by Domain

- For each domain, sum the weighted scores of its elements.

Step 3: Apply Domain Weights

- Multiply the aggregated domain scores by the domain weights and sum to get the CORE Score for each company in the pilot group.

Example Calculation for Pilot Company 1

For Pilot Company 1, starting with the AC domain, the weighted score is calculated for each element:

- $AC1 = 0.155 * 100 = 15.5$
- $AC2 = 0.159 * 100 = 15.9$
- $AC3 = 0.173 * 40 = 6.92$
- $AC4 = 0.158 * 50 = 7.9$

- $AC5 = 0.184 * 20 = 3.68$
- $AC9 = 0.170 * 100 = 17.0$

Followed by the sum of the weighted scores within the domain:

- $AC\ Score = 15.5 + 15.9 + 6.92 + 7.9 + 3.68 + 17.0 = 66.9$

Followed by the product of the domain weight:

- $Weighted\ AC\ Score = 66.9 * 0.181 = 12.1$

Repeating the steps for the IA, MP, PE, SC, and SI domains, the weighted scores are 17.7, 9.7, 7.9, 10.1, and 9.3, respectively. The CORE Score for the first company in the pilot group is calculated by aggregating the weighted scores across all domains. The consistently calculated CORE Score for each company in the pilot group through multiple trials indicates reliability, indicating the validity and reliability of the calculations and measurement procedures. Table 33 and Table 34 reflect the progression of the weighted element scores, domain scores, and resulting CORE Scores for each company in the pilot group.

Table 33

Pilot Companies' Summed Weighted Element Scores by Domain (N=6)

Pilot Company	Summed Weighted Element Scores by Domain					
	AC	IA	MP	PE	SC	SI
1	66.9	100.0	65.4	52.1	59.4	54.3
2	65.7	100.0	55.5	25.4	39.6	85.7
3	34.4	10.0	10.0	13.1	54.4	67.2
4	46.1	10.0	10.0	31.5	39.6	79.2

5	69.2	100.0	10.0	81.6	74.7	56.5
6	68.9	100.0	10.0	37.6	100.0	67.6

Table 34

Pilot Companies' Weighted Domain Scores and CORE Score (N=6)

Pilot Company	Domain Scores						CORE Score
	AC	IA	MP	PE	SC	SI	
1	12.1	17.7	9.7	7.9	10.1	9.3	66.9
2	11.9	17.7	8.3	3.8	6.7	14.7	63.2
3	6.2	1.8	1.5	2.0	9.2	11.6	32.3
4	8.3	1.8	1.5	4.8	6.7	13.6	36.7
5	12.5	17.7	1.5	12.3	12.7	9.7	66.4
6	12.5	17.7	1.5	5.7	17.0	11.6	66.0

Moreover, to further ensure reliability, a web-based prototype was developed to calculate CORE Scores. Based on the selection options for Pilot Company 1, the web-based form was submitted, and the resulting calculated CORE Score of 66.9 was displayed, as shown in Appendix H.

To address RQ4, three different CFI-Mfg Scores were devised based on the number of tiers, the number of entities in each tier, and their associated CORE Scores. This was conducted using the CORE Scores from the companies in the Pilot Group.

Pilot Companies' CFI-Mfg Score Calculation Assumptions

The CFI-Mfg Score is calculated based on the following assumptions:

- The tier % values depend on the index's number of tiers.

- The number in tier % values depend on the number of entities in the given tiers.
- The contribution % values are calculated as a % ratio based on the calculation of tier % multiplied by the number in tier %.
- The normalized value for the tier is based on the average of the calculated normalized values between 0 and 1.
- For each CORE Score (CS), find the minimum and maximum CORE Score and subtract the minimum CORE Score from the particular CORE Score, which shifts the value. Hence, the minimum value in the range becomes 0, such that the range (difference) between the maximum CORE Score and minimum CORE Score values becomes the denominator, resulting in a value between 0 and 1.
- The average of the calculated values is the tier's normalized value (NV):

$$NV_t = \sum_{(1-n)} ((CS - (CS)_{min}) / ((CS)_{max} - (CS)_{min})) / \text{Number of CS}$$

Calculating CFI-Mfg Score Based on One, Two, and Three Tiers

CFI-Mfg Scores were calculated with data provided by Pilot Companies' CORE Scores in one, two, and three tiers by repeating the following detailed steps:

Step 1: Apply the Tier % Based on the Number of Tiers

- If there is one tier in the index, tier 1 = 100%
- If there are two tiers in the index, tier 1 = 72.5% and tier 2 = 27.5%
- If there are 3 tiers in the index, tier 1 = 66.9%, tier 2 = 25.3%, and tier 3 = 7.8%

Step 2: Calculate the No. in Tier %

- For each tier, sum the number of entities divided by the total number of entities in all the tiers.

Step 3: Calculate the Contribution %

- For each tier, divide the product of tier % and num in tier % by the sum of the tier % and num in tier % for all the tiers.

Step 4: Calculate the Normalized Value for the Tier

- For each tier, calculate a normalized value, which is the average of each normalized value for each CORE Score based on the minimum CORE Score and the maximum CORE Score, calculating a range (difference) used to realize a value between 0 and 1.

Step 5: Calculate the CFI-Mfg Score

- Sum of the total products of each tier's normalized value and contribution %.

Example Calculation of CFI-Mfg Score with Pilot Companies in Two Tiers

The CFI-Mfg Score of 51.26, reflected in Table 36, is calculated by the following steps and calculations:

Step 1: Apply the Tier % Based on the Number of Tiers

- Given two tiers in this index model, the %s are 72.5% for tier 1 and 27.5% for tier 2.

Step 2: Calculate the No. in Tier %

- The total number of entities in the index model is six, with two in tier one and four in tier two; the respective No. in Tier % are 33.3% and 66.7%.

Step 3: Calculate the Contribution %

- For tier one, the contribution % is based on the product of the tier weight of 72.5% and the number in tier % of 33.3%, resulting in an interim value of 24.2%.
- For tier two the contribution % is based on the product of the tier weight of 27.5% and the number in tier % of 66.7% resulting in an interim value of 18.3%.
- Each of the interim values is divided by the sum of the interim values to calculate each tier's contribution %:
 - o Tier one contribution % = $24.2\% / 42.5\% = 56.9\%$
 - o Tier two contribution % = $18.3\% / 42.5\% = 43.1\%$

Step 4: Calculate the Normalized Value for each Tier

- For tier one, the average normalized values equal the sum of the normalized values divided by the total number of entities, calculated as $1 / 2 = 0.5000$
- For tier two, the average normalized values equal the sum of the normalized values divided by the total number of entities, calculated as $2.12 / 4 = 0.5293$

Step 5: Calculate the CFI-Mfg Score

- The resulting CFI-Mfg Score is 51.26 based on the sum of the products of 56.9% and 0.500 and 43.10% and 0.5293.

In Table 35, Table 36, and Table 37, the calculated example CFI-Mfg Scores are 66.33, 51.26, and 60.26, respectively, addressing RQ4.

Table 35

An Example CFI-Mfg Score with Pilot Companies in One Tier (N=6)

Tiers	Tier %	No. in Tier%	Contribution %	CORE Score	Normalized Value	CFI-Mfg Score
				66.9		
				63.2		
Tier 1	100.00%	100.00%	100.00%	32.3	0.6633	66.33
				36.7		
				66.4		
				66.0		

Table 36

An Example CFI-Mfg Score with Pilot Companies in Two Tiers (N=6)

Tiers	Tier %	No. in Tier%	Contribution %	CORE Score	Normalized Value	CFI-Mfg Score
Tier 1	72.53%	33.30%	56.90%	$\frac{66.9}{63.2}$	0.5000	
Tier 2	27.46%	66.70%	43.10%	$\frac{32.3}{36.7}$ $\frac{66.4}{66.0}$	0.5293	51.26

Table 37

An Example CFI-Mfg Score with Pilot Companies in Three Tiers (N=6)

Tiers	Tier %	No. in Tier%	Contribution %	CORE Score	Normalized Value	CFI-Mfg Score
Tier 1	66.88%	16.70%	47.50%	66.9	0.6690	
Tier 2	25.32%	33.30%	35.90%	$\frac{66.4}{32.3}$ $\frac{66.0}{36.7}$	0.5000	60.26
Tier 3	7.80%	50.00%	16.60%	$\frac{63.2}{36.7}$	0.6350	

In addition to the quantitative survey data collected, Table 38 depicts the feedback provided by the pilot companies for each survey question. The qualitative feedback is organized by survey questions and the corresponding corrective actions taken for the subsequent CORE survey instrument (Appendix D).

Table 38*Summary of Phase 2 Pilot Group Qualitative Results (N=6)*

Survey Question	Qualitative Feedback	Corrective Action
Number of authorized users (AC1).	<p>Consider specifying whether this refers to active or total users (including inactive accounts).</p> <p>Maybe define "authorized users" and what they are authorized to do. For example, can they access the company network, systems, and data?</p> <p>It should include employee and contractor/consultant access.</p>	Revised text to include [Consists of active accounts for employees, contractors, and consultants].
Number of authorized devices (AC2).	<p>Clarify whether this refers to active devices or total devices.</p> <p>Is this inclusive of all interconnected devices, including IoT?</p>	Revised text to include [Consists of end-user devices used by employees, contractors, and consultants].
Number of connections to external information systems (AC5).	<p>Ensure clarity in a "connection" to an external information system. It might be beneficial to specify whether this includes active and passive connections.</p> <p>Does this mean third-party connections? Is this limited to site-to-site VPN-type connections or any SaaS applications?</p>	Revised text to include [Consists of data flow in and out from systems your company does not manage].
Number of unsensitized or non-destroyed information systems media containing	<p>What media is being referred to? This needs clarification.</p>	Revised text by adjusting information systems media to media devices and included examples [information systems such

Survey Question	Qualitative Feedback	Corrective Action
Organizational Information before disposal or release for reuse (MP1).		as PCs, servers, storage devices, etc.]
Average number of non-licensed applications per employee on work assigned device (MP3).	Does non-licensed mean "using without paying - aka illegal," or "open source," which is technically licensed?	Revised text to include [not purchased by the company].
Number of provided TOOLS to protect from malicious code at appropriate locations within the organizational information systems (SI1).	You should specify the type of tools or what they do, for example, stop malicious code. Do you want to know the total number of security tools used?	Revised text to include [detect, prevent, deter, or stop].
Number of periodic scans of information systems per month (SI3).	Are you asking for vulnerability scans?	Revised text to include [periodic vulnerability and malware scans].
General	Statements would be better phrased as questions.	Revised text to rephrase all statements to questions.
General	What happens if we don't have a response because it is zero?	Revised text of scale in certain instances to start with 0.

Phase 3 - Quantitative Research

In Phase 3, 71 companies participated in the CORE Survey, resulting in a population of 57 companies (roughly 80.3%) supporting manufacturers and 14 companies (roughly 19.7%) supporting other companies in the manufacturing industry. Table 39 shows the

respective CORE Score for each company and its supply chain connection to manufacturing.

Table 39

Calculated Core Scores (N = 71)

Entity #	CORE Score	Mfg Vendor	Entity #	CORE Score	Mfg Vendor
1	54.9	Yes	33	61.2	Yes
2	56.8	Yes	34	35.9	Yes
3	49.1	No	35	37.3	Yes
4	44.8	No	36	50.5	Yes
5	46.5	Yes	37	42.9	Yes
6	30.8	Yes	38	63.4	Yes
7	30.4	Yes	39	66.4	Yes
8	60.4	Yes	40	34.5	No
9	37.9	Yes	41	53.2	Yes
10	65.9	Yes	42	29.9	Yes
11	59.5	Yes	43	44.5	Yes
12	31.4	Yes	44	59.0	Yes
13	28.7	No	45	28.9	Yes
14	41.5	Yes	46	53.6	Yes
15	54.8	Yes	47	29.1	No
16	48.8	Yes	48	38.3	Yes
17	26.3	Yes	49	75.2	Yes
18	43.7	Yes	50	42.7	Yes
19	60.2	Yes	51	44.4	No
20	60.8	No	52	24.7	Yes
21	36.2	Yes	53	32.6	Yes
22	32.5	Yes	54	54.0	Yes
23	35.5	No	55	63.2	Yes
24	32.5	No	56	50.0	Yes
25	38.6	Yes	57	65.3	Yes
26	17.5	Yes	58	27.4	Yes
27	39.2	No	59	41.6	Yes
28	48.1	Yes	60	52.3	No
29	29.5	Yes	61	61.2	Yes
30	66.3	Yes	62	25.6	No
31	45.5	Yes	63	27.5	Yes
32	32.1	Yes	64	55.3	No

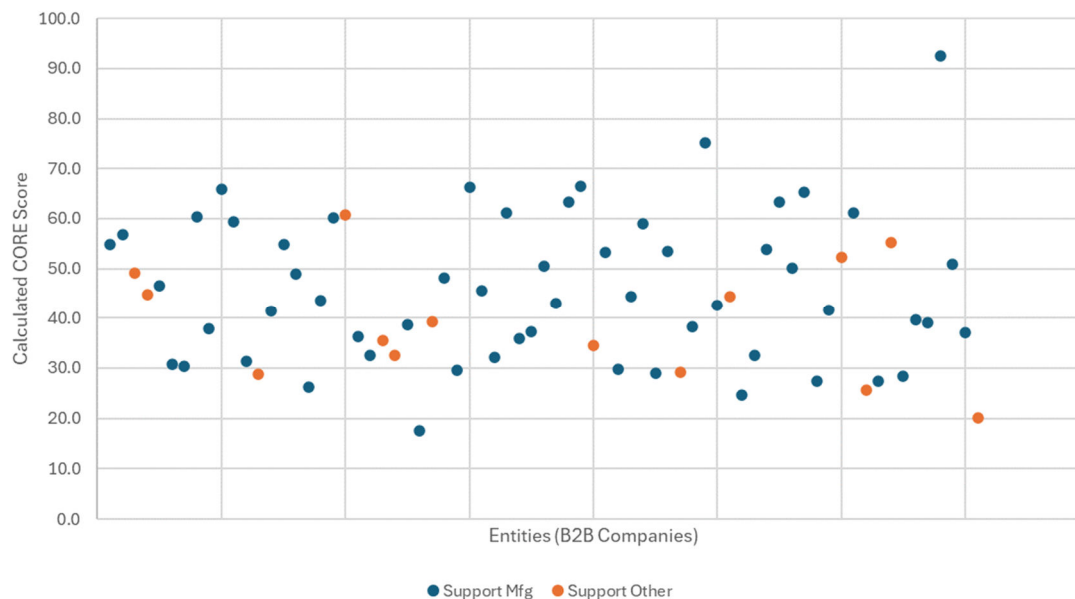
Entity #	CORE Score	Mfg Vendor	Entity #	CORE Score	Mfg Vendor
65	28.4	Yes	69	51.0	Yes
66	39.7	Yes	70	37.2	Yes
67	39.0	Yes	71	20.1	No
68	92.5	Yes			

The CORE Scores of each participating company are graphed on a scatter plot in Figure 11. This chart illustrates the range of values from 17.53 to 92.50, with a mean of 44.59 and a standard deviation of 14.50. The CORE Scores are delineated by companies supporting manufacturers and other companies in the manufacturing industry. As shown in Table 40, the mean of the CORE Scores for those supporting other companies was lower than those supporting manufacturing companies, respectively, with 39.42 versus 45.86. Likewise, the standard deviation was also lower for those supporting other companies than those supporting manufacturing companies, respectively, with 12.08 versus 14.85. This was attributed to a range of 74.97 between the lowest and highest CORE Scores for companies supporting manufacturing. The mean and standard deviations of CORE Scores by type of entity is illustrated in Figure 12.

There was a higher mean and variability among the companies that support manufacturers than those that support other companies in the manufacturing industry. The sample size of those that support manufacturers (57) versus those that support other companies in the manufacturing industry (14) had a significant impact on the statistical measure, such that the estimates are generally more stable for those that support manufacturers due to the larger sample. The two datasets are not used to compare CORE Scores or CFI-Mfg Scores since these differences can influence the statistical tests.

Figure 11

Scatter Plot of CORE Scores (N=71)

**Table 40**

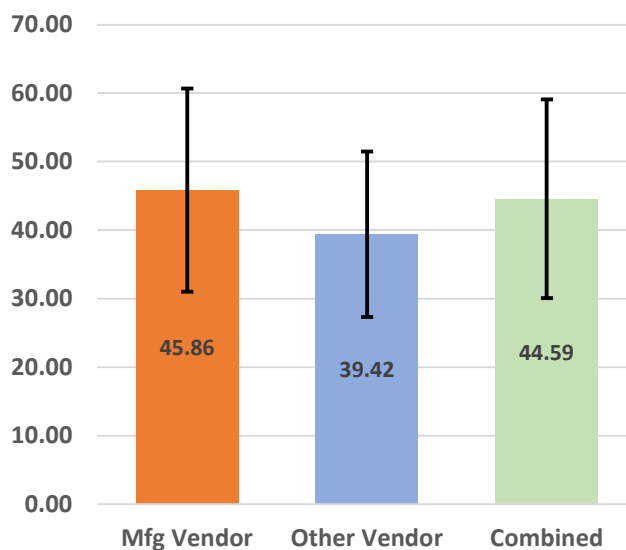
Descriptive Statistics of Calculated CORE Scores (N=71)

Statistic	Mfg Vendor	Other Vendor	Combined
Mean	45.86	39.42	44.59
Standard Error	1.96	3.23	1.72
Median	43.67	37.36	42.95
Standard Deviation	14.85	12.08	14.50
Sample Variance	220.50	145.88	210.14
Skewness	0.56	0.22	0.57
Range	74.97	40.75	74.97
Minimum	17.53	20.09	17.53
Maximum	92.50	60.84	92.50
Sum	2614.19	552.0	3166.19
Count	57	14	71
Largest(1)	92.50	60.84	92.50
Smallest(1)	17.53	20.09	17.53

Statistic	Mfg Vendor	Other Vendor	Combined
Confidence Level (95.0%)	3.94	6.97	3.431

Figure 12

Mean and Standard Deviations of CORE Scores by Type of Entity (N=71)



To further the quantitative research, organizations listed by Org No. were structured with varying numbers of entities in each of the tiers of the CFI-Mfg index model, as shown in Table 41. For example, the first three organizations have 30, 38, and 29 entities in their respective CFI-Mfg index models. The list consists of organizations with indexes of two tiers and three tiers of entities. Each organization's number of entities and respective CORE Score is used to calculate the resulting CFI-Mfg used in subsequent analysis.

Table 41*Summary of Tiers, Entities, and CFI-Mfg by Org No. (N=60)*

Org No.	Tier 1	Tier 2	Tier 3	Total Entities	No. of Tiers	CFI-Mfg
1	7	23	0	30	2	47.30
2	8	30	0	38	2	36.00
3	5	24	0	29	2	51.63
4	10	40	0	50	2	47.88
5	8	40	0	48	2	40.88
6	10	50	0	60	2	44.63
7	6	19	0	25	2	64.60
8	7	29	0	36	2	45.20
9	6	22	0	28	2	46.51
10	7	25	0	32	2	53.42
11	8	34	0	42	2	41.78
12	7	27	0	34	2	46.28
13	8	24	0	32	2	39.00
14	9	32	0	41	2	49.99
15	10	44	0	54	2	37.33
16	6	18	0	24	2	30.22
17	5	22	0	27	2	52.78
18	9	37	0	46	2	44.31
19	7	32	0	39	2	40.01
20	9	28	0	37	2	46.82
21	6	26	0	32	2	50.76
22	10	39	0	49	2	47.99
23	9	41	0	50	2	37.21
24	5	18	0	23	2	49.60
25	9	33	0	42	2	35.88
26	6	28	0	34	2	40.36
27	7	21	0	28	2	48.13
28	9	43	0	52	2	41.90
29	9	41	0	50	2	42.06
30	9	32	0	41	2	52.01
31	10	17	22	49	3	53.99
32	10	29	11	50	3	43.40
33	10	40	20	70	3	55.01
34	10	16	30	56	3	46.56

Org No.	Tier 1	Tier 2	Tier 3	Total Entities	No. of Tiers	CFI-Mfg
35	8	36	22	66	3	49.58
36	8	15	41	64	3	51.69
37	5	24	41	70	3	50.81
38	9	25	27	61	3	43.98
39	8	19	43	70	3	38.15
40	8	22	32	62	3	51.25
41	9	23	34	66	3	45.00
42	8	17	12	37	3	46.14
43	9	33	18	60	3	45.29
44	10	38	22	70	3	43.17
45	10	25	35	70	3	46.64
46	5	16	43	64	3	40.52
47	6	27	29	62	3	37.27
48	10	23	33	66	3	41.98
49	5	15	28	48	3	43.70
50	7	21	16	44	3	39.78
51	6	16	40	62	3	35.85
52	5	15	47	67	3	41.57
53	10	25	35	70	3	40.32
54	10	22	36	68	3	48.92
55	7	26	26	59	3	48.12
56	5	18	45	68	3	43.93
57	10	37	23	70	3	36.63
58	7	22	34	63	3	46.07
59	8	18	38	64	3	44.18
60	10	41	20	71	3	43.09

Table 42

Descriptive Statistics of CFI-Mfg Scores (N=60)

Statistics	All Tiers	2 Tiers	3 Tiers
Mean	44.92	45.08	44.75
Standard Error	0.76	1.25	0.91
Median	44.82	45.74	44.08
Standard Deviation	5.93	6.84	4.96
Sample Variance	35.17	46.83	24.66

Statistics	All Tiers	2 Tiers	3 Tiers
Skewness	0.35	0.37	0.19
Range	34.38	34.38	19.16
Minimum	30.22	30.22	35.85
Maximum	64.6	64.6	55.01
Sum	2695.06	1352.47	1342.59
Count	60	30	30
Largest(1)	64.6	64.6	55.01
Smallest(1)	30.22	30.22	35.85
Confidence Level (95.0%)	1.53	2.56	1.85

Figure 13

Mean and Standard Deviations of CFI-Mfg Scores (N=60)

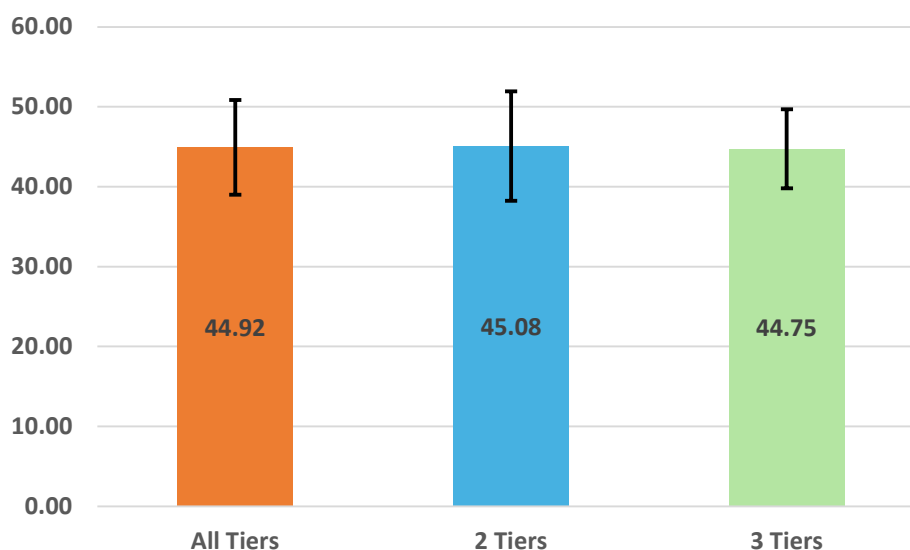


Table 42 indicates the descriptive statistics for the CFI-Mfg scores across all tiers and separately for two and three tiers. The CFI-Mfg mean scores are similar across all the tiers, with 44.92 for all tiers, 45.08 for two tiers, and 44.75 for three tiers. However, the standard deviation for CFI-Mfg of two tiers was 6.84 compared to 4.96 for CFI-Mfg of three tiers. The range of CFI-Mfg scores for two tiers was 34.38 compared to 19.16 for

three tiers. These differences in variability and range indicate that while the average scores are similar, the distribution of scores differs between the tiers, with two tiers having a wider spread of scores. Figure 13 illustrates the comparison of the mean and standard deviation of CFI-Mfg Scores.

Quantitative Analysis of the Number of Interconnected Suppliers/Vendors

To address RQ5, further analysis was conducted to determine whether there is a statistically significant mean difference in CFI-Mfg Scores based on the number of entities (also referred to as interconnected suppliers/vendors).

Table 43

ANOVA Results for the Number of Entities (N=60)

	Sum of Squares (SS)	Degrees of Freedom (df)	Mean Square (MS)	<i>F</i>	<i>p</i> -value	<i>F</i> -crit
Between Groups	1287.819	32	40.244	1.381	0.198	1.827
Within Groups	787.051	27	29.150			
Total	2074.870	59				

Using one-way ANOVA with the CFI-Mfg Scores for the number of entities, the calculated *p*-value was 0.198, more significant than 0.05. This means there is no statistically significant difference in the CFI-Mfg scores based on the number of entities. The *F* statistics indicated that *F* (1.381) was lower than the *F*-critical value (1.827), supporting this conclusion in answering RQ5.

Quantitative Analysis of the Number of Tiers of Suppliers/Vendors

To address RQ6, further analysis was conducted to determine whether there is a statistically significant mean difference in CFI-Mfg Scores based on the number of tiers. The CFI-Mfg scores for 60 organizations were calculated for an index with two or three tiers, shown in Table 43. The range of the CFI-Mfg Scores differed from two tiers to three tiers, respectively, with 34.38 and 19.16. The mean and standard deviation of the CFI-Mfg for the two tiers were 45.08 and 1.25, while the mean and standard deviation of the CFI-Mfg for the three tiers were 44.75 and 0.91, respectively. This indicated that the variability in CFI-Mfg scores is more significant for two than three tiers. The higher standard deviation for the two tiers indicated that the CFI-Mfg scores are more spread out from the mean, while the CFI-Mfg scores are closer to the mean for the three tiers. The variability between the CFI-Mfg of two and three tiers is notably different, with less consistency for two and more consistency for three. ANOVA results for two tiers and three tiers of CFI-Mfg scores are shown in Table 44.

Table 44

ANOVA Results for Two Tiers and Three Tiers of CFI-Mfg Scores (N=60)

	Sum of Squares (SS)	Degrees of Freedom (df)	Mean Square (MS)	<i>F</i>	<i>p</i> -value	<i>F</i> -crit
Between Groups	1.627	1	1.627	0.046	0.832	4.006
Within Groups	2073.243	58	35.746			
Total	2074.870	59				

Using one-way ANOVA with the CFI-Mfg Scores for the number of tiers, the calculated p -value was 0.832, more significant than 0.05. This means there is no statistically significant difference in the CFI-Mfg scores based on the number of tiers. Additionally, the F statistics indicated that the F (0.046) was extremely low and smaller than the F -crit (4.006), which also supports this conclusion to answer RQ6.

Quantitative Analysis of the Attack Surfaces

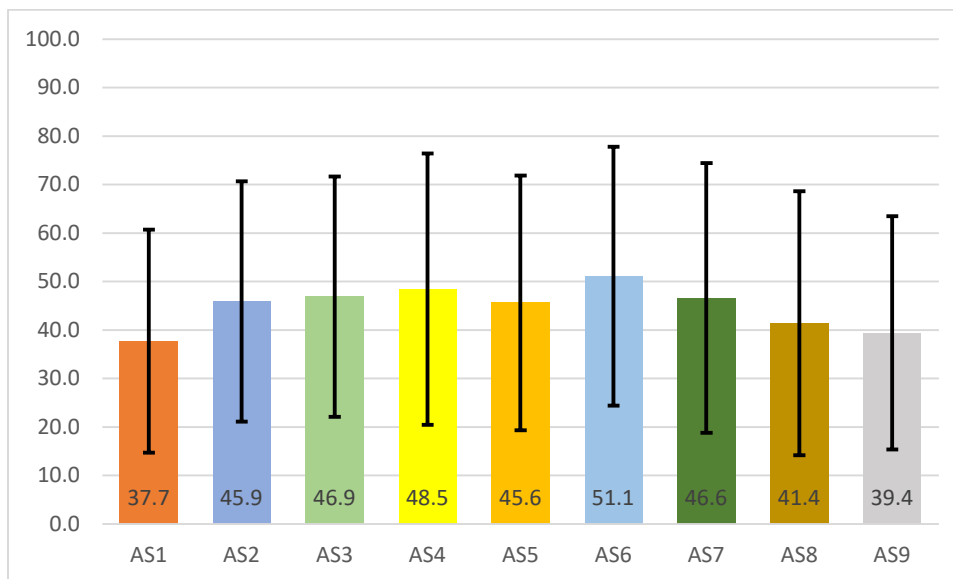
To address RQ7, further analysis was conducted to determine whether there is a statistically significant mean difference in CFI-Mfg Scores based on the attack surfaces of entities. The survey responses for attack surfaces were translated to values between 10 and 100, respectively, of the scale options (Appendix D, questions 19 through 27). Based on the descriptive statistics shown in Table 45, AS6 had the highest mean score, 51.13, while AS1 had the lowest mean score, 37.75. Furthermore, AS4 had the highest standard deviation of 27.96, indicating that this attack surface had the most variability. AS1 had the lowest standard deviation of 23.00, indicating that this attack surface had the most minor score variability. The data suggested that the variability in scores for attack surfaces is somewhat consistent across the entities, as the standard deviations are relatively similar. However, AS9 does not follow the same pattern, such that AS9 had a mean of 39.44 with a high standard deviation of 24.08, suggesting a wide range of scores despite the lower average. Figure 14 illustrates the comparison of mean and standard deviation of attack survey responses.

Table 45*Descriptive Statistics of Attack Surface Survey Responses (N=71)*

Statistic	AS1	AS2	AS3	AS4	AS5	AS6	AS7	AS8	AS9
Mean	37.75	45.92	46.90	48.45	45.63	51.13	46.62	41.41	39.44
Standard Error	2.73	2.94	2.94	3.32	3.12	3.17	3.30	3.23	2.86
Median	30	50	50	50	50	50	50	40	30
Mode	50	50	60	50	50	40	50	10	30
Standard Deviation	23.00	24.76	24.76	27.96	26.28	26.70	27.82	27.22	24.08
Sample Variance	529.1	613.1	613.1	781.9	690.7	713.0	774.1	740.8	579.7
Range	90	90	90	90	90	90	90	90	90
Minimum	10	10	10	10	10	10	10	10	10
Maximum	100	100	100	100	100	100	100	100	100
Sum	2680	3260	3330	3440	3240	3630	3310	2940	2800
Count	71	71	71	71	71	71	71	71	71
Largest(1)	100	100	100	100	100	100	100	100	100
Smallest(1)	10	10	10	10	10	10	10	10	10
Confidence Level (95.0%)	5.44	5.86	5.86	6.62	6.22	6.32	6.59	6.44	5.70

Figure 14

Mean and Standard Deviation of Attack Surface Survey Responses (N=71)



Individual one-way ANOVA tests were conducted for each attack surface variable, the results of which are summarized in Table 46.

Table 46

ANOVA Results for CFI-Mfg and Individual Attack Surface Variables (N=60)

	Sum of Squares (SS)	Degrees of Freedom (df)	Mean Square (MS)	<i>F</i>	<i>p</i> -value	<i>F</i> -crit
AS1	1961.468	51	38.460	2.713	0.068	3.019
AS2	1237.869	51	24.272	0.232	0.999	3.019
AS3	1789.484	49	36.520	1.280	0.354	2.639
AS4	1997.103	54	36.983	2.378	0.168	4.438
AS5	1997.442	56	35.669	1.382	0.458	8.575

	Sum of Squares (SS)	Degrees of Freedom (df)	Mean Square (MS)	<i>F</i>	<i>p</i> -value	<i>F</i> -crit
AS6	1932.877	54	35.794	1.260	0.441	4.438
AS7	1970.084	53	37.171	2.128	0.172	3.749
AS8	1583.758	51	31.054	0.506	0.932	3.019
AS9	1745.253	55	31.732	0.385	0.954	5.693

Using one-way ANOVA for each of the attack surface survey responses individually and the CFI-Mfg Scores, shown in Table 46, the *p*-value for all AS variables is more significant than 0.05. This means no statistically significant difference exists in the CFI-Mfg mean scores for the individual attack surface responses. Additionally, for the *F* statistics, each *F* was low and smaller than the respective *F*-crit values, supporting this conclusion to answer RQ7 for each attack surface.

Summary

Phase 1 of this research study involved surveying 30 SMEs with cybersecurity experience to gather valuable insights toward developing a CFI-Mfg index to assess the organization's cyber posture. Using a survey instrument ensured the anonymity of the participants, which is a critical aspect of preventing bias and ensuring equal participation (Hallowell & Gambatese, 2010; Taylor, 2020). The goal of Phase 1 was to address the research questions: (1) determining the number of supply chain tiers to include in the

index for assessment, (2) establishing the weights of these tiers, (3) as well as the weights of domains and elements.

This research progressed through two subsequent phases to gain reliable insights from manufacturing companies and B2B companies. Developmental research provides reliable and valuable information to practitioners through a systematic approach to evaluate tools, processes, and models (Richey & Klein, 2005). Phase 2 involved the participation of six manufacturing companies in a pilot of the CORE survey, which collected data and calculated a risk exposure score based on the previously established weights in Phase 1. As a result of Phase 2, the CORE Score survey instrument and index model were validated and refined.

Phase 3 utilized the finalized CORE Score survey instrument to conduct a quantitative empirical study involving 71 small to medium-sized B2B companies. This phase concluded with calculating 60 CFI-Mfg Scores based on varying numbers of entities for two and three tiers in the index model. The study concluded with detailed data analysis identifying whether there were statistically significant mean differences in the CFI-Mfg Scores based on factors such as the number of interconnected entities, number of tiers, and aspects of the attack surface. This research showed that while there was variability among the independent variables, represented by the number of entities, the number of tiers, and the attack surfaces, there were no statistically significant mean differences with the dependent variable of CFI-Mfg scores.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

Cybersecurity vulnerabilities are a significant concern for businesses utilizing interconnected technologies to remain competitive in today's marketplace. Manufacturing companies, in particular, depend heavily on third-party service providers, making protection against successful cybersecurity attacks crucial to prevent various losses. For example, such losses include deterioration of product/production qualities, damage to brand reputations, impacts on sales revenues, and jeopardy of human lives (Syed et al., 2022; Ani et al., 2017). In response to this problem, the primary objective of this research study was to design, develop, and validate a Cybersecurity Footprint Index for Manufacturing (CFI-Mfg) to assess organizations' cybersecurity posture through the input of interconnected vendors and suppliers.

The key findings of this research include the establishment of weights for tiers, domains, and elements, which addressed the first three research questions in Phase 1. SMEs played a vital role in developing these weights and survey scale options. The index was subsequently validated with a pilot group, providing data to ensure the reliability of the CORE Score and the index model. A web-based prototype was created to calculate CORE Scores, offering an additional quantification method for validation in Phase 2.

The final phase of the study involved 71 businesses completing the CORE Survey, which provided data for calculating CFI-Mfg scores and analyzing the statistical significance of the differences between means. Data analysis using one-way ANOVA in this phase indicated that the number of tiers, entities, and attack surface variables did not appear to influence organizations' CFI-Mfg scores. The statistical significance of the means was determined by p -values greater than 0.05 and the F statistics, which supported a conclusion of insignificance for each of the final research questions, respectively: RQ5, RQ6, and RQ7.

Moreover, the results of this research study suggest a contradiction to the number of tiers and weights of the tiers provided by the SMEs for the index model. In this regard, higher levels of importance were placed on tiers closer to the originating organization with respect to cyber risk exposure. However, the insignificance of the mean differences based on two and three tiers implies lesser importance and that an entity anywhere in the supply chain, regardless of tier position, would not influence an organization's calculated CFI-Mfg Score.

Levy and Gafni (2021) noted an organization can adjust its cybersecurity footprint through active and passive actions. An example of an active action is an entity reducing the number of devices or users within their organization. Passive actions are the result of actions performed by an external entity or several interconnected entities that can have positive and negative implications on an organization. While Levy and Gafni (2021) claimed passive actions would change the size of the entity's cybersecurity footprint, this research study found the insignificance of the means based on the number of entities

implies the calculated CFI-Mfg Score of an organization would not be influenced, regardless of the number of entities in the cybersecurity footprint.

Implications

The findings of this study have significant implications for cybersecurity practices in the manufacturing industry concerning interconnected entities and supply chains. By examining the significance between CFI-Mfg scores and factors such as the number of tiers, the number of interconnected suppliers/vendors, and attack surfaces, a better understanding is gained regarding the extent to which manufacturing companies should assess cyber posture within their supply chain. Literature indicates a quantifiable index based on CMMC and associated weights for domains and elements was previously unavailable. This research study contributed to the cybersecurity body of knowledge by developing an index based on CMMC to measure the cyber posture of manufacturing organizations. A methodological approach has been confirmed for data collection, establishing SME weights for domains and elements, and formulating calculations for quantifying cyber posture. This research study's methodology for creating a Cybersecurity Footprint Index can be applied to manufacturing, other industries, and critical infrastructure sectors. Moreover, other implications include stressing the importance of risk management, conducting cyber posture benchmarking, improving communications, and allocating resources effectively. By calculating CORE Scores of interconnected entities, organizations can determine and compare numeric representations of cyber posture within their supply chain. This ensures consistency and

reliability when evaluating the cybersecurity posture of different entities within the supply chain. Organizations can identify strengths and weaknesses in their practices by benchmarking and comparing cyber posture against potential peer standards. Clear measures of cybersecurity posture could enable organizations to adhere more easily to regulatory and industry standards.

The validated and proven CORE Score instrument provides a brief and straightforward survey, adaptable to the unique needs of different industries, unlike an extensive assessment questionnaire that is difficult to compare across entities in the supply chain. This adaptability ensures that organizations can evaluate their cybersecurity protection mechanisms, fostering meaningful discussions about cyber posture. With visibility into their supply chain's cyber posture, organizations can prioritize and allocate resources effectively, identifying the areas within the supply chain that require the most attention and improvement.

A measurable index could strengthen business relationships among trusted supply chain partners by demonstrating a strong cybersecurity posture. This index, providing quantifiable and clear measures, fosters better communication and a sense of shared responsibility among supply chain partners about cybersecurity expectations, requirements, and performance. It encourages the implementation of proactive risk management and mitigation strategies based on the potential vulnerabilities and risks identified in the supply chain.

Organizations will have concrete data with which to make improved and informed decisions about cybersecurity performance, strategic planning, and investments.

Investments can be effectively targeted toward specific areas of weakness to reduce costs associated with breaches and non-compliance. Lastly, measurements can provide a baseline for continuous monitoring and improvement of cybersecurity practices, ensuring organizations adapt to evolving threats and maintain a robust security posture.

Recommendations and Future Research

This research study developed a method and survey instruments to create an index for measuring the cyber posture of manufacturing companies. As discussed, the approach can be applied to other industries and critical infrastructure sectors by establishing weights for domains and elements, leading to other Cybersecurity Framework Indices (CFI). Additionally, these CFIs can be used for benchmarking within and across different industries. As with all research, this study presents opportunities for further refinement. Specifically, the first would be to assess the domains and elements used in this study to determine their relevance and applicability to other industries. This will help understand whether the framework can be generalized or needs industry-specific adjustments. The second is to develop and implement industry-specific scales for the CORE Score survey, tailored to various business types (e.g., NAIC codes) or other relevant criteria. This alignment will enhance the survey's relevance to different industries. The third is to evaluate maturity levels and corresponding scores based on the CMMC framework rather than relying solely on numerical scores. This approach may provide a more nuanced assessment of cyber posture. The fourth is to explore alternative cybersecurity frameworks beyond CMMC to determine if they offer better alignment or additional

insights for evaluating cyber posture. The fifth is to study broader aspects of the attack surface beyond those covered in this research to understand potential vulnerabilities and threats better. The sixth is to determine whether other factors, such as business type or geography, influence the CFI-Mfg to assess their impact on the index. The seventh should focus on refining the survey instruments, enhancing scales, and incorporating additional criteria beyond the current domains and elements. Lastly, the eighth would be to develop a more precise benchmarking scale that extends beyond a simple 0 to 100 range. A refined scale could offer more detailed insights and improve the accuracy of the benchmarking process.

Summary

Significant challenges were encountered while conducting this research study. In Phase 1, information security leaders were contacted via LinkedIn, Email, or phone. With a target list of more than 90 security leaders in the manufacturing industry, multiple email requests for research participation as an SME or an organization resulted in no responses. Nevertheless, through direct personal networking and contacts, Phase 1 engaged 30 SMEs; however, Phase 2 faced difficulties due to limited interest and commitment from manufacturing companies to participate and coordinate with entities in their supply chain. Although several engaging conversations occurred with manufacturing associations and manufacturers, a considerable and consistent lack of interest remained. Some claimed the sensitivity of the information requested even though the responses would have been anonymous, unidentifiable, and general.

There was apparent naivety and ignorance across many of the manufacturing organizations and associations. While offering free cybersecurity training in return for research participation, a contact responsible for the IT sector of a manufacturing association stated, “Companies don’t know and don’t want to know. They don’t have the financial and personnel resources to address cybersecurity”. This particular response suggested a potential position of deniability if a cyber incident were to occur. Furthermore, more than a dozen manufacturing associations were contacted. They were provided with a one-page overview explaining this research study and several review meetings for those interested. However, with continued follow-up to confirm their willingness to participate, there was either no response or they were uninterested. Likewise, several contacts of manufacturing associations expressed a lack of interest from members due to limited time, claiming to have already the means to assess third parties or voiced a general disdain for research.

Additional associations with compliance and regulatory company members focused on information security were also contacted, but no responses were received. The associations were offered a webinar on issues with cybersecurity in manufacturing and free training for their employees. Some of these organizations were extensions of NIST and chapters of InfraGard. Manufacturing companies that initially responded with interest ultimately did not follow through after several follow-ups.

Reviewing manufacturing associations and the programs they promote on their websites, many include opportunities for networking, sharing solutions, business referrals, sales opportunities, peer groups, and round tables. Furthermore, several other

areas include education, training, and workforce development, as well as receiving legislative support, economic growth, and aligning with standards and regulatory requirements. The information available on the websites for cybersecurity is limited to disaster recovery, business continuity, data protection, endpoint protection, and cybersecurity services. Of the manufacturing association websites reviewed, there was a lack of information concerning supply chain and third-party cybersecurity management.

Through personal connections and continued follow-ups, 30 SMEs participated in Phase 1 of this research; likewise, through personal connections with individuals in manufacturing, six distinct manufacturing companies participated in Phase 2 to provide feedback on the survey instrument, input to calculate CORE Scores and test the reliability of the index model. For Phase 3, more than 70 B2B companies were sourced through strong client relationships of a few key individuals (with specific roles and titles of Owner and Partner) in the information security consulting industry. The request to participate in a research study for a better understanding of the cybersecurity field was met with significant challenges by a population that has been shown to require it considerably.

By leveraging a standard framework CMMC 2.0 Level 1 regarding cyber hygiene, a quantifiable method is used to quantify cyber posture among organizations. An empirical assessment of the Cybersecurity Footprint of an organization can provide valuable insight into the cyber risk exposure of their supply chain. Such an understanding can provide valuable visibility into the interconnected relationship with third parties. This research study added to the cybersecurity body of knowledge by developing and validating an

index to measure the cyber posture of manufacturing organizations. Moreover, this research study provided the basis, background, and means necessary to establish a CFI for other industries.

First, this study took the initial set of CMMC 2.0 Level 1 domains and elements from Levy and Gafni (2020) as input to the study. Based on a thorough literature review, it was clear that manufacturing has been a targeted industry, seen by detailed evidence of impacts, compromise, and data breaches from third parties within the supply chain. The main goal of this research study was to develop a quantifiable index to measure the cyber posture of manufacturing organizations. This research study set seven specific RQs to be addressed through a multi-phased approach to achieve the primary goal.

In Phase 1, this study used a group of cybersecurity SMEs to answer the initial three research questions:

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?

To capture the SMEs' input, an anonymous online survey was used to determine the number of tiers, the associated level of importance for the tiers, and the level of importance of the domains and elements. The first research question was answered by

SME consensus, resulting in all six domains being important, 18 of the 26 elements, and the use of central tendency to establish the number of tiers and their associated weights. Additionally, SMEs provided survey responses to establish survey scales based on central tendencies and qualitative feedback.

Phase 2 of this research study used a pilot group of key IT contacts from manufacturing companies to assist in answering the fourth research question:

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

In Phase 2, using an anonymous online survey, also known as a draft CORE Survey, the key IT contacts responded to the survey on behalf of their company. The data collected from the surveys was used to calculate six distinct and individual CORE Scores and confirm the approach and calculations toward an overall CFI-Mfg score, thus answering the fourth research question. Additionally, the SMEs provided qualitative feedback to the overall survey, which modified several questions to clarify the CORE Survey for Phase 3.

Phase 3 of this research study included companies that provide products or services to manufacturing companies or other companies in B2B relationships. This modification among the participants' relationships was not directly interconnected with each other, and the originating organization was required due to the lack of commitment and interest by manufacturing companies. Nonetheless, this group of B2B companies was used to answer the fifth, sixth, and seventh research questions:

- 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 mobile devices, (h) number of IoT devices, and (i) number of employees.

Using one-way ANOVA in Phase 3, research questions five and six were answered. This research found no significant mean difference between the number of tiers on the CFI-Mfg nor significant mean differences in the number of entities in each tier. Likewise, there were no significant mean differences on the CFI-Mfg for the seventh and final question, using one-way ANOVA for each of the individual attack surfaces.

This research study had several limitations surrounding participation beyond the SMEs for manufacturing companies. Although numerous manufacturing associations existed, finding interested and engaging participants was improbable and practically impossible. Efforts to work through central organizations, such as the NIST Manufacturing Extension Partnership (MEP), yielded limited success due to restricted pass-through capabilities. The second limitation was the narrow outreach scope that limited the participant pool's breadth. The third limitation was the inability to establish

genuine relationships among the businesses, necessitating the calculation of CFI-Mfg based on the composition of CORE Scores.

To mitigate these limitations, data collection focused on companies with B2B interactions to calculate CORE Scores and CFI-Mfg Scores. Survey instruments were progressively shortened to enhance commitment and accuracy, as some SMEs initially provided responses based on estimates rather than firsthand knowledge. Additionally, misunderstood questions were excluded from the analysis to maintain data integrity. CFI-Mfg scores were calculated based on data collected from B2B companies when interconnected entities were unavailable for data collection.

Despite these challenges, this research study made significant contributions to the field of cybersecurity and the body of knowledge. It resulted in the development and validation of measures for domains, elements, and tiers, with input from SMEs guiding the elimination of less important elements. This study also established specific weights for these domains, elements, and tiers tailored to the manufacturing industry, leading to the creation of the CFI-Mfg index model. The study found no significant mean difference between the number of tiers, the number of entities, or attack surfaces on the CFI-Mfg. This confirms that the CFI-Mfg of an organization can be quantified without considering the weights of tiers, relying instead on the normalization of CORE Scores from entities within the supply chain. Moreover, other industries can benefit from the methodology and findings presented in this research. This research can be applied to critical infrastructure sectors, including the Defense Industrial Base (DIB) and any company that

relies on supply chains and suppliers. Organizations can quantify and improve their cyber posture by learning from the challenges faced and following the outlined methodology.

Appendix A

CMMC 2.0 – Level Domains and Cybersecurity Footprint Elements

Domain	Description	Elements
AC - Access Control	Applies to both physical and logical assets, only allowing access based upon regular review and assessment of authorized access based on role, identity, and privileges controlled through systems where appropriate.	<ul style="list-style-type: none"> - Number of authorized users. - Number of authorized devices. - Number of information system access to the types of transactions and functions that authorized users are permitted to execute. - Number of transactions and functions that authorized users are permitted to execute for each type of information classification level. - Number of connections to external information systems. - Volume of using external information systems connections. - Volume of information posted or processed on publicly accessible information systems. - Number of employees. - Number of Bring Your Own Device (BYOD) devices connected to the organizational network. - Average number of BYOD device applications per employee.
IA – Identification and Authentication	Users are to be uniquely and genuinely identified and authenticated prior to accessing a system or application in order for systems to remain secure.	<ul style="list-style-type: none"> - Number of individuals sharing the same user credentials, and/or devices.

Domain	Description	Elements
MP – Media Protection	Data and intellectual property (IP) are important for the organization in the form of contracts, personnel records, designs, manufacturing instructions, applications, sales, invoices, procurement and finance records, with are to be identified, marked appropriately and secured throughout the life cycle of its use.	<ul style="list-style-type: none"> - Number of unsensitized or non-destroyed information system media containing organizational information before disposal or release for reuse. - Volume of data in the information systems. - Average number of non-licensed applications per employee on work assigned devices. - Average number of social media accounts per employee
PE – Physical Protection	Physical and logical protection are linked. In order to protect technical assets, there needs to physical security measures to prevent unauthorized users from gaining access to areas within an organization they are not authorized to access to ensure unauthorized persons are unable to damage, destroy or steal assets.	<ul style="list-style-type: none"> - Number of devices with physical access to non-authorized individuals. - Number of escorted visitors per month. - Number of non-escorted visitors per month. - Volume of logs of physical access per month. - Number of physical access devices (CCTV, IP cameras, NVRs, etc.).
SC - System and Communications Protections	A clear view of all technology, processes, people and data, where the maturity of the security solutions provides an adequate level of security including but not limited to network security, access management, data loss prevention, application code security, encryption, etc.	<ul style="list-style-type: none"> - Volume of organizational communications at the external boundaries of the information systems. - Number of subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
SI - Information Integrity	Requires the confidentiality, integrity and availability of information by adopting a broad	<ul style="list-style-type: none"> - Number of provided tools to protect from malicious code at appropriate locations with

Domain	Description	Elements
	range of security practices such as vulnerability scanning, patch management, malware/anti-virus software, SPAM protection, systems monitoring, oversight of security alerts, security threat assessments, information handling and retention (per regulations).	organizational information systems. - Volume of up-to-date malicious code protection patched systems. - Number of periodic scans of the information systems per month. - Volume of scanned files from external sources as files are downloaded, opened, or executed.

Note. Adapted from CMMC-EU (n.d.); Levy & Gafni, 2022.

Appendix B

Phase 1 SME Survey

Questions marked with * are required.

A. Demographics

- * A1. How long have you been working in the field of IT/Cybersecurity?
 - 5 or less years
 - 6 - 10 years
 - 11 - 15 years
 - 16 - 20 years
 - More than 20 years

- * A2. What is your highest level of education achieved?
 - High school diploma
 - 2-year college (associate degree)
 - 4-year college (bachelor's degree)
 - Master's degree
 - Doctorate degree

- * A3. What is your current job function?
 - Administrative/executive
 - Cybersecurity/IT staff
 - Engineer
 - Manager
 - Professional staff
 - Academics/professor/faculty member
 - Other

- * A4. How many years have you been in your current role?
- 5 or less years
 - 6 - 10 years
 - 11 - 15 years
 - 16 - 20 years
 - More than 20 years
- * A5. How many years have you been in the Manufacturing Industry?
- 5 or less years
 - 6 - 10 years
 - 11 - 15 years
 - 16 - 20 years
 - More than 20 years
 - No prior experience in Manufacturing
- * A6. What information security certificates do you hold?
- CISSP – Certified Information Systems Security Professional
 - CISM – Certified Information Security Manager
 - CISA – Certified Information Security Auditor
 - CIRSC - Certified in Risk and Information Systems Control
 - CompTIA Security+
 - None
 - Other _____
- * A7. How familiar are you with (Cybersecurity Maturity Model Certification) CMMC 2.0?
- Not at all familiar

- Slightly familiar
- Moderately familiar
- Very familiar
- Extremely familiar

* A8. What is the size of your company based on Annual Revenue?

- < \$10M
- \$10M < \$50M
- \$50M < \$200M
- \$200M < \$500M
- \$500M < \$1B
- Equal or greater than \$1B

* A9. What is the size of your company based on the number of Employees?

- < 500
- 500 < 1,000
- 1,000 < 1,500
- 1,500 < 2,000
- 2,000 < 2,500
- Equal or greater than 2,500

B. In this section, please respond to the following questions related to Tiers. A Tier represents a level down from an Originating Organization (Top Level) that is comprised of third parties, such as suppliers and/or partners.

* B1.1. The image illustrates the relationship among interconnected entities (third parties) from Organization A in a hierarchy structure with lower-level Tiers from Tier 1 through Tier n.

Based on the potential risk exposure from interconnected entities (third parties), *how many Tiers (lower levels) should be included to assess the cyber posture of Organization A (Tier 0)?*

Please enter your response (a number):

* B1.2.

* B2.1. Based on the number of Tiers you indicated, what level of influence based on percentages would you assign to each Tier to assess the risk exposure of Organization A?

Copy / Paste the following structure in your answer. Enter a percentage number for each of the Tiers that have a level of influence and enter a zero (0) for each of the Tiers that you think have no influence. (Ensure the sum of Tiers is equal to 100%).

Tier 1 = %
 Tier 2 = %
 Tier 3 = %
 Tier 4 = %
 Tier 5 = %

--- if needed, add additional lines to correspond to number you provided---
 Sum of Tiers = 100%

Please justify your response.

* B2.2.

C. Domain Evaluation

Please evaluate the following CMMC 2.0 Domains. Select from 1 “Not at all important” to 7 “Very important” to provide your feedback on the level of importance each Domain has on the cyber posture of an organization when interconnected to other organizations.

* C1. Access Control (AC): 1 2 3 4 5 6 7

* C2. Identification and Authentication (IA): 1 2 3 4 5 6 7

* C3. Media Protection (MP): 1 2 3 4 5 6 7

* C4. Physical Protection (PE): 1 2 3 4 5 6 7

* C5. Systems and Communications Protections (SC): 1 2 3 4 5 6 7

* C6. System and Information Integrity (SI): 1 2 3 4 5 6 7

D. Element Evaluation

Please evaluate the following Elements by each CMMC 2.0 Domain. Select from 1 “Not at all important” to 7 “Very important” to provide your feedback on the level of importance each Element has on the cyber posture of an organization when interconnected to other organizations.

D1. Access Control (AC)

* D1.1. Number of authorized users. 1 2 3 4 5 6 7

* D1.2. Number of authorized devices. 1 2 3 4 5 6 7

* D1.3. Number of information system access to the types of transactions and functions that authorized users are permitted to execute. 1 2 3 4 5 6 7

* D1.4. Number of transactions and functions that authorized users are permitted to execute for each type of information classification level. 1 2 3 4 5 6 7

* D1.5. Number of connections to external information systems. 1 2 3 4 5 6 7

* D1.6. Volume of transactions using external information systems connections (per month). 1 2 3 4 5 6 7

* D1.7. Volume of information posted or processed on publicly accessible information systems (per month). 1 2 3 4 5 6 7

* D1.8. Number of employees. 1 2 3 4 5 6 7

* D1.9. Number of Bring Your Own Device (BYOD) devices connected to the organizational network. 1 2 3 4 5 6 7

* D1.10. Average number of BYOD device applications per employee. 1 2 3 4 5 6 7

D2: Identification and Authentication (IA)

- * D2.1. Number of individuals sharing the same user credentials, and/or devices. 1 2 3 4 5 6 7

D3. Media Protection (MP)

- * D3.1. Number of unsensitized or non-destroyed information systems media containing Organizational Information before disposal or release for reuse. 1 2 3 4 5 6 7
- * D3.2. Volume of data in the information systems (# of records). 1 2 3 4 5 6 7
- * D3.3. Average number of non-licensed applications per employee on work assigned device. 1 2 3 4 5 6 7
- * D3.4. Average number of social media accounts per employee. 1 2 3 4 5 6 7

D4. Physical Protection (PE)

- * D4.1. Number of devices (organizational information systems, equipment, and the respective operating environments) with physical access to non-authorized individuals. 1 2 3 4 5 6 7
- * D4.2. Number of escorted visitors (per month). 1 2 3 4 5 6 7
- * D4.3. Number of non-escorted visitors (per month). 1 2 3 4 5 6 7
- * D4.4. Volume of logs of physical access (per month). 1 2 3 4 5 6 7
- * D4.5. Number of physical access devices (CCTV, IP Cameras, NVRs, etc.) 1 2 3 4 5 6 7

D5. Systems and Communications Protections (SC)

- * D5.1. Volume of organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. 1 2 3 4 5 6 7
- * D5.2. Number of subnetworks for publicly accessible system components that are physically or logically separated from internal networks. 1 2 3 4 5 6 7

D6. System and Information Integrity (SI)

- * D6.1. Number of provided TOOLS to protect from malicious code at appropriate locations within the organizational information systems. 1 2 3 4 5 6 7
- * D6.2. Number of up-to-date malicious code protection patched systems. 1 2 3 4 5 6 7
- * D6.3. Number of periodic scans of information systems per month. 1 2 3 4 5 6 7
- * D6.4. Volume of scanned files from external sources as files are downloaded, opened, or executed. 1 2 3 4 5 6 7

E. Element Value Evaluation

For each of the following statements, select the best value to represent the [Highest End Number] for the scale. If the number should be higher than those provided, select the "Other" option and enter a number divisible by 10.

- * E1.1. For the Number of authorized users, what should the [Highest End Number] be on the scale?
 1,000 1,500 2,000 2,500 3,000 3,500 4,000
 Other - enter a value
- * E2.1. For the Number of authorized devices, what should the [Highest End Number] be on the scale?
 250 500 750 1,000 1,250 1,500 1,750
 Other - enter a value

- * E3.1. For the Number of types of transactions and functions that authorized users are permitted to execute given information system access, what should the [Highest End Number] be on the scale?
 5 10 15 20 25 30 35
 Other - enter a value

- * E4.1. For the Number of transactions and functions that authorized users are permitted to execute for each type of information classification level (role), what should the [Highest End Number] be on the scale?
 1 4 7 10 14 17 20
 Other - enter a value

- * E5.1. For the Number of connections to external information systems, what should the [Highest End Number] be on the scale?
 10 20 30 40 50 60 70
 Other - enter a value

- * E6.1. For the Number of transactions using external information systems connections (per month), what should the [Highest End Number] be on the scale?
 1,500 2,000 2,500 3,000 3,500 4,000 4,500
 Other - enter a value

- * E7.1. For the Number of transactions (or posts) processed on publicly accessible information systems (per month), what should the [Highest End Number] be on the scale?
 250 500 750 1,000 1,250 1,500 1,750
 Other - enter a value

- * E8.1. For the Number of employees, what should the [Highest End Number] be on the scale?
 1,000 1,500 2,000 2,500 3,000 3,500 4,000
 Other - enter a value

- * E9.1. For the Number of Bring Your Own Device (BYOD) devices connected to the organizational network, what should the [Highest End Number] be on the scale?

75 150 300 450 600 750 900
 Other - enter a value

- * E10.1. For the Number of applications on BYOD devices per employee, what should the [Highest End Number] be on the scale?

25 50 75 100 125 150 175
 Other - enter a value

- * E11.1. For the Number of individuals sharing the same user credentials and/or devices, what should the [Highest End Number] be on the scale?

5 10 15 20 25 30 35
 Other - enter a value

- * E12.1. For the Number of unsensitized or non-destroyed information systems media containing organizational information before disposal or release for reuse, what should the [Highest End Number] be on the scale?

1 4 7 10 13 17 20
 Other - enter a value

- * E13.1. For the Volume of data (# of records) in the information systems, what should the [Highest End Number] be on the scale?

100,000 150,000 200,000 250,000 300,000
 350,000 400,000 Other - enter a value

- * E14.1. For the Number of non-licensed applications per employee on work assigned device (on average), what should the [Highest End Number] be on the scale?

1 4 7 10 13 17 20
 Other - enter a value

- * E15.1. For the Number of social media accounts per employee (on average), what should the [Highest End Number] be on the scale?

1 4 7 10 13 17 20
 Other - enter a value

- * E16.1. For the Number of devices (organizational information systems, equipment, and the respective operating environments) with physical access to non-authorized individuals, what should the [Highest End Number] be on the scale?

 1 4 7 10 13 17 20
 Other - enter a value

- * E17.1. For the Number of escorted visitors (per month), what should the [Highest End Number] be on the scale?

 10 15 20 25 30 35 40
 Other - enter a value

- * E18.1. For the Number of non-escorted visitors (per month), what should the [Highest End Number] be on the scale?

 1 4 7 10 13 17 20
 Other - enter a value

- * E19.1. For the Number of records of physical access in logs (per month), what should the [Highest End Number] be on the scale?

 1,000 1,250 1,500 1,750 2,000 2,250
 2,500 Other - enter a value

- * E20.1. For the Number of physical access devices (CCTV, IP Cameras, Network Video Recorders, etc.), what should the [Highest End Number] be on the scale?

 50 75 100 125 150 175 200
 Other - enter a value

- * E21.1. For the Number of records of organizational communications (i.e., email transmitted or received) at the external boundaries and key internal boundaries of the information systems (per month), what should the [Highest End Number] be on the scale?

 150,000 300,000 600,000 900,000 1,200,000
 1,500,000 1,800,000 Other - enter a value

- * E22.1. For the Number of subnetworks for publicly accessible system components that are physically or logically separated from internal networks, what should the [Highest End Number] be on the scale?

1 4 7 10 13 17 20
 Other - enter a value

- * E23.1. For the Number of tools to protect from malicious code at appropriate locations within the organizational information systems, what should the [Highest End Number] be on the scale?
 1 4 7 10 13 17 20
 Other - enter a value
- * E24.1. For the Number of up-to-date malicious code protection patched systems, what should the [Highest End Number] be on the scale?
 1,000 1,500 2,000 2,500 3,000 3,500 4,000
 Other - enter a value
- * E25.1. For the Number of periodic scans of information systems per month, what should the [Highest End Number] be on the scale?
 1 4 7 10 13 17 20
 Other - enter a value
- * E26.1. For the Number of scanned files from external sources as files are downloaded, opened, or executed per month, what should the [Highest End Number] be on the scale?
 10,000 20,000 30,000 40,000 50,000
 60,000 70,000 Other - enter a value

F. Attack Surface Evaluation

For each of the following statements for Attack Surface, select the best value to represent the [Highest End Number] for the scale.

If the number should be higher than those provided, select the "Other" option and enter a number divisible by 10.

- * F1.1. For the Number of workstations and laptops deployed and in use, what should the [Highest End Number] be on the scale?
 1,000 1,500 2,000 2,500 3,000 3,500 4,000
 Other - enter a value
- * F2.1. For the Number of network file servers deployed and in use, what should the [Highest End Number] be on the scale?

10 20 30 40 50 60 70
 Other - enter a value

- * F3.1. For the Number of application servers deployed and in use, what should the [Highest End Number] be on the scale?
 10 20 30 40 50 60 70
 Other - enter a value
- * F4.1. For the Number of public cloud instances deployed and in use, what should the [Highest End Number] be on the scale?
 1 4 7 10 13 17 20
 Other - enter a value
- * F5.1. For the Number of firewalls and switches deployed and in use, what should the [Highest End Number] be on the scale?
 100 150 200 250 300 350 400
 Other - enter a value
- * F6.1. For the Number of multi-function printers deployed and in use, what should the [Highest End Number] be on the scale?
 10 15 20 25 30 35 40
 Other - enter a value
- * F7.1. For the Number of mobile devices deployed and in use, what should the [Highest End Number] be on the scale?
 100 250 400 550 700 850 1,000
 Other - enter a value
- * F8.1. For the Number of IoT devices deployed and in use, what should the [Highest End Number] be on the scale?
 100 125 150 175 200 225 250
 Other - enter a value
- * F9.1. For the Number of employees, what should the [Highest End Number] be on the scale?
 1,000 1,500 2,000 2,500 3,000 3,500 4,000
 Other - enter a value

Appendix C

Phase 2 Pilot Group – CORE Score Survey

Please select the choice that best represents your organization and provide feedback you may have concerning the phrasing of the statement and the scale of the values.

Questions marked with * are required.

- * 1. Number of authorized users.

- 1 – 240
- 241 – 480
- 481 – 720
- 721 – 960
- 961 – 1,200
- 1,201 – 1,440
- 1,441 – 1,680
- 1,681 – 1,920
- 1,921 – 2,160
- 2,161 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 2. Number of authorized devices.

- 1 – 120
- 121 – 240
- 241 – 360
- 361 – 480
- 481 – 600
- 601 – 720
- 721 – 840
- 841 – 960
- 961 – 1080
- 1081 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 3. Number of information system access to the types of transactions and functions that authorized users are permitted to execute.

1 – 3

4 – 6

7 – 9

10 – 12

13 – 15

16 – 18

19 – 21

22 – 24

25 – 27

28 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 4. Number of transactions and functions that authorized users are permitted to execute for each type of information classification level.

1 – 2

3 – 4

5 – 6

7 – 8

9 – 10

11 – 12

13 – 14

15 – 16

17 – 18

19 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 5. Number of connections to external information systems.

1 – 4

5 – 8

9 – 12

13 – 16

17 – 20

21 – 24

25 – 28

29 – 32

33 – 36

37 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 6. Number of Bring Your Own Device (BYOD) devices connected to the organizational network.

1 – 40

41 – 80

81 – 120

121 – 160

161 – 200

201 – 240

241 – 280

281 – 320

321 – 360

361 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 7. Number of individuals sharing the same user credentials and/or devices.

- 1
 2
 3
 4
 5
 6
 7
 8
 9
 10 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 8. Number of unsensitized or non-destroyed information systems media containing Organizational Information before disposal or release for reuse.

- 1
 2
 3
 4
 5
 6
 7
 8
 9
 10 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 9. Average number of non-licensed applications per employee on work assigned device.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 10. Number of devices (organizational information systems, equipment, and the respective operating environments) with physical access to non-authorized individuals.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 11. Number of non-escorted visitors (per month).

- 1
 2
 3
 4
 5
 6
 7
 8
 9
 10 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 12. Number of physical access devices (Closed-caption TV, IP Cameras, Network Video Recorders, etc.)

- 1 – 13
 14 – 26
 27 – 39
 40 – 52
 53 – 65
 66 – 78
 79 – 91
 92 – 104
 105 – 117
 118 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 13. Number of records of organizational communications (i.e., email transmitted or received) at the external boundaries and key internal boundaries of the information systems (per month).

- 1 – 80,000
 80,001 – 160,000
 160,001 – 240,000
 240,001 – 320,000
 320,001 – 400,000
 400,001 – 480,000
 480,001 – 560,000
 560,001 – 640,000
 640,001 – 720,000
 720,001 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 14. Number of subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

- 1
 2
 3
 4
 5
 6
 7
 8
 9
 10 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 15. Number of provided TOOLS to protect from malicious code at appropriate locations within the organizational information systems.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 16. Number of up-to-date malicious code protection patched systems.

- 1 – 250
- 251 – 500
- 501 – 750
- 751 – 1,000
- 1,001 – 1,250
- 1,251 – 1,500
- 1,501 – 1,750
- 1,751 – 2,000
- 2,001 – 2,250
- 2,251 or Greater

- * What feedback do you have concerning the statement and the scale?

* 17. Number of periodic scans of information systems per month.

1 – 2

3 – 4

5 – 6

7 – 8

9 – 10

11 – 12

13 – 14

15 – 16

17 – 18

19 or Greater

* What feedback do you have concerning the statement and the scale?

* 18. Number of scanned files from external sources as files are downloaded, opened, or executed per month.

1 – 4,000

4,001 – 8,000

8,001 – 12,000

12,001 – 16,000

16,001 – 20,000

20,001 – 24,000

24,001 – 28,000

28,001 – 32,000

32,001 – 36,000

36,001 or Greater

* What feedback do you have concerning the statement and the scale?

Attack Surface (Organizational Demographics)

- * 19. How many workstations and laptops are deployed and in use in your organization?
 - 1 - 220
 - 221 - 440
 - 441 - 660
 - 661 - 880
 - 881 - 1,100
 - 1,101 - 1,320
 - 1,321 - 1,540
 - 1,541 - 1,760
 - 1,761 - 1,980
 - 1,981 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 20. How many network file servers are deployed and in use in your organization?
 - 1 - 3
 - 4 - 6
 - 7 - 9
 - 10 - 12
 - 13 - 15
 - 16 - 18
 - 19 - 21
 - 22 - 24
 - 25 - 27
 - 28 or Greater

* What feedback do you have concerning the statement and the scale?

* 21. How many application servers are deployed and in-use in your organization?

- 1 – 4
- 5 – 8
- 9 – 12
- 13 – 16
- 17 – 20
- 21 – 24
- 25 – 28
- 29 – 32
- 33 – 36
- 37 or Greater

* What feedback do you have concerning the statement and the scale?

* 22. How many public cloud instances are deployed and in-use in your organization?

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 23. How many firewalls and switches are deployed and in-use in your organization?

- 1 – 20
 21 – 40
 41 – 60
 61 – 80
 81 – 100
 101 – 120
 121 – 140
 141 – 160
 161 – 180
 181 or Greater

- * What feedback do you have concerning the statement and the scale?

- * 24. How many multi-function printers are deployed and in-use in your organization?

- 1 – 3
 4 – 6
 7 – 9
 10 – 12
 13 – 15
 16 – 18
 19 – 21
 22 – 24
 25 – 27
 28 or Greater

* What feedback do you have concerning the statement and the scale?

* 25. How many mobile devices are deployed and in-use in your organization?

1 - 50

51 - 100

101 - 150

151 - 200

201 - 250

251 - 300

301 - 350

351 - 400

401 - 450

451 or Greater

* What feedback do you have concerning the statement and the scale?

* 26. How many IoT devices are deployed and in-use in your organization?

1 – 25

26 – 50

51 – 75

76 – 100

101 – 125

126 – 150

151 – 175

176 – 200

201 – 225

226 or Greater

* What feedback do you have concerning the statement and the scale?

* 27. How many employees are in your organization?

- 1 – 200
- 201 – 400
- 401 – 600
- 601 – 1,000
- 1,001 – 1,250
- 1,251 – 1,500
- 1,501 – 1,750
- 1,751 – 2,000
- 2,001 – 2,250
- 2,251 or Greater

* What feedback do you have concerning the statement and the scale?

Appendix D

Phase 3 CORE Score Survey

Please select the choice that best represents your organization.

Questions marked with * are required.

- * 1. How many authorized users are in your company? [Consists of active accounts for employees, contractors, and consultants]
 - 0 – 240
 - 241 – 480
 - 481 – 720
 - 721 – 960
 - 961 – 1,200
 - 1,201 – 1,440
 - 1,441 – 1,680
 - 1,681 – 1,920
 - 1,921 – 2,160
 - 2,161 or Greater

- * 2. How many authorized devices are in your company? [Consists of end-user devices used by employees, contractors, and consultants]
 - 0 – 120
 - 121 – 240
 - 241 – 360
 - 361 – 480
 - 481 – 600
 - 601 – 720
 - 721 – 840
 - 841 – 960
 - 961 – 1080
 - 1081 or Greater

- * 3. What is the average number of distinct types of information system transactions and functions authorized users are permitted to execute in your company?
 - 0 – 3
 - 4 – 6
 - 7 – 9
 - 10 – 12
 - 13 – 15

- 16 – 18
 - 19 – 21
 - 22 – 24
 - 25 – 27
 - 28 or Greater
- * 4. What is the average number of transactions and functions that authorized users are permitted to execute for each type of information classification level in your company?
- 0 – 2
 - 3 – 4
 - 5 – 6
 - 7 – 8
 - 9 – 10
 - 11 – 12
 - 13 – 14
 - 15 – 16
 - 17 – 18
 - 19 or Greater
- * 5. What is the number of connections to external information systems for your company? [Consists of data flow in and out from systems that your company does not manage]
- 0 – 4
 - 5 – 8
 - 9 – 12
 - 13 – 16
 - 17 – 20
 - 21 – 24
 - 25 – 28
 - 29 – 32
 - 33 – 36
 - 37 or Greater
- * 6. What is the number of Bring Your Own Device (BYOD) devices connected to your company network?
- 0 – 40
 - 41 – 80
 - 81 – 120
 - 121 – 160
 - 161 – 200

- 201 – 240
- 241 – 280
- 281 – 320
- 321 – 360
- 361 or Greater

- * 7. What is the number of individuals sharing the same user credentials and/or devices in your company?
 - 0 or 1
 - 2
 - 3
 - 4
 - 5
 - 6
 - 7
 - 8
 - 9
 - 10 or Greater

- * 8. What is the average number of unsensitized or non-destroyed media devices (information systems such as PCs, servers, storage devices, etc.) containing Organizational Information before disposal or release for reuse (per month) in your company?
 - 0 or 1
 - 2
 - 3
 - 4
 - 5
 - 6
 - 7
 - 8
 - 9
 - 10 or Greater

- * 9. What is the average number of non-licensed (not purchased by the company) applications per employee on work assigned device in your company?
 - 0 or 1
 - 2
 - 3
 - 4
 - 5

- 6
- 7
- 8
- 9
- 10 or Greater

- * 10. What is the average number of devices (organizational information systems, equipment, and the respective operating environments) physically accessible to non-authorized individuals (per month) in your company?

- 0 or 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10 or Greater

- * 11. What is the average number of non-escorted visitors (per month) in your company?

- 0 or 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10 or Greater

- * 12. What is the number of physical access devices (Closed-caption TV, IP Cameras, Network Video Recorders, etc.) in your company?

- 0 – 13
- 14 – 26
- 27 – 39
- 40 – 52
- 53 – 65

- 66 – 78
- 79 – 91
- 92 – 104
- 105 – 117
- 118 or Greater

- * 13. What is the average number of records of organizational communications (i.e., email transmitted or received) at the external boundaries and key internal boundaries of the information systems (per month) in your company?

- 0 – 80,000
- 80,001 – 160,000
- 160,001 – 240,000
- 240,001 – 320,000
- 320,001 – 400,000
- 400,001 – 480,000
- 480,001 – 560,000
- 560,001 – 640,000
- 640,001 – 720,000
- 720,001 or Greater

- * 14. What is the number of subnetworks for publicly accessible system components that are physically or logically separated from internal networks in your company?

- 0 or 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10 or Greater

- * 15. What is the number of tools used to protect (detect, prevent, deter, or stop) from malicious code at appropriate locations within the information systems in your company?

- 0 or 1
- 2
- 3

- 4
 - 5
 - 6
 - 7
 - 8
 - 9
 - 10 or Greater
- * 16. What is the average number of patched systems (per month) up-to-date malicious code protection in your company?
- 0 – 250
 - 251 – 500
 - 501 – 750
 - 751 – 1,000
 - 1,001 – 1,250
 - 1,251 – 1,500
 - 1,501 – 1,750
 - 1,751 – 2,000
 - 2,001 – 2,250
 - 2,251 or Greater
- * 17. What is the average number of periodic vulnerability and malware scans of information systems (per month) in your company?
- 0 – 2
 - 3 – 4
 - 5 – 6
 - 7 – 8
 - 9 – 10
 - 11 – 12
 - 13 – 14
 - 15 – 16
 - 17 – 18
 - 19 or Greater
- * 18. What is the average number of scanned files from external sources as files are downloaded, opened, or executed (per month) in your company?
- 1 – 4,000
 - 4,001 – 8,000
 - 8,001 – 12,000
 - 12,001 – 16,000

- 16,001 – 20,000
- 20,001 – 24,000
- 24,001 – 28,000
- 28,001 – 32,000
- 32,001 – 36,000
- 36,001 or Greater

Other Company Questions:

- * 19. How many workstations and laptops are deployed and in use in your organization?
 - 0 - 220
 - 221 – 440
 - 441 – 660
 - 661 – 880
 - 881 – 1,100
 - 1,101 – 1,320
 - 1,321 – 1,540
 - 1,541 – 1,760
 - 1,761 – 1,980
 - 1,981 or Greater

- * 20. How many network file servers are deployed and in use in your organization?
 - 0 – 3
 - 4 – 6
 - 7 – 9
 - 10 – 12
 - 13 – 15
 - 16 – 18
 - 19 – 21
 - 22 – 24
 - 25 – 27
 - 28 or Greater

- * 21. How many application servers are deployed and in-use in your organization?
 - 0 – 4
 - 5 – 8

- 9 – 12
 - 13 – 16
 - 17 – 20
 - 21 – 24
 - 25 – 28
 - 29 – 32
 - 33 – 36
 - 37 or Greater
- * 22. How many public cloud instances are deployed and in-use in your organization?
- 0 or 1
 - 2
 - 3
 - 4
 - 5
 - 6
 - 7
 - 8
 - 9
 - 10 or Greater
- * 23. How many firewalls and switches are deployed and in-use in your organization?
- 0 – 20
 - 21 – 40
 - 41 – 60
 - 61 – 80
 - 81 – 100
 - 101 – 120
 - 121 – 140
 - 141 – 160
 - 161 – 180
 - 181 or Greater
- * 24. How many multi-function printers are deployed and in-use in your organization?
- 0 – 3
 - 4 – 6

- 7 – 9
- 10 – 12
- 13 – 15
- 16 – 18
- 19 – 21
- 22 – 24
- 25 – 27
- 28 or Greater

* 25. How many mobile devices are deployed and in-use in your organization?

- 0 - 50
- 51 - 100
- 101 - 150
- 151 - 200
- 201 - 250
- 251 - 300
- 301 - 350
- 351 - 400
- 401 - 450
- 451 or Greater

* 26. How many IoT devices are deployed and in-use in your organization?

- 0 – 25
- 26 – 50
- 51 – 75
- 76 – 100
- 101 – 125
- 126 – 150
- 151 – 175
- 176 – 200
- 201 – 225
- 226 or Greater

* 27. How many employees are in your organization?

- 1 – 200
- 201 – 400
- 401 – 600
- 601 – 1,000

- 1,001 – 1,250
- 1,251 – 1,500
- 1,501 – 1,750
- 1,751 – 2,000
- 2,001 – 2,250
- 2,251 or Greater

- * 28. Does your company (as a third-party) provide goods or services to one or more manufacturing companies?
- Yes
 - No

Appendix E

Participation Email to Experts

Dear Cybersecurity Expert,

I am requesting your help in providing expert input and feedback for my doctoral research study.

I am a Ph.D. Candidate in Cybersecurity Management at the College of Computing and Engineering, Nova Southeastern University (NSU), under the supervision of Professor Dr. Yair Levy, and a member of his Levy CyLab (<http://infosec.nova.edu/cylab/>).

I am conducting a research study based on the Theory of Cybersecurity Footprint, which emphasizes the relationship among interconnected entities and the risks and damage one organization can have on another regardless of size. My research seeks to develop Cybersecurity Footprint index to assess the cybersecurity posture of Manufacturing Companies (CFI-Mfg) based on their interconnected entities.

A set of six domains from CMMC 2.0 Level 1 and 26 associated elements have been identified from previous literature review that will be input to the research. In order to develop an index, I need your assistance to (1) confirm the maximum number of tiers of interconnected entities to account in the supply chain, (2) level of importance associated to the tiers, (3) level of importance of the domains, and (4) level of importance of the elements. Additionally, you will provide feedback and validation toward the development of a survey and index model.

The surveys you will receive will follow the Delphi method. This may require additional rounds of surveys to form a consensus. Once a consensus is achieved, the study will proceed to the next phase.

By participating in this study, you agree and understand that your responses are voluntary, and you certify that you are over the age of 18 years old. Procedures will be taken to ensure that responses are anonymous and cannot be traced to any individual. You may stop participating in this study at any time. If you are willing to participate, please click on the following link for access to the SME survey:

http://address_of_survey

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study. If you wish to receive the findings of the study, please contact me via email and I will be happy to provide you with information about the academic research publication(s) resulting from this study.

Sincerely,

John Del Vecchio, Ph.D. Candidate
E-mail: jd2940@mynsu.nova.edu
Nova Southeastern University

Appendix F

Participation Email to Pilot Group

Dear Manufacturing Company Point of Contact,

I am a Ph.D. Candidate in Cybersecurity Management at the College of Computing and Engineering, Nova Southeastern University (NSU), under the supervision of Professor Dr. Yair Levy, and a member of his Levy CyLab (<http://infosec.nova.edu/cylab/>).

I am conducting a research study based on the Theory of Cybersecurity Footprint, which emphasizes the relationship among interconnected entities and the risks and damage one organization can have on another regardless of size. My research seeks to develop Cybersecurity Footprint index to assess the cybersecurity posture of Manufacturing Companies (CFI-Mfg) based on their interconnected entities.

I am requesting your help to coordinate with companies in your supply chain to complete a short online survey as a Pilot Group. If you are willing to assist, please respond to this message or contact me at the email below and I will be in contact with more details.

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study. I will be more than happy to share with you the findings for your particular company.

Sincerely,

John Del Vecchio, Ph.D. Candidate
E-mail: jd2940@mynsu.nova.edu
Nova Southeastern University

Appendix G

Participation Email to Manufacturing Companies

Dear Manufacturing Company Point of Contact,

I am a Ph.D. Candidate in Cybersecurity Management at the College of Computing and Engineering, Nova Southeastern University (NSU), under the supervision of Professor Dr. Yair Levy, and a member of his Levy CyLab (<http://infosec.nova.edu/cylab/>).

I am conducting a research study based on the Theory of Cybersecurity Footprint, which emphasizes the relationship among interconnected entities and the risks and damage one organization can have on another regardless of size. My research seeks to develop Cybersecurity Footprint index to assess the cybersecurity posture of Manufacturing Companies (CFI-Mfg) based on their interconnected entities.

I am requesting your help to coordinate with companies in your supply chain to complete a short online survey. If you are willing to assist, please respond to this message or contact me at the email below and I will be in contact with more details.

Thank you in advance for your consideration. I appreciate your assistance and contribution to this research study. I will be more than happy to share with you the findings for your particular company.

Sincerely,

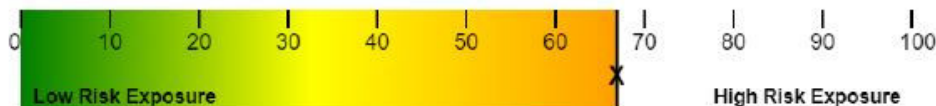
John Del Vecchio, Ph.D. Candidate
E-mail: jd2940@mynsu.nova.edu
Nova Southeastern University

Appendix H

Web-Based Prototype of CORE Score Survey and Results

Questions	Selections
Number of authorized users.	2181 or Greater
Number of authorized devices.	1081 or Greater
Number of information system access to the types of transactions and functions that authorized users are permitted to execute.	10-12
Number of transactions and functions that authorized users are permitted to execute for each type of information classification level.	9-10
Number of connections to external information systems.	5-8
Number of Bring Your Own Device (BYOD) devices connected to the organizational network.	361 or Greater
Number of individuals sharing the same user credentials and/or devices.	10 or Greater
Number of unsensitized or non-destroyed information systems media containing Organizational Information before disposal or release for reuse.	10 or Greater
Average number of non-licensed applications per employee on work assigned device.	3
Number of devices (organizational information systems, equipment, and the respective operating environments) with physical access to non-authorized individuals.	1
Number of non-escorted visitors (per month).	10 or Greater
Number of physical access devices (CCTV, IP Cameras, NVRs, etc.).	53-65
Number of records of organizational communications (e.g., email transmitted or received) at the external boundaries and key internal boundaries of the information systems (per month).	720001 or Greater
Number of subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	2
Number of provided TOOLS to protect from malicious code at appropriate locations within the organizational information systems.	2
Number of up-to-date malicious code protection patched systems.	2501 or Greater
Number of periodic scans of information systems per month.	19 or Greater
Number of scanned files from external sources as files are downloaded, opened, or executed per month.	4001-8000

Calculate CORE Score



CORE Score = 66.9

Appendix I

The IRB Approval



INSTITUTIONAL REVIEW BOARD
3301 College Avenue
Fort Lauderdale, Florida 33314-7796
PHONE: (954) 262-5369

MEMORANDUM

To: John Del Vecchio
College of Engineering and Computing

From: Ling Wang, Ph.D.
College Representative, College of Engineering and Computing

Date: September 26, 2023

Subject: IRB Exempt Initial Approval Memo

TITLE: Development of Cybersecurity Footprint Index for Manufacturing Companies to Assess Organizational Cyber Posture– NSU IRB Protocol Number 2023-470

Dear Principal Investigator,

Your submission has been reviewed and Exempted by your IRB College Representative or their Alternate on **September 26, 2023**. You may proceed with your study.

NOTE: Exempt studies do not require approval stamped documents. If your study site requires stamped copies of consent forms, recruiting materials, etc., contact the IRB Office.

Level of Review: Exempt

Type of Approval: Initial Approval

Exempt Review Category: Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies

Annual Status of Research Update: You are required to notify the IRB Office annually if your research study is still ongoing via the *Exempt Research Status Update xForm*.

Changes: Any changes in the study (e.g., procedures, consent forms, investigators, etc.) must be approved by the IRB prior to implementation using the *Amendment xForm*.



INSTITUTIONAL REVIEW BOARD
3301 College Avenue
Fort Lauderdale, Florida 33314-7796
PHONE: (954) 262-5369

Post-Approval Monitoring: The IRB Office conducts post-approval review and monitoring of all studies involving human participants under the purview of the NSU IRB. The Post-Approval Monitor may randomly select any active study for a Not-for-Cause Evaluation.

Final Report: You are required to notify the IRB Office within 30 days of the conclusion of the research that the study has ended using the *Exempt Research Status Update xForm*.

Translated Documents: No

Retain this document in your IRB correspondence file.

CC: Ling Wang, Ph.D.

Yair Levy, Ph.D.

Other

References

- Accenture. (2019). *Cyber threatscape report*. https://www.accenture.com/_acnmedia/pdf-107/accenturesecurity-cyber.pdf
- Adesemowo, A. K. (2021). Towards a conceptual definition for IT assets through interrogating their nature and epistemic uncertainty. *Computers & Security, 105*, 102131. <https://doi.org/10.1016/j.cose.2020.102131>
- Afroz, S., Islam, A. C., Santell, J., Chapin, A., & Greenstadt, R. (2013, June). How privacy flaws affect consumer perception [Paper presentation]. *2013 Third Workshop on Socio-Technical Aspects in Security and Trust* (pp. 10-17). IEEE. New Orleans, LA, USA. <https://doi.org/10.1109/STAST.2013.13>
- Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1), ty006. <https://doi.org/10.1093/cybsec/ty006>
- Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2023). A systematic method for measuring the performance of a cyber security operations centre analyst. *Computers & Security, 124*, 102959. <https://doi.org/10.1016/j.cose.2022.102959>
- Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security, 101*, 102122. <https://doi.org/10.1016/j.cose.2020.102122>
- Ahuja, L., Singh, B., & Simon, R. (2024). Data cleaning: Paving a way for accurate and clean data. *Global Journal of Enterprise Information System, 16*(1), 18-25. <https://doi.org/10.18311/gjeis/2024>
- Ajayi, W., Ibeto, O., Olomola, T., & Madewa, M. (2022). Analysis of modern cybersecurity threat techniques and available mitigating methods. *International Journal of Advanced Research in Computer Science, 13*(2). <https://doi.org/10.26483/ijarcs.v13i2.6815>
- Alarabiat, A., & Ramos, I. (2019). The Delphi method in information systems research (2004-2017). *Electronic Journal of Business Research Methods, 17*(2), 86-99. <https://doi.org/10.34190/JBRM.17.2.04>

- Algarni, A. M., & Malaiya, Y. K. (2016, May). A consolidated approach for estimation of data security breach costs [Paper presentation]. *2016 2nd International Conference on Information Management (ICIM)* (pp. 26-39). IEEE. London, UK.
<https://doi.org/10.1109/INFOMAN.2016.7477530>
- Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, *100*, 212-223.
<https://doi.org/10.1016/j.compind.2018.04.017>
- Ali, Z., & Bhaskar, S. B. (2016). Basic statistical tools in research and data analysis. *Indian Journal of Anaesthesia*, *60*(9), 662-669.
<https://doi.org/10.4103/0019-5049.190623>
- Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications*, *155*, 1-8.
<https://doi.org/10.1016/j.comcom.2020.03.007>
- Almaiah, M. A., Hajjej, F., Lutfi, A., Al-Khasawneh, A., Alkhdour, T., Almomani, O., & Shehab, R. (2022). A conceptual framework for determining quality requirements for mobile learning applications using Delphi Method. *Electronics*, *11*(5), 788.
<https://doi.org/10.3390/electronics11050788>
- Almehmadi, A., & El-Khatib, K. (2013, November). Authorized! access denied, unauthorized! access granted [Paper presentation]. *Proceedings of the 6th International Conference on Security of Information and Networks* (pp. 363-367). Aksaray, Turkey. <https://doi.org/10.1145/2523514.2523612>
- Alora, A., & Barua, M. K. (2022). Development of a supply chain risk index for manufacturing supply chains. *International Journal of Productivity and Performance Management*, *71*(2), 477-503. <https://doi.org/10.1108/IJPPM-11-2018-0422>
- Ameyaw, E. E., Hu, Y., Shan, M., Chan, A. P., & Le, Y. (2016). Application of Delphi method in construction engineering and management research: A quantitative perspective. *Journal of Civil Engineering and Management*, *22*(8), 991-1000.
<https://doi.org/10.3846/13923730.2014.945953>
- Andrade, C. (2021). The inconvenient truth about convenience and purposive samples. *Indian Journal of Psychological Medicine*, *43*(1), 86-88.
<https://doi.org/10.1177/0253717620977000>
- 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>

- Arctic Wolf. (2023, March 30). *Biggest manufacturing industry cyberattacks*.
<https://arcticwolf.com/resources/blog/top-8-manufacturing-industry-cyberattacks/>
- Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks: The International Journal of Computer and Telecommunications Networking*, 165(C), 106946.
<https://doi.org/10.1016/j.comnet.2019.106946>
- Avdibasic, E., Toksanovna, A. S., & Durakovic, B. (2022). Cybersecurity challenges in Industry 4.0: A state of the art review. *Defense and Security Studies*, 3, 32-49.
<https://doi.org/10.37868/dss.v3.id188>
- Avella, J. R. (2016). Delphi panels: Research design, procedures, advantages, and challenges. *International Journal of Doctoral Studies*, 11, 305-321.
<https://doi.org/10.28945/3561>
- Awang, N., Samy, G. N., & Hassan, N. H. (2022). Prioritizing cybersecurity management guidelines using analytical hierarchy process (AHP) decision technique. *Open International Journal of Informatics*, 10(Special Issue 1), 1-10.
<https://oiji.utm.my/index.php/oiji/article/download/175/129>
- Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393-410. <https://doi.org/10.1108/ICS-07-2018-0080>
- Banker, R. D., & Feng, C. (2019). The impact of information security breach incidents on CIO turnover. *Journal of Information Systems*, 33(3), 309-329.
<https://doi.org/10.2308/isys-52532>
- Barata, J., Rupino Da Cunha, P., & Stal, J. (2018). Mobile supply chain management in the Industry 4.0 era: An annotated bibliography and guide for future research. *Journal of Enterprise Information Management*, 31(1), 173-192.
<https://doi.org/10.1108/JEIM-09-2016-0156>
- Barbosa, I. A. D. P., Dos Reis, R. L. B., Saldanha, W. E., Lugli, A. B., Do Carmo, F. D. A. S., & Ribeiro, S. L. (2021). Security risks assessment in an industry 4.0 plant [Paper presentation]. *2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)* (pp. 1-6). IEEE. Mauritius, Mauritius. <https://doi.org/10.1109/ICECCME52200.2021.9591040>
- Barrios, M., Guilera, G., Nuño, L., & Gómez-Benito, J. (2021). Consensus in the Delphi method: What makes a decision change? *Technological Forecasting and Social Change*, 163, 120484. <https://doi.org/10.1016/j.techfore.2020.120484>

- Battaglioni, M., Rafaiani, G., Chiaraluce, F., & Baldi, M. (2022). MAGIC: A method for assessing cyber incidents occurrence. *IEEE Access*, *10*, 73458-73473. <https://doi.org/10.1109/ACCESS.2022.3189777>
- Baylan, E. B. (2020). A novel project risk assessment method development via AHP-TOPSIS hybrid algorithm. *Emerging Science Journal*, *4*(5), 390-410. <https://dx.doi.org/10.28991/esj-2020-01239>
- Beiderbeck, D., Frevel, N., Heiko, A., Schmidt, S. L., & Schweitzer, V. M. (2021). Preparing, conducting, and analyzing Delphi surveys: Cross-disciplinary practices, new directions, and advancements. *MethodsX*, *8*, 101401, 1-20. <https://doi.org/10.1016/j.mex.2021.101401>
- Beiderbeck, D., Evans, N., Frevel, N., & Schmidt, S. L. (2023). The impact of technology on the future of football—A global Delphi study. *Technological Forecasting and Social Change*, *187*, 122186. <https://doi.org/10.1016/j.techfore.2022.122186>
- Bello, A. G., Murray, D., & Armarego, J. (2017). A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information & Computer Security*, *25*(4), 475-492. <https://doi.org/10.1108/ICS-03-2016-0025>
- Belton, I., MacDonald, A., Wright, G., & Hamlin, I. (2019). Improving the practical application of the Delphi method in group-based judgment: A six-step prescription for a well-founded and defensible process. *Technological Forecasting and Social Change*, *147*, 72-82. <https://doi.org/10.1016/j.techfore.2019.07.002>
- Ben-Daya, M., Hassini, E., & Bahrour, Z. (2019). Internet of things and supply chain management: A literature review. *International Journal of Production Research*, *57*(15-16), 4719-4742. <https://doi.org/10.1080/00207543.2017.1402140>
- Benotmane, R., Kovács, G., & Dudás, L. (2019). Economic, social impacts and operation of smart factories in Industry 4.0 focusing on simulation and artificial intelligence of collaborating robots. *Social Sciences*, *8*(5), 143. <https://doi.org/10.3390/socsci8050143>
- Berezina, K., Cobanoglu, C., Miller, B. L., & Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, *24*(7), 991-1010. <https://doi.org/10.1108/09596111211258883>

- 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>
- Bhargava, B., Ranchal, R., & Othmane, L. B. (2013, February). Secure information sharing in digital supply chains. *2013 3rd IEEE International Advance Computing Conference (IACC)* (pp. 1636-1640). IEEE. Ghaziabad, India. <https://doi.org/10.1109/IAdCC.2013.6514473>
- Bibby, L., & Dehe, B. (2018). Defining and assessing industry 4.0 maturity levels—case of the defence sector. *Production Planning & Control*, 29(12), 1030-1043. <https://doi.org/10.1080/09537287.2018.1503355>
- Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: Uncertainties, risks and cyber security. *Procedia computer science*, 149, 65-70. <https://doi.org/10.1016/j.procs.2019.01.108>
- Bottomley, P. A., & Doyle, J. R. (2001). A comparison of three weight elicitation methods: Good, better, and best. *Omega*, 29(6), 553-560. [https://doi.org/10.1016/S0305-0483\(01\)00044-5](https://doi.org/10.1016/S0305-0483(01)00044-5)
- Bottomley, P. A., Doyle, J. R., & Green, R. H. (2000). Testing the reliability of weight elicitation methods: Direct rating versus point allocation. *Journal of Marketing Research*, 37(4), 508-513. <https://doi.org/10.1509/jmkr.37.4.508.18794>
- Bouayad, H., Benabbou, L., & Berrado, A. (2018, October). An Analytic Hierarchy Process based approach for information technology governance framework selection [Paper presentation]. *Proceedings of the 12th International Conference on Intelligent Systems: Theories and Applications* (pp. 1-6). Rabat, Morocco. <https://doi.org/10.1145/3289402.3289515>
- Boukakedid, R., Abdoul, H., Loustau, M., Sibony, O., & Alberti, C. (2011). Using and reporting the Delphi method for selecting healthcare quality indicators: A systematic review. *PloS One*, 6(6), e20476. <https://doi.org/10.1371/journal.pone.0020476>
- Bowman, R. J. (2013). Why cybersecurity is a supply-chain problem. *Supply Chain Brain*. <https://www.supplychainbrain.com/blogs/1-think-tank/post/16330-why-cybersecurity-is-a-supply-chain-problem>
- Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, 34(7), 342-353. <https://doi.org/10.1016/j.technovation.2014.02.001>

- Brady, S. R., Jason, L. A., & Glenwick, D. S. (2015). The Delphi method. *Handbook of Methodological Approaches to Community-Based Research*; Oxford University Press: Oxford, UK, 61-68.
- Brandao, P. R. (2019). Bases, challenges, and main dangers for deploying cybersecurity in industry 4.0. *Advances in Wireless Communications and Networks*, 5(1), 33 - 40. <https://doi.org/10.11648/j.awcn.20190501.15>
- Brandao, P. R., & Rezende, M. (2020). Data: The most valuable commodity. *Kriativ. tech*, 8(1), 1-7. <https://doi.org/10.31112/kriativ-tech-2020-08-47>
- Burke, W., Oseni, T., Jolfaei, A., & Gondal, I. (2019). Cybersecurity indexes for eHealth [Paper presentation]. *Proceedings of the Australasian Computer Science Week Multiconference* (pp. 1-8). Canberra, Australia. <https://doi.org/10.1145/3290688.3290721>
- Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer security*, 11(3), 431-448. <https://doi.org/10.3233/JCS-2003-11308>
- Canizo, M., Conde, A., Charramendieta, S., Minon, R., Cid-Fuentes, R. G., & Onieva, E. (2019). Implementation of a large-scale platform for cyber-physical system real-time monitoring. *IEEE Access*, 7, 52455-52466. <https://doi.org/10.1109/ACCESS.2019.2911979>
- Caston, S., Chowdhury, M. M., & Latif, S. (2021, October). Risks and anatomy of data breaches. *2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)* (pp. 1-6). IEEE. <https://doi.org/10.1109/ICECCME52200.2021.9590895>
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9(1), 70-104. <https://doi.org/10.1080/10864415.2004.11044320>
- Chalmers, J. & Armour, M. (2019). *The Delphi technique* (E. Liamputtong, Ed.). Springer Nature.
- Choi, B. C., Kim, S. S., & Jiang, Z. (2016). Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems*, 33(3), 904-933. <https://doi.org/10.1080/07421222.2015.1138375>

- Choong, P., Hutton, E., Richardson, P., & Rinaldo, V. (2016). Assessing the cost of security breach: A marketer's perspective. *Proceedings of Academy of Marketing Studies, Allied Academies International Conference* (Vol. 21, No. 1, p. 1). Jordan Whitney Enterprises, Inc.
- Choong, P., Hutton, E., Richardson, P. S., & Rinaldo, V. (2017). Protecting the brand: Evaluating the cost of security breach from a marketer's perspective. *Journal of Marketing Development and Competitiveness*, 11(1), 59.
- Chowdhury, S., & Squire, L. (2006). Setting weights for aggregate indices: An application to the commitment to development index and human development index. *The Journal of Development Studies*, 42(5), 761-771.
<https://doi.org/10.1080/00220380600741904>
- Ciano, M. P., Ardolino, M., & Müller, J. M. (2022, July 26 - 28). Digital supply chain: conceptualisation of the research domain. *Proceedings of the 5th European International Conference on Industrial Engineering and Operations Management*. Rome, Italy. <https://ieomsociety.org/proceedings/2022rome/77.pdf>
- Cicchetti, D. V., Showalter, D., & Tyrer, P. J. (1985). The effect of number of rating scale categories on levels of interrater reliability: A Monte Carlo investigation. *Applied Psychological Measurement*, 9(1), 31-36.
<https://doi.org/10.1177/014662168500900103>
- Cinelli, M., Spada, M., Kim, W., Zhang, Y., & Burgherr, P. (2021). MCDA index tool: An interactive software to develop indices and rankings. *Environment Systems and Decisions*, 41(1), 82-109. <https://doi.org/10.1007/s10669-020-09784-x>
- CMMC-EU (n.d.) *DFARS and CMMC Cybersecurity Risk Management Compliance*. CMMS 2.0: 14 Interdependent Cyber Domains. <https://cmmc-eu.com/cmmc-domains-2-0/>
- Collins, S., & McCombie, S. (2012). Stuxnet: The emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*, 7(1), 80-91.
<https://doi.org/10.1080/18335330.2012.653198>
- Cornish, P. (Ed.). (2021). *The Oxford handbook of cyber security*. Oxford University Press.
- 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>

- Craigien, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10), 13-21.
- 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>
- Cumberbatch, T. V. (2004). *Research methods: Data analysis*. <http://mountappsych.pbworks.com/w/file/45664995/Data%20Analysis.pdf>
- Cybersecurity and Infrastructure Security Agency (CISA). (2020, October 21). *Critical infrastructure sectors*. <https://www.cisa.gov/critical-infrastructure-sectors>
- da Silva Neves, A. J., & Camanho, R. (2015). The use of AHP for IT project prioritization – a case study for oil & gas company. *Procedia Computer Science*, 55, 1097-1105. <https://doi.org/10.1016/j.procs.2015.07.076>
- Dash, P., & Sar, J. (2020). Identification and validation of potential flood hazard area using GIS-based multi-criteria analysis and satellite data-derived water index. *Journal of Flood Risk Management*, 13(3), e12620. <https://doi.org/10.1111/jfr3.12620>
- Dastbaz, M. (2019). Industry 4.0 (i4.0): The Hype, the reality, and the challenges ahead. In: Dastbaz, M., Cochrane, P. (eds) *Industry 4.0 and Engineering for a Sustainable Future*. Springer, Cham. https://doi.org/10.1007/978-3-030-12953-8_1
- Day, J., & Bobeva, M. (2005). A generic toolkit for the successful management of Delphi studies. *Electronic Journal of Business Research Methods*, 3(2), pp103-116.
- 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>
- Dean, M. (2022). *A practical guide to multi-criteria analysis*. UCL: London, UK.
- 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>
- Department of Defense (DoD). (2021, November 4). *Strategic direction for cybersecurity maturity model certification (CMMC) program* [Press Release]. <https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/>

- Di Zio, S. (2018). Convergence of experts' opinions on the territory: The Spatial Delphi and the Spatial Shang. *Innovative Research Methodologies in Management: Volume II: Futures, Biometrics and Neuroscience Research*, 1-29.
https://doi.org/10.1007/978-3-319-64400-4_1
- Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, 92, 101747.
<https://doi.org/10.1016/j.cose.2020.101747>
- Dinger, M., & Wade, J. T. (2019). The strategic problem of information security and data breaches. *The Coastal Business Journal*, 17(1), 1-25.
<https://digitalcommons.coastal.edu/cbj/vol17/iss1/1>
- 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>
- Duo, Z., Chen, Z., Liang, Y., Dai, M., & Guo, H. (2021). Risk rating framework of power grid business entities based on AHP. *ACM Turing Award Celebration Conference-China (ACM TURC 2021)*, 273-277. Hefei, China.
<https://doi.org/10.1145/3472634.3474084>
- 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>
- Farrelly, J. (2023, May 9). *High-profile company data breaches 2023*. Electric.
<https://www.electric.ai/blog/recent-big-company-data-breaches>
- Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., ... & Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications*, 61, 102916.
<https://doi.org/10.1016/j.jisa.2021.102916>
- Fisher, H., Erasmus, A. C., & Viljoen, A. T. (2020). Adaptation of the Delphi technique for electronic application in the food industry. *African Journal of Hospitality, Tourism and Leisure*, 9(5), 823-841. <https://doi.org/10.46222/ajhtl.19770720-54>
- Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2014). Embracing digital technology: A new strategic imperative. *MIT Sloan Management Review*, 55(2), 1.
<https://emergenceweb.com/blog/wp-content/uploads/2013/10/embracing-digital-technology.pdf>

- Flatt, H., Schriegel, S., Jasperneite, J., Trsek, H., & Adamczyk, H. (2016, September 6 - 9). Analysis of the cyber-security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements. *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)* (pp. 1-4). IEEE. Berlin, Germany. <https://ieeexplore.ieee.org/document/7733634/>
- Furlani, C. (2009). FIPS 200: Minimum security requirements for federal information and information systems.
- Gallagher, K. P., Zhang, X., & Gallagher, V. C. (2016). Measuring the organizational impact of security breaches: Patterns of factors and correlates. *CONF-IRM 2016 Proceedings*, 36. <http://aisel.aisnet.org/confirm2016/36>
- Gallo, A. (2016). A refresher on statistical significance. *Harvard Business Review*, 16. https://web.dsa.missouri.edu/static/PDF/HBR_Statistical_Significance.pdf
- Garay-Rondero, C. L., Martinez-Flores, J. L., Smith, N. R., Morales, S. O. C., & Aldrette-Malacara, A. (2020). Digital supply chain model in Industry 4.0. *Journal of Manufacturing Technology Management*, 31(5), 887-933. <https://doi.org/10.1108/JMTM-08-2018-0280>
- Gardner, D. (2021). *Overview of practices and processes of the CMMC assessment guides*. <https://apps.dtic.mil/sti/pdfs/AD1149125.pdf>
- Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, 11(2), 74-83. <https://doi.org/10.1108/09685220310468646>
- Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, 25(2), 223-240. <https://10.1108/SCM-10-2018-0357>
- Ghobakhloo, M. (2018). The future of manufacturing industry: A strategic roadmap toward Industry 4.0. *Journal of manufacturing technology management*, 29(6), 910-936. <https://doi.org/10.1108/JMTM-02-2018-0057>
- Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Quarterly*, 41(3), 703-A16. <https://doi.org/10.25300/MISQ/2017/41.3.03>
- Goode, J., Levy, Y., Hovav, A., & Smith, J. (2018). Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness. *Online Journal of Applied Knowledge Management*, 6(1), 54-66. [https://doi.org/10.36965/OJAKM.2018.6\(1\)67-80](https://doi.org/10.36965/OJAKM.2018.6(1)67-80)

- Goluchowicz, K. & Blind, K. (2011). Identification of future fields of standardisation: An explorative application of the Delphi methodology. *Technological Forecasting and Social Change*, 78(9), 1526-1541. <https://doi.org/10.1016/j.techfore.2011.04.014>
- Gourisetti, S. N. G., Mylrea, M., Reeve, H. M., Rotondo, J. A., Richards, G. T., & Irwin, J. A. (2021). *Facility cybersecurity framework best practices version 2.0* (No. PNNL-30291 Ver 2.0). Pacific Northwest National Lab. (PNNL), Richland, WA (United States).
- Green, P. J. (1982, March). The content of a college-level outdoor leadership course [Paper presentation]. Conference of the Northwest District Association for the American Alliance for Health, Physical Education, Recreation, and Dance, Spokane, WA.
- Griffey, R. T., Schneider, R. M., Adler, L. M., Capp, R., Carpenter, C. R., Farmer, B. M., ... & Wiler, J. L. (2020). Development of an emergency department trigger tool using a systematic search and modified Delphi process. *Journal of Patient Safety*, 16(1), e11-e17. <https://doi.org/10.1097/PTS.0000000000000243>
- Gupta, N., Tiwari, A., Bukkapatnam, S. T., & Karri, R. (2020). Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks. *IEEE Access*, 8, 47322-47333. <https://doi.org/10.1109/ACCESS.2020.2978815>
- Gwebu, K. L., Wang, J., & Xie, W. (2014). Understanding the cost associated with data security breaches. *PACIS* (p. 386). <http://aisel.aisnet.org/pacis2014/386>
- Haislip, J., Kolev, K., Pinsker, R., & Steffen, T. (2019, June 3 - 4). *The economic cost of cybersecurity breaches: A broad-based analysis*. Workshop on the Economics of Information Security (WEIS), 1-37. https://weis2017.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_13.pdf
- Hallowell, M. R., & Gambatese, J. A. (2010). Qualitative research: Application of the Delphi method to CEM research. *Journal of construction engineering and management*, 136(1), 99-107. [https://doi.org/10.1061/\(ASCE\)CO.1943-7862.0000137](https://doi.org/10.1061/(ASCE)CO.1943-7862.0000137)
- Harker, P. T., & Vargas, L. G. (1987). The theory of ratio scale estimation: Saaty's analytic hierarchy process. *Management science*, 33(11), 1383-1403.
- Harley, K., & Cooper, R. (2021). Information integrity: Are we there yet? *ACM Computing Surveys (CSUR)*, 54(2), 1-35. <https://doi.org/10.1145/3436817>
- Hassija, V., Chamola, V., Gupta, V., Jain, S., & Guizani, N. (2020). A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE*

- Internet of Things Journal*, 8(8), 6222-6246.
<https://doi.org/10.1109/JIOT.2020.3025775>
- He, C., HuangFu, J., Kohlbeck, M. J., & Wang, L. (2020). *The impact of customer's reported cybersecurity breaches on key supplier's relationship-specific investments and relationship duration*. <https://doi.org/10.2139/ssrn.3544245>
- Heinbockel, W. J., Laderman, E. R., & Serrao, G. J. (2017). *Supply chain attacks and resiliency mitigations*. The MITRE Corporation, 1-30.
<https://www.mitre.org/sites/default/files/2021-11/pr-18-0854-supply-chain-cyber-resiliency-mitigations.pdf>
- 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.
- Hemsley, K. E., & Fisher, E. (2018). *History of industrial control system cyber incidents* (No. INL/CON-18-44411-Rev002). Idaho National Lab. (INL), Idaho Falls, ID (United States). <https://doi.org/10.2172/1505628>
- Hertzog, M. A. (2008). Considerations in determining sample size for pilot studies. *Research in Nursing & Health*, 31(2), 180-191.
<https://doi.org/10.1002/nur.20247>
- 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>
- Hoehle, H., Wei, J., Schuetz, S., & Venkatesh, V. (2021). *User compensation as a data breach recovery action: A methodological replication and investigation of generalizability based on the Home Depot breach*. *Internet Research*.
<https://doi.org/10.1108/intr-02-2020-0105>
- Hofmann, E., & Rüsçh, M. (2017). Industry 4.0 and the current status as well as future prospects on logistics. *Computers in industry*, 89, 23-34.
<https://doi.org/10.1016/j.compind.2017.04.002>
- Hohmann, E., Angelo, R., Arciero, R., Bach, B. R., Cole, B., Cote, M., ... & Tetsworth, K. (2020). Degenerative meniscus lesions: An expert consensus statement using the modified Delphi technique. *Arthroscopy: The Journal of Arthroscopic & Related Surgery*, 36(2), 501-512. <https://doi.org/10.1016/j.arthro.2019.08.014>

- Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime*, 22(2), 242-260.
<https://doi.org/10.1108/JFC-09-2013-0055>
- Howard, M. (2003). *Fending off future attacks by reducing attack surface*. Microsoft Corporation.
- Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Association for Information Systems*, 34(1), 50. <https://doi.org/10.17705/1CAIS.03450>
- Hsu, C. C. & Sandford, B. A. (2007). The Delphi technique: Making sense of consensus. *Practical Assessment, Research & Evaluation*, 12(10), 1-8.
<https://doi.org/10.7275/pdz9-th90>
- 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>
- Hsu, P. F., Lan, K. Y., & Tsai, C. W. (2013). Selecting the optimal vendor of customer relationship management system for medical tourism industry using Delphi and AHP. *International Journal of Enterprise Information Systems (IJEIS)*, 9(1), 62-75.
<https://doi.org/10.4018/jeis.2013010104>
- Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys (CSUR)*, 51(4), 1-36.
<https://doi.org/10.1145/3199674>
- Hyperproof Team (2022). *What is third-party risk? Key features*. Hyperproof.
<https://hyperproof.io/resource/what-is-third-party-risk/>
- IBM Security. (2023). *X-force threat intelligence index*.
<https://www.ibm.com/reports/threat-intelligence>
- Identity Theft Resource Center (ITRC). (2022). *Annual data breach report*.
<https://www.idtheftcenter.org/publication/2022-data-breach-report/>
- Identity Theft Resource Center (ITRC). (2023). *Q1 data breach analysis*.
<https://www.idtheftcenter.org/publication/q1-2023-data-breach-analysis/>
- Idrus, S. Z. S., Cherrier, E., Rosenberger, C., & Schwartzmann, J. J. (2013). A review on authentication methods. *Australian Journal of Basic and Applied Sciences*, 7(5), 95-

107.

https://www.researchgate.net/publication/281109747_A_Review_on_Authentication_Methods

İlhan, İ., & Karaköse, M. (2019, September 21-22). Requirement analysis for cybersecurity solutions in industry 4.0 platforms. *Proceedings of the 2019 International Artificial Intelligence and Data Processing Symposium (IDAP)*, 1-7, Malatya, Turkey. <https://doi.org/10.1109/IDAP.2019.8875930>

Immerman, G. (2021). *Why industry 4.0 is important and why manufacturers should care*. MachineMetrics. <https://www.machinemetrics.com/blog/why-industry-4-0-is-important>

Irvine, J. (2021). Distributed leadership in practice: A modified Delphi method study. *Journal of Instructional Pedagogies*, 25.

Isaac, S., & Michael, W. B. (1995). *Handbook in research and evaluation: A collection of principles, methods, and strategies useful in the planning, design, and evaluation of studies in education and the behavioral sciences* (3rd ed.). EdITS Publishers.

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>

Ivanov, D., Tsipoulanidis, A., and Schönberger, J. (2017). *Global supply chain and operations management. A decision-oriented introduction to the creation of value*. Springer, Cham. <https://link.springer.com/book/10.1007/978-3-319-94313-8>

Ivaturi, K., & Bhagwatwar, A. (2020). Mapping sentiments to themes of customer reactions on social media during a security hack: A justice theory perspective. *Information & Management*, 57(4), 103218. <https://doi.org/10.1016/j.im.2019.103218>

Jakupovic, A., Pavlic, M., & Candrlic, S. (2010, May 19 - 20). Application of analytic hierarchy process (AHP) to measure the complexity of the business sector and business software. *Proceedings of the third C* Conference on Computer Science and Software Engineering* (pp. 35-42). Montréal Quebec, Canada.

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of marketing*, 82(2), 85-105. <https://doi.org/10.1509/jm.16.0124>

- Jbair, M., Ahmad, B., Maple, C., & Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. *Computers in Industry*, 137, 103611. <https://doi.org/10.1016/j.compind.2022.103611>
- Jirkovský, V., Obitko, M., & Mařík, V. (2016). Understanding data heterogeneity in the context of cyber-physical systems integration. *IEEE Transactions on Industrial Informatics*, 13(2), 660-667. <https://doi.org/10.1109/TII.2016.2596101>
- Johnson A, Dempsey K, Ross R, Gupta S, Bailey D (2011) *Guide for security-focused configuration management of information systems*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128. <https://doi.org/10.6028/NIST.SP.800-128>
- Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, 139(3), 719-749. <https://doi.org/10.1016/j.jfineco.2019.05.019>
- Karnouskos, S. (2011, November 7 -10). Stuxnet worm impact on industrial cyber-physical system security. *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society*, 4490-4494. IEEE. Melbourne, Australia. <https://doi.org/10.1109/IECON.2011.6120048>
- Karwatzki, S., Trenz, M., Tuunainen, V. K., & Veit, D. (2017). Adverse consequences of access to individuals' information: An analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems*, 26, 688-715. <https://doi.org/10.1057/s41303-017-0064-z>
- Kashmiri, S., Nicol, C. D., & Hsu, L. (2017). Birds of a feather: Intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science*, 45, 208-228. <https://doi.org/10.1007/s11747-016-0486-5>
- Keeney, S., Hasson, F., & McKenna, H. P. (2001). A critical review of the Delphi technique as a research methodology for nursing. *International Journal of Nursing Studies*, 38(2), 195-200. [https://doi.org/10.1016/S0020-7489\(00\)00044-4](https://doi.org/10.1016/S0020-7489(00)00044-4)
- Kermanshachi, S., Rouhanizadeh, B., & Dao, B. (2020). Application of Delphi method in identifying, ranking, and weighting project complexity indicators for construction projects. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, 12(1), 04519033. <https://doi.org/10.1061/%28ASCE%29LA.1943-4170.0000338>

- Kermanshachi, S., & Safapour, E. (2019). Identification and quantification of project complexity from perspective of primary stakeholders in US construction projects. *Journal of Civil Engineering and Management*, 25(4), 380-398. <https://doi.org/10.3846/jcem.2019.8633>
- 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>
- Khalid, H., Hashim, S. J., Ahmad, S., Hashim, F., & Chaudary, M. A. (2020). Cybersecurity in industry 4.0 context: Background, issues, and future directions. *The Nine Pillars of Technologies for Industry*, 4, 263-307. https://doi.org/10.1049/PBTE088E_ch14
- Khan, F. S., Kim, J. H., Moore, R. L., & Mathiassen, L. (2019). Data breach risks and resolutions: A literature synthesis. *Proceedings of the 25th Americas Conference on Information Systems*. Cancun, Mexico. https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/14
- Khan, F. S., Kim, J. H., Moore, R., & Mathiassen, L. (2021). Data breach management: An integrated risk model. *Information & Management*, 58(1), 103392. <https://doi.org/10.1016/j.im.2020.103392>
- Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, 106, 102267. <https://doi.org/10.1016/j.cose.2021.102267>
- Kharat, M. G., Raut, R. D., Kamble, S. S., & Kamble, S. J. (2016). The application of Delphi and AHP method in environmentally conscious solid waste treatment and disposal technology selection. *Management of Environmental Quality: An International Journal*, 27(4), 427-440. <https://doi.org/10.1108/MEQ-09-2014-0133>
- Khorramshahgol, R., & Moustakis, V. S. (1988). Delphic hierarchy process (DHP): A methodology for priority setting derived from the Delphi method and analytical hierarchy process. *European Journal of Operational Research*, 37(3), 347-354. [https://doi.org/10.1016/0377-2217\(88\)90197-X](https://doi.org/10.1016/0377-2217(88)90197-X)
- Kim, D. S., & Tran-Dang, H. (2019). An overview on industrial control networks. *Industrial Sensors and Controls in Communication Networks*, 3-16. https://doi.org/10.1007/978-3-030-04927-0_1

- Kim, S. T., Lee, H. H., & Hwang, T. (2020). Logistics integration in the supply chain: A resource dependence theory perspective. *International Journal of Quality Innovation*, 6, 1-14. <https://doi.org/10.1186/s40887-020-00039-w>
- Kolevski, D., Michael, K., Abbas, R., & Freeman, M. (2021, July). Cloud data breach disclosures: The consumer and their personally identifiable information (PII)? [Presentation paper]. *2021 IEEE Conference on Norbert Wiener in the 21st century (21CW)* (pp. 1-9). Chennai, India. IEEE. <https://doi.org/10.1109/21CW48944.2021.9532579>
- Lal, N. A., Prasad, S., & Farik, M. (2016). A review of authentication methods. 5, 246-249. https://www.researchgate.net/publication/311514269_A_Review_Of_Authentication_Methods
- Leatham, K. R. (2012). Problems identifying independent and dependent variables. *School Science and Mathematics*, 112(6), 349-358. <https://doi.org/10.1111/j.1949-8594.2012.00155.x>
- Lee, A. H., Chen, W. C., & Chang, C. J. (2008). A fuzzy AHP and BSC approach for evaluating performance of IT department in the manufacturing industry in Taiwan. *Expert systems with applications*, 34(1), 96-107. <https://doi.org/10.1016/j.eswa.2006.08.022>
- Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing letters*, 3, 18-23. <https://doi.org/10.1016/j.mfglet.2014.12.001>
- Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: The International Journal of an Emerging Transdiscipline*, 9, 181-212. <https://doi.org/10.28945/479>
- 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>
- 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](https://doi.org/10.36965/OJAKM.2022.10(1)43-61)

- Levy, Y., & Gafni, R. (2023). Experts' feedback on the cybersecurity footprint elements: In pursuit of a quantifiable measure of SMBs' cybersecurity posture. *Information & Computer Security*. <https://doi.org/10.1108/ICS-05-2023-0083>
- Li, M., & Chen, H. (2021, September 27 - 29). Road safety evaluation based on analytic hierarchy process and entropy weight method. *The 2021 7th International Conference on Industrial and Business Engineering*, 345-350. Macau, China. <https://doi.org/10.1145/3494583.3494586>
- Liang, Z., & Anni, Y. (2021, May 25 - 27). Design of performance evaluation system for transformation of patent achievements in colleges and universities based on AHP. *2021 2nd International Conference on Computers, Information Processing and Advanced Education*, 1070-1076. Ottawa, ON, Canada. <https://doi.org/10.1145/3456887.3457463>
- Liao, L. L., & Lai, I. J. (2017). Construction of nutrition literacy indicators for college students in Taiwan: A Delphi consensus study. *Journal of Nutrition Education and Behavior*, 49(9), 734-742. <https://doi.org/10.1016/j.jneb.2017.05.351>
- Linstone, H. A. & Turoff, M. (2011). Delphi: A brief look backward and forward. *Technological Forecasting and Social Change*, 78(9), 1712-1719. <https://doi.org/10.1016/j.techfore.2010.09.011>
- Linstone, H. A., & Turoff, M. (Eds.). (1975). *The Delphi method* (pp. 3-12). Addison-Wesley.
- Lipner, S. (2004). The trustworthy computing security development lifecycle. *Proceedings of the 20th Annual Computer Security Applications Conference*, 2-13. IEEE, Tucson, Arizona, United States. <https://doi.org/10.1109/CSAC.2004.41>
- Lynch, V. (2017, May 26). *Cost of 2013 Target data breach nears \$300 million*. Hashedout by The SSL Store. <https://www.thesslstore.com/blog/2013-target-data-breach-settled/>
- Ma, Z., Nejat, M. H., Vahdat-Nejad, H., Barzegar, B., & Fatehi, S. (2022). An efficient hybrid ranking method for cloud computing services based on user requirements. *IEEE Access*, 10, 72988-73004. <https://doi.org/10.1109/ACCESS.2022.3189172>
- Madsen, D. Ø. (2019). The emergence and rise of industry 4.0 viewed through the lens of management fashion theory. *Administrative Sciences*, 9(3), 71. <http://dx.doi.org/10.3390/admsci9030071>

- 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>
- Makrakis, G. M., Koliass, C., Kambourakis, G., Rieger, 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>
- Martin, C., Kadry, A., & Abu-Shady, G. (2014, July 23 - 24). Quantifying the financial impact of IT security breaches on business processes. *2014 Twelfth Annual International Conference on Privacy, Security and Trust* (pp. 149-155). IEEE. Toronto, ON, Canada. <https://doi.org/10.1109/PST.2014.6890934>
- Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36-58. <https://doi.org/10.1509/jm.15.0497>
- Masum, R. (2023). Cyber security in smart manufacturing (threats, landscapes challenges). *arXiv preprint arXiv:2304.10180*. <https://doi.org/10.48550/arXiv.2304.10180>
- Matsuda, W., Fujimoto, M., Hashimoto, Y., & Mitsunaga, T. (2021, August). Cyber security risks of technical components in Industry 4.0. *2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS)*, 1-7. IEEE. <https://doi.org/10.1109/COINS51742.2021.9524088>
- Mattoon, J. S. (2005). Designing and developing technical curriculum: Finding the right subject matter expert. *Journal of STEM Teacher Education*, 42(2), 5. <https://ir.library.illinoisstate.edu/jste/vol42/iss2/5>
- McKay, F. H., Zinga, J., & van der Pligt, P. (2022). Consensus from an expert panel on how to identify and support food insecurity during pregnancy: A modified Delphi study. *BMC Health Services Research*, 22(1), 1-11. <https://doi.org/10.1186/s12913-022-08587-x>
- McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. *The Proceedings of the IEEE*, 104(5), 1039-1057. <https://doi.org/10.1109/JPROC.2015.2512235>
- McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, 108, 57-68. <https://doi.org/10.1016/j.dss.2018.02.007>

- Meisner, M. (2017). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting*, 6(3), 63-73. <https://doi.org/10.12775/CJFA.2017.017>
- 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>
- Meng, M. (2013, November). The research and application of the risk evaluation and management of information security based on AHP method and PDCA method [Paper presentation]. *2013 6th International Conference on Information Management, Innovation Management and Industrial Engineering* (Vol. 3, pp. 379-383). IEEE. Xi'an, China. <https://doi.org/10.1109/ICIII.2013.6703597>
- Mertler, C. A., Vannatta, R. A., & LaVenita, K. N. (2021). *Advanced and multivariate statistical methods: Practical application and interpretation*. Routledge. <https://doi.org/10.4324/9781003047223>
- Mishra, P., Pandey, C. M., Singh, U., & Gupta, A. (2018). Scales of measurement and presentation of statistical data. *Annals of Cardiac Anesthesia*, 21(4), 419-422. https://doi.org/10.4103/aca.ACA_131_18
- Mohamed, A. K. Y. S., Auer, D., Hofer, D., & Küng, J. (2022). A systematic literature review for authorization and access control: definitions, strategies and models. *International Journal of Web Information Systems*, 18(2/3), 156-180. <https://doi.org/10.1108/IJWIS-04-2022-0077>
- Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., ... & Ueda, K. (2016). Cyber-physical systems in manufacturing. *Cirp Annals*, 65(2), 621-641. <https://doi.org/10.1016/j.cirp.2016.06.005>
- Morgan, S. (Ed.). (2021, April 27). *Cybercrime to cost the world \$10.5 trillion annually by 2025*. *Cybercrime Magazine*. <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>
- Müller, J. M., & Voigt, K. I. (2018). Sustainable industrial value creation in SMEs: A comparison between industry 4.0 and made in China 2025. *International Journal of Precision Engineering and Manufacturing-Green Technology*, 5, 659-670. <https://doi.org/10.1007/s40684-018-0056-z>

- Mullet, V., Sonni, 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>
- Muzatko, S., & Bansal, G. (2020). Consumer skepticism as it relates to E commerce data breaches and company efforts to enhance trust. *Proceedings of the 2020 Midwest Association for Information (WAIS)*. <https://aisel.aisnet.org/mwais2020/22/>
- Naanani, A. (2021). Security in Industry 4.0: Cyber-attacks and countermeasures. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(10), 6504-6512. <https://doi.org/10.17762/turcomat.v12i10.5501>
- Nahar, K., Gill, A. Q., & Roach, T. (2021). Developing an access control management metamodel for secure digital enterprise architecture modeling. *Security and Privacy*, 4(4), e160. <https://doi.org/10.1002/spy2.160>
- Nasa, P., Jain, R., & Juneja, D. (2021). Delphi methodology in healthcare research: How to decide its appropriateness. *World Journal of Methodology*, 11(4), 116. <https://doi.org/10.5662/wjm.v11.i4.116>
- 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>
- National Defense Industrial Association (NDIA) (2014). *Cybersecurity for advanced manufacturing*. https://www.ndia.org/-/media/sites/ndia/policy/documents/cyber/cyber_for_manufacturing_white_paper_5may14.ashx?la=en
- Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security*, 92, 101731. <https://doi.org/10.1016/j.cose.2020.101731>
- 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>
- Norman, D., Bhargava, N., Harmon, M., Wright, J., Springs, D., & Dawson, M. (2020). Supply chain and logistics management and an open door policy concerning cyber

- security introduction. *International Journal of Management*, 9(1), 1-10.
<https://doi.org/10.18488/journal.11.2020.91.1.10>
- Odu, G. O. (2019). Weighting methods for multi-criteria decision making technique. *Journal of Applied Sciences and Environmental Management*, 23(8), 1449-1457. <https://doi.org/10.4314/jasem.v23i8.7>
- Önder, E., & Hepsten, A. (2013). Combining time series analysis and multi criteria decision making techniques for forecasting financial performance of banks in Turkey. *International Journal of Latest Trends in Finance and Economic Sciences*, 3(3), 530-555. <https://ssrn.com/abstract=2332207>
- Ouellette, M. (2023). Operational technology vulnerabilities combined with low tolerance for downtime to put manufacturers in cyber-attackers' crosshairs. <https://www.engineering.com/story/manufacturing-was-the-most-targeted-sector-for-ransomware-attacks-in-2022-says-ibm>
- O. U. S. D. A. S. (n.d.). Securing the defense industrial base. OUSD A&S - Cybersecurity Maturity Model Certification (CMMC). <https://www.acq.osd.mil/cmmc/>
- Palanisamy, R., Norman, A. A., & Kiah, M. L. M. (2020). Compliance with bring your own device security policies in organizations: A systematic literature review. *Computers & Security*, 98, 101998. <https://doi.org/10.1016/j.cose.2020.101998>
- Pamidimukkala, A., Kermanshachi, S., & Kamali Rad, S. (2023). Ranking and weighting effective project-based communication indicators for primary and secondary stakeholders in construction projects. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, 15(1), 05022006. [https://doi.org/10.1061/\(ASCE\)LA.1943-4170.0000581](https://doi.org/10.1061/(ASCE)LA.1943-4170.0000581)
- Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: A conceptual framework. *Journal of Global Operations and Strategic Sourcing*. <https://doi.org/10.1108/JGOSS-05-2019-0042>
- Paraskevas, A. & Saunders, M.N. (2012). Beyond consensus: An alternative use of Delphi enquiry in hospitality research. *International Journal of Contemporary Hospitality Management*, 24(6), 907-924. <https://doi.org/10.1108/09596111211247236>
- Pei, J., Liu, W., & Han, L. (2019). Research on evaluation index system of Chinese City safety resilience based on Delphi method and cloud model. *International Journal of Environmental Research and Public Health*, 16(20), 3802. <https://doi.org/10.3390/ijerph16203802>

- Peisheng, L., Yunping, H., Xiaole, Z., Shunshun, W., & Zhenglin, L. (2020). Research on information system risk assessment based on improved AHP-fuzzy theory. In *Journal of Physics: Conference Series* (Vol. 1693, No. 1, p. 012046).
<https://doi.org/10.1088/1742-6596/1693/1/012046>
- Peters, H. M. (2020). *Defense acquisitions: DODs cybersecurity maturity model certification framework*. Library of Congress, Washington, D.C.
<https://apps.dtic.mil/sti/pdfs/AD1146340.pdf>
- Petrova, V. (2021). A cybersecurity risk assessment. *Industry 4.0*, 6(1), 37-40.
- Pilloni, V. (2018). How data will transform industrial processes: Crowdsensing, crowdsourcing and big data as pillars of industry 4.0. *Future Internet*, 10(3), 24.
<https://doi.org/10.3390/fi10030024>
- 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
- Powell, C. (2003). The Delphi technique: myths and realities. *Journal of Advanced Nursing*, 41(4), 376-382. <https://doi.org/10.1046/j.1365-2648.2003.02537.x>
- Prinsloo, J., Sinha, S., & von Solms, B. (2019). A review of industry 4.0 manufacturing process security risks. *Applied Sciences*, 9(23), 5105.
<https://doi.org/10.3390/app9235105>
- Qader, G., Junaid, M., Abbas, Q., & Mubarik, M. S. (2022). Industry 4.0 enables supply chain resilience and supply chain performance. *Technological Forecasting and Social Change*, 185, 122026. <https://doi.org/10.1016/j.techfore.2022.122026>
- Quyên, D. T. N. (2014). Developing university governance indicators and their weighting system using a modified Delphi method. *Procedia-Social and Behavioral Sciences*, 141, 828-833. <https://doi.org/10.1016/j.sbspro.2014.05.144>
- Rad, F. F., Oghazi, P., Palmié, M., Chirumalla, K., Pashkevich, N., Patel, P. C., & Sattari, S. (2022). Industry 4.0 and supply chain performance: A systematic literature review of the benefits, challenges, and critical success factors of 11 core technologies. *Industrial Marketing Management*, 105, 268-293.
<https://doi.org/10.1016/j.indmarman.2022.06.009>
- Radichel, T. (2014). Case study: Critical controls that could have prevented Target breach. *SANS Institute InfoSec Reading Room*.

- Raghuram, P., Sandeep, P., Sreedharan, V. R., & Saikouk, T. (2021). Development of a supply chain risk mitigation index for distillery. *The TQM Journal*, 33(3), 618-639. <https://doi.org/10.1108/TQM-01-2020-0008>
- Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, 2(1), 122-136. http://www.iiakm.org/ojakm/articles/2014/volume2_1/OJAKM_Volume2_1pp122-136.pdf
- Richardson, V. J., Smith, R. E., & Watson, M. W. (2019). Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems*, 33(3), 227-265. <https://doi.org/10.2308/isys-52379>
- Richey, R. C., & Klein, J. D. (2005). Developmental research methods: Creating knowledge from instructional design and development practice. *Journal of Computing in higher Education*, 16(2), 23-38. <https://doi.org/10.1007/BF02961473>
- 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. <https://www.earticle.net/Article/A147480>
- Romano, A. R. (2010). Malleable Delphi: Delphi research technique, its evolution, and business applications. *International Review of Business Research Papers*, 6(5), 235-243.
- Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121-135. <https://doi.org/10.1093/cybsec/tyw001>
- Roszkowska, E. (2013). Rank ordering criteria weighting methods—a comparative overview. *Optimum. Studia Ekonomiczne*, 5(65), 14-33. <https://doi.org/10.15290/ose.2013.05.65.02>
- 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>
- Savin, V. D. (2021). Cyber-security in the new era of integrated operational-informational technology systems. *Business Excellence and Management*, 11(1), 68-79. <https://doi.org/10.24818/beman/2021.11.1-05>

- Say, G., & Vasudeva, G. (2020). Learning from digital failures? The effectiveness of firms' divestiture and management turnover responses to data breaches. *Strategy Science*, 5(2), 117-142. <https://doi.org/10.1287/stsc.2020.0106>
- Schiliro, F. (2023). *Building a resilient cybersecurity posture: A framework for leveraging prevent, detect and respond functions and law enforcement collaboration*. arXiv e-prints:2303.10874. <https://doi.org/10.48550/arXiv.2303.10874>
- Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information & Management*, 103638. <https://doi.org/10.1016/j.im.2022.103638>
- Schroeder, A., Ziaee Bigdeli, A., Galera Zarco, C., & Baines, T. (2019). Capturing the benefits of industry 4.0: A business network perspective. *Production Planning & Control*, 30(16), 1305-1321. <https://doi.org/10.1080/09537287.2019.1612111>
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. John Wiley & Sons.
- Setiadi, F., Rubhasy, A., & Hasibuan, Z. A. (2018). *Identifying and validating components for national cyber security framework* [Presentation paper]. 2018 Third International Conference on Informatics and Computing (ICIC), 1-5. IEEE. Palembang, Indonesia. <https://doi.org/10.1109/IAC.2018.8780441>
- Sharma, S. K. (2014). Risk management in construction projects using combined analytic hierarchy process and risk map framework. *The IUP Journal of Operations Management*, 7(4), 23 – 53.
- Shaver, J. P. (1993). What statistical significance testing is, and what it is not. *The Journal of Experimental Education*, 61(4), 293-316. <https://doi.org/10.1080/00220973.1993.10806592>
- Shen, L., Yang, J., Jin, X., Hou, L., Shang, S., & Zhang, Y. (2019). Based on Delphi method and analytic hierarchy process to construct the evaluation index system of nursing simulation teaching quality. *Nurse Education Today*, 79, 67-73. <https://doi.org/10.1016/j.nedt.2018.09.021>
- Shi, C., Zhang, Y., Li, C., Li, P., & Zhu, H. (2020). Using the Delphi method to identify risk factors contributing to adverse events in residential aged care facilities. *Risk Management and Healthcare Policy*, 13, 523. <https://doi.org/10.2147/RMHP.S243929>

- Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017). Breaking the target: An analysis of target data breach and lessons learned. *arXiv preprint arXiv:1701.04940*.
<https://arxiv.org/pdf/1701.04940>
- Sikich LLP. (2019). *Transforming for tomorrow*. <https://sikich.com/wp-content/uploads/2019/06/SKCH-MD-Report-2019-1.pdf>
- Sipahi, S., & Timor, M. (2010). The analytic hierarchy process and analytic network process: An overview of applications. *Management decision*, 48(5), 775-808.
<https://10.1108/00251741011043920>
- Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education: Research*, 6(1), 1-21.
Retrieved February 25, 2023, from <https://www.learntechlib.org/p/111405/>
- Small Business Agency (SBA) (2019). *SBA's size standards methodology*.
<https://www.sba.gov/sites/default/files/2021-02/SBA%20Size%20Standards%20Methodology%20April%2011%2C%202019-508.pdf>
- Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics*, 9(11), 1864-1895.
<https://doi.org/10.3390/electronics9111864>
- Soltovski, R., Rodrigues, T. V., Pontes, J., & Resende, L. M. M. (2019). Theoretical framework of the industry 4.0 risks from sustainability perspective. *Revista Competitividade e Sustentabilidade*.
- Song, H., Lu, X., Wu, Q., Xu, Y., & Peng, B. (2020). Weight calculation method for consumer goods risk assessment indexes based on analytic hierarchy process [Paper presentation]. *Proceedings of the IOP Conference Series: Earth and Environmental Science*. <https://doi.org/10.1088/1755-1315/440/4/042001>
- Song, Y., Faklaris, C., Cai, Z., Hong, J. I., & Dabbish, L. (2019). Normal and easy: Account sharing practices in the workplace. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1-25. <https://doi.org/10.1145/3359185>
- Song, Z., Wang, G. A., & Fan, W. (2017, January 4 - 7). Firm actions toward data breach incidents and firm equity value: An empirical study [Paper presentation]. *Proceedings of the 50th Hawaii International Conference on System Sciences*, Hawaii, USA.
<https://doi.org/10.24251/HICSS.2017.602>.

- Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, 58, 216-229. <https://doi.org/10.1016/j.cose.2015.12.006>
- Srinivas, S., & Liang, H. (2022). Being digital to being vulnerable: Does digital transformation allure a data breach? *Journal of Electronic Business & Digital Economics*, 1(1/2), 111-137. <https://doi.org/10.1108/JEBDE-08-2022-0026>
- Statista, I. H. S. (2018). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>
- Still, J. D., Cain, A., & Schuster, D. (2017). Human-centered authentication guidelines. *Information & Computer Security*, 25(4), 437-453. <https://doi.org/10.1108/ICS-04-2016-0034>
- Stokes, A., & Childress, M. (2020). The cybersecurity maturity model certification explained: What defense contractors need to know. <https://www.csoonline.com/article/3535797/the-cybersecurity-maturity-model-certification-explained-what-defense-contractors-need-to-know.html>
- Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, 22(2), 1191-1221. <https://doi.org/10.1109/COMST.2019.2962586>
- 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.
- Suparji, S., Nugroho, H. S. W., & Martiningsih, W. (2021). Tips for distinguishing nominal and ordinal scale data. *Aloha International Journal of Multidisciplinary Advancement (AIJMU)*, 1(6), 133-135. <https://doi.org/10.33846/aijmu10602>
- Sutadian, A. D., Muttill, N., Yilmaz, A. G., & Perera, B. J. C. (2016). Development of river water quality indices—a review. *Environmental Monitoring and Assessment*, 188, 1-29. <https://doi.org/10.1007/s10661-015-5050-0>
- Sutrisno, S., Prasetyo, H. A., & Faot, A. I. (2022). The measurement of human resources employees by using human resources score card method and analytical hierarchy process method. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, 5(2). <https://doi.org/10.33258/birci.v5i2.5713>

- Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security*, 12(3), 417-432. <https://doi.org/10.17762/ijcnis.v12i3.4817>
- Syed, N. F., Shah, S. W., Trujillo-Rasua, R., & Doss, R. (2022). Traceability in supply chains: A cyber security analysis. *Computers & Security*, 112, 102536. <https://doi.org/10.1016/j.cose.2021.102536>
- Syed, R. (2019). Enterprise reputation threats on social media: A case of data breach framing. *The Journal of Strategic Information Systems*, 28(3), 257-274. <https://doi.org/10.1016/j.jsis.2018.12.001>
- Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards: A review and comprehensive overview. *Electronics*, 11(14), 2181, 1-20. <https://doi.org/10.3390/electronics1114218>
- Tanimura, J. K., & Wehrly, E. W. (2009). The market value and reputational effects from lost confidential information. *International Journal of Financial Management (October 2015) Vol, 5*, 18-35. <https://dx.doi.org/10.2139/ssrn.1083891>
- Tanriverdi, H., Kwon, J., & Im, G. (2020). Data Breaches in multihospital systems: Antecedents and mitigation mechanisms. https://aisel.aisnet.org/icis2020/cyber_security_privacy/cyber_security_privacy/10/
- Taylor, E. (2020). We agree, don't we? The Delphi method for health environments research. *HERD: Health Environments Research & Design Journal*, 13(1), 11-23. <https://doi.org/10.1177/1937586719887709>
- Tavana, M., Soltanifar, M., & Santos-Arteaga, F. J. (2021). Analytical hierarchy process: Revolution and evolution. *Annals of operations research*, 1-29. <https://doi.org/10.1007/s10479-021-04432-2>
- Teng, Y. M., Wu, K. S., & Wang, M. J. (2020). Using the analytic hierarchy process (AHP) and Delphi analysis to evaluate key factors in the development of the Taiwan cruise tourism industry. *Journal of Coastal Research*, 36(4), 828-833. <https://doi.org/10.2112/JCOASTRES-D-19-00162.1>
- Trappey, A. J., Trappey, C. V., Govindarajan, U. H., Sun, J. J., & Chuang, A. C. (2016). A review of technology standards and patent portfolios for enabling cyber-physical systems in advanced manufacturing. *IEEE Access*, 4, 7356-7382. <https://doi.org/10.1109/ACCESS.2016.2619360>

- Tuptuk, N., & Hailes, S. (2018). Security of smart manufacturing systems. *Journal of Manufacturing Systems*, 47, 93-106. <https://doi.org/10.1016/j.jmsy.2018.04.007>
- Turnbull, A. E., Dinglas, V. D., Friedman, L. A., Chessare, C.M., Sepúlveda, K. A., Bingham, C. O., Needham, D. M. (2018). A survey of Delphi panelists after core outcome set development revealed positive feedback and methods to facilitate panel member participation. *Journal of Clinical Epidemiology*, 102(410), 99–106. <https://doi.org/10.1016/j.jclinepi.2018.06.007>
- Turnbull, B. (2018). Cyber-resilient supply chains: Mission assurance in the future operating environment. *Australian Army Journal*, 14(2), 41-56. <https://search.informit.org/doi/pdf/10.3316/ielapa.344417545553155>
- Udofot, M., & Topchyan, R. (2020). Factors related to small business cyber-attack protection in the United States. *International Journal of Cyber-Security and Digital Forensics*, 9(1), 12-25.
- Ulschak, F. L. (1983). Human resource development: The theory and practice of need assessment. Reston Publishing Company.
- Verizon. (2022). Data breach investigations report (DBIR). <https://www.verizon.com/business/resources/Tfa7/reports/dbir/2022-data-breach-investigations-report-dbir.pdf>
- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118-144. <https://doi.org/10.1016/j.jsis.2019.01.003>
- Vincent, H., Wells, L., Tarazaga, P., & Camelio, J. (2015). Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems. *Procedia Manufacturing*, 1, 77-85. <https://doi.org/10.1016/j.promfg.2015.09.065>
- von der Gracht, H.A. (2012). Consensus measurement in Delphi studies: Review and implications for future quality assurance. *Technological Forecasting and Social Change*, 79(8), 1525–1536. <https://doi.org/10.1016/j.techfore.2012.04.013>
- Wang, G. (2021). Research on network security risk assessment method based on improved analytic hierarchy process. *International Journal of Network Security*, 23(3), 515-521. [https://doi.org/10.6633/IJNS.202105_23\(3\).17](https://doi.org/10.6633/IJNS.202105_23(3).17)

- Wang, H., Liu, H., Kim, S. J., & Kim, K. H. (2019). Sustainable fashion index model and its implication. *Journal of Business Research*, 99, 430-437.
<https://doi.org/10.1016/j.jbusres.2017.12.027>
- Wang, P., D'Cruze, H., & Wood, D. (2019). Economic costs and impacts of business data breaches. *Issues in Information Systems*, 20(2), 162-173.
https://doi.org/10.48009/2_iis_2019_162-171
- Wang, Y., & Liu, B. (2021). The effect of supplier globalization on firm innovation: A resource dependence theory perspective. *Industrial Management & Data Systems*, 121(12), 2450-2466. <https://doi.org/10.1108/IMDS-01-2021-0070>
- Warren, M., & Hutchinson, W. (2000). Cyber attacks against supply chain management systems: A short note. *International Journal of Physical Distribution & Logistics Management*, 30(7/8), 710-716. <https://doi.org/10.1108/09600030010346521>
- Wash, R., & Rader, E. (2021). Prioritizing security over usability: Strategies for how people choose passwords. *Journal of Cybersecurity*, 7(1), 1-17.
<https://doi.org/10.1093/cybsec/tyab012>
- Wei, C. C., Chien, C. F., & Wang, M. J. J. (2005). An AHP-based approach to ERP system selection. *International Journal of Production Economics*, 96(1), 47-62.
<https://doi.org/10.1016/j.ijpe.2004.03.004>
- Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X., & Terpenney, J. (2018). Cybersecurity for digital manufacturing. *Journal of Manufacturing Systems*, 48, 3-12.
<https://doi.org/10.1016/j.jmsy.2018.03.006>
- Wu, J. J., Mazzuchi, T. A., & Sarkani, S. (2023). Comparison of multi-criteria decision-making methods for online controlled experiments in a launch decision-making framework. *Information and Software Technology*, 155, 107115.
<https://doi.org/10.1016/j.infsof.2022.107115>
- Xiao, C., Petkova, B., Molleman, E., & van der Vaart, T. (2019). Technology uncertainty in supply chains and supplier involvement: The role of resource dependence. *Supply Chain Management: An International Journal*, 24(6), 697-709.
<https://doi.org/10.1108/SCM-10-2017-0334>
- Xinlan, Z., Zhifang, H., Guangfu, W., & Xin, Z. (2010, December). Information security risk assessment methodology research: Group decision making and analytic hierarchy process. 2010 Second World Congress on Software Engineering (Vol. 2, pp. 157-160). IEEE. <https://doi.org/10.1109/WCSE.2010.55>

- Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems*, 77, 103201. <https://doi.org/10.1016/j.micpro.2020.103201>
- Yao, X., Zhou, J., Lin, Y., Li, Y., Yu, H., & Liu, Y. (2019). Smart manufacturing based on cyber-physical systems and beyond. *Journal of Intelligent Manufacturing*, 30, 2805-2817. <https://doi.org/10.1007/s10845-017-1384-5>
- Yeboah-Ofori, A., Abdulai, J., & Katsriku, F. (2019). Cybercrime and risks for cyber physical systems. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 8(1), 43-57. <https://doi.org/10.17781/P002556>
- Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. *Future Internet*, 11(3), 63-88. <https://doi.org/10.3390/fi11030063>
- Zaburko, J., & Szulżyk-Cieplak, J. (2019, December). Information security risk assessment using the AHP method. *IOP Conference Series: Materials Science and Engineering*, 701(1), 012036. <https://doi.org/10.1088/1757-899X/710/1/012036>
- Zafar, H., Ko, M., & Osei-Bryson, K. M. (2012). Financial impact of information security breaches on breached firms and their non-breached competitors. *Information Resources Management Journal (IRMJ)*, 25(1), 21-37. <https://doi.org/10.4018/irmj.2012010102>
- Zheng, T., Ardolino, M., Bacchetti, A., & Perona, M. (2021). The applications of industry 4.0 technologies in manufacturing context: A systematic literature review. *International Journal of Production Research*, 59(6), 1922-1954. <https://doi.org/10.1080/00207543.2020.1824085>
- Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access*, 9, 29775-29818. <https://doi.org/10.1109/ACCESS.2021.3058403>
- Zviran, M., & Erlich, Z. (2006). Identification and authentication: Technology and implementation issues. *Communications of the Association for Information Systems*, 17(1), 4. <https://doi.org/10.17705/1CAIS.01704>