Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 10, Issue 1, 2022

Towards the quantification of cybersecurity footprint for SMBs using the CMMC 2.0

Yair Levy, Nova Southeastern University, USA, levyy@nova.edu

Ruti Gafni, The Academic College of Tel Aviv Yaffo, Israel, rutigafn@mta.ac.il

Abstract

Organizations, small and big, have been facing major cybersecurity challenges over the past several decades, as the proliferation of information systems and mobile devices expand. While larger organizations invest significant efforts in developing approaches to deal with cybersecurity incidents, Small and Medium Businesses (SMBs) are still struggling with ways to both keep their businesses alive and secure their systems to the best of their abilities. When it comes to critical systems, such as defense industries, the interconnectivities of organizations in the supply-chain have demonstrated to be problematic given the depth required to provide a high-level cybersecurity posture. The United States (U.S.) Department of Defense (DoD) with the partnership of the Defense Industrial Base (DIB) developed the Cybersecurity Maturity Model Certification (CMMC) in 2020 with a third-party mandate for Level 1 certification. Following an outcry from many DIB organizations, a newly revised CMMC 2.0 was introduced in late 2021 where Level 1 (Fundamental) was adjusted for annual self-assessment. CMMC 2.0 provides the 17 practices that organizations should self-assess. While these 17 practices provide initial guidance for assessment, the specific level of measurement and how it impacts their overall cybersecurity posture is vague. Specifically, many of these practices use non-quantifiable terms such as "limit", "verify", "control", "identify", etc. The focus of this work is to provide SMBs with a quantifiable method to self-assess their Cybersecurity Footprint following the CMMC 2.0 Level 1 practices. This paper outlines the foundational literature work conducted in support of the proposed quantification Cybersecurity Footprint Index (CFI) using 26 elements that correspond to the relevant CMMC 2.0 Level 1 practices.

Keywords: Cybersecurity of SMBs, CMMC, Cybersecurity Footprint, cybersecurity self-assessment, Cybersecurity Footprint Index (CFI), CFI Elements.

Introduction

Small and Medium Businesses (SMBs) are significant to economic development in most countries, especially within the western world, as they represent the majority of businesses (Renaud & Ophoff, 2021; Ward, 2021). Gafni and Pavel (2019) noted that SMBs, a term usually used in the United States (U.S.), while in Europe it is known as Small and Medium Enterprises (SME), may vary in size between countries. Different regions have their own definition of "small or medium" and often is measured by the number of employees. For example, the European Commission (2022) indicated that organizations with less than 250 employees are considered SMEs. In the U.S., organizations with less than 500 employees are considered SMBs (U.S. Small Business

Agency, 2020), while other countries such as Israel are accounting SMBs as organizations with 100 or fewer employees (Israel - Small Business Agency, 2022). When it comes to Information Systems (IS), SMBs are different than larger companies as a significant number of SMBs rely on basic IS and don't have an Information Technology (IT) or IT staff on-premises given that their IT needs are usually limited (Lopez-Nicolas & Soto-Acosta, 2010; Gafni & Pavel, 2019). Additionally, news media, scholarly research outlets, and government reports have documented the massive increase in data breaches as well as cyberattacks along with their daily impact on large and small organizations (Gafni & Pavel, 2019). While larger organizations have teams of IS professionals to mitigate such cybersecurity risks, and also ensure the organization is prepared for a data breach, SMBs have limited awareness, and therefore, lack cybersecurity preparedness (Bada & Nurse, 2019). The current level of data breach risk as well as the cybersecurity awareness and business preparedness (if any) of SMBs are still unclear. While underestimating the risk, SMBs are very vulnerable to cyberattacks. The Federal Bureau of Investigation (FBI)'s Internet Crime Report estimated that in 2021, the cost of cybercrimes reached $6.9 trillion (FBI, 2022). Additionally, according to the U.S. Small Business Administration (2022), "Small businesses are attractive targets because they have information that cybercriminals want, and they typically lack the security infrastructure of larger businesses" (para. 2). Moreover, a recent U.S. Small Business Administration (2022) survey revealed that "88% of small business owners felt their business was vulnerable to a cyber-attack. Yet many businesses can't afford professional IT solutions, have limited time to devote to cybersecurity, or they don't know where to begin" (para. 3).

Many SMBs are part of the supply-chain of larger organizations and can cause significant disruptions to a whole industry if compromised and triggered a ripple effect (Rezaei et al., 2015). Thakkar et al. (2008) indicated this interconnection by noting that the "present focus of SCM [Supply-Chain Management] research is found inclined to large-scale organizations where small businesses act as an ancillary/1st and 2nd tier suppliers in their supply-chain" (p. 98). Levy and Gafni (2021) described that supply-chain impact on interconnected entities as "the domino effect" when introducing the concept of Cybersecurity Footprint, which is "the potential malicious impact to an entity (organizational or individual) and/or its cascading effects on interconnected entities" (p. 725). They further noted that Cybersecurity Footprint emerges from cybersecurity incidents during data movements, data processing, leakage from data storage, or other traceable digital footprints activities. According to Levy and Gafni (2021), Cybersecurity Footprint provides a theoretical approach for organizations to track their own cybersecurity posture, understand how the actions of others in their supply-chain impact their cybersecurity posture, and be able to assess how their decisions may impact other organizations in their supply-chain, especially upstream. However, when it comes to SMBs, researchers have been warning that they are lacking proper cybersecurity practices (Bada & Nurse, 2019). Moreover, it appears that the business owners or key decision makers of SMBs aren't fully comprehending how to assess the cybersecurity posture of their organization (Udofot & Topchyan, 2020).

The United States (U.S.) Department of Defense (DoD) has worked over the past several years to develop and implement the Cybersecurity Maturity Model Certification (CMMC) to address the Cybersecurity Footprint in the Defense Industrial Base (DIB)'s supply-chain which includes over 300,000 companies, many of which are SMBs. However, the CMMC includes requirements that are difficult for such SMBs to implement. Therefore, in this research-in-progress, we propose a process for the quantification of Cybersecurity Footprint for SMBs following the CMMC 2.0 (U.S. DoD, 2022) to form the Cybersecurity Footprint Index (CFI) that will provide organizations an index measure ranging from 0 to 100 to further help executives realize the level of Cybersecurity Footprint their organization has at any given point. To accomplish the development of such CFI, two steps were identified. First, the proper elements to measure the CFI should be identified following CMMC 2.0. Second, once the elements are identified, an empirical assessment should be conducted to collect the weight of each domain and the aggregation method to combine them into a single CFI. This research-in-progress paper deals with the first step, in which the Cybersecurity Footprint elements are identified, linked to the CMMC 2.0, and a significant peer-review publications assessment was done to identify the relevant literature in support of the elements.

Background

The Cybersecurity Challenge at SMBs

Contemporary societies and their organizational systems are increasingly exposed to unexpected disruptive events (Pettit et al., 2013; Tu et al., 2018). The actual global pandemic scenario is arguably one of the most impacting scenarios after World War II. The social distancing rules created due to COVID-19 provide a massive acceleration for the digital revolution, increasing the use of the Internet in activities for transactions in many areas of the world and also for people of every age. The social changes due to the COVID-19 pandemic have seriously impacted the majority of SMBs (Baron & Francois, 2020). Even before this digital revolution, evidence from different reports and global analyses affirms that cyber threats do not only continuously spread to every size of organizations, but are increasingly more being directed at SMBs (U.S. Small Business Agency, 2020). At the same time, cyberattacks become increasingly sophisticated, targeted, and coordinated, resulting in advanced persistent threats (Farwell et al., 2011). These threats become progressively more complex and take full advantage of the vulnerabilities—such as insider threats and human errors—within applications, network infrastructure assets, and social engineering (Carlton & Levy, 2017). Additionally, the Federal Bureau of Investigation (FBI) (2021) Internet Computer Complaint Center (IC3) reported an over 230% increase in cyberattacks in 2020 due to COVID-related scams, many of them targeted at SMBs. Moreover, Gafni and Pavel (2021) noted that “there was a significant growth in reports of cyberattacks on the health-care sector” (p. 137). Consequently, a new approach is necessary especially because the use of IS has become more widespread and organizations rely on IS to the extent that it would be impossible to manage their business without technology solutions (Paananen et al., 2020).

Organizations usually recognize that cybersecurity is a challenge to manage, but they often do not know how to deal with it (Tu et al., 2018). However, it is noteworthy that there are significant differences, depending on the size of the organization under attack, regarding the strategic approach to mitigate cyber threats (Goel et al., 2020). Particularly, SMBs have a weak understanding of IS, security technologies, and control measures, while appearing to neglect risk assessments or the development of security policies (Bada & Nurse, 2019). It is evident that most of the SMBs depended on their IS for their various business activities without even knowing how to secure their information and data from cyberattacks (Gafni & Pavel, 2019). However, cybersecurity nowadays, is the most pervasive challenge for SMBs because, according to Bell (2017), cybersecurity requires an element of specialist knowledge to be operational, often thought to be a technical person, and it also requires a budget. This is because owners, managers, and decision-makers of small businesses are worried about everyday business matters, mainly their revenues, and often neglect cybersecurity issues, resulting in an increase in vulnerability to cybercrime (Bhattacharya, 2013).

Researchers have recommended a multi-perspective approach for SMBs to protect organizations' information assets against threats, i.e., risks of data breach and cyber incidents (Tu et al., 2018; Udofot & Topchyan, 2020). A comprehensive cybersecurity approach normally includes physical, procedural, and logical forms of protection (Baskerville et al*.,* 2014; Goel et al., 2020). In this perspective, organizations need to implement appropriate employee awareness training to foster a security culture, particularly within SMBs where resources have usually been limited (Sadok et al., 2020). Technical solutions to the cybersecurity problem are not sufficient in providing total organizational cybersecurity (Li et al., 2019). Moreover, the organizational cybersecurity challenge is not new and has been a major challenge for over four decades, especially as it is considered to be related not only to the security of the official organizational IS but also to the unofficial ISs, such as Bring Your Own Device (BYOD) (Bello et al., 2017; Von Solms, & Von Solms, 2018). However, the challenge is even greater for SMBs, especially as they do not have the sources required for such sophisticated monitoring systems and security technologies (Levy & Niccolini, 2019; Verizon, 2020; U.S. Small Business Administration, 2022). For SMBs, a fundamental approach to cyber-attacks is first and foremost cyber preparedness (Bodeau & Graubart, 2017).

To face the cybersecurity threats effectively, SMBs need to develop a networking approach, especially creating relationships with strategic partners and national authorities (Baskerville et al., 2014; Bada & Nurse, 2019). A relevant goal of this approach is to create an extensive and systemic situational awareness perspective about potential threats (Skopik et al., 2016). This goal appears to be crucial in today's scenarios due to the significant absence of policies and procedures about cybersecurity implemented by many SMBs (U.S. Small Business Administration, 2022). However, accurate knowledge management and artificial intelligence are essential to identify cyber threats, reduce risks and uncertainty, and stimulate awareness management (Gafni & Pavel, 2019). Awareness refers to continuous and regular attention that protects the organization (Safa et al., 2015). Cybersecurity awareness, also noted as the Security Education, Training, and Awareness (SETA) program, is the first step to protecting against cyber threats (Angst et al., 2017). SETA has been traditionally viewed as an initial condition for organizational users to develop a deep consciousness of the organizational security mission (Alshaikh et al., 2020). According to the literature, SETA has played a major role in cybersecurity preparedness, as users are well prepared to deal with cyber threats (Alshaikh et al., 2020; Yoo et al., 2018). Furthermore, SETA provides organizational awareness about acceptable behavior, as it relates to the cybersecurity triad concepts: Confidentiality, Availability, and Integrity (CIA) (Uchendu et al., 2021). Hence, SETA as the first foundational step toward cybersecurity preparedness must be embedded in the organizational culture. All the other typologies of culture—also cybersecurity preparedness—should be considered and approached as a collective phenomenon that constantly changes over time and that can be promoted by the leaders because cybersecurity preparedness emerges as a competency that is presently critical for the survival of organizations (Benz & Chatterjee, 2020).

The development of a cybersecurity culture involves knowledge sharing and learning mechanisms (Uchendu et al., 2021). Moreover, it must rely on continuous training, communication, analysis, and evaluation to continuously increase the awareness of all employees, improve skills, fill knowledge gaps, and ensure responsibility as well as accountability (Macmillan, 2017). It has been pointed out that in many cyberattacks, the behaviors of employees are the root cause of the exploited organization (Leukfeldt, 2014). Furthermore, the end-user has often been a critical backdoor into the organizational network, even if the system has a high level of security in place (Ani et al., 2019). In this perspective, human aspects become central, particularly as a source of organizational resilience (Neigel et al., 2020). Therefore, organizational resilience can be understood as the ability of an organization to persist after a disturbance and to reorganize or arise while sustaining essentially the same functions (Sepúlveda Estay et al., 2020). According to McDonald (2017), resilience represents the capacity of an organization to anticipate and manage risk effectively through an appropriate adaptation of its employees' actions, systems, and processes, to ensure that the organization's core functions are carried out in a stable and effective relationship with the environment.

Overview of Maturity Models

Maturity is not a new term and has been defined in various disciplines of an individual, object, process, concept, entity, or organization (Mirskaia & Crew, 1931; Serenko et al., 2016). In its basic form, maturity is defined as how close an individual, process, or organization is to the most advanced stage (Mettler, 2011). Serenko et al. (2016) defined maturity as "the state of perfection, fullness, or readiness which evolved from an initial (embryonic) to an advanced stage" (p. 340). Maturity is commonly expressed in several stages of development that are characterized by the ability of the individual, process, or organization to achieve the required tasks indicated for a given level (Rabii et al., 2020; Schmitz et al., 2021). Such expressions of maturity are conceptualized in a tiered model, known as a Maturity Model, which has been developed for various fields of practice. Maturity models emerged from the software engineering and process improvement areas in the late 1980s. They represent sequentially increasing maturity stages of the assessed entity, known as Maturity Levels (Mettler, 2011). When attempting to progress in the maturity levels, one must first complete and be able to attain all the requirements in one level to move consecutively to the next level, and then must complete all that next level requirements before it can be recognized at that next level. An analogy can be made to the maturity of a human motor skills development. Similar to that of a newborn which first crawls (e.g. Level 1) and then matures to a walking child level (e.g. Level 2), which then matures to a running child (e.g. Level 3), and into adulthood (e.g. Levels 4+5) - hence their often another name in the social sciences "stages-of-growth models" (Serenko et al., 2016). Assessment of the requirements can be done either via self-assessment, which can be questionable in some fields of practice, or conducted by a third party (Mettler, 2011).

CMMC 1.0 and 2.0

The Cybersecurity Maturity Model Certification (CMMC) was established in 2019 from the initial work of the U.S. DoD to enhance the cybersecurity posture of the DIB that includes a supply-chain with over 300,000 companies (Stokes & Childress, 2020). The initial work, noted as CMMC 1.0, included five maturity levels with 15 original domains. It was put in place in 2020, and later in December 2021 was revised to include three maturity levels with 14 domains, and also aligned Level 2 to the NIST SP 800-171-R2 (Ross, Pillitteri, Dempsey, et al., 2021) and Level 3 to the NIST SP 800-172 (Ross, Pillitteri, Guissanie, et al., 2021) (U.S. DoD, 2022). Table 1 below outlines the differences between CMMC 1.0 and CMMC 2.0 along with the removal of the organizational processes from the model, reduction to three levels, and the adjustment of Level 1 from third-party assessment to self-assessment. Additionally, Table 2 provides a summary of the domain changes from CMMC 1.0 to CMMC 2.0.

Table 1. Differences between CMMC 1.0 and CMMC 2.0 on Model, Assessment, and Levels (Adopted from U.S. DoD, 2022)

CMMC 1.0				→	**CMMC 2.0**		
Model		**Assessment**	**Levels**		**Levels**	**Model**	**Assessment**
171 Practices	5 Processes	Third-party	Level 5: **Advanced** *CUI, Critical Programs*	→	Level 3: **Expert**	110+ Practices based on NIST SP-172	Triennial Government-led assessment
156 Practices	4 Processes	None	Level 4: **Proactive** *Transition Level*				
130 Practices	3 Processes	Third-party	Level 3: **Good** *CUI*	→	Level 2: **Advanced**	110+ Practices aligned with NIST SP-171	Triennial third-party assessment for critical national security information; Annual self-assessment for select programs
72 Practices	2 Processes	None	Level 2: **Intermediate** *Transition Level*				
17 Practices		Third-party	Level 1: **Basic** *FCI Only*	→	Level 1: **Foundational**	17 Practices	Annual self-assessment

Each of the CMMC 2.0 levels includes a set of required practices across the 14 domains, which are defined as specific technical activities that are required and performed to achieve a specific level of cybersecurity maturity for a given capability in a domain. The first level, "Level 1 - Foundational", comprises 17 practices that are self-assessed by the organization itself annually. The self-assessment is challenging, as most SMBs have no expertise in cybersecurity, let alone how to conduct an assessment on their organization (Gafni & Pavel, 2019; Levy & Gafni, 2021). Thus, the focus of this paper provides further assistance for SMBs in the ability to follow a quantifiable scorecard approach using Cybersecurity Footprint elements in measuring their overall organizational cybersecurity posture when it comes to the CMMC 2.0 Level 1. The second level, "Level 2 - Advanced", comprises 110+ practices aligned with NIST SP-171 that are assessed every three years by a third party for critical national security information or annual self-assessment for select programs. The third level, "Level 3 - Expert", comprises 110+ practices aligned with NIST SP-172 that are assessed every three years by a government-led assessment team.

Table 2. Differences Between CMMC 1.0 and CMMC 2.0 on the Domains (Highlighted in Red)

CMMC 1.0 Domains	→	CMMC 2.0 Domains
1. Access Control (AC)	→	1. Access Control (AC)
2. Awareness and Training (AT)		2. Awareness and Training (AT)
3. Audit and Accountability (AU)		3. Audit and Accountability (AU)
4. Configuration Management (CM)		4. Configuration Management (CM)
5. Identification and Authentication (IA)		5. Identification and Authentication (IA)
6. Incident Response (IR)		6. Incident Response (IR)
7. Maintenance (MA)		7. Maintenance (MA)
8. Media Protection (MP)		8. Media Protection (MP)
9. Personnel Security (PS)		9. Personnel Security (PS)
10. Physical Protection (PE)		10. Physical Protection (PE)
11. Recovery (RE)		~~Recovery (RE)~~
12. Risk Management (RM)		11. Risk Assessment (RA)
13. Security Assessment (CA)		12. Security Assessment (CA)
14. System and Communication Protection (SC)		13. System and Communications Protections (SC)
15. System and Information Integrity (SI)		14. System and Information Integrity (SI)

Given the complexity of Levels 2 and 3 in the CMMC 2.0 framework and the fact that most SMBs do not have the resources to attempt addressing such complex requirements, Level 1 appears as a suitable venue for the assessment of the Cybersecurity Footprint at SMBs and will serve as the starting point for the quantification of CFI. The ability for SMBs to quantify their Cybersecurity Footprint provides significant benefits including their ability to recognize cybersecurity threats, and to reduce the risks and uncertainty both to their organization by mitigating the domino's effect on other companies in the supply-chain or interconnected entities. Additionally, we anticipate that the quantifications of the Cybersecurity Footprint using the CFI will assist in reducing bankruptcies of SMBs due to cyberattacks and to cope with emerging cyberthreats such as Ransomware 2.0.

Methodology

In this initial research toward the quantification of the CFI, a review of all the CMMC 2.0 domains that are relevant to Level 1 – Foundational was conducted, followed by a review of the 17 practices across the 14 domains that correspond to Level 1 – Foundational. Next, the body of knowledge relevant to Cybersecurity Footprint was defined by using peer-review literature databases and journal articles. To achieve that, a comprehensive list of relevant journals was first constructed that can then be used in support of the CFI elements. In each journal, the relevant articles, published during the last five years, for the CFI were identified and extracted. Following that, each of the 17 practices was translated into a measurable element relevant to CFI. At this step, some of the CMMC 2.0 17 practices were either expanded into multiple CFI elements or dimmed irrelevant in the context of Cybersecurity Footprint. Finally, the literature gathered was searched to find support and evidence for the CFI elements in the relevant domains of CMMC 2.0, which we document in the Findings section below. Following a review of all the 14 CMMC 2.0 domains that are relevant to Level 1 – Foundational, we have identified six of the 14 domains with practices relevant to CFI. These six domains include: Access Control (AC), Identification and Authentication (IA), Media Protection (MP), Physical Protection (PE), System and Communications Protections (SC), System and Information Integrity (SI). Table 3 outlines all the six relevant domains for Level 1 of the CMMC 2.0 and the 17 associated practices (P1 to P17). While these 17 practices provide a starting point for assessment as the foundation for the 26 CFI elements that we will introduce and discuss later, their specific way of implementation, as well as how they affect the overall cybersecurity posture of a given organization in the current CMMC 2.0 documentation is vague and non-standardized. Specifically, many of these practices use non-quantifiable terms such as "limit", "verify", "control", "identify", etc., as seen in Table 3. In the context of our proposed Cybersecurity Footprint, the operationalizing of the 17 practices is done via the CFI elements. These CFI elements have a weight for each, given that not all elements have the same level of impact on the overall organizational Cybersecurity Footprint.

Table 3. The Six Domains and 17 Practices Relevant to the CMMC 2.0 Level 1 – Foundational

CMMC 2.0 Domains	CMMC 2.0 - Level 1 - 17 Practices
Access Control (AC)	**(P1) AC.L1-3.1.1 - Authorized Access Control** Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). **(P2) AC.L1-3.1.2 - Transaction & Function Control** Limit information system access to the types of transactions and functions that authorized users are permitted to execute. **(P3) AC.L1-3.1.20 - External Connections** Verify and control/limit connections to and use of external information systems. **(P4) AC.L1-3.1.22 - Control Public Information** Control information posted or processed on publicly accessible information systems.
Identification and Authentication (IA)	**(P5) IA.L1-3.5.1 - Identification** Identify information system users, processes acting on behalf of users, or devices. **(P6) IA.L1-3.5.2 - Authentication** Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
Media Protection (MP)	**(P7) MP.L1-3.8.3 - Media Disposal** Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
Physical Protection (PE)	**(P8) PE.L1-3.10.1 - Limit Physical Access** Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. **(P9) PE.L1-3.10.3 - Escort Visitors** Escort visitors and monitor visitor activity. **(P10) PE.L1-3.10.4 - Physical Access Logs** Maintain audit logs of physical access. **(P11) PE.L1-3.10.5 - Manage Physical Access** Control and manage physical access devices.
System and Communications Protections (SC)	**(P12) SC.L1-3.13.1 - Boundary Protection** Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. **(P13) SC.L1-3.13.5 - Public-Access System Separation** Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
System and Information	**(P14) SI.L1-3.14.1 - Flaw Remediation**

CMMC 2.0 Domains	CMMC 2.0 - Level 1 - 17 Practices
Integrity (SI)	Identify, report, and correct information and information system flaws in a timely manner. **(P15) SI.L1-3.14.2 - Malicious Code Protection** Provide protection from malicious code at appropriate locations within organizational information systems. **(P16) SI.L1-3.14.4 - Update Malicious Code Protection** Update malicious code protection mechanisms when new releases are available. **(P17) SI.L1-3.14.5 - System & File Scanning** Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Then, we defined the body of knowledge relevant to Cybersecurity Footprint by using peer-review literature databases and journal articles. To achieve that, we compiled a comprehensive list of relevant journals that we can then use in support of the CFI elements. In each journal, we identified and extracted the relevant articles, published during the last five years, for the CFI. Our findings from this step provided a list of all the 24 peer-reviewed journals identified (Table 4 exhibits the list of relevant journals found) and 144 total relevant articles that related to the CFI.

Table 4. List of Cybersecurity Relevant Journals (in Alphabetical Order)

Journal name	Journal Acronym	ISSN	eISSN	publishing years
ACM Transactions on Privacy and Security	TOPS	2471-2566	2471-2574	1998 -
Communications of the Association for Information Systems	CAIS	1529-3181	-	2008 -
Computers and Security		0167-4048	-	1982 -
Cybernetics and Systems		0196-9722	1087-6553	1980 -
Cybersecurity		-	2523-3246	2018-
Information and Computer Security	ICS	2056-4961	-	2015 -
Information and Security	ISIJ	0861-5160	1314-2119	1998 -
International Journal of Business Continuity and Risk Management	IJBCRM	1758-2164	1758-2172	2010 -
International Journal of Cyber-Security & Digital Forensics	IJCSDF	-	2305-0012	2012-
International Journal of Information and Computer Security	IJICS	1744-1765	1744-1773	2007 -
International Journal of Information Security		1615-5262	1615-5270	2003 -
International Journal of Information security and privacy	IJISP	1930-1650	1930-1669	2007 -
Journal of Cyber Policy		2373-8871	2373-8898	2016-2021
Journal of Cyber Security	JCS	2579-0072	2579-0064	2019-2021
Journal of Cybersecurity		2057-2085	2057-2093	2015 -
Journal of Cybersecurity and Mobility		2245-1439	2245-4578	2012 -
Journal of Cybersecurity and Privacy	JCP	2624-800X	-	2021 -
Journal of Cybersecurity Education Research and Practice	JCERP	2472-2707	-	2016 -
Journal of Information Security and Applications	JISA	2214-2126	-	2013-
Journal of Information Systems Security	JISSEC	1551-0123	1551-0808	2005-

Journal name	Journal Acronym	ISSN	eISSN	publishing years
Journal of Surveillance, Security and Safety	JSSS	-	2694-1015	2020-2021
Organizational Cybersecurity Journal	OCJ	2635-0270	2635-0289	2021
Security and Privacy		-	2475-6725	2018-
The Journal of Cybersecurity Research	JCR	-	2471-2485	2016-2018

Findings

We translated each of the 17 practices that are part of the CMMC 2.0 Level 1 into a measurable element relevant to CFI. At this step, some of the CMMC 2.0 17 practices were either expanded into multiple CFI elements or dimmed irrelevant in the context of Cybersecurity Footprint. Specifically, we have expanded the original four Access Control (AC) practices into a total of 10 relevant CFI elements, contracted the two Identification and Authentication (IA) practices into one relevant CFI element, expanded the one Media Protection (MP) practice into four relevant CFI elements, expanded the four Physical Protection (PE) practices into five relevant CFI elements, converted the two System and Communications Protections (SC) practices into two relevant CFI elements, and converted the four System and Information Integrity (SI) practices into four relevant CFI elements. In total, based on the original 17 practices of CMMC 2.0 Level 1, we came up with a total of 26 CFI elements (E1 to E26) (See Table 5). Finally, using the set of the 144 articles found in our establishment of the foundational body of knowledge for this study, we have provided support for the relevant domains.

Table 5. The Proposed CFI Elements Relevant to the CMMC 2.0 Level 1 – Foundational

CMMC 2.0 Domains	Proposed Cybersecurity Footprint Element	Supporting References
Access Control (AC)	**(E1)** AC.L1-3.1.1-CF1 Number of authorized users **(E2)** AC.L1-3.1.1-CF2 Number of authorized devices **(E3)** AC.L1-3.1.2-CF1 Number of information system access to the types of transactions and functions that authorized users are permitted to execute **(E4)** AC.L1-3.1.2-CF2 Number of transactions and functions that authorized users are permitted to execute for each type of information classification level **(E5)** AC.L1-3.1.20-CF1 - Number of connections to external information systems. **(E6)** AC.L1-3.1.20-CF2 - Volume of using external information systems connections **(E7)** AC.L1-3.1.22-CF1 Volume of information posted or processed on publicly accessible information systems. **(E8)** RY.L1-1.2-CF1 - Number of employees **(E9)** RY.L1-1.3-CF1 - Number of BYOD	Bello et al. (2017) Khando et al. (2021) Nahar et al. (2021) Neigel et al. (2020) Palanisamy et al. (2020) Philippou et al. (2020) Still et al. (2017)

CMMC 2.0 Domains	Proposed Cybersecurity Footprint Element	Supporting References
	devices connected to the organizational network **(E10)** RY.L1-1.5-CF1 - Average number of BYOD device apps per employee	
Identification and Authentication (IA)	**(E11)** IA.L1-3.5.1-CF1 - Number of individuals sharing the same user credentials, and/or devices.	Fischer-Hübner et al. (2021) Philippou et al. (2020) Sinigaglia et al. (2020) Wash and Rader (2021)
Media Protection (MP)	**(E12)** MP.L1-3.8.3 - Number of unsensitized or non-destroyed information system media containing Organizational Information before disposal or release for reuse. **(E13)** RY.L1.1-CF1 - Volume of data in the information systems **(E14)** RY.L1.4-CF1 - Average number of non-licensed apps per employee on work assigned device **(E15)** RY.L1.6-CF1 - Average number of social media accounts per employee	Adesemowo (2021) Bada and Nurse (2019) Neigel et al. (2020)
Physical Protection (PE)	**(E16)** PE.L1-3.10.1-CF1 - Number of devices (organizational information systems, equipment, and the respective operating environments) with physical access to non-authorized individuals. **(E17)** PE.L1-3.10.3-CF1 - Number of escorted visitors (per month) **(E18)** PE.L1-3.10.3-CF2 - Number of non-escorted visitors (per month) **(E19)** PE.L1-3.10.4-CF1 - Volume of logs of physical access (per month) **(E20)** PE.L1-3.10.5-CF1 - Number of physical access devices (CCTV, IP cameras, NVRs, etc.)	Adesemowo (2021) Bada and Nurse (2019) Bello et al. (2017) Diesch et al. (2020) Neigel et al. (2020)
System and Communications Protections (SC)	**(E21)** SC.L1.175-CF1 - 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. **(E22)** SC.L1.176-CF1 - Number of subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Neigel et al. (2020) Palanisamy et al. (2020)
System and Information Integrity (SI)	**(E23)** SI.L1-3.14.2-CF1 - Number of provided TOOLS to protect from malicious code at appropriate locations within organizational information systems. **(E24)** SI.L1-3.14.4-CF1 - Volume of up-to-date malicious code protection patched systems. **(E25)** SI.L1-3.14.5-CF1 - Number of periodic scans of the information system per month **(E26)** SI.L1-3.14.5-CF2 - Volume of scanned	Ahmad et al. (2021) Fischer-Hübner et al. (2021) Leszczyna (2021)

CMMC 2.0 Domains	Proposed Cybersecurity Footprint Element	Supporting References
	files from external sources as files are downloaded, opened, or executed."	

Proposed Cybersecurity Footprint Index (CFI) Quantification

Following the extensive literature meta-analysis described above, and in our pursuit of a quantifiable measure to help organizations, especially SMEs, establish a benchmarking assessment for their cybersecurity posture, we are proposing here an initial equation to quantify CFI that accounts also the CFI of their interconnected supply-chain organizations. Given the hierarchical nature of organizations in the supply-chain (See Levy & Gafni, 2021 for additional information), the CFI will need to account for the cascading interconnected entities that are in the supply-chain of a given organization. It is important to note that each organization (e.g. Org$_A$) will account in its own CFI all organizations that are only one level (L1) down in its supply-chain (Org$_{A.L1}$), while within the CFI of each interconnected entity from L1 will account in their CFI their own one level down in its supply-chain. We anticipate the CFI for Org$_A$ to be calculated as noted in Equation 1.

The normalizing coefficient for Org$_A$

The sum of all 26 Weights times the value of the 26 CFI Elements for Org$_A$

The normalizing coeff. for all Level 1 organizations in Org$_A$ supply-chain

The sum of all CFIs of interconnected organizations in Level 1 downstream of Org$_A$ Supply-Chain

$$CFI_{OrgA} = C_{OrgA} \cdot \left[\sum_{x=1}^{26} \left(W_{E.xOrgA} \cdot Ex_{OrgA} \right) + C_{Org_{A.L1}} \cdot \sum_{Org_{A.L1}=1}^{n} \left(W_{OrgA.L1} \cdot CFI_{OrgA.L1} \right) \right] \qquad (1)$$

Where:

OrgA – Organization A – the main organization assessed for Cybersecurity Footprint Index

CFI$_{OrgA}$ – The Cybersecurity Footprint Index for Organization A (values from 0% to 100%)

C$_{OrgA}$ – The normalization coefficient for CFI of Organization A to enable CFI values from 0% to 100%

W$_{E.OrgA}$ – the weight of CFI elements E$_x$ of Organization A

x – the elements number from 1 to 26

E*x* represents each of the 26 CFI elements across the 17 CMMC 2.0 practice (See Table 3)

OrgA.L1 = 1 to *n* – each of the organization that is interconnected at one (1) level down in the supply-chain of Organization A

n – the total number of interconnected entities at one (1) level down in the supply-chain of the main assessed Organization A

W$_{OrgA.L1}$ – the weight of each CFI of Organization A.L1 (=1 to *n* interconnected entities), which is at one (1) level down in the supply-chain of the main assessed Organization A

$\mathrm{CFI}_{\mathrm{Org}A.L1}$ – the CFI of Organization A.L1 (=1 to *n* interconnected entities), which is at one (1) level down in the supply-chain of the main assessed Organization A

The proposed CFI calculation is somewhat complex as we anticipate that each company that is within the focus of the assessment (Organization A in our example above) will also have to account to some extent (i.e. the weights) the CFI value of their *n* interconnected organizations in their supply-chain. This is valid given that any organization is dependent to some extent based on their interconnected organizations in their supply-chain. Additionally, with the 16 Critical Infrastructure sectors defined by the U.S. Department of Homeland Security (U.S. DHS), we anticipate that the weights of the CFI elements may be different for a particular sector.

Discussions, Conclusions, and Future Work

In this research-in-progress, we have documented the steps we have taken to develop the foundational work for the identification of the Cybersecurity Footprint elements to develop a quantifiable index (CFI) to assist organizations, especially SMBs, in measuring their Cybersecurity Footprint following the CMMC 2.0 – Level 1- Foundational. For SMBs, understanding the requirements of CMMC 2.0 is a difficult mission. Moreover, coping with cybersecurity threats is, for most of them, an impossible task. Therefore, defining an index on a scale of 0 to 100 to quantify the SMBs Cybersecurity Footprint, which can be easily comprehendible for executives, is an important contribution, as the move to embrace CMMC 2.0 is growing by the U.S. DoD's DIB organizations and they need a self-assessment method that is quantifiable as well as one that allows for benchmarking. The foundations of the CFI elements are defined according to the CMMC 2.0 and supported by prior research found in the relevant academic peer-reviewed journals. Future research should focus on the use of the Delphi method with an expert panel, following prior literature such as Ramim and Lichvar (2014), to validate the initial CFI elements, define the proper weight for each CFI element, and prepare a valid, solid, and easy for use Index for use with SMBs. Additionally, as noted above, we recommend future research to uncover the weights of the 26 CFI elements in the different 16 Critical Infrastructure sectors given that we anticipate differences among the sectors.

References

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

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, M. T., Whitty, R. L. Baskerville (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

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly, 41*(3), 893-916. https://doi.org/10.25300/MISQ/2017/41.3.10

Ani, U. D., Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology, 21*(1), 2-35. https://doi.org/10.1108/jsit-02-2018-0028

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2020). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers & Security, 100*, 102090. https://doi.org/10.1016/j.cose.2020.102090

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security Journal, 27*(3), 393-410. https://doi.org/10.1108/ICS-07-2018-0080

Baron. J., & Francois, B. (2020, April 27). *A crisis playbook for family businesses.* Harward Business Review.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management, 51*(1), 138–151. https://doi.org/10.1016/j.im.2013.11.004

Bell, S. (2017). Cybersecurity is not just a 'big business' issue. *Governance Directions*, *69*(9), 536-539.

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 and Computer Security, 25*(4), 475-492. https://doi.org/10.1108/ICS-03-2016-0025

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons, 63*(4), 531-540.

Bhattacharya, D. (2013). Evolution of information security issues in small businesses. *The Colloquium for Information System Security Education, 1*(1)*,* 1-10.

Bodeau, D., & Graubart, R. (2017). Cyber prep 2.0: Motivating organizational cyber strategies in terms of threat preparedness. *MITRE, Bedford, MA, USA, Tech. Rep*, 15-0797.

Carlton, M., & Levy, Y. (2017). Cybersecurity skills: The cornerstone of advanced persistent threats (APTs) mitigation. *Online Journal of Applied Knowledge Management, 5*(2), 16-28. https://doi.org/10.36965/OJAKM.2017.5(2)16-28

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

European Commission (2022). What is an SME? https://ec.europa.eu/growth/smes/sme-definition_en

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23-40.

Federal Bureau of Investigation (FBI) (2022, March 22). FBI releases the Internet crime complaint center 2021 Internet crime report. https://www.fbi.gov/news/press-releases/press-releases/fbi-releases-the-internet-crime-complaint-center-2021-internet-crime-report

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., Islami, L., & 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

Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB's cybersecurity. *Online Journal of Applied Knowledge Management (OJAKM)* 7(1), 14-26. DOI: https://doi.org/10.36965/OJAKM.2019.7(1)14-26

Gafni, R., & Pavel, T. (2021). Cyberattacks against the healthcare sectors during the coronavirus era. *Information and Computer Security, 30*(1), 137-150. https://doi.org/10.1108/ICS-05-2021-0059

Goel, R., Kumar, A., & Haddow, J. (2020). PRISM: A strategic decision framework for cybersecurity risk assessment. *Information and Computer Security, 28*(4), 591-625. https://doi.org/10.1108/ICS-11-2018-0131

Israel - Small Business Agency (2022). https://www.sba.org.il/ and https://www.gov.il/en/departments/units/small_medium_business_agency_about

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

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

Levy, Y., & Niccolini, F. (2019). Research agenda to assess cybersecurity preparedness and risk management of Tuscan small to medium businesses. *Proceedings of the International Institute for Applied Knowledge Management,* KM Conference, Warsaw, Poland.

Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security, 108*, 102376. https://doi.org/10.1016/j.cose.2021.102376

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551-555.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24.

Lopez-Nicolas, C., & Soto-Acosta, P. (2010). Analyzing ICT adoption and use effects on knowledge creation: An empirical investigation in SMEs. *International Journal of Information Management, 30*(6), 521-528.

Macmillan, S., (2017). The best defense against cyber-attacks: People not technology. *Human Resources Magazine*, 9.

McDonald, N. (2017). Organisational resilience and industrial risk. In *Resilience Engineering* (pp. 155-180). CRC Press.

Mettler, T. (2011). Maturity assessment models: A design science research approach. *International Journal of Society Systems Science,* 3(1/2), 213–222. https://doi.org/10.1504/IJSSS.2011.038934

Mirskaia, L., & Crew, F. A. E. (1931). XIV.—Maturity in the female mouse. *Proceedings of the Royal Society of Edinburgh*, 50, 179-186.

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

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

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computer & Security, 88*, 101608. https://doi.org/10.1016/j.cose.2019.101608

Palanisamy, R., Norman, A. A., & Kiah, 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

Pettit, T. J., Croxton, K. L., & Fiksel, J. (2013). Ensuring supply chain resilience: Development and implementation of an assessment tool. *Journal of Business Logistics*, *34*(1), 46-76.

Philippou, E., Frey, S., & Rashid, A. (2020). Contextualising and aligning security metrics and business objectives: A GQM-based methodology. *Computers & Security, 88*, 101634. https://doi.org/10.1016/j.cose.2019.101634

Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: A systematic literature review. *Information and Computer Security, 28*(4), 627-644. https://doi.org/10.1108/ICS-03-2019-0039

Ramim, M., & Lichvar, B. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management, 2*(1), 122-126. http://www.iiakm.org/ojakm/articles/2014/volume2_1/OJAKM_Volume2_1pp122-136.pdf

Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal: Practice, Process and People*.

Rezaei, J., Ortt, R. & Trott, P. (2015). How SMEs can benefit from supply chain partnerships. *International Journal of Production Research*, *53*(5), 1527-1543.

Ross, R. Pillitteri, V., Dempsey, K., Riddle, M, & Guissanie, G. (2021). Protecting controlled unclassified information in nonfederal systems and organizations. National Institute of

Standards and Technology (NIST) Special Publication (SP) 800-171 Rev. 2. https://doi.org/10.6028/NIST.SP.800-171r2

Ross, R. Pillitteri, V., Guissanie, G., Wagner, R, Graubart, R., & Bodeau, D. (2021). Protecting controlled unclassified information in nonfederal systems and organizations. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-172. https://doi.org/10.6028/NIST.SP.800-172

Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job: Exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information and Computer Security, 28*(3), 467-483. https://doi.org/10.1108/ICS-01-2019-0010

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Abdul Ghani, N., & Herawan, T. (2015). Information security conscious care behavior formation in organizations. *Computer & Security,* 53, 65-78.

Schmitz, C., Schmid, M., Harborth, D., & Pape, S. (2021). Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities. *Computers & Security, 108*, 102306. https://doi.org/10.1016/j.cose.2021.102306

Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security, 97*, 101996. https://doi.org/10.1016/j.cose.2020.101996

Serenko, A., Bontis, N., & Hull, E. (2016). An application of the knowledge management maturity model: The case of credit unions. *Knowledge Management Research & Practice*, 14(3), 338-352.

Sinigaglia, F., Carbone, R., Costa, G., & Zannone, N. (2020). A survey on multi-factor authentication for online banking in the wild. *Computers & Security, 95*, 101745. https://doi.org/10.1016/j.cose.2020.101745

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154-176.

Still, J. D., Cain, A., & Schuster, D. (2017). Human-centered authentication guidelines. *Information and Computer Security, 25*(4), 437-453. https://doi.org/10.1108/ICS-04-2016-0034

Stokes, A., & Childress, M. (2020, April 8). 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

Thakkar, J., Kanda, A., & Deshmukh, S. G. (2008). Supply chain management in SMEs: development of constructs and propositions. *Asia Pacific Journal of Marketing and Logistics, 20*(1), 97-131.

Tu, C. Z., Yuan, Y., Archer, N., & Connelly, C. E. (2018). Strategic value alignment for information security management: A critical success factor analysis. *Information and Computer Security, 26*(2), 150-170. https://doi.org/10.1108/ICS-06-2017-0042

Uchendu, B., Nurse, J. R. C., Bada, M, & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*, 102387, https://doi.org/10.1016/j.cose.2021.102387

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. https://doi.org/10.17781/P002644

U.S. Department of Defense (U.S. DoD) (2022). Securing the defense industrial base - CMMC 2.0. Office of Undersecretary of Defense, Acquisition and Sustainment. https://www.acq.osd.mil/cmmc/

U.S. Department of Homeland Security (U.S. DHS) (2020). Critical infrastructure sectors. https://www.cisa.gov/critical-infrastructure-sectors

U.S. Small Business Administration (2022). Stay safe from cybersecurity threats. https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats

Verizon. (2020). *2020 Data breach investigation report.* https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security, 26*(1), 2-9.

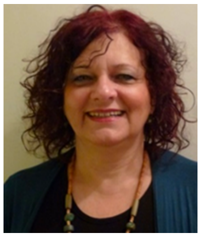
Ward, M. (2021). “Business statistics. briefing paper number 06152”, available at: https:// researchbriefings.files.parliament.uk/documents/SN06152/SN06152.pdf (accessed 4 March 2021).

Wash, R., & Rader, E. (2021). Prioritizing security over usability: Strategies for how people choose passwords. *Journal of Cybersecurity, 7*(1), tyab012. https://doi.org/10.1093/cybsec/tyab012

Yoo, C. W., Sanders, G. L., & Cerveny, R. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, *108*, 107-118.

Authors Biographies

Yair Levy, Ph.D. is a Professor of Information Systems and Cybersecurity at the College of Computing and Engineering at Nova Southeastern University, the Director of the Center for Information Protection, Education, and Research (CIPhER) (http://infosec.nova.edu/), and chair of the Cybersecurity curriculum committee at the college along with serving as the director of the M.S. and Ph.D. programs in Cybersecurity. He conducts innovative research from the 'human factor' in cybersecurity, including social engineering. Levy authored numerous peer reviewed journal articles, conference proceedings, book chapters, and other publications. His scholarly research has been cited over 7,000 times. Dr. Levy has been an active member of the U.S. Secret Service (USSS)'s - Miami Electronic Crimes Task Force (MECTF) and FDLE South Florida Cybercrime Working Group (SFCWG). He was trained by the Federal Bureau of Investigation (FBI) on various topics and actively serves as a board member on the South Florida FBI/InfraGard. He consults federal agencies including the National Security Agency (NSA), state and local government groups on cybersecurity topics. He is also a frequent invited keynote speaker at national and international meetings, as well as regular media interviews as a Subject Matter Expert (SME) on cybersecurity topics. Read more about Dr. Levy via: https://sites.nova.edu/levyy/



Ruti Gafni, Ph.D. is an Associate Professor, Dean, and establisher of the School of Information Systems at The Academic College of Tel Aviv Yaffo. She holds a Ph.D. from Bar-Ilan University, Israel (in the Business Administration School), focusing on Information Systems, an M.Sc. from Tel Aviv University, in Information Systems Management, and a B.A. (Cum Laude) in Economics and Computer Science from Bar-Ilan University. She has more than 40 years of practical experience as a Software Project Manager and Analyst of information systems. Her research interests include cybersecurity and new technology adoption.