A systematic synthesis of critical success factors for cybersecurity

William Yeoh[a,b,*], Shan Wang[c], Aleš Popovi[ˇc d,e], Noman H. Chowdhury[f]

[a] Department of Information Systems and Business Analytics, Deakin University, Australia

[b] Centre for Cyber Security Research and Innovation, Deakin University, Australia

[c] Edwards School of Business, University of Saskatchewan, Canada

[d] School of Economics and Business, University of Ljubljana, Slovenia

[e] NOVA Information Management School, Universidade Nova de Lisboa, Campus de Campolide, Portugal

[f] School of Economics and Management, Xiamen University Malaysia, Malaysia

This is the accepted author *manuscript of the following article published by Elsevier*: *Yeoh, W., Wang, S., Popovič, A., & Chowdhury, N. H. (2022). A Systematic Synthesis of Critical Success Factors for Cybersecurity. Computers and Security, 118(July), 1-17. [102724].* https://doi.org/10.1016/j.cose.2022.102724

A Systematic Synthesis of Critical Success Factors for Cybersecurity

ABSTRACT

Extant studies suggest cybersecurity is critical and among the IT spending priorities of organizations. In response, the literature draws attention to the cybersecurity Critical Success Factors (CSFs), enabling organizations to focus their scarce resources accordingly. Following a systematic literature review method, we analyze and synthesize extant CSFs studies on cybersecurity implementation and management for organizations. Then, drawing on the synthesized CSFs and blending them with IT capability theory, we present an overarching cybersecurity CSFs framework building upon 79 cybersecurity elements grouped into 11 CSFs under five dimensions of cybersecurity capability: organizational, infrastructural, strategic, process, and external. In addition, the descriptive analysis of the search results reveals the importance of the various factors and capabilities, the trend of the cybersecurity capability dimensions, the frequency and types of research methods, and the contextual impact of the factors. This research makes an important contribution to the literature on cybersecurity management. The CSFs framework serves as the foundation for future researchers interested in measuring organizational cybersecurity success. At the same time, the synthesized CSFs and associated elements can be employed by practitioners to guide their cybersecurity management.

Keywords: Critical success factors; cybersecurity; systematic literature review; synthesis, classification; IT capability theory

1. Introduction

Cybersecurity protects an organization's data and information technology (IT) assets from security threats and vulnerabilities (Chowdhury et al., 2019; Yeoh et al., 2021). However, the successful implementation of organizational cybersecurity remains a theoretical and managerial challenge. A recent study of cybersecurity trends found that 68% of business leaders feel their cybersecurity risks are increasing (Sobers, 2021). The consequences of an escalating cyberattack can be significant. On May 7, 2021, a ransomware attack hit the IT system of Colonial Pipeline in the United States, forcing the shutdown of the country's largest pipeline, which transports 45% of the East Coast's fuel supply (Jeffers & Turton, 2021). This cybersecurity incident caused fuel supply shortages and panic buying.

Cybersecurity has never been more urgent and critical for organizations. It is among the top IT spending priorities of chief information officers (CIOs). According to a 2021 CIO survey of IT executives, the organizations surveyed will spend 37% of their IT budget on cybersecurity and risk management (Ambrosio, 2021). In addition, the COVID-19 pandemic has forced organizations to allow remote operation and home offices for employees, creating new vulnerabilities for businesses (Yeoh et al., 2021). Given the hybrid work environment and the rise of sophisticated cyberattacks in a rapidly evolving threat landscape, organizations need to adapt their security management (Ahmad et al., 2020). Implementing organizational cybersecurity does not entail merely the installation of security software; rather, it is a complex undertaking involving multifaceted technological, organizational, and process issues (Ahmad et al., 2020). In response, the literature draws attention to the critical success factors (CSFs) and urges organizations to focus their scarce resources on these critical areas.

Despite the vibrant security market and the multidimensional complexities surrounding cybersecurity, there remains a lack of an overarching cybersecurity CSFs framework to guide cybersecurity management in organizations. Although there are some review articles in the literature on cybersecurity success factors (Atkins & Lawson, 2021; Diesch et al., 2020; Hussain et al., 2020), they focus on issues such as cybersecurity policy for critical infrastructure and information security factors for decision-makers. Yet, the literature summary in these articles is not theory-driven, resulting in a fragmented landscape of cybersecurity CSFs.

Hence, this paper draws on IT capability theory and builds an overarching framework of cybersecurity CSFs through a systematic literature review (SLR). Rowe (2014) asserted that SLR is a valuable research method, especially for achieving goals such as developing an

annotated summary of existing works, examining current contributions and findings, and outlining alternative frameworks or paths of prior research. Although SLR can be useful for exploring research opportunities and challenges, it is equally important to use SLR to develop an innovative framework that can provide practical value (Rowe, 2014), which is particularly important for cybersecurity as both threats and security practices are rapidly evolving. In the field of cybersecurity, a comprehensive CSFs framework that could offer practical value to organizations will be useful. With that backdrop, the research question for this study is: *What are the critical success factors (CSF) in implementing and managing cybersecurity in organizations, and how can the CSFs be conceptualized into an integrative framework?*

To support the systematic synthesis of cybersecurity CSFs, we adopt the lens of IT capability theory. According to the resource-based view (Barney, 1991) and IT capability theory (Wade & Hulland, 2004), an organization's capabilities result from tightly integrated business processes, practices, and IT. Cybersecurity is embedded in organizational business processes and practices because of the ubiquity of IT within organizations. To achieve sustainable success in managing cybersecurity in modern organizations, an organization must build IT security capabilities. The literature has long used the term security capability, and there is research on security capability maturity (Le & Hoang, 2017, Mohammed & Bade, 2019). However, this stream of research has emphasized maturity more than capability, and the research on capabilities is not based on organizational capabilities, especially IT capability theory.

This research contributes to the literature by creating a comprehensive cybersecurity CSFs framework for organizations based on IT capability theory. It also provides practical value to practitioners as the synthesized factors and generated elements can be readily used to guide their cybersecurity management. The remainder of this paper is structured as follows. Section 2 provides an overview of the cybersecurity concept and the IT capability theory. Section 3 presents the SLR methodology. Section 4 presents the CSFs classification and associated elements. Section 5 presents the descriptive analysis. Section 6 highlights the contributions to research and practice and puts forward proposals for future research. Finally, section 7 concludes the paper.

2. Background

2.1 Cybersecurity

Cybersecurity is emerging from traditional information security as information systems and devices are increasingly connected to the Internet and often operate in the cloud, creating more vulnerabilities and high demand for security (Baikloy et al., 2020). Because of the evolving nature of cybersecurity, there is no single definition of cybersecurity. Using a semantic analysis of 28 cybersecurity definitions, Schatz et al. (2017, p.66) define cybersecurity as "*the approach and actions associated with security risk management processes followed by organizations and states to protect the confidentiality, integrity, and availability of data and assets used in cyberspace.*" Their comprehensive conceptualization of cybersecurity covers organizational artifacts ranging from cybersecurity guidelines, policies, and technological infrastructure to processes, measures, and training. We adopt this definition and guide our search for relevant literature.

The study of cybersecurity success or failure is a central topic for information systems (IS) researchers. Some studies approach the subject from a specific perspective, such as information security governance (AlGhamdi et al., 2020), culture (Alnatheer, 2015), and human risk (Cuchta et al., 2019); some focus on a specific IT artifact, such as cloud computing (Alassafi et al., 2017), industrial control systems, and critical infrastructure (Asghar et al., 2019, Atkins and Lawson, 2021), and some take a holistic approach to investigate cybersecurity measures. For example, through a literature review and interviews with 19 experts, Diesch et al. (2020) summarize 12 factors that influence security decisions: vulnerability, compliance and policy, risk, physical security, continuity, infrastructure, confidentiality, integrity, and availability (CIA), security management, awareness, resources and access control, and organizational factors.

Compared with research streams that focus on a particular perspective or IT artifact, research that takes a holistic approach is more valued given the complex landscape of IT use in organizations (Soomro et al., 2016). According to a McAfee (2014) report, the average enterprise has 464 custom applications in use, and it is estimated that enterprises will develop and deploy even more applications soon. Therefore, the large number of applications used by contemporary organizations and the interdependence of systems requires a holistic approach to cybersecurity measures.

There are some review articles in the literature; however, few are oriented toward IS theories. For example, Diesch et al. (2020) use the lens of the CIA in explaining the goal of information security (Goldstein et al., 2011, Zalewski et al., 2014). Still, the CIA seems to be a factor in the framework and is not used to guide the literature summary. This research fills this gap by incorporating the IT capability theory to analyze the literature.

2.2 IT Capability

The resource-based view (RBV) has been proposed to investigate the impact of IT investments on firm performance. Researchers have shown that a firm's ability to effectively leverage its IT investments by developing a strong IT capability can result in improved firm performance (Santhanam & Hartono, 2013Based on the RBV, when combining IT capability with resources and capabilities of the firm, that can provide the needed competitive advantage (Bharadwaj A. S., 2000).

IT capability refers to an organization's ability to identify, mobilize, and deploy IT assets and resources that meet business needs, improve business processes with IT applications, and provide long-term support for IT-based systems (Karimi et al., 2007). It can leverage different IT assets and resources for various organizational benefits and business values (Wade & Hulland, 2004).

Researchers have indicated that IT capability is an essential organizational capability (Wade & Hulland, 2004). Firms can achieve a competitive advantage by acquiring or developing organizational capabilities. Organizational capabilities have a hierarchy with lower-order capabilities that help them build higher-order capabilities (Rai, Patnayakuni, & Seth, 2006). IT capabilities are described as lower-order capabilities that enable developing higher-order ones, such as organizational agility (Chakravarty, Grewal, & Sambamurthy, 2013; Lu & Ramamurthy., 2011; Roberts & Grover, 2012). Organizational capabilities are the ability of a firm to perform functions in a reliable way (Grant & Verona, 2015). They consist of routines and processes that have repeatable patterns of activities and typically involve and integrate multiple actors and assets within the firm (Becker, 2004; Felin & Foss, 2009). Because routines are complex, multi-factor phenomena, the capabilities they create can be path-dependent, causally ambiguous, or socially complex, thus becoming difficult for competitors to imitate. Due to inimitability, impaired mobility, and non-substitutability, organizational capabilities are valuable resources that help organizations sustain competitive advantages (Peteraft, 1993).

Taking full advantage of their existing IT capability, firms can enhance their competitive advantage and performance (Bhatt & Grover, 2005; Santhanam & Hartono, 2003; Chen, Wang, Nevo, Jin, Wang, & Chow, 2014). IT capability enables the firm to build on its existing technology resources and the associated knowledge and skills. The emphasis is more on the exploitation side of technology (Nwankpa & Datta, 2017). The dynamic side of IT capability enables exploring technological opportunities and integrating them with the existing resources base.

IT capability theory applies the RBV (Barney, 1991) to explain the value of IT assets. The proper configuration of IT assets in combination with other complementary organizational assets (Wade & Hulland, 2004, Bharadwaj, 2000) forms IT capabilities that are valuable, rare, non-substitutable, and inimitable; thus providing firms with a sustainable competitive advantage. There are various conceptualizations of IT capabilities. Mata et al. (1995) conceptualize three dimensions of IT capability: proprietary technology, technical IT skills, and managerial IT skills. Bhatt and Grover (2005) propose three IT capabilities: IT infrastructure, IT management capabilities (i.e., IT business experience and business relationships), and dynamic capabilities. Ravichandran and Lertwongsatien (2005) adopt a business process perspective and propose that IT capabilities consist of IS planning capability, system development capability, IS support maturity, and IS operations capability. Based on a thorough literature review, Melville et al. (2004) propose that IT capability consists of technical IT resources, human IT resources, and complementary organizational resources. Combining these resources is embedded in an organization and its processes and creates competitive advantages.

IT capability theory has been applied to study various IT artifacts, such as e-commerce capability (Zhuang & Lederer, 2006), social media capability (Wang & Kim, 2017), big data analytics capability (Gupta & George, 2016), artificial intelligence capability (Mikalef & Gupta, 2021), and general IT capability (Yoon, 2011). However, there is still no conceptualization of cybersecurity capability. Several studies have investigated security capability (Le & Hoang, 2017, Mohammed & Bade, 2019). Still, the theoretical basis is the Capability Maturity Model (Paulk, 2009), which is mainly a process-level model that does not cover all aspects of cybersecurity management.

This research adopts the IT capability theory from industry (see Figure 1), which suggests that IT capability consists of the following four dimensions: IT strategy, IT processes, IT organization (e.g., skills, structure, and knowledge/know-how), and IT assets/infrastructure (e.g., hardware, software, applications, network, database, and tools) (Zhang et al., 2008). The dimensions fit the conceptualization of IT capability from academia. It encompasses both the technical IT capability (i.e., IT assets and infrastructure) and the management capabilities covering various aspects of IT management, including strategy, process, and organization. According to RBV, organization capability is combinative. An organization creates value through IT capability by leveraging a unique combination and configuration of these dimensions, including IT strategic planning capability, IT operational (i.e., process) capability, IT organization capability, and IT infrastructure and assets. The dimensions of this IT capability theory also guide us to classify and analyze the critical success factors of cybersecurity, which are, in fact, resources that companies invested or built when dealing with cybersecurity, and such resources are integrated to help an organization nullify the potential threats from the cyberspace.

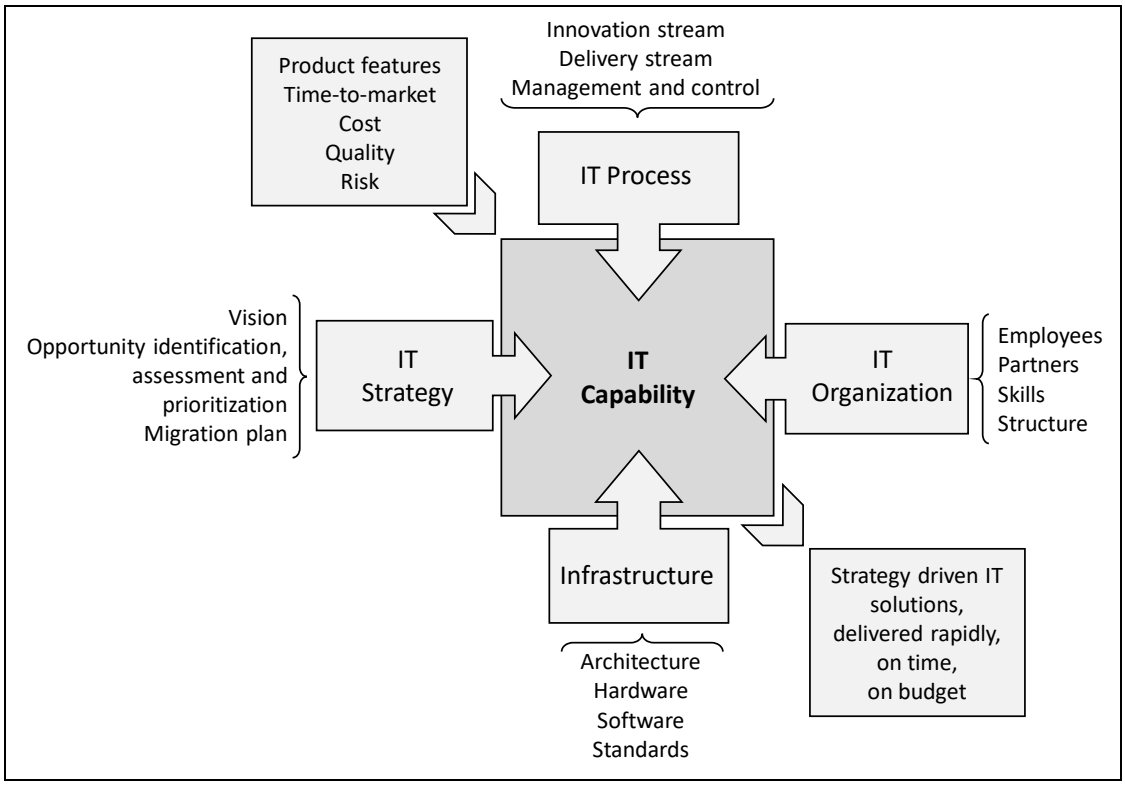

FIGURE 1. Dimensions of IT Capability.

3. Research methodology

We identified and synthesized different critical success factors (CSFs) under each of the dimensions in IT Capability Theory through a Systematic Literature Review (SLR).

Following Kitchenham's (2004) guidelines, to identify and evaluate the current state of relevant literature, we completed the SLR in three phases: *planning the review*, *conducting the review*, and *reporting the review*. In the first phase (i.e., planning), we established the need for SLR, designed and evaluated the review protocol, and iteratively developed a search string. In the second phase (i.e., conducting), we searched and shortlisted the literature for full-text analysis. In the final phase (i.e., reporting), we presented the identified CSFs in different dimensions of IT Capability Theory with evidence from analyzed articles. In that regard, analysis and presentation of findings from our SLR followed a concept-centric approach (e.g., Griffith, 1999; Webster and Watson, 2002).

To cover a wide range of literature, we first decided to develop a search string consisting of two key terms:

("cybersecurity" AND "success factors")

We then conducted an initial search of scholar.google.com and google.com and identified seven articles and three industry reports. From the preliminary analysis of these documents, we identified additional relevant terminologies/phrases that capture potentially relevant literature and therefore refined the search string as follows:

("cybersecurity" OR "cyber security" OR "information security" OR "data security" OR "IT security") AND ("success factors" OR "risk factors")

We then used this search string in Google Scholar and nine major online databases (Science Direct, ACM, AIS, Emerald, IGI, Informs, Springer, Taylor & Francis, Wiley) across multiple disciplines (see Figure 2). From the Google Scholar search results, we considered the first 100 articles as the most relevant articles are included within the first few pages of results.

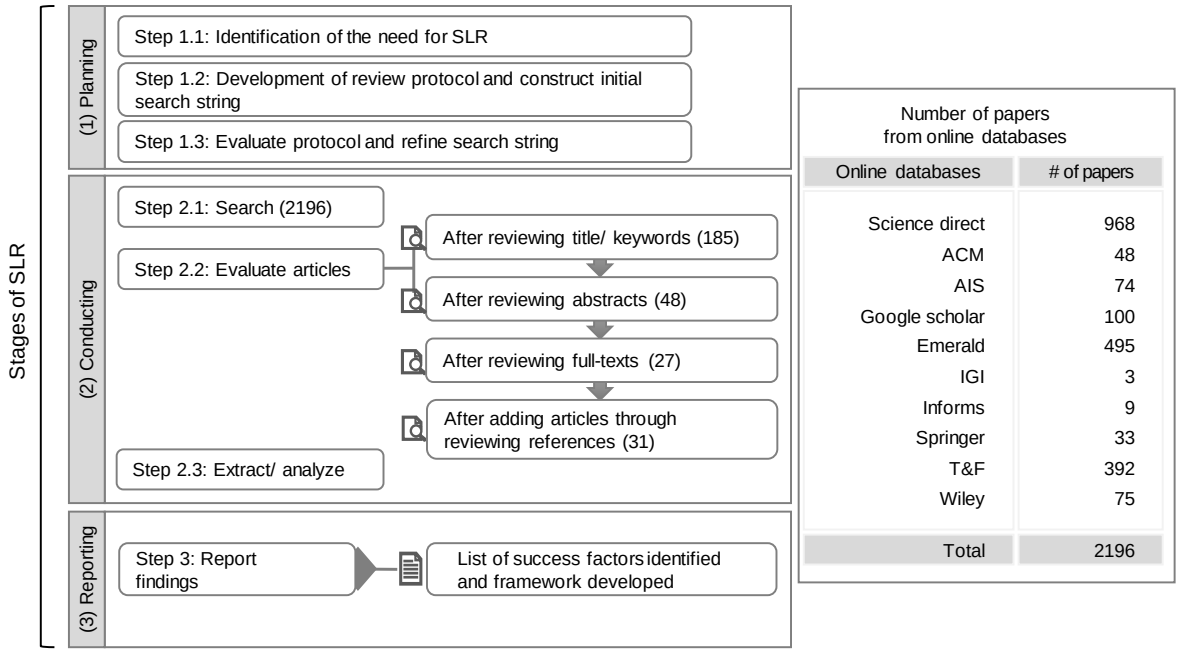

FIGURE 2. SLR stages and distribution of papers.

We only considered peer-reviewed journals and international conferences (in English) for academic literature and excluded technical reports, white papers, and pre-print papers. Since our focus is developing cybersecurity capability based on recent literature, we considered articles published since 2010. Also, because Singh et al. (2014) has partially covered the relevant search till 2013, we researched from 2010 onwards. Cybersecurity has shifted from pure technical countermeasures to a comprehensive management strategy (e.g., Soomro et al., 2016). Further, due to the changing nature of workplace environments, managers are increasingly bringing non-technical factors, e.g., culture, human behavior (e.g., Williams, 2011; Chowdhury et al., 2019) into their account and technical measures to formulate cybersecurity decisions and strategies. Thus, this study is timely and fills the research gap.

R programming language was used for web scraping of article metadata and finding and eliminating duplicates. In total, we started with 2196 articles. We then performed a rigorous stepwise screening (titles, keywords, abstracts, and full texts) to select 27 articles for analysis. By reviewing our collection of articles and references of the selected articles, an additional four articles were considered for analysis, for a total of 31 articles. The inclusion criterion for selection is whether the research article covers critical success factors for cybersecurity. In the process, we excluded articles that were merely referenced in the background, grey literature and duplicate articles that appeared in different databases.

In total, we identified and analyzed 31 relevant papers (11 conference papers and 20 journal papers). Concerning the study type, there were reviews (e.g., systematic literature reviews, narrative reviews), qualitative studies (involving, e.g., interviews of employees and experts), quantitative studies/surveys (e.g., questionnaire surveys), as well as mixed studies involving, e.g., both review and qualitative studies, or both review and survey studies. The context of the papers analyzed ranged from industrial and cloud security to general cybersecurity implementation and management in organizations (both governmental and private). Of the 31 papers, 17 explicitly proposed a list of success factors in different contexts. We extracted the success factors for the remaining 14 papers through our analysis. Table A1 presents the list of analyzed articles, their context, detailed methodology, and relevant contribution to our research.

4. Synthesizing cybersecurity CSFs into a framework

To develop a list of CSFs in different dimensions, we analyzed the selected articles following a stepwise approach suggested by Bowen (2009).

In the first step (i.e., familiarizing), the authors introduced themselves to the content of the articles through reading and re-reading. In the second step (i.e., first-level coding), one author with extensive experience in qualitative research in the cybersecurity domain coded the articles identifying elements about cybersecurity in the organizational context. Through iterative discussion and validation with other authors, a revised list with 79 elements is finalized.

In the third step (i.e., second-level coding or identifying themes), these elements are then further assessed thematically to understand their dimension (e.g., process vs. infrastructure), context (e.g., risk assessment vs. reporting and performance measurement), as well as the interrelationship among themselves. Elements alluding to a similar theme (i.e., dimension, context) are grouped and identified as broader factors (i.e., CSFs). For example, “Identifying and assessing risks from threats/vulnerabilities”, “Integrating security metrics in risk management process” and “Developing action/recovery plans for threats/vulnerabilities” – these three elements are grouped under the CSF of “Risk assessment of potential threats/vulnerabilities” (RTV). Once this grouping is done, the underlying elements are short-coded and numbered accordingly (e.g., RTV1, RTV2, RTV3). In the same way, CSF of “knowledge and awareness of employees” (KWE) comprises the elements KWE1–KWE5. Here we refer to the acronyms of the CSFs (e.g., RTV, KWE) as second-level coding. Table 1 presents the list of identified elements with their CSF short codes. Furthermore, Table A2 in

the appendix offers the detailed mapping between the identified elements and the analyzed articles.

Definitions of different CSFs are also formulated in this step (i.e., third step) based on the underlying elements in each of the CSFs. The IT capability theory (Figure 1) guided us in assessing the elements dimension-wise (e.g., process, infrastructure). In total, we identified 11 CSFs.

In the fourth step (i.e., conceptualizing the framework), we categorized the 11 CSFs into different dimensions. Table 2 presents the list of CSFs (with acronyms and definitions) under different dimensions. We found that one CSF related to external relationship management did not fit into any of the dimensions put forth by the IT capability Theory. Therefore, we created an additional dimension, namely, external. We finally presented the framework with five cybersecurity capability dimensions: organizational, infrastructural, strategic, process, and external. Figure 3 depicts the conceptualization of the overarching cybersecurity CSFs framework for organizations that include both internal and external factors.

TABLE 1. List of elements and their CSF short codes.

#	*Elements of cybersecurity success factors*	*Short Code**	#	*Elements of cybersecurity success factors*	*Short Code*
1	Top management's knowledge/awareness about security	KWE1	41	Considering/integrating security goals in a mission statement	BSSC1
2	Employees' security compliance and behavior	KWE2	42	More active role of CIO in executive decision-making	BSSC2
3	Employees' understanding of impact from security breaches	KWE3	43	Linking security metrics to management goals	BSSC3
4	Employees' awareness/ knowledge about policy/procedures	KWE4	44	Integrating security goals with organizational strategic plans	BSSC4
5	Employees' knowledge/awareness about security requirements	KWE5	45	Considering security in business continuity plans	BSSC5
6	IS teams' commitment toward security	SCT1	46	Integrating security requirements in organizational processes	BSSC6
7	IS teams' business knowledge/skill	SCT2	47	Security professionals participating in business decisions	BSSC7
8	IS teams' security knowledge, skill, and past experience	SCT3	48	Alignment of organizational culture and information security	BSSC8
9	IS teams' coordination	SCT4	49	Faster/effective business processes relevant to fulfilling security needs	BSSC9
10	Skills of IS audit teams	SCT5	50	Identifying and assessing risks from threats/vulnerabilities	RTV1
11	Top management's accountability about information security	OSP1	51	Integrating security metrics in the risk management process	RTV2
12	Identifying and safeguarding organizational information assets	OSP2	52	Developing action/recovery plans for threats/vulnerabilities	RTV3
13	Complying with security policies	OSP3	53	Awareness programs for top management	DCA1
14	Complying with security laws/legislation	OSP4	54	Training programs for security professionals	DCA2
15	Organizational security compliance	OSP5	55	Training programs to train general employees about security	DCA3
16	Organizational structure with clear roles/responsibilities	OSP6	56	Awareness programs for third parties	DCA4
17	Top management's security behavior	SPC1	57	Training programs for IS audit teams	DCA5
18	Top management's support/encouragement	SPC2	58	Hands-on training for general employees	DCA6
19	Top management's commitment toward implementing security	SPC3	59	Simulating security incidents (e.g., phishing emails)	DCA7
20	Top management's support toward developing security policies	SPC4	60	Awareness programs for employees	DCA8

TABLE 1. (Continued)

#	*Elements of cybersecurity success factors*	*Short Code*	#	*Elements of cybersecurity success factors*	*Short Code*
21	Top management's involvement/participation in the implementation	SPC5	61	Communicating security expectations	RAR1
22	Employees' positive attitude toward security	SPC6	62	Documenting and reporting security incidents	RAR2
23	Employees' perception of the usefulness of security measures	SPC7	63	Communicating security incidents and lessons learned	RAR3
24	Top management's effort to build a pro-security culture	SPC8	64	Reporting adequacy and effectiveness of security programs	RAR4
25	Establishing security policy at early stages of implementation	SPG1	65	Reporting findings from the audit process	RAR5
26	Developing security policy	SPG2	66	Communicating security threats and vulnerabilities	RAR6
27	Developing best practice documents, frameworks	SPG3	67	Documentation practice in the organization	RAR7
28	Standard security tools/applications	SPG4	68	Having confidential reporting process (whistle-blowing)	RAR8
29	Developing user instructions and manuals	SPG5	69	Auditing of security systems and rules/guidelines	RAR9
30	Strict procedure for managing network configuration	SPG6	70	Measuring and tracking of progress in security goals	RAR10
31	SLA/NDA for all relevant stakeholders	SPG7	71	Reviewing processes/policy/procedures regularly	RAR11
32	Security infrastructure and tools	SIF1	72	Monitoring/measuring efficacy of security measures	RAR12
33	Enforcing restrictions on systems and users' behavior	SIF2	73	Measuring effectiveness of training programs	RAR13
34	Monitoring systems	SIF3	74	Business processes conducive to security (e.g., travel restrictions)	EXT1
35	Physical access control	SIF4	75	Non-disclosure agreement with external stakeholders	EXT2
36	Security technology (e.g., encryption, device hardening)	SIF5	76	Security compliance by external stakeholders	EXT3
37	Security processes (e.g., incident management, configuration management)	SIF6	77	Access to external expertise	EXT4
38	Asset classification and access control	SIF7	78	Collaboration with other firms	EXT5
39	Change management system	SIF8	79	Sharing information with other firms/agencies	EXT6
40	High usability of security tools	SIF9			

Note: *Because of space limitation, the CSF acronyms are detailed in Table 2 (e.g., KWE represents "knowledge and awareness of employees").

TABLE 2. Definitions of CSFs under different dimensions.

Dimension	#	Critical success factor & acronym	CSF definition	Examples of supporting articles
Organizational	1	Knowledge and awareness of employees [KWE]	This CSF refers to the existence of high-level awareness and knowledge of all organizational stakeholders regarding cybersecurity and the impact of their behaviors and compliance.	Alnatheer, 2015; Bobbert & Mulder, 2015; Maarop et al., 2015; Zammani et al., 2019
	2	Skilled and committed security team [SCT]	This CSF refers to solid security skills, business knowledge, and commitment from security professionals, audit teams, and IS teams.	Maarop et al., 2015; Tisdale, 2016; Zammani et al., 2019
	3	Organizational structure and priorities [OSP]	This CSF refers to a well-defined organizational structure with clear accountability, compliance, and priority on securing corporate information assets.	Singh et al., 2014; AlGhamdi et al., 2020; Diesch et al., 2020; Atkins & Lawson, 2021
	4	Pro-security culture [SPC]	This CSF refers to pro-security culture through top management's attitude and support toward developing and implementing security management.	Corriss, 2010; Williams, 2011; Alnatheer, 2015; AlGhamdi et al., 2020
Infrastructural	5	Security policy/guidelines [SPG]	This CSF refers to well-established security policies, frameworks, procedures, manuals, and best practices in organizations.	Singh et al., 2014; Tu & Yuan, 2014; Hussain et al., 2020
	6	Security infrastructure [SIF]	This CSF refers to appropriate security infrastructure and tools, including access control, monitoring system, encryption, and incident management process in organizations.	Norman & Yasin, 2012; Choejey et al., 2016; Sadeghi, 2016; Diesch et al., 2020
Strategic	7	Business strategy incorporating security considerations [BSSC]	This CSF refers to integrating security considerations into business strategic plans and processes and involving security professionals in business decisions.	Bayuk & Mostashari, 2011; Henrie, 2013; Atkins & Lawson, 2021
Process	8	Risk assessment of potential threats/ vulnerabilities [RTV]	This CSF refers to continuously identifying and assessing security risks and developing security metrics and recovery plans for threats and vulnerabilities.	Sadeghi, 2016; Zammani & Razali, 2016; Diesch et al., 2020; Hussain et al., 2020
	9	Developing competency and increasing awareness [DCA]	This CSF refers to structured programs to train security professionals and increase	Henrie, 2013; Zammani & Razali, 2016; Kirova & Baumoel, 2018

			awareness of security among organizational stakeholders.	
	10	Reviewing/auditing, measuring performance, and reporting [RAR]	This CSF refers to regular review and audit of security rules and systems, measuring the efficacy of security procedures, reporting security incidents, and auditing findings to organizational stakeholders.	Bobbert & Mulder, 2015; Soomro et al., 2016; Tisdale, 2016; AlGhamdi et al., 2020; Diesch et al., 2020; Atkins & Lawson, 2021
External	11	Security compliance of transactional stakeholders and collaboration with others [EXT]	This CSF refers to security compliance by external stakeholders and non-disclosure agreements with whom the organization has shared information and collaboration.	Maarop et al., 2015; Pandey et al., 2020; Atkins & Lawson, 2021

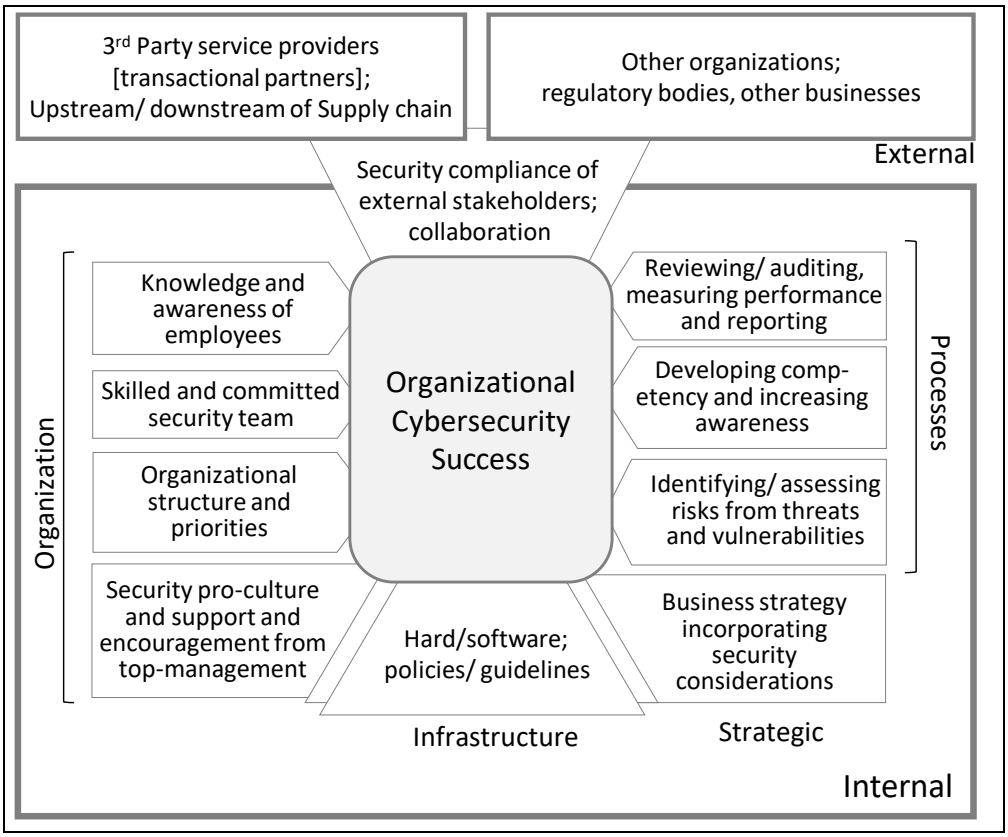

FIGURE 3. A framework of cybersecurity CSFs for organizations.

5. Descriptive analysis of search results

The critical success factors, cybersecurity elements (also known as items) and papers were further analyzed and visualized to understand the cybersecurity CSFs study better. In the following, we summarize the key findings.

Figure 4 uses a tree map to show the frequency of the different factors colored by the capability dimension to which they belong. As shown in Figure 4, process capability and organizational capability are the most commonly studied capabilities. This result highlights that one should take a social-technical approach to cybersecurity management and that processes and organizations are more emphasized than IT security infrastructure. This is in line with the general finding that human error is the biggest threat to IT security. RAR (reviewing, auditing, measuring performance, and reporting) is the most studied process level factor at the factor level, and SPC (pro-security culture) is the most studied organizational capability. The area chart of the item frequency in each dimension (organizational, infrastructural, strategic, process, and external) is further depicted in Figure 5.

At the individual level, there are three very frequently mentioned items, as shown in Figure 5: top management commitment to security implementation (SPC3), top management awareness programs (DCA3), and threat/vulnerability risk identification and assessment (RTV1). This result is very interesting as these items cover the two extremes of the organizational hierarchy: top management and IT operational staff. DCA3 and SPC3 emphasize the importance of informed top management support, while RTV1 emphasizes detailed daily threat identification and assessment.

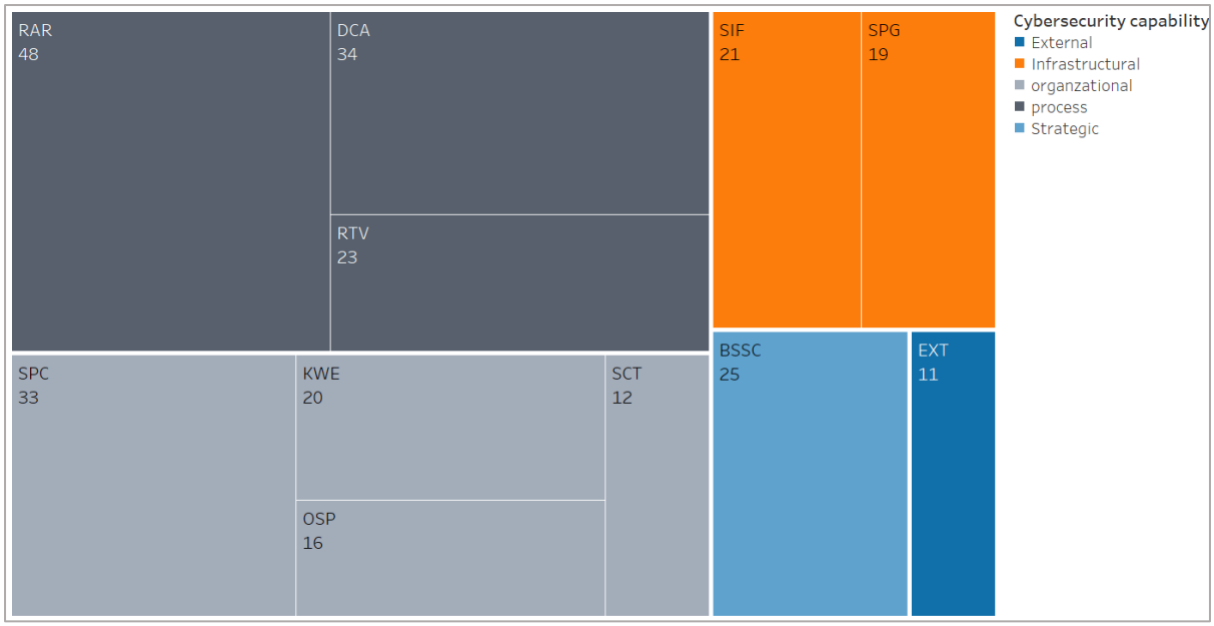

FIGURE 4. Tree map of success factors (Note: the numerical label is the item frequency—the frequency at which the literature pool mentions the item).

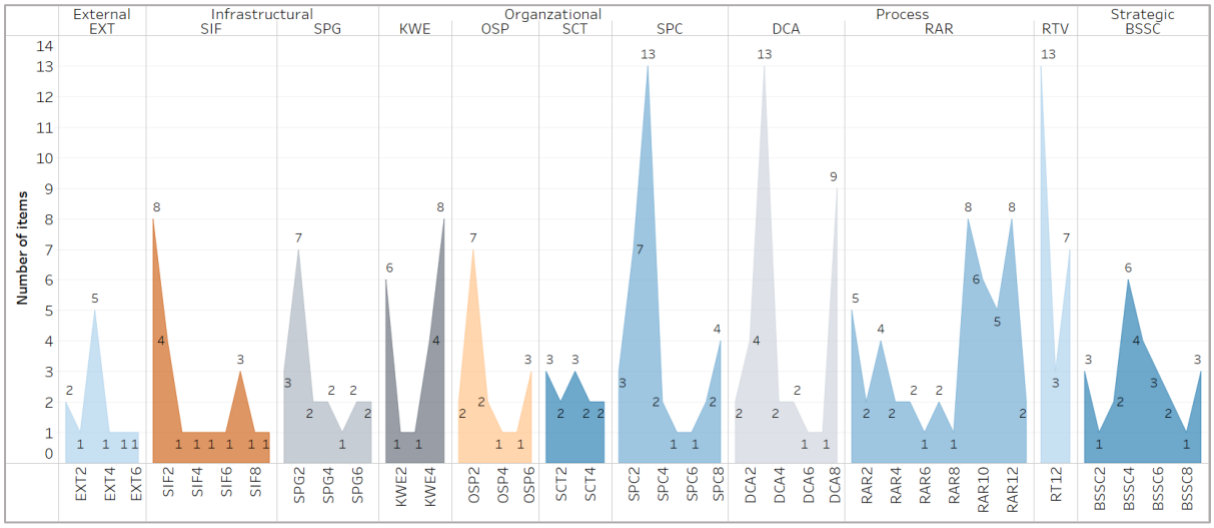

FIGURE 5. Area chart of cybersecurity item frequency.

The yearly trend of article frequency, as shown in Figure 6, is consistent with the trend of papers, as shown in Figure 4. 2016 is the big year of cybersecurity CSFs research, with more publications and mentioned items. The distribution of item frequency across all dimensions is similar to Figure 5. The yearly trend of the factors is shown in Figure 7 as the running total of each capability dimension over the years. As we can see, the total external partnership dimension increases by 150% after 2016; the process, organization, and infrastructure dimensions of cybersecurity also experience high growth, while the growth of the item

frequency of the strategic planning capability is relatively stable. This indicates that cybersecurity management is becoming more complicated, especially at the operational level.

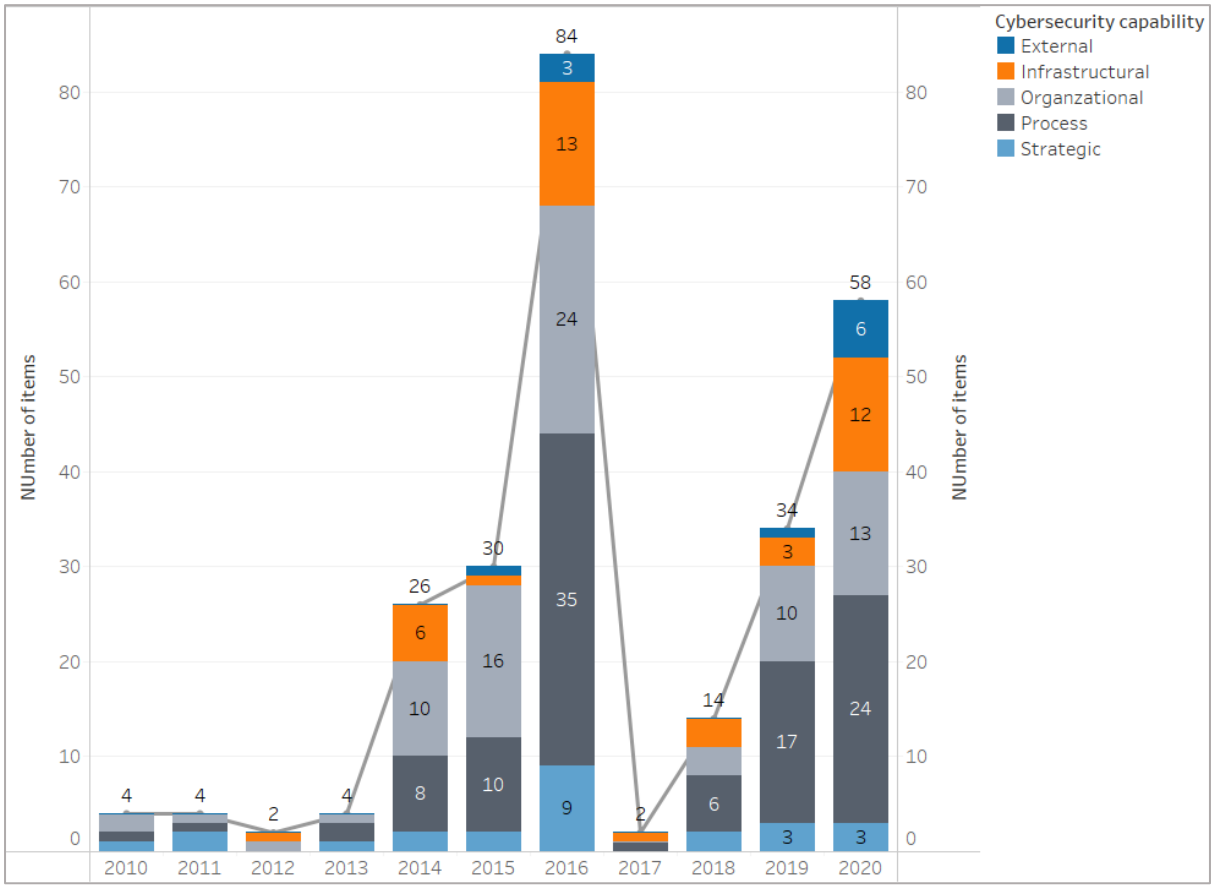

FIGURE 6. Line and stacked bar charts of item frequency by year and capability dimension.

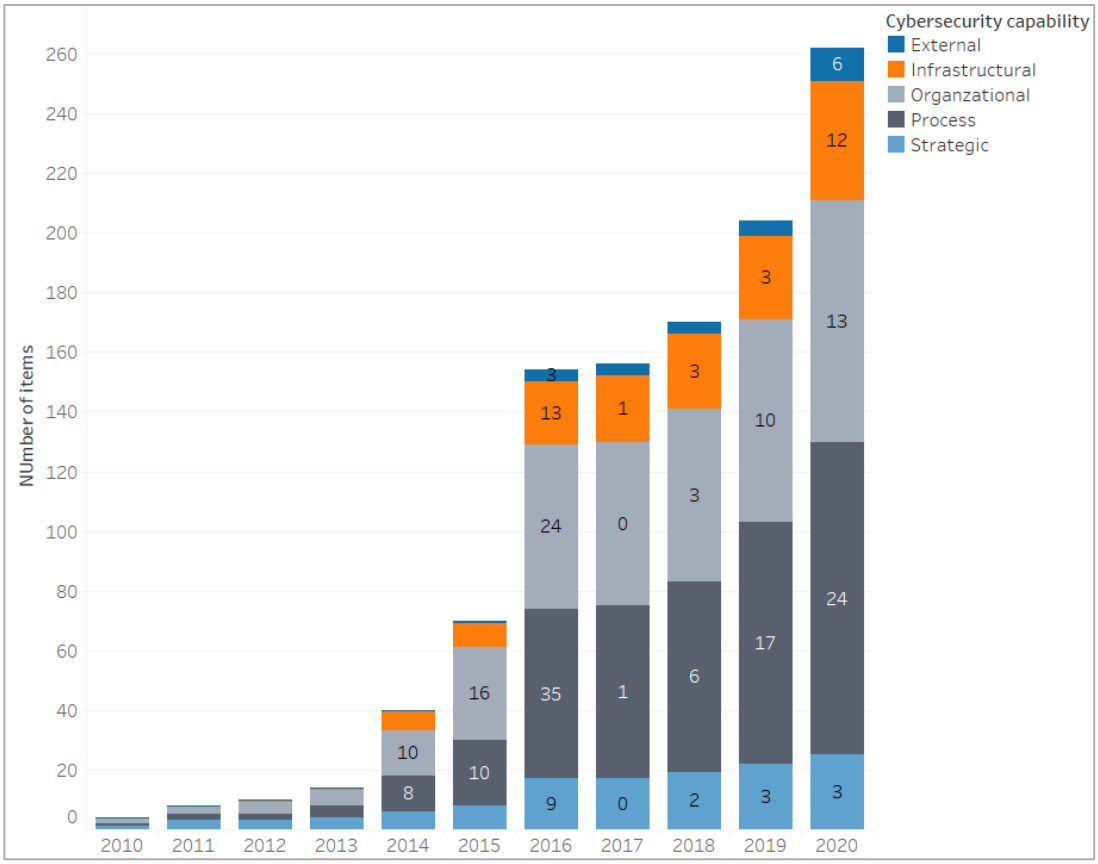

FIGURE 7. Stacked bar charts of item frequency by year and capability dimension (running total) (Note: 1. the numerical label is the item frequency of the year; 2. the item frequency less than three is not shown; 3. bar length indicates the running total of item frequency).

As shown in Figure 8, mixed research methods generate the highest number of items, while quantitative research methods cover the lowest number of items. Mixed methods combine literature review and survey or qualitative studies (Diesch et al., 2020; Pandey et al., 2020), resulting in the richest findings. Our literature pool found only one paper that uses a simulated experiment to study the safety of IT (Cuchta et al., 2019), and it covers only human factors. From an IT management perspective, quantitative research is probably a less ideal method as this type of research focuses on hypothesis testing and can only cover limited points.

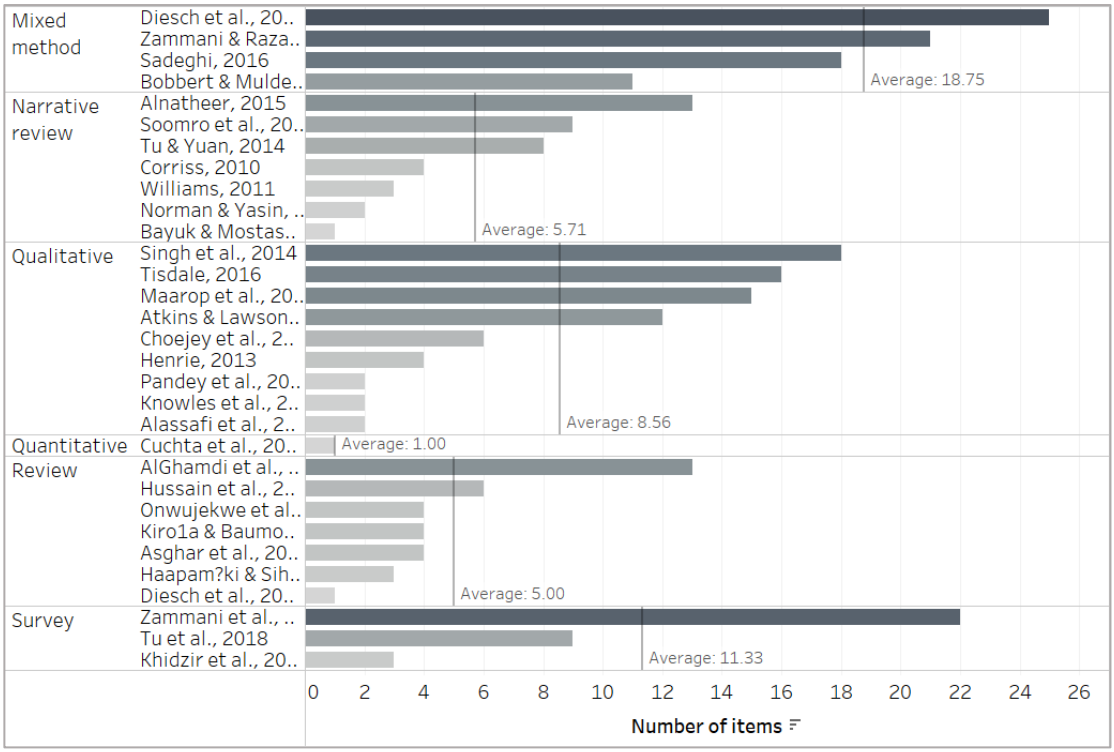

FIGURE 8. Item frequency by paper and research method (Note: the reference line indicates the average item frequency for a specific pane).

Cybersecurity measures depend on context. We classify the context of papers into three categories: general cybersecurity; a specific IT domain such as cloud computing, social media, or industrial systems (which includes industrial control systems and critical infrastructure); and a specific business domain such as cybersecurity governance, culture, strategic direction, or a particular industry. Table A2 in the appendix presents all the items and the category of each item. Figures 9–11 below list the item frequency by research context and paper, research context and factors, and research context and cybersecurity dimensions. As indicated by item frequency, the complexity of cybersecurity management depends on the research context, with general cybersecurity being the most complicated to manage and IT-specific cybersecurity the easiest. Figure 11 shows that the process dimension is the most emphasized. One difference between all contexts is that building infrastructure capabilities is emphasized more than other capabilities for cybersecurity management-specific IT.

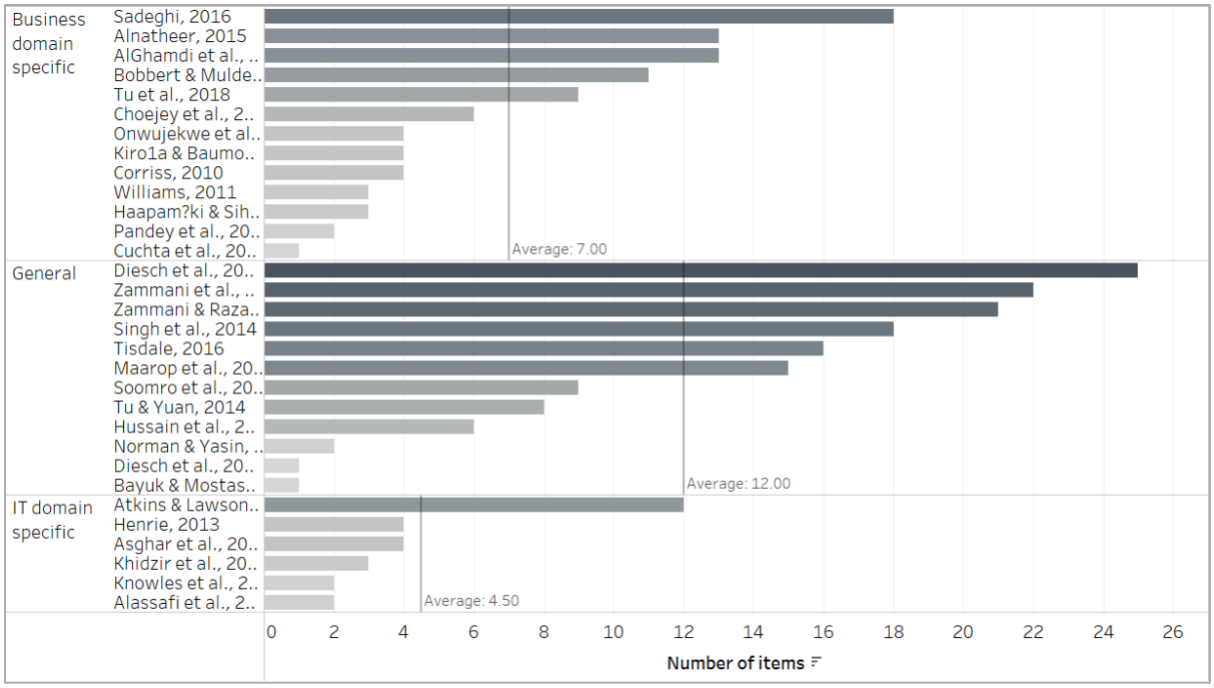

FIGURE 9. Item frequency by research context and paper (Note: the reference line indicates the average item frequency for a specific pane).

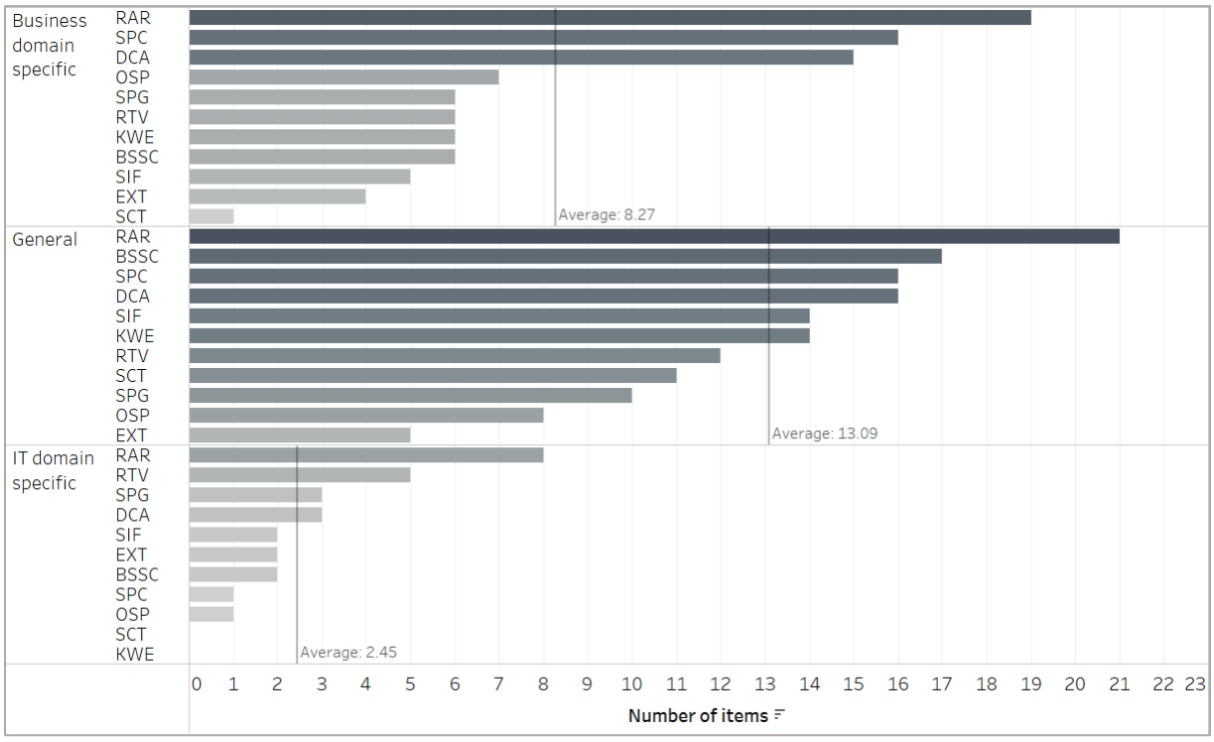

FIGURE 10. Item frequency by research context and critical success factors (Note: the reference line indicates the average item frequency for a specific pane).

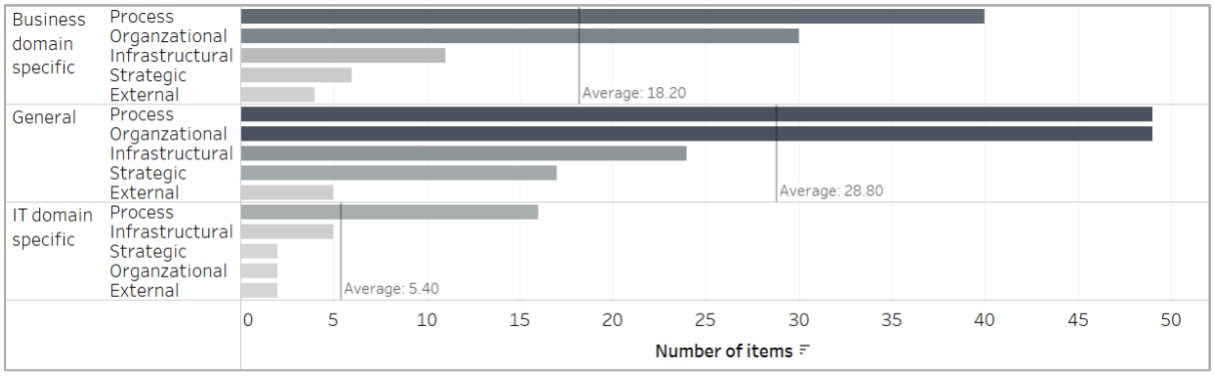

FIGURE 11. Item frequency by research context and cybersecurity dimensions (Note: the reference line indicates the average item frequency for a specific pane).

6. Discussion

This research makes an important contribution to the literature on cybersecurity success factors. We conduct a rigorous literature review following the SLR methodology. An SLR approach minimizes the biases that may occur during the research process and increases the validity of the findings. We found that during the 2019–2020 period, the process and organizational aspects of cybersecurity attract the most attention from researchers; the partnership dimension of cybersecurity is experiencing rapid growth, while that of the strategic dimension is steadily increasing. This is because the processes of cybersecurity management are becoming more complicated. After all, new technologies are emerging in cyberspace, such as cloud computing, the Internet of Things, social media, big data analytics, and artificial intelligence. At the same time, the strategic planning process remains the same. We also suggest that a mixed research method can generate the richest insights regarding the number of points covered and should be considered by future researchers.

Second, we take a step further toward a theory of cybersecurity capability. We adopt the perspective of IT capability theory to organize the cybersecurity CSFs and associated key elements. The advantage of using an established theory to guide the new theorizing is that the established theories have been confirmed and validated by researchers and can provide the right direction for the new theorizing and facilitate comparison between different studies. The detailed items we provide in Table 1 serve as the foundation for future researchers interested in further developing and validating instruments to measure organizational cybersecurity capability.

Third, this research adds to the pool of IT capability research by exploring another critical domain—cybersecurity—of IT capability. IT capability theory is one of the most important and classic theories in IS research (Melville et al., 2004, Wade & Hulland, 2004). It has been used repeatedly to study emerging technologies such as big data and artificial intelligence (Gupta & George, 2016; Mikalef & Gupta, 2021), yet, it has not yet been studied for cybersecurity; thus, this paper fills the research gap.

This research also contributes to cybersecurity management. First, the CSFs and generated items in Table 1 can be employed by practitioners by deploying the items list as a guidance checklist. The checklist will help guide their organizational cybersecurity management. Second, managers can also target cybersecurity capability building, and the proposed dimensions and associated elements can be used for self-assessment to inform cybersecurity strategic planning, budgeting, and resource allocation. Third, a holistic approach to cybersecurity management is advocated because the weakest link in the process determines cybersecurity. In addition, managers should be aware that cybersecurity measures are influenced by context, and they need to adjust their efforts accordingly. Attention should also be paid to the technical infrastructure for specific IT security to ensure that the most relevant security systems are in place.

7. Conclusion

Understanding CSFs is key for cybersecurity success. This paper systematically synthesized cybersecurity CSFs and built a comprehensive cybersecurity CSFs framework grounded in IT capability theory through SLR and subsequent analysis. The CSFs framework includes five dimensions of cybersecurity capability, 11 CSFs, and 79 items that fall into one of the 11 CSFs. The descriptive analysis of the search results also revealed new insights, including the importance of the various factors and capabilities, the frequently mentioned items, the yearly trend of the cybersecurity capability dimensions, and the contextual impact of the cybersecurity capability and factors. Contributing to both research and practice, this research allows cybersecurity stakeholders to holistically understand the CSFs and the associated elements that affect organizational cybersecurity success.

Like all other studies, this study has some limitations, which also offer opportunities for future research. First, we only include references after 2010 because we focus on contemporary cybersecurity. This may limit the audiences interested in the historical perspective of cybersecurity. Future research can expand the scope of the literature search to include

references older than 2010 to gain insight into the historical trend of cybersecurity research. Second, we summarize CSFs categorized according to the IT capability theory. This is a step toward building a theory of cybersecurity capability along the IT capability theory. Researchers can conduct survey-based research to develop and validate cybersecurity capability theory. In addition, researchers can apply the CSFs framework to different business and IT contexts and compare how required cybersecurity capabilities vary across contexts.

Acknowledgement

The authors acknowledge the financial support from the Slovenian Research Agency (research core funding no. P5-0410).

References

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939-953.

Alassafi, M. O., Alharthi, A., Walters, R. J., & Wills, G. B. (2017). A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies. *Telematics and Informatics*, *34*(7), 996–1010.

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers and Security*, *99*(2020), 102030.

Alnatheer, M. A. (2015). Information security culture critical success factors. *12th International Conference on Information Technology: New Generations, ITNG 2015*, 731–735. Las Vegas, NV, USA.

Ambrosio., J. (2021). *Top IT spending priorities for 2021*. https://www.cio.com/article/3611342/top-it-spending-priorities-for-2021.html

Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, *165*(2019), 1–49.

Atkins, S., & Lawson, C. (2020). An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure. *Public Administration Review*, *81*(5), 847–861.

Baikloy, E., Praneetpolgrang, P., Jirawichitchai, N. (2020). Development of cyber resilient capability maturity model for cloud computing services. *TEM Journal*, *9*(3), 915–923.

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, *17*(1), 99–120.

Bayuk, J. L., & Mostashari, A. (2011). Measuring cyber security in intelligent urban infrastructure systems. *8th International Conference and Expo on Emerging Technologies for a Smarter World, CEWIT 2011*, 1–6. Long Island, New York, USA.

Becker, M. C. (2004). Organizational routines: a review of the literature. *Industrial and corporate change*, *13*(4), 643-678.

Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: an empirical investigation. *MIS Quarterly*, *24*(1), 169–196.

Bhatt, G. D., & Grover, V. (2005). Types of information technology capabilities and their role in competitive advantage: An empirical study. *Journal of Management Information Systems*, *22*(2), 253–277.

Bobbert, Y., & Mulder, H. (2016). Governance Practices and Critical Success Factors Suitable for Business Information Security. *CICN 2015 Proceedings*, 1097–1104. Jabalpur.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 1–14.

Choejey, P., Murray, D., & Fung, C. C. (2016). Exploring Critical Success Factors for Cybersecurity in Bhutan's Government Organizations. *International Conference on*

Networks & Communications, 49–61.

Chowdhury, N. H., Adam, M. T. P., & Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: A systematic literature review. *Behaviour & Information Technology*, *38*(12), 1–19.

Corriss, L. (2010). Information security governance: Integrating security into the organizational culture. *GTIP 2010 Proceedings*, 35–41. Austin, Texas, USA: ACM.

Cuchta, T., Blackwood, B., Devine, T. R., Niichel, R. J., Daniels, K. M., Lutjens, C. H., Maibach, S., & Stephenson, R. J. (2019). Human risk factors in cybersecurity. *SIGITE 2019 Proceedings*, 87–92. Tacoma, WA, USA: ACM.

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers and Security*, *92*(2020), 1–21.

Diesch, R., Pfaff, M., & Krcmar, H. (2018). Prerequisite to Measure Information Security A State of the Art Literature Review. *ICISSP 2018 Proceedings*, 201–207. Funchal, Madeira, PT.

Felin, T., & Foss, N. J. (2009). Organizational routines and capabilities: Historical drift and a course-correction toward microfoundations. *Scandinavian Journal of Management*, *25*(2), 157-167.

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An event study analysis of the economic impact of IT operational risk and its subcategories. *Journal of the Association for Information Systems*, *12*(9), 606–631.

Grant, R. M., & Verona, G. (2015). What's holding back empirical research into organizational capabilities? Remedies for common problems. *Strategic Organization*, *13*(1), 61-74.

Griffith, T. L. (1999). Technology features as triggers for sensemaking. *Academy of Management review*, *24*(3), 472-488.

Gupta, M., & George, J. F. (2016). Toward the development of a big data analytics capability. *Information & Management*, *53*(8), 1049–1064.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), 808–834.

Henrie, M. (2013). Cyber security risk management in the SCADA critical infrastructure environment. *Engineering Management Journal*, *25*(2), 38–45.

Hussain, A., Mohamed, A., & Razali, S. (2020). A review on cybersecurity: Challenges & emerging threats. *NISS 2020 Proceedings*, 1–7. Marrakech, MR: ACM.

Jeffers, M., & Turton, W. (2021). *Ransomware attack shuts down biggest U.S. gasoline pipeline*. Gulf Publishing Company LLC. www.worldoil.com

Karimi, J., Somers, T. M., & Bhattacherjee, A. (2007). The role of information systems resources in ERP capability building and business process outcomes. *Journal of Management Information Systems*, *24*(2), 221–260.

Khidzir, N. Z., Ismail, A. R., Daud, K. A. M., Afendi, M. S., Ghani, A., & Ibrahim, M. A. H. (2016). Critical cybersecurity risk factors in digital social media: Analysis of information security requirements. *Lecture Notes on Information Theory*, *4*(1), 1–7.

Kirova, D., & Baumoel, U. (2018). Factors that affect the success of Security Education, Training, and Awareness programs: A literature review. *Journal of Information Technology Theory and Application (JITTA)*, *19*(4), 56–82.

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, 1-26.

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, *9*(2015), 52–80.

Le, N. T., & Hoang, D. B. (2017). Capability maturity model and metrics framework for cyber cloud security. *Scalable Computing*, *18*(4), 277–290.

Maarop, N., Mustapha, N. M., Yusoff, R., Ibrahim, R., & Zainuddin, N. M. M. (2015). Understanding success factors of an information security management system plan phase self-implementation. *International Journal of Computer and Information Engineering*, *9*(3), 884–889.

Mata, F. J., Fuerst, W. L., & Barney, J. B. (1995). Information technology and sustained competitive advantage: A resource-based analysis. *MIS Quarterly*, *19*(4), 487–505.

Mcafee. (2014). *Every Company is a Software Company [Online]*. Mcafee. https://www.mcafee.com/blogs/enterprise/cloud-security/every-company-is-a-software-company-today/

Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Review: Information technology and organizational performance: An integrative model of IT business value. *MIS Quarterly*, *28*(2004), 283–322.

Mikalef, P., & Gupta, M. (n.d.). Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. *Information & Management*, *58*(3), 1–20.

Mohammed, I., & Bade, A. M. (2019). Cybersecurity capability maturity model for network system. *International Journal of Development Research*, *9*(7), 28637–28641.

Narain Singh, A., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management." *Journal of Enterprise Information Management*, *27*(5), 644–667.

Norman, A. A., & Yasin, N. M. (2012). Information systems security management (ISSM) success factor: Retrospection from the scholars. *European Conference on Information Warfare and Security*, 1–7.

Onwujekwe, G., Thomas, M., & Osei-Bryson, K. M. (2019). Using robust data governance to mitigate the impact of cybercrime. *Proceedings of the 2019 3rd International Conference on Information System and Data Mining*, 70–79. Houston, TX, USA: ACM.

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103–128.

Paulk, M. C. (2009). A history of the capability maturity model for software. *ASQ Software Quality Professional*, *12*(1), 5–19.

Peteraf, M. A. (1993). The cornerstones of competitive advantage: a resource‐based view. *Strategic Management Journal*, *14*(3), 179-191.

Ravichandran, T., Lertwongsatien, C., & Lertwongsatien, C. (2005). Effect of information systems resources and capabilities on firm performance: A resource-based perspective. *Journal of Management Information Systems*, *21*(4), 237–276.

Rowe, F. (2014). What literature review is not: diversity, boundaries and recommendations. *European Journal of Information Systems*, *23*(3), 241–255.

Sadeghi, R. A. (2016). Identifying key success factors in the implementation of information security systems on service businesses: A case study of the private banks of Tehran. *American Journal of Theoretical and Applied Business*, *2*(4), 28–37.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 1–23.

Sobers, R. (2021). *134 Cybersecurity Statistics and Trends for 2021*. https://www.varonis.com/blog/cybersecurity-statistics/

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225.

Tisdale, S. M. (2016). Architecting A cybersecurity managment framework. *Issues In Information Systemstion Systems*, *17*(IV), 227–236.

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.

Tu, Z., & Yuan, Y. (2014). Critical success factors analysis on effective information security management: A literature review. *20th Americas Conference on Information Systems*, 1–13. Savannah, GA.

Wade, M., & Hulland, J. (2004). The resource-based view and information systems research: Review, extension, and suggestions for future research. *MIS Quarterly*, *28*(1), 107–142.

Wang, Z., & Kim, H. G. (2017). Can social media marketing improve customer relationship capabilities and firm performance? Dynamic capability perspective. *Journal of Interactive Marketing*, *39*(2017), 15–26.

Webster, J., & Watson, R. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), xiii–xxiii.

Williams, N. (2011). The importance of governance and culture on strategic information security. *Proceedings of the 17th International Business Information Management Association (IBIMA)*, 1–8. Milan, IT.

Yeoh, W., Huang, H., Lee, W. S., Al Jafari, F., & Mansson, R. (2021). Simulated phishing attack and embedded training campaign. *Journal of Computer Information Systems*, *Online*(2021), 1–20.

Yoon, C. Y. (2011). Measuring enterprise IT capability: A total IT capability perspective. *Knowledge-Based Systems*, *24*(1), 113–118.

Zalewski, J., Drager, S., McKeever, W., & Kornecki, A. J. (2014). Measuring security: A

challenge for the generation. *2014 Federated Conference on Computer Science and Information Systems*, 131–140. Warsaw, PL.

Zammani, M., & Razali, R. (2016). An empirical study of information security management success factors. *International Journal on Advanced Science, Engineering and Information Technology*, *6*(2016), 1–10.

Zammani, M., Razali, R., & Singh, D. (2019). Factors contributing to the success of information security management implementation. *International Journal of Advanced Computer Science and Applications*, *10*(11), 384–391.

Zhang, M., Sarker, S., & Sarker, S. (2008). Unpacking the effect of IT capability on the performance of export-focused SMEs: a report from China. *Information Systems Journal*, *18*(4), 357–380.

Zhuang, Y., & Lederer, A. L. (2006). A resource-based view of electronic commerce. , 43, 251-261. *Information & Management*, *43*(2), 251–261.

Appendix

TABLE A1. List of analyzed articles.

Author(s) (Year)	*Article type*	*Topic area and context*	*Methodology*	*Contribution*
Corriss (2010)	Review	Cybersecurity governance and culture in business organizations	Narrative review	Highlighting the importance of security to be integrated in culture
Williams (2011)	Review	Cybersecurity governance and culture in business organizations	Narrative review	Highlighting the importance of awareness beyond technological implementation
Bayuk & Mostashari (2011)	Review	Technical and historical perspective of security metrics	Narrative review	Developing security system diagram and highlighting the importance of security metrics to be linked with business goals
Norman & Yasin (2012)	Review	Information system security management comprises technology characteristics, organizational structure, and environmental influence	Narrative review	Developing a model for information system security management success and suggesting 10 CSFs in 3 categories
Henrie (2013)	Qualitative	Cybersecurity for SCADA in oil & gas industry	Semi-structured interviews (n=47), workshops (n=94) involving professionals	Suggesting 4 success factors
Narain Singh et al. (2014)	Qualitative	Organizational cybersecurity management	Keyword analysis of literature and expert opinions (n=24), item development, survey	Suggesting 10 success factors
Tu & Yuan (2014)	Review	Organizational cybersecurity management	Narrative review	Suggesting 8 success factors
Alnatheer (2015)	Review	Security culture in organizations	Narrative review	Suggesting 8 success factors
Bobbert & Mulder (2015)	Review and qualitative	Business information security maturity	Narrative review of literature since 2009; Group Support System of 12 experts	Suggesting 22 core principles for business information security maturity
Knowles et al. (2015)	Qualitative	Cybersecurity management in Industrial control system	Analysis of security standards and guidelines	Suggesting 5 success factors
Maarop et al. (2015)	Qualitative	Cybersecurity management system implementation	Semi-structured interviews (n=5) of security professionals	Suggesting 4 success factors
Choejey et al. (2016)	Qualitative	Government organizations (Bhutan)	Open-ended questions (n=157), ICT professionals in government organizations	Suggesting 5 success factors
Khidzir et al. (2016)	Survey*	Digital social media (Malaysia)	Cyber community/knowledge society individuals (n=33)	18 cybersecurity risk factors
Sadeghi (2016)	Review and survey	Cybersecurity implementation in service businesses (Tehran)	Narrative review; survey (n=131) of bank managers	Identification and ranking of 25 CSFs categorized in 4 broader categories.

TABLE A1. (Continued)

Author(s) (Year)	*Type*	*Context*	*Methodology details*	*Contribution*
Soomro et al. (2016)	Review	Cybersecurity management	Narrative review of 67 articles	Suggesting 6 success factors
Tisdale (2016)	Qualitative	Cybersecurity management	Semi-structured interviews (n=19), participants from different IS/business domains	Suggesting 13 success factors
Zammani & Razali (2016)	Review and qualitative	Cybersecurity management (Malaysia)	Semi-structured interviews (n=5) of cybersecurity professionals, focus group discussion (n=4)	Suggesting 13 success factors along with elements pertaining to each factor
Alassafi et al. (2017)	Qualitative	Cloud adoption (Saudi Arabia)	Interviews (n=18) of experts	Identifying factors behind cloud adoption decisions
Diesch et al. (2018)	Review	Cybersecurity performance measurements	Systematic review of 70 articles	Classifying themes in security literature
Kirova & Baumöl (2018)	Review	Security education, training, and awareness programs	Systematic review of 42 papers	Identifying factors affecting the success of Security Education, Training and Awareness (SETA) programs and organizing them into a conceptual classification
Tu et al. (2018)	Survey	Strategic value alignment for information security management	Survey (n=219) of CIO, CSO, IT/CS managers, senior IT staff	Testing a model capturing the main antecedents of cybersecurity management performance
Asghar et al. (2019)	Review	Industrial control systems security	Review of 33 solutions suggested in literature	Suggesting protection measures of industrial control systems
Cuchta et al. (2019)	Quantitative	Human factors in cybersecurity	Simulated phishing experiment (n=4769)	Suggesting how to increase effectiveness of training programs to reduce non-secure behavior
Haapamäki & Sihvonen (2019)	Review	Cybersecurity accounting	Systematic review of 39 studies (2000–2018)	Suggesting 4 success factors
Onwujekwe et al. (2019)	Review	Data governance	45 studies (2014–2017)	Suggesting 5 success factors
Zammani et al. (2019)	Survey	Cybersecurity management (Malaysia)	Cybersecurity experts, practitioners from statutory bodies, public and private orgs	Confirming the success factors identified in Zammani & Rozali (2016). Further, adding a new success factor (i.e., infrastructure) and ranking them based on participants' responses
AlGhamdi et al. (2020)	Review	Cybersecurity governance	Systematic review of 136 studies (since 2000)	Suggesting 27 success factors in 7 domains
Diesch et al. (2020)	Review and qualitative	Cybersecurity factors for decision-makers	Systematic review of 136 articles; semi-structured interviews of experts (n=19)	Identifying success factors in 12 areas
Hussain et al. (2020)	Review	Organizational cybersecurity management	Narrative review of 33 articles	Suggesting 3 success factors

TABLE A1. (Continued)

Author(s) (Year)	*Type*	*Context*	*Methodology details*	*Contribution*
Pandey et al. (2020)	Qualitative	Cybersecurity risks in globalized supply chains	Review, case study and focused grp discussion with SC professionals (n=11)	Identifying and categorizing cybersecurity risks across global supply chains
Atkins & Lawson (2021)	Qualitative	Cybersecurity policy for critical infrastructure	Comparative study across industry	Identifying 2 predictors for security policy success

Note: The table lists the studies in chronological order by year of publication.
* *Survey* means questionnaire-based survey.

TABLE A2. Mapping between elements of critical success factors and the analyzed articles. (Note: V in the matrix indicates a place; total: 262 Vs/places).

Short Code of cybersecurity elements	*Corriss, 2010*	*Williams, 2011*	*Bayuk & Mostashari, 2011*	*Norman & Yasin, 2012*	*Henrie, 2013*	*Singh et al., 2014*	*Tu & Yuan, 2014*	*Alnatheer, 2015*	*Bobbert & Mulder, 2015*	*Knowles et al., 2015*	*Maarop et al., 2015*	*Choejey et al., 2016*	*Khidzir et al., 2016*	*Sadeghi, 2016*	*Soomro et al., 2016*	*Tisdale, 2016*	*Zammani & Razali, 2016*	*Alassafi et al., 2017*	*Diesch et al., 2018*	*Kirova & Baumoel, 2018*	*Tu et al., 2018*	*Asghar et al., 2019*	*Cuchta et al., 2019*	*Haapamäki & Sihvonen, 2019*	*Onwujekwe et al., 2019*	*Zammani et al., 2019*	*AlGhamdi et al., 2020*	*Atkins & Lawson, 2021*	*Diesch et al., 2020*	*Hussain et al., 2020*	*Pandey et al., 2020*
KWE1								V	V		V				V		V									V					
KWE2						V																									
KWE3																V															
KWE4							V										V				V					V					
KWE5								V	V		V			V		V	V									V			V		
SCT1											V						V									V					
SCT2											V					V															
SCT3											V						V									V					
SCT4																	V									V					
SCT5																V								V							
OSP1									V																		V				
OSP2						V	V				V					V					V				V				V		
OSP3						V		V																							
OSP4						V																									
OSP5																											V				
OSP6																											V	V	V		

TABLE A2. (Continued)

Short Code of cybersecurity elements	*Corriss, 2010*	*Williams, 2011*	*Bayuk & Mostashari, 2011*	*Norman & Yasin, 2012*	*Henrie, 2013*	*Singh et al., 2014*	*Tu & Yuan, 2014*	*Alnatheer, 2015*	*Bobbert & Mulder, 2015*	*Knowles et al., 2015*	*Maarop et al., 2015*	*Choejey et al., 2016*	*Khidzir et al., 2016*	*Sadeghi, 2016*	*Soomro et al., 2016*	*Tisdale, 2016*	*Zammani & Razali, 2016*	*Alassafi et al., 2017*	*Diesch et al., 2018*	*Kirova & Baumoel, 2018*	*Tu et al., 2018*	*Asghar et al., 2019*	*Cuchta et al., 2019*	*Haapamäki & Sihvonen, 2019*	*Onwujekwe et al., 2019*	*Zammani et al., 2019*	*AlGhamdi et al., 2020*	*Atkins & Lawson, 2021*	*Diesch et al., 2020*	*Hussain et al., 2020*	*Pandey et al., 2020*
SPC1		V							V																		V				
SPC2	V					V		V			V	V					V									V					
SPC3	V			V		V	V	V			V			V	V		V				V					V	V		V		
SPC4					V																						V				
SPC5								V																							
SPC6														V																	
SPC7											V																		V		
SPC8						V		V						V																V	
SPG1																	V					V				V					
SPG2						V	V	V				V	V		V						V										
SPG3						V																								V	
SPG4							V														V										
SPG5																															
SPG6																V													V		
SPG7														V				V													
SIF1				V								V		V	V											V		V	V	V	

TABLE A2. (Continued)

Short Code of cybersecurity elements	*Corriss, 2010*	*Williams, 2011*	*Bayuk & Mostashari, 2011*	*Norman & Yasin, 2012*	*Henrie, 2013*	*Singh et al., 2014*	*Tu & Yuan, 2014*	*Alnatheer, 2015*	*Bobbert & Mulder, 2015*	*Knowles et al., 2015*	*Maarop et al., 2015*	*Choejey et al., 2016*	*Khidzir et al., 2016*	*Sadeghi, 2016*	*Soomro et al., 2016*	*Tisdale, 2016*	*Zammani & Razali, 2016*	*Alassafi et al., 2017*	*Diesch et al., 2018*	*Kirova & Baumoel, 2018*	*Tu et al., 2018*	*Asghar et al., 2019*	*Cuchta et al., 2019*	*Haapamäki & Sihvonen, 2019*	*Onwujekwe et al., 2019*	*Zammani et al., 2019*	*AlGhamdi et al., 2020*	*Atkins & Lawson, 2021*	*Diesch et al., 2020*	*Hussain et al., 2020*	*Pandey et al., 2020*
SIF2																V					V							V	V		
SIF3																											V				
SIF4																													V		
SIF5																													V		
SIF6						V																									
SIF7						V						V																	V		
SIF8																													V		
SIF9																V															
BSSC1	V										V			V																	
BSSC2		V																													
BSSC3			V																V												
BSSC4					V		V								V	V					V							V			
BSSC5						V											V									V			V		
BSSC6																	V									V			V		
BSSC7																V								V							
BSSC8														V																	

TABLE A2. (Continued)

Short Code of cybersecurity elements	*Corriss, 2010*	*Williams, 2011*	*Bayuk & Mostashari, 2011*	*Norman & Yasin, 2012*	*Henrie, 2013*	*Singh et al., 2014*	*Tu & Yuan, 2014*	*Alnatheer, 2015*	*Bobbert & Mulder, 2015*	*Knowles et al., 2015*	*Maarop et al., 2015*	*Choejey et al., 2016*	*Khidzir et al., 2016*	*Sadeghi, 2016*	*Soomro et al., 2016*	*Tisdale, 2016*	*Zammani & Razali, 2016*	*Alassafi et al., 2017*	*Diesch et al., 2018*	*Kirova & Baumoel, 2018*	*Tu et al., 2018*	*Asghar et al., 2019*	*Cuchta et al., 2019*	*Haapamäki & Sihvonen, 2019*	*Onwujekwe et al., 2019*	*Zammani et al., 2019*	*AlGhamdi et al., 2020*	*Atkins & Lawson, 2021*	*Diesch et al., 2020*	*Hussain et al., 2020*	*Pandey et al., 2020*
BSSC9											V				V	V															
RTV1						V	V	V	V		V		V	V			V				V	V				V			V	V	
RTV2										V				V														V			
RTV3														V		V	V									V		V	V	V	
DCA1		V																									V				
DCA2					V	V											V									V					
DCA3					V	V		V				V	V		V	V	V			V			V		V	V			V		
DCA4																	V									V					
DCA5																	V									V					
DCA6														V																	
DCA7																				V											
DCA8						V		V	V			V								V					V		V		V	V	
RAR1	V														V	V									V				V		
RAR2						V								V																	
RAR3								V	V							V								V							
RAR4									V						V																

TABLE A2. (Continued)

Short Code of cybersecurity elements	*Corriss, 2010*	*Williams, 2011*	*Bayuk & Mostashari, 2011*	*Norman & Yasin, 2012*	*Henrie, 2013*	*Singh et al., 2014*	*Tu & Yuan, 2014*	*Alnatheer, 2015*	*Bobbert & Mulder, 2015*	*Knowles et al., 2015*	*Maarop et al., 2015*	*Choejey et al., 2016*	*Khidzir et al., 2016*	*Sadeghi, 2016*	*Soomro et al., 2016*	*Tisdale, 2016*	*Zammani & Razali, 2016*	*Alassafi et al., 2017*	*Diesch et al., 2018*	*Kirova & Baumoel, 2018*	*Tu et al., 2018*	*Asghar et al., 2019*	*Cuchta et al., 2019*	*Haapamäki & Sihvonen, 2019*	*Onwujekwe et al., 2019*	*Zammani et al., 2019*	*AlGhamdi et al., 2020*	*Atkins & Lawson, 2021*	*Diesch et al., 2020*	*Hussain et al., 2020*	*Pandey et al., 2020*
RAR5																	V									V					
RAR6																													V		
RAR7											V																		V		
RAR8									V																						
RAR9						V			V		V							V				V					V	V	V		
RAR10							V	V						V							V						V	V			
RAR11									V								V			V					V		V				
RAR12										V				V			V					V			V	V	V	V			
RAR13														V															V		
EXT1																													V		V
EXT2														V																	
EXT3																V	V								V	V					V
EXT4											V																				
EXT5																												V			
EXT6																												V			

TABLE A3. Domain context of analyzed papers.

Category	Context	Number of papers	References
Business domain specific	Culture	1	Alnatheer (2015)
	Governance perspective	5	AlGhamdi et al. (2020) Bobbert & Mulder (2015) Corriss (2010) Onwujekwe et al. (2019) Williams (2011)
	Human factors	2	Cuchta et al. (2019) Kirova & Baumöl (2018)
	Organization/industry specific	4	Choejey et al. (2016) Haapamäki & Sihvonen (2019) Pandey et al. (2020) Sadeghi (2016)
	Strategic alignment	1	Tu et al. (2018)
General	General	12	Bayuk & Mostashari (2011) Diesch et al. (2018) Diesch et al. (2020) Hussain et al. (2020) Maarop et al. (2015) Norman & Yasin (2012) Narain Singh et al. (2014) Soomro et al. (2016) Tisdale (2016) Tu & Yuan (2014) Zammani & Razali (2016) Zammani et al. (2019)
IT domain specific	Cloud computing	1	Alassafi et al. (2017)
	Industrial systems	4	Asghar et al. (2019) Atkins & Lawson (2021) Henrie (2013) Knowles et al. (2015)
	Social media	1	Khidzir et al. (2016)