A Classification of Essential Factors for the Development and Implementation of Cyber Security Strategy in Public Sector Organizations

Waqas Aman*, Jihan Al Shukaili
Department of Information Systems, College of Economics and Political Science
Sultan Qaboos University, Muscat, Sultanate of Oman

***Abstract*—To ensure the achievement of quality security to safeguard business objectives, implementing, and maintaining an effective Cyber Security Strategy (CSS) is crucial. Inevitably, we need to recognize and evaluate the essential factors, such as technological, cultural, regulatory, economic, and others, that may hinder the efficacy of a CSS development and implementation. From the literature review, it is evident that such factors are either abstractly stated, or only assessed from singular viewpoint and are scattered across the literature. Moreover, there is a lack of holistic studies that could assist us in comprehending the critical factors affecting a CSS. In this paper, we present a systematic classification of distinct, structured, and comprehensive list of key factors covering multiple aspects of an organization's CSS, including organizational, cultural, economic, legal and political, and security, to provide a more complete view of understanding the essentials and analyzing the aptitude of a planned or given CSS. The proposed classification is further evaluated to examine the critical factors verified by conducting semi-structured interviews from security experts in different public sector organizations. Furthermore, we present a comparison of our work with the recent attempts that reflects that a significant accumulation of essential factors have been holistically identified in this study.**

***Keywords*—Cyber security strategy; critical factors; risk treatment; culture; threats**

I. INTRODUCTION

This Cyber security is a vital concern for both the public and private sectors. However, the public sector is unique as it comparatively has a vast IT infrastructure covering a broader and general user base [1]. Public sector organizations have experienced targeted attacks continuously and increasingly [2]. Around 70% of breaches target public or government organizations [3].

Security is becoming harder to manage in today's dynamic information systems and necessitates an efficient strategy to deal with the adverse incidents and to protect the organization from the potential risks [4]. A Cyber Security Strategy (CSS) is a long–term high-level plan designed to achieve security goals to ensure that the business meets its set objectives, mission, and vision effectively [5]. It provides a collection of frameworks, procedures, and corresponding objectives that aim to achieve certain quality in securing the organization infrastructure and operations.

As stressed in [6] and [7], CSS is very important to the public sector because:

- Cyber-attacks in this domain is more permanent and their consequences can last for a long period.
- The public sector is composed of the most sensitive and critical infrastructure.
- There is a need to develop justifications for and foresee low risk investments of public funds in cyber security solutions and services.
- It will assist in implementing a uniform plan across the organization to protect public resources, and therefore assist in building and retaining a high-level public trust.

The reliance of technology for almost every single process in an organization has led to push CSS and its success factors to the top of the business agenda. A CSS can only be designed and implemented efficaciously, if we recognize and assess the corresponding influencing factors [8]. During our study, we found that there have been numerous efforts made in highlighting these factors however, their focus is either a particular aspect of business like regulatory needs and technical concerns, or abstractly identified in a particular operational infrastructure, e.g., healthcare. We couldn't find any appropriate study that provides a holistic and comprehensive classification or list of essential factors, which we can refer to for (re)consideration, while we plan to design and implement an effective CSS.

In this study, we present a classification of distinct and well-structured list of more than twenty essential factors that will help a public sector's organization to evaluate key business and operational aspects when designing or implementing their CSS. For every long-term planning, such as a CSS, it is vital to consider the major business contexts. This includes the human factors, regulatory and political contexts, economic capabilities, the potential threat landscape and its methodological management, etc. [9]. To ensure that our classification encompasses all major and mission-critical business themes, we developed our classification to include six principal classes as: Organizational, Cultural, Legal and Political, Economic, Technical, and Risk. Similar business themes are also stressed to be evaluated in [9-11]. This classification ensures that all the identified factors are aligned with and cover the vital concerns related to the key contexts of

*Corresponding Author

an organization. To further refine the factors and to highlight the critical ones, we have conducted open-ended semi-structure interviews. The interviews, comprising of seventy questions, were held with experts in the field to comprehend what they believe to be crucial factors for a successful CSS. Moreover, a comparative analysis is performed with the existing related work that shows that our classification provides a more comprehensive and complete list of factors, and provides an organization a broader view of the dynamics related to the development and implementation of an effective CSS.

The rest of the article is structured as follows: In Section 2, we summarize the area, factors and methodology used in the related work. The methodology used and results are detailed in Section 3. This section also highlights the reflection made on the critical factors identified. A comparison of the proposed classification with related work is provided in Section 4. Finally, the study limitations and conclusion are presented in Section 5.

II. Related Work

Several studies highlighted some of the factors that can influence the design and implementation of CSS. In this section, we have reviewed the most related literature. These works also form the basis of the proposed classification and are also used in the comparison.

Jalaai et al. [2] has explored the organizational perspective of cyber security in the Healthcare sector. The study followed a systematic literature review and focused on the most important aspects needed to tackle a successful strategy adopted for healthcare. The study highlighted and focused on organizational factors that also touched the technical readiness of the healthcare institutes. The factors identified in this study were software development security, disaster recovery planning and business continuity.

The human factor in the current cyber security landscape is studied by Benson et al. [12]. Using a systematic literature review, the authors outlined the most critical factors in human element domain are: Awareness, Individual Attitudes, Norms and Cultural context.

Fritzvold, in [13], has focused on the Cyber security in the organization with focus on the sectors of power distributions, railway and healthcare. The study followed a case study approach to explore the factors that directly or indirectly influence the cyber security posture in the mentioned domains. The key factors outlined in this work are: competence, compliance, awareness, leadership engagement and system technology management.

Awan et al., in [14], have studied the security strategies to overcome security measures, the authors pointed out the effective factors that influence the success of implementing such strategies to overcome such measures. Following a systematic literature review, the factors stressed are: Level of governance in critical information infrastructure (CII), level of protection, sharing of Cyber-security information and insufficient market preparation.

In [15], the authors studied the human factors in the information security culture and stated that the human factor has always been the weakest link when it comes to security enforcement. To strengthen this aspect, some procedures need to be taken into consideration. Following a systematic literature review, the authors included that the essential human factors that form the basis for a successful security program enforcement are: information security (IS) policy, deterrence, incentives, attitude, involvement, training and awareness and management support. The authors concluded that only employing technology-oriented security controls are not sufficient, and that people at all levels of the organization play an important role in bringing a positive value to the information security culture and therefore, should be assessed and addressed in any security program.

Khansa et al. [16], have followed two rounds of a qualitative survey to study the impact of organizational control in cyber environment. The study emphasized on exploring the relationship between employees' cyberloafing and formal organization control. Cyberloafing is defined as the surfing of employees over the internet for personal reasons during work hours [17, 18]. Such a behavior negatively affects the productivity and may lead to unwanted and severe security issues. The study suggested that that factors such as, attitude, subjective norms perceived, behavioral controls and lack of punishment. These factors play a vital role in designing organization controls that are crucial to be considered for any given CSS.

Ebenezer [19] studied how staff accessing, using and sharing published information online is conducted within the National Health Service (NHS) in England along with the potential impacts they may have on the trust of these services. The author makes use of semi-structured interviews and document analysis methods and shows risk factors that can adversely affect the security of these services are information manipulation, identity theft, insider, productivity loss and cyber-attacks.

Cooke [20] conducted a systematic literature review to identify the factors related to the success of strategies implemented in the public sector. The study concluded factors such as, IT skills, adequate funding, engagement to CSS, cybercrime law and public enlightenment programs are inevitable to be considered for a successful strategy.

Choejey et al. [21] explored the critical success factors for cybersecurity in government organizations in Bhutan. The authors conducted a questionnaire-based survey for data collection. The study concluded several critical factors needed for the successful implementation of cyber security. They are: awareness and training, security policy, budget, security audit, security responsibility, organization structure, change management, and communication and collaboration.

Peursum [22] studied the building blocks necessary for a security strategy from an organization perspective. The author adopted an expert interviews methodology to confirm data collected from the literature. The key factors highlighted are, systems, skills, staff, strategy, style shared value and structure.

While developing and implementing the cyber security strategy the alignment with business objectives should be taken into consideration. Developing a CSS is certainly not a single

perspective task. It should be aligned with the organization's objectives and vision. It should also build the trust that needed to realize the objectives and protecting the organization from the cyber-threats [23]. The key factors and the focus area of the reviewed literature are summarized in Table I.

III. Methodology and Results

To achieve our objective of a well-defined and structured classification of the essential factors for an effective CSS, we have utilized two-step approach; first, to develop the classification, and second, to recognize the most critical factors.

A. Factors Classification

Firstly, a literature review method has been employed to devise a structured classification of the essential factors. This was necessary to collect the necessary factors, summarized in the Table I that are scattered across the literature, some of them were synonymous. For instance, awareness, public enlightenment programs, and training and awareness have the same meaning and objective, which need to be transformed to a common terminology. Similarly, as productivity loss, cyber-attacks, and insider threats represent instances of threats and attacks, they are accumulated in accordingly. Moreover, there was a need to re-label a few of them to widely recognized terminology in the context of CSS, e.g., "structure" needs to be resolved to organizational structure, which is less confusing and a more commonly known phrase. Therefore, to have a refined classification and to avoid the mentioned concerns in a systematic manner, we exercised the following steps in a process manner as shown in Fig. 1.

Factors are classified in accordance with essential business themes to ensure that all mission-critical contexts are appropriately addressed and are underlined as: Organizational, Cultural, Legal/Political, Economic, Technical, and Risk. By exercising the above listed steps, a set of 31 factors were finalized and mapped to the respective classes as illustrated in Fig. 2.

TABLE I. List of Identified Factors

Factor (Revised Label): [Study]	Factor (Revised Label): [Study]
1. Information Security Policy: [15, 21]	
2. Deterrence:[15, 24]	**26.** Individual attitude and norms (Attitude and Behavior): [12, 25]
3. Attitude (Attitude and Behavior): [15, 16, 25]	**27.** Cultural based strategy (Strategy): [12]
4. Involvement: [15, 16, 26]	**28.** Compliance: [13, 27]
5. Training & Awareness (Awareness): [12, 13, 15, 16, 21]	**29.** Awareness (Awareness): [20, 26, 28]
6. Management Support: [15, 16]	**30.** Leadership engagement (Management Support): [13]
7. Identity Theft (Threats and Attacks): [19]	**31.** System Technology Management (Systems): [13, 22]
8. Insider (Threat Actor): [19]	**32.** Interest level of government on CII(Critical Information Infrastructure) (Govt. Interest): [14]
9. Productivity Loss (Threat and Attacks): [19]	**33.** level of protection: [14, 26]
10. Cyber-attacks (Threats and Attacks): [19]	**34.** Insufficient market preparation (Competence): [14]
11. Information Manipulation (Threat and Attacks) [19]	**35.** Systems (Systems): [22]
12. Behavioral Controls (Deterrence): [16]	**36.** Skills (Skills and Experience):[22]
13. Lack of Punishment (Detterence): [16]	**37.** Strategy (Strategy): [22]
14. IT Skills (Skills & Expertise): [20]	**38.** Style (Strategy): [22]
15. Adequate Funding (Funding): [20, 21]	**39.** Shared value: [22]
16. Motivation (Involvement): [20]	**40.** Personality traits (Attitude and Behavior): [25, 29]
17. Cybercrime Law: [20, 26]	**41.** Impulsiveness (Attitude and Behavior): [25]
18. Public Enlightenment Prog. (Awareness): [20, 26]	**42.** Computer skills (Skills and Experience): [30]
19. Security Audit: [21]	**43.** Experience with CS practices (Skills and Experience): [30]
20. Security Responsibility (Due Diligence): [21]	**44.** Risk Posture: [29]
21. Change Mangement: [21]	**45.** Flexibility (Attitude and Behavior): [29]
22. Structure (Organization Structure): [21, 22]	**46.** Ethical Attributes (Attitude and Behavior):[29]
23. Software Development Security (Application Security): [2]	**47.** Connectedness (Collaboration): [29]
24. Disaster Recovery Planning: [2]	
25. Business Continuity: [2, 21]	

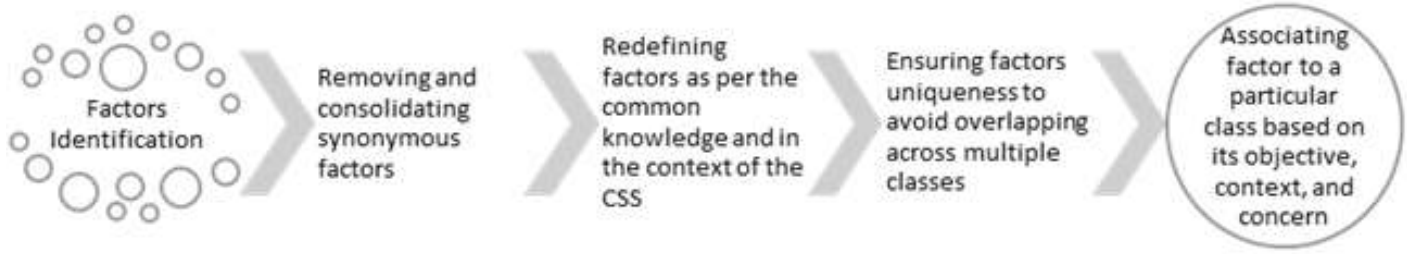

Fig. 1. Classification Development Process.

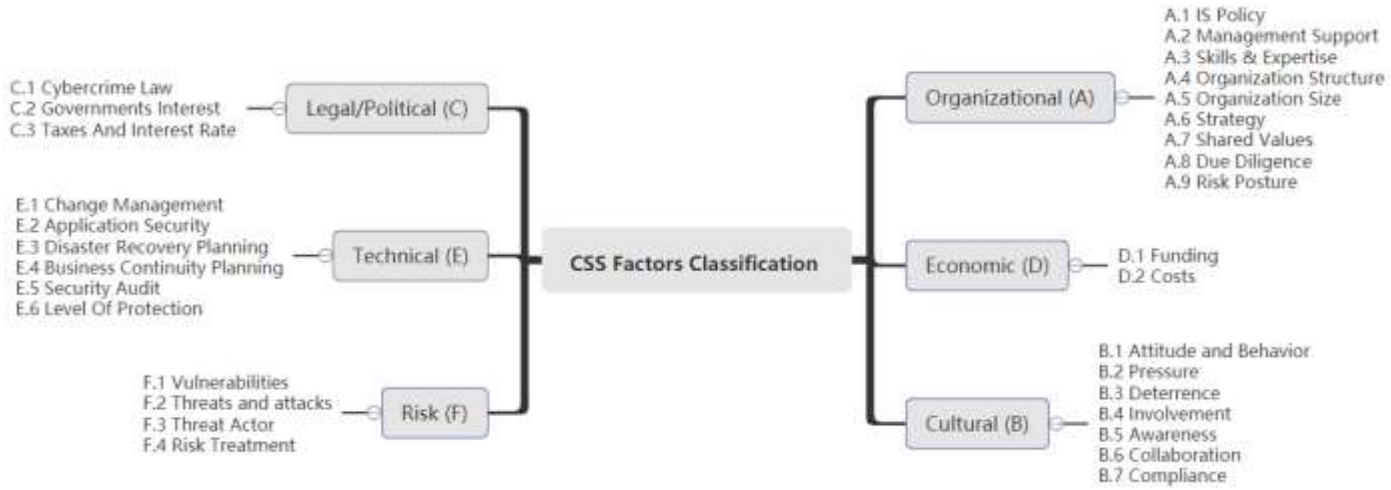

Fig. 2. Proposed CSS Factors Classification.

B. Identifying Critical Factors

Critical factors may vary from the type of organization to country or region they are operating in, as they might be influenced by their respective regulations, culture, threat spectrum, and other circumstances. In this study, we have explored critical factors in the context of public sector organizations working in Oman. We conducted open-ended and semi-structured interviews from a target group of ten participants to further refine and confirm these critical factors. Participants were selected based on the criteria such that they have at least a five years' experience in the security domain and have been involved in key business processes related to CSS at the organizational level in the public sector. A summary of the participants' profiles is highlighted in Table II.

Seventy questions were asked in each interview with at least two distinct questions to assess the importance (criticality) of each factor listed in the classification. The questions were validated using face validation and pilot testing with two experts, as suggested in [31] that assisted us to eliminate and modify the redundant and out-of-context questions. The interview sessions were recorded and transcribed into text, and analyzed using the Interactive Analysis Model [32]. A Likert-scale was then used to evaluate the overall feedback concerning the importance of a given factor. The importance scale used was: Very Important= 5, Important=4, Moderately Important=3, Less important =2, Unimportant= 1). Factors having an average value of 4 and above are characterized as critical. The factors criticality level of each factors with respect to each participant (P) response is depicted in Table III to VIII.

1) Organizational factors: As can be seen in Table III, Organizational Size, Shared Values, and Risk Postures were considered as no critical. The majority of the participants concurs that the organizational size does not affect the CSS development and execution as long as there is a clear structure, guideline, and resources available. Risk posture was dominated because the majority of participants acknowledged that they adapt from the existing standard risk management methodologies and practices as per their needs instead of defining and utilizing their own as it takes considerable time and effort to conclude it. Moreover, since shared values are motivated by the competitiveness in the market, it is less perceived in the public sector [33] and was therefore not acknowledged by the P2, which lowered its overall score in the class.

2) Cultural factors: From all the interviews conducted, as evident in Table IV, it was concluded that the majority of the participant, based on their experiences, believed that the employees' positive attitude, knowledge, and collaboration are critical to complete tasks in a teamwork. Employee compliance with the organizations policy and rules is also accounted as critical. The popular perception about deterrence was that although related penalties and actions exist, it is not usually experienced in practice. Pressure was believed to be rarely existed, as government authorities do not frequently introduce changes.

3) Legal and political factors: The interviews were conducted before April 2021 when there were no taxes and interest rates introduced in Oman. They were not applicable and therefore were unimportant, as reflected in Table V. Even with their introduction an application, it is still a nominal concern for government driven organizations. On the other hand, laws and regulations and government interest were marked as critical as commonly commented as actively overseen in the participants' organization as key factors.

4) Economic factors: As primarily based on government funding, all participants concur that it is critical. As for the cost and budget, the majority believes that although cost is an important factor to invest in the efficacy of the CSS, it has not been a key problem for the public sector. These verdicts are also reflected in Table VI.

5) Technical factors: As reflected in Table VII, all participants strongly believed that the technical aspects of the CSS are of utmost importance. This perception is true mainly because a substantial part of the operations and processes are supported by IT-based systems in which the listed factors are inevitable. However, a few participants pointed out that change

management is unless important. They remarked that the changes introduced are either infrequent or are easily manageable. This notion is also supported the perception about the pressure factor in the Cultural class.

6) Risk factors: The common consensus about the risk factors was that all of them are high importance as they all are necessary to be monitored, analyzed, and managed earnestly not just in the context of an effective CSS but, also with regards the sensitivity of the public information that they are dealing with. They also indicated to have a clear risk treatment plan and protocols that their organization follow. P2 stated that they don't have such plan and mechanism in place and that their organization tends to decide one when there is a need and that too for only severe and organizational wide risks. Table VIII highlights the scores associated with the risk factors.

Based on the interviews and the scaled defined, the list of critical factors are identified, as illustrated in Fig. 3.

TABLE II. PARTICIPANT PROFILE SUMMARY

Interviewee Code	Age	Qualification	Designation	Overall experience	Experience in security setting
P1	35	Bachelor	Security Analyst	5	5
P2	38	Master	Head of Data center	8	8
P3	38	Master	Senior Security Specialist	10	8
P4	31	Bachelor	Security Specialist	5	5
P5	30	Bachelor	Data Security Analyst	5	5
P6	37	Master	IT Deputy Manager	10	5
P7	34	Master	System Developer	7	5
P8	35	Bachelor	Head Security Operation Dept.	7	7
P9	36	Master	Network Deputy Manager	9	5
P10	45	Ph.D.	Associate professor	15	10

TABLE III. ORGANIZATIONAL FACTORS' LEVEL OF IMPORTANCE

Factor	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	Average
IS Policy	5	5	5	5	5	5	5	5	5	5	5
Management Support	5	5	5	5	5	5	5	5	5	5	5
Skills & Expertise	5	5	5	5	5	5	5	5	5	5	5
Organization Structure	2	5	4	4	4	4	4	4	4	5	4
Organization Size	1	4	2	4	4	3	2	2	2	3	2.7
Strategy	5	4	5	5	5	5	5	5	5	5	4.9
Shared Values	4	1	4	4	4	4	4	4	4	4	3.7
Due Diligence	5	5	5	5	5	4	5	5	5	4	4.8
Risk Posture	1	5	5	5	5	2	4	4	4	4	3.9

TABLE IV. CULTURAL FACTORS' LEVEL OF IMPORTANCE

Factor	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	Average
Attitude & Behavior	5	5	5	5	5	5	5	5	5	5	5
Pressure	1	4	2	4	5	2	3	3	3	4	3
Deterrence	1	4	4	4	4	4	4	4	4	4	3.7
Involvement	1	5	5	5	5	4	5	5	4	4	3.8
Awareness	5	5	5	5	5	5	5	5	5	5	5
Collaboration	4	4	5	5	5	5	5	5	5	4	4.7
Compliance	4	4	4	4	4	4	4	4	4	4	4

TABLE V. LEGAL/POLITICAL FACTORS' LEVEL OF IMPORTANCE

Factor	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	Average
Cybercrime law	5	5	5	5	5	4	5	5	5	5	4.9
Government Interest	5	5	5	5	5	5	5	5	5	5	5
Taxes and Interest rates	1	1	1	1	1	1	1	1	1	1	1

TABLE VI. ECONOMIC FACTORS' LEVEL OF IMPORTANCE

Factor	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	Average
Funding	5	5	5	5	5	5	5	5	5	5	5
Costs	1	4	1	4	4	3	4	4	2	5	3.2

TABLE VII. TECHNICAL FACTORS' LEVEL OF IMPORTANCE

Factor	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	Average
Change Management	1	1	1	5	5	5	2	5	5	5	3.5
Application Security	5	5	5	5	5	5	5	5	5	5	5
Disaster Recovery Planning	5	5	5	5	5	5	5	5	5	5	5
Business continuity planning	5	5	5	5	5	5	5	5	5	5	5
Security Audit	4	4	5	5	5	4	5	5	5	4	4.6
Level of protection	5	5	5	5	5	5	5	5	5	5	5

TABLE VIII. RISK FACTORS' LEVEL OF IMPORTANCE

Factor	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	Average
Vulnerabilities	4	4	4	4	4	5	5	5	5	5	4.5
Threats & attacks	4	5	4	4	4	5	5	4	4	5	4.4
Threat actor	4	5	4	4	4	5	5	5	5	5	4.6
Risk Treatment	4	2	4	4	4	4	4	4	4	4	3.8

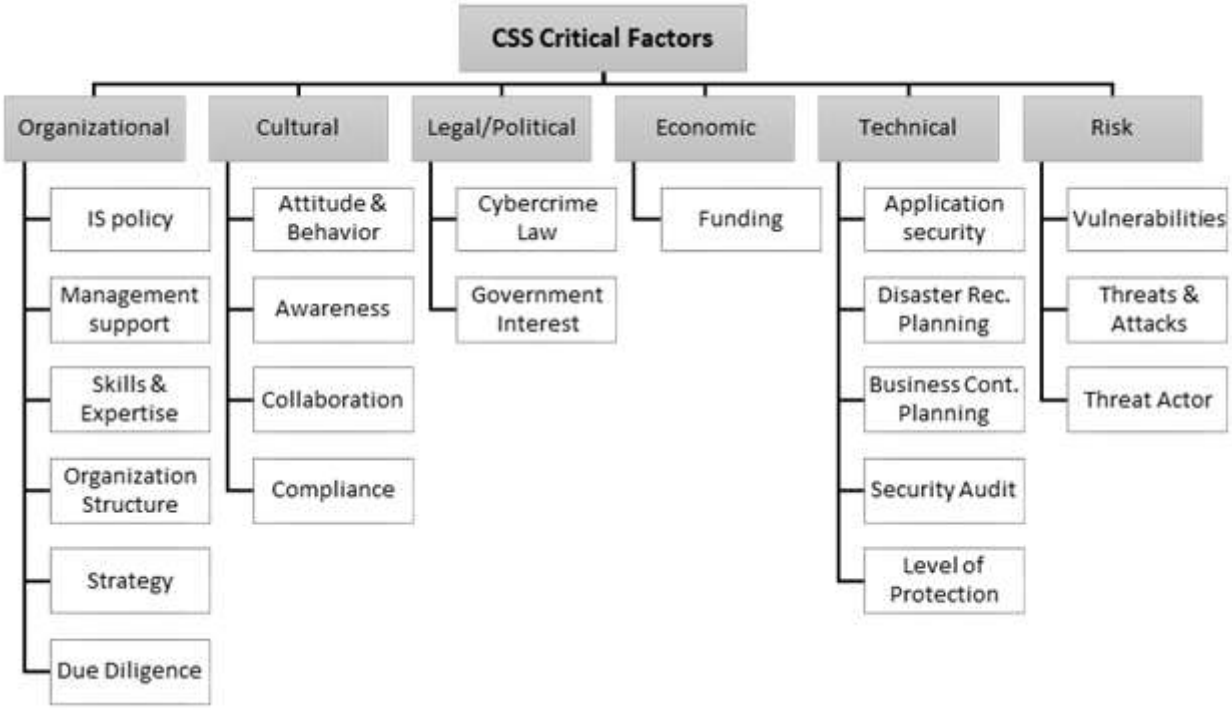

Fig. 3. List of Critical CSS Factors.

IV. COMPARISON

In this section, we provide a comparison of our classification with the studies summarized in Table I. However, we have selected only the 10 most relevant ones that cover the majority of the factors that are also common in the other attempts listed there. The comparison is provided in Table IX to XI. The tick mark indicates that a particular factor is stressed as an essential CSS factor whereas, the cross sign highlights that the given factor is not addressed essential. Overall, it can be concluded that our work provides a more complete list of factors rather than emphasizing a particular set of factors. Moreover, it can be observed that most of these works have mainly focused on the organizational and cultural aspects, whereas other key contexts of the business have been overlooked.

TABLE IX. COMPARISON OF ORGANIZATIONAL FACTORS

Work	Class (A) Organizational Factors								
	A.1	A.2	A.3	A.4	A.5	A.6	A.7	A.8	A.9
This work	✓	✓	✓	✓	✓	✓	✓	✓	✓
Jalali et al. [2]	×	×	×	×	×	×	×	×	×
Benson et al. [12]	×	×	×	×	×	✓	×	×	×
Fritzvold [13]	×	✓	×	×	×	×	×	×	×
Awan et al. [14]	×	×	×	×	×	×	×	×	×
Glaspie et al.[15]	✓	✓	×	×	×	×	×	×	×
Khansa et al. [16]	×	×	×	×	×	×	×	×	×
Ebenezer [19]	×	×	×	×	×	×	×	×	×
Cooke. [20]	×	×	✓	×	×	✓	×	×	×
Choejey et al. [21]	✓	×	×	✓	×	×	×	✓	×
Peursm [22]	×	×	✓	✓	×	✓	✓	×	×

TABLE X. COMPARISON OF CULTURAL, LEGAL/POLITICAL AND ECONOMIC FACTORS

Work	Class (A) Organizational Factors							Class (C) Legal/Political Factors			Class (D) Economic Factors	
	B.1	B.2	B.3	B.4	B.5	B.6	B.7	C.1	C.2	C.3	D.1	D.2
This work	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Jalali et al. [2]	×	×	×	×	×	×	×	×	×	×	×	×
Benson et al. [12]	✓	×	×	×	✓	×	×	×	×	×	×	×
Fritzvold [13]	×	×	×	×	✓	×	✓	×	×	×	×	×
Awan et al. [14]	×	×	×	×	×	×	×	×	✓	×	×	×
Glaspie et al.[15]	✓	×	✓	✓	✓	×	×	×	×	×	×	×
Khansa et al. [16]	✓	×	✓	✓	✓	×	×	×	×	×	×	×
Ebenezer [19]	×	×	×	×	×	×	×	×	×	×	×	×
Cooke. [20]	×	×	×	✓	✓	×	×	✓	×	×	✓	×
Choejey et al. [21]	×	×	×	×	✓	×	×	×	×	×	✓	×
Peursm [22]	×	×	×	×	×	×	×	×	×	×	×	×

TABLE XI. COMPARISON OF TECHNICAL AND RISK FACTORS

Work	Class (E) Technical Factors						Class (F) Risk Factors			
	E.1	E.2	E.3	E.4	E.5	E.6	F.1	F.2	F.3	F4
This work	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Jalali et al. [2]	×	✓	✓	✓	×	×	×	×	×	×
Benson et al. [12]	×	×	×	×	×	×	×	×	×	×
Fritzvold [13]	×	×	×	×	×	×	×	×	×	×
Awan et al. [14]	×	×	×	×	×	✓	×	×	×	×
Glaspie et al.[15]	×	×	×	×	×	×	×	×	×	×
Khansa et al. [16]	×	×	×	×	×	×	×	×	×	×
Ebenezer [19]	×	×	×	×	×	×	×	✓	✓	×
Cooke. [20]	×	×	×	×	×	×	×	×	×	×
Choejey et al. [21]	✓	×	×	✓	✓	×	×	×	×	×
Peursm [22]	×	×	×	×	×	×	×	×	×	×

V. CONCLUSION

To develop and implement an effective CSS, we need to recognize and evaluate the necessary factors that might influence its efficacy. In this article, we have accumulated a comprehensive list of such essential factors in accordance with the critical areas of an organization that are vital to be recognized and evaluated for any long-term planning, such as developing a CSS. The comparison depicts that the proposed classification covers and provides a broader view of the essential CSS Factors as compared to the current attempts that emphasize on a specific domain or context of a business. Such a holistic classification of essential factors can provide a fundamental ground for organizations planning to develop and implement a CSS to understand and evaluate the influencing aspects of it and to plan accordingly. Furthermore, we have also listed the critical factors in the public sector in Oman. However, we believe that this study is limited in scope and that the corresponding critical factors assessed may vary considerably in regions or spaces with different legal, political, economic, and cultural backgrounds. More data need to be collected and analyzed to conclude whether this list of critical factors will shrink or grow, and it will be interesting to see how different types or organizations in a broader geospatial context comprehend the criticality of the different factors. In future, we plan to further refine the classification proposed and conduct a wider data collection approach to evaluate the critical factors.

REFERENCES

[1] Grobman, S. and A. Cerra, Cybersecurity's Second Wind, in The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War. 2016, Apress: Berkeley, CA. p. 175-189.

[2] Jalali, M.S., et al., EARS to cyber incidents in health care. Journal of the American Medical Informatics Association, 2019. 26(1): p. 81-90.

[3] Finnerty, K., et al., Cyber security breaches survey 2018: Statistical release. 2018.

[4] Simmonds, M., Instilling a culture of data security throughout the organisation. Network Security, 2018. 2018(6): p. 9-12.

[5] Fianyi, I.D., Curbing cyber-crime and Enhancing e-commerce security with Digital Forensics. International Journal of Computer Science Issues (IJCSI), 2015. 12(6): p. 78.

[6] Smith, S. Five Cybersecurity Insights for the Public Sector. March 2019 [cited 2021 March 4 2019]; Available from: https://www.tenable.com/blog/five-cybersecurity-insights-for-the-public-sector.

[7] Tu, C.Z., et al., Strategic value alignment for information security management: a critical success factor analysis. Information & Computer Security, 2018. 26(2): p. 150-170.

[8] Gcaza, N. and R. Von Solms, A strategy for a cybersecurity culture: A South African perspective. The Electronic Journal of Information Systems in Developing Countries, 2017. 80(1): p. 1-17.

[9] Srinivas, J., A.K. Das, and N. Kumar, Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems, 2019. 92: p. 178-188.

[10] Jawad, W.K. Assessing an Organization Security Culture Based on ENISA Approach. 2021. Cham: Springer International Publishing.

[11] Jayanthi, M.K. Strategic Planning for Information Security -DID Mechanism to befriend the Cyber Criminals to assure Cyber Freedom. in 2017 2nd International Conference on Anti-Cyber Crimes (ICACC). 2017.

[12] Benson, V., J. McAlaney, and L.A. Frumkin, Emerging threats for the human element and countermeasures in current cyber security landscape, in Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications. 2019, IGI Global. p. 1264-1269.

[13] Fritzvold, E., Cyber Security in Organizations. 2017, University of Stavanger, Norway.

[14] Awan, J.H., et al., Security strategies to overcome cyber measures, factors and barriers. 2017.

[15] Glaspie, H.W. and W. Karwowski. Human factors in information security culture: A literature review. in International Conference on Applied Human Factors and Ergonomics. 2017: Springer.

[16] Khansa, L., et al., To cyberloaf or not to cyberloaf: The impact of the announcement of formal organizational controls. Journal of Management Information Systems, 2017. 34(1): p. 141-176.

[17] Lim, V.K.G. and T.S.H. Teo, Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: An exploratory study. Information & Management, 2005. 42(8): p. 1081-1093.

[18] Vitak, J., J. Crouse, and R. LaRose, Personal Internet use at work: Understanding cyberslacking. Computers in Human Behavior, 2011. 27(5): p. 1751-1759.

[19] Ebenezer, C., "Access denied"? Barriers for staff accessing, using and sharing published information online within the National Health Service (NHS) in England: technology, risk, culture, policy and practice. 2017, University of Sheffield.

[20] Cooke, P., 'Digital tech' and the public sector: what new role after public funding? European Planning Studies, 2017. 25(5): p. 739-754.

[21] Choejey, P., D. Murray, and C.C. Fung, Exploring Critical Success Factors for Cybersecurity in Bhutan'S Government Organizations. no. December, 2016: p. 49-61.

[22] Peursum, L., The building blocks for a cyber security strategy. 2015.

[23] Kovács, L., National cyber security as the cornerstone of national security. Land Forces Academy Review, 2018. 23(2): p. 113-120.

[24] Schannep, J.H., et al. Advancing cybersecurity from Medieval Castles to STrategic Deterrence: A Systems Approach to cybersecurity. in Proceedings of the International Annual Conference of the American Society for Engineering Management, Coeur d'Alene, ID, USA. 2018.

[25] Hadlington, L., Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 2017. 3(7): p. e00346.

[26] Koepke, P., Cybersecurity information sharing incentives and barriers. 2017, Sloan School of Management, MIT.

[27] Reddy, D. and V. Rao, Cybersecurity Skills: The Moderating Role in the Relationship between Cybersecurity Awareness and Compliance, in 2nd Americas Conference on Information Systems, AMCIS 2016. 2016, Association for Information Systems: SAn Diego, CS, USA.

[28] Reddy, D. and V. Rao, Cybersecurity skills: The moderating role in the relationship between cybersecurity awareness and compliance. 2016.

[29] Henshel, D., et al., Integrating cultural factors into human factors framework and ontology for cyber attackers, in Advances in Human Factors in Cybersecurity. 2016, Springer. p. 123-137.

[30] Anwar, M., et al., Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 2017. 69: p. 437-443.

[31] Kumar, R., Research methodology: A step-by-step guide for beginners. Fifth ed. 2018, New Delhi: Sage Publications.

[32] Miles, M.B. and A.M. Huberman, Qualitative data analysis: An expanded sourcebook. Second ed. 1994: SAGE Publications.

[33] Kramer, M.R. and M.W. Pfitzer, The ecosystem of shared value. Harvard Business Review, 2016. 94(10): p. 80-89.