International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V69I11P105

Volume 69 Issue 11, 29-36, Nov, 2021

Review Article

The Effectiveness of the Current Cybersecurity Framework used by the UAE's Oil and Gas Industry: The Perspective of the Cybersecurity Practitioners

Mohamed Jumah AL Dhanhani[1], Jessnor Elmy Mat Jizat[2]

[1]*Ph.D Student, Faculty of Management & Economics, University Pendidikan Sultan Idris, 35900 TanjongMalim, Perak, Malaysia,*

[2]*Senior Lecturer, Department of Business Management & Entrepreneurship, Faculty of Management & Economics, Universiti Pendidikan Sultan Idris, 35900 TanjongMalim, Perak, Malaysia*

Received Date: 05 October 2021
Revised Date: 12 November 2021
Accepted Date: 24 November 2021

Abstract *- As acknowledged, any organization involved in critical industries, such as the oil and gas sector, needs to employ effective cybersecurity measures to protect its critical infrastructure from cyber threats. As such, this study was carried out to determine the adaptability, flexibility, and effectiveness of the cybersecurity framework currently used by various companies involved in oil and gas production in the UAE. This study was based on a quantitative approach involving a survey methodology through which a sample of the target population was surveyed to elicit their professional feedback or expert opinions. The study sample consisted of 94 cybersecurity practitioners or subject matter experts (SMEs) who were randomly selected from 15 companies operating in the UAE's oil and gas sector of the economy. The research instrument used in this study was based on a survey questionnaire consisting of 44 items to elicit respondents' demography and their perceptions regarding the flexibility, adaptability, and effectiveness of the cybersecurity framework. Data were analyzed descriptively using Statistical Package for Social Science (SPSS). Demographically, the findings showed that the majority of the respondents were males, had at least a Bachelor's degree, had more than 10 years of work experience, and worked on the sites. Specifically, the findings showed that the flexibility, adaptability, and effectiveness of the current cybersecurity framework were highly rated by the respondents, suggesting that the cybersecurity practitioners in the UAE believe that this framework is very effective, adaptable, and flexible in helping them to develop superior cybersecurity programs and systems to deal with any form of cyber threats. As such, this finding provides strong evidence for all the major players in the UAE's oil and gas industry to utilize the current cybersecurity framework in their ongoing efforts to provide strong protection for their critical assets against cyber threats.*

Keywords *- Cyberattacks, Cybersecurity framework, Oil and gas industry, Safety, and Security measures.*

I. INTRODUCTION

The United Arab Emirates (UAE) is one the leading oil and gas (O&G) producers in the world, whose oil and gas production has significantly contributed huge revenues to its GDP, amounting to billions of dollars [1]. Similar to those leading nations, its O&G industry has been under constant threats of cyber attacks from unscrupulous hackers, whose intentions are to disrupt and hurt its vibrant economy. Typically, such threats include infrastructure sabotage, data leaks, attacks on webmail and corporate VPN servers, DNS (domain name server) hijacking, espionage, data theft, external emails, and malware [2]. Inevitably, these attacks have become more frequent and intense, causing serious concern among the stakeholders, especially the industrial practitioners [3]. As such, appropriate measures have to be put in place lest all related technologies used in its critical infrastructure in several productions and processing facilities could be rendered unusable at best or defective at worst. Invariably, a majority of cyber attacks were aimed at such plants and facilities in which a diverse range of information technology is used for a wide range of services, including customer data, web service, accounting systems, and email systems [4].

Of late, however, such malicious attacks have shifted to targeting more critical operations of its O&G sector, notably industrial control systems and SCADA, if unresolved, could lead to serious service disruptions [5]. As revealed by a study carried out by [3], more than half of cyber attacks in the UAE were directed toward such critical operational facilities. Likewise, other leading O&G producers have also experienced such attacks, with more than three-quarters of companies experiencing a minimum of one security breach that had incurred huge losses

because of disrupted operations and confidential data [5]. Thus, the need to implement effective cybersecurity measures to counter such growing threats, especially in this highly lucrative but complexly demanding industry, requires the highest priority from the stakeholders [6].

In view of the increasing occurrences of attempts of cyber attacks, it becomes imperative to review the effectiveness, adaptability, and flexibility of the cybersecurity framework currently used by major O&G companies in the UAE to establish strong safeguard for all their critical, sensitive assets and infrastructures. Preferably, the current framework that has been put in place should be able to provide the levels of security and safety that are badly needed by the cybersecurity practitioners to deal with potentially harmful cyberattacks that could grind their operations to a halt, resulting in massive operational downtime that ultimately leads to huge losses of revenues [3]. Ideally, the current framework should be able to guide the security practitioners to institute resilient, robust cybersecurity measures, without which such companies will be made highly vulnerable to cyber-attacks through which malicious hackers could evade their critical network defences to destroy or steal sensitive data and information. If left unmitigated, this could adversely impair the companies' operations, which could lead to severe financial and reputational damages [7].

As such, the feedback or professional opinions of the key players of the UAE's O&G sector, especially the cybersecurity practitioners, on the capability of the current cybersecurity framework to help guide them to establish strong, solid cybersecurity of their critical assets against damaging cyber attacks are needed. Against such a backdrop, this study was conducted to address the research objectives as follows:

(a) To examine the flexibility and adaptability of the current cybersecurity framework to respond to emerging cybersecurity needs in the UAE's O&G industry.
(b) To examine whether the current cybersecurity framework can provide long-term cyber security for the UAE's O&G industry.
(c) To examine the effectiveness of the current cybersecurity framework to provide superior cyber security in the UAE's O&G industry.

Accordingly, three research questions were formulated to guide this study as follows:

(a) How flexible and adaptable is the current cybersecurity framework to respond to emerging cybersecurity needs in the UAE's oil and gas industry?
(b) How able is the current cybersecurity framework to provide long-term cyber security for the UAE's oil and gas industry?
(c) How effective is the current cybersecurity framework to establish superior cyber security in the UAE's oil and gas industry?

II. RESEARCH BACKGROUND

Of late, the number of cyber-attacks facing many organizations throughout the world has climbed steeply to a level that caused major concern to many nations, notably oil-producing countries, prompting them to take the necessary measures to protect their critical assets against adverse intrusions and break-ins [8]. Such occurrences have triggered many nations to review their information safety systems and put in the necessary precautionary measures. For example, the UAE has taken a similar approach to protect its important infrastructures and systems from cyber attacks [9]. Specifically, the UAE's government has played a central role to ensure proper strategies are taken to enhance the performance of its cyber security system to deal with harmful cyberattacks, made evident by the adoption of the cybersecurity framework that is currently being used by various oil and gas companies in the UAE. Essentially, this framework comprises elements adopted from several standards, guidelines, and practices for managing the operations of the oil and gas industry [10]. Collectively, these elements help provide a mechanism for assessing the abilities and preparedness of cyber attackers to unleash a series of cyberattacks, which can severely compromise the safety of data and information [11]. Admittedly, over the years, cyber attackers have unleashed more sophisticated, intelligent malware that can easily bypass or weave through security defences, entailing a need to put in place cybersecurity measures that are highly adaptable and flexible [12]. Such measures must, therefore, have the necessary safeguards to deal with the growing cyber threats. In this regard, cybersecurity personnel can use the CIS controls as guidelines to help them build robust, resilient cybersecurity to protect their organizations' assets from a wide spectrum of cyber threats [13]. (Brooks, 2018).

In the literature, studies of data breaches and other security incidents have shown that the majority of security incidents occurred because highly established security controls and practices had not been implemented properly as they were supposed to be or were not working as organizations had assumed. Further compounding this issue is a lack of defined and repeatable processes for choosing, deploying, and keeping track of effective security controls to deal with increasing cyber threats [14]. Moreover, the rapidly evolving cyber threat landscape entails relevant stakeholders to enhance their cyber competencies to understand cyber risks, appraise their organizations' cyber programs and initiatives, and assess the degree of the cyber risks facing their organizations [15]. In total, there were 20 CIS controls, but they have been reduced to 18 that are applicable for organizations seeking to establish resilient, robust cybersecurity as follows: (a) Inventory and Control of Enterprise Assets, (b) Inventory and Control of Software Assets, (c) Data Protection, (d) Secure Configuration of Enterprise Assets and Software, (e) Account Management, (f) Access Control Management, (g) Continuous Vulnerability Management, (h) Audit Log Management, (i) Email Web Browser and Protections, (j) Malware Defenses, (k) Data

Recovery (l) Network Infrastructure Management, (m) Monitoring and Defense, (n) Security Awareness and Skills Training, (o) Service Provider Management, (p) Application Software Security, (q) Incident Response Management, and (r) Penetration Testing. Among these, version 7.0 of the Critical Security Controls recommends the first six Critical Controls as the highest priority and considered as among the very first set of activities to be accomplished. CIS refers to these Controls as Cyber Hygiene – the basic things that an organization has to perform to develop a strong foundation for its defence.

Initially, the CIS Controls involved the practices of security personnel to identify and deal with common cyber attacks that had affected many organizations' everyday operational activities. The knowledge acquired and lessons learned were then used to help such personnel put in place appropriate measures to protect their critical, sensitive assets against potential cyber threats. Over the years, the accrued knowledge was documented and shared with the rest of the other users and practitioners. In a nutshell, the main aim of such an undertaking is to help organizations, irrespective of their scale and size, to follow the recommended steps to protect their infrastructures and assets, which are invariably interconnected within their organizations, from cyber threats [16]. Under the leadership of the Center for Internet Security (CIS), the CIS Controls have gained recognition and support from a growing number of institutions, practitioners, and users, whose knowledge and expertise are used to carry out the following tasks, namely (a) sharing insights into cyber threats and attackers; (b) identifying root causes and translating them into classes of defensive action, developing and sharing tools, aids, and experiences of adoption and problem-solving, (c) mapping and aligning the CIS Controls to regulatory and compliance frameworks; and (d) identifying common challenges and barriers and solving them as a community.

Over time, the CIS Controls has become more comprehensive as its knowledge base continues to grow by pulling together all the knowledge, expertise, and best practices from the community of interest, such as business organizations, corporations, governments, and academic institutions, and research centres. Given the wide spectrum of roles played by the members of this community (such as security engineers, system analysts, technologists, information technology (IT) officers, auditors, and consultants) who work in various industries (such as oil and gas, mining, government, finance, security, IT, and military), the knowledge being shared helps improve the utility of such controls. The process of best practice recommendations (namely, the CIS Benchmarks and the CIS Controls) has continued to improve as more and the latest data are being collected with greater rigor and transparency, which are essential to the maturation of the science that underlies cyber defence [17]. Through such an improvement, cybersecurity actions or measures that are applicable to specific cases can be instituted more effectively. In the earliest versions of the CIS Controls, a standard list of publicly known attacks was released to highlight a simple and informal test of the usefulness of specific recommendations. Later, in 2013, the collaboration between the CIS team and the Verizon Data Breach Investigations Report (DBIR) team helped develop a standard program for defensive improvement by matching the results of the latter's large-scale data analysis directly to the CIS Controls.

Admittedly, cyber threats have targeted not only large organizations but also small- and medium-sized organizations too. This is due to the current nature of today's industry in which many companies have to rely on systems that are invariably interconnected that increases the system complexity and creates conducive conditions for vulnerabilities to be exploited by cyber attackers [18]. Clearly, the levels of cybersecurity of organizations depend on their specific needs that are dictated by their assets and infrastructures, such as information and control systems, which keep and maintain sensitive data and information. In simple terms, the use of the appropriate CIS controls relies on the scale or scope of each specific organization [19]. Hence, the concept of the Implementation Group (IG) of various levels, namely IG1, IG2, and IG3, was proposed to help these organizations to focus on controls that are appropriate to fulfil their cybersecurity requirements [20]. Small- and medium-sized organizations are classified as IG1 organizations whose expertise in information technology (IT) and cybersecurity to protect critical, sensitive IT assets and infrastructures is limited. In principle, such an organization is primarily concerned with keeping its business activities operational as much as possible, given its low tolerance for downtime. On the other hand, IG2 organizations are manned with specific personnel to manage and protect their IT asset or infrastructure. In general, organizations under this category provide assistance for multiple departments with differing risk profiles based on job function and mission. As opposed to the above two types of organizations, IG3 organizations engage a group of security experts who specialize in a wide spectrum of cybersecurity facets, such as data protection, risk management, access control management, and application security. Typically, the assets and infrastructures of such an organization utilize data containing sensitive information or functions that are subject to regulatory and compliance requirements.

III. RESEARCH METHODOLOGY

The following subsections provide a detailed account of the research methodology used in this research.

A. Research Design

This study was based on the quantitative approach involving a survey methodology through which a sample of the target population was surveyed to elicit their professional feedback or expert opinions regarding the effectiveness, adaptability, and flexibility of the current cybersecurity framework that they have been using to provide them with the governing guidelines to develop and use information security systems to deal with cyber threats.

B. Study Sample

The study sample consisted of 94 cybersecurity practitioners or subject matter experts (SME) who were randomly selected from 15 companies operating in the UAE's oil and gas sector. They were chosen as the survey respondents based on the following criteria: (a) They must have worked as information technology (IT) or operational technology (OT) specialists in the gas and oil industry in the UAE, (b) They could be fresh graduates who have recently joined the oil and gas companies or have been working in such companies for more than three months, (c) They should have working experiences of more than five years.

C. Research Instrument

The research instrument used in this study was based on a survey questionnaire consisting of 44 ' items, with the first four being used to record the respondents' demographic background, namely gender, academic qualification, work experience, and work location. The remaining 40 items were framed based on the 18 CIS controls highlighted above. Specifically, the items were divided into three categories that were used to address the three research questions. The first category consisted of 12 questionnaire items relating to the flexibility and adaptability of the cybersecurity framework, while the second category comprised 13 questionnaire items pertaining to the ability of the framework to provide long-term cybersecurity in their organizations. Finally, the third category consisted of 15 questionnaire items relating to the effectiveness of the cybersecurity framework. Each item of the survey questionnaire was rated along with 5-point Likert-type scales, ranging from '1' (*Strongly disagree*) to '5' (*Strongly agree*), to indicate the degree to which they agreed or disagreed.

D. Procedure

The researcher had to perform the normal procedure used in many online surveys to collect data, which consisted of several steps that had to be carried out in sequence. Firstly, the email addresses of employees working as operational technology officers or specialists in each of the 15 companies were obtained after securing appropriate approvals from the heads or directors of their respective cybersecurity departments. Then, an email with a link to the online survey developed on Survey Monkey was sent to each participant. This online survey platform was chosen to maintain the confidentiality of the participants so that they could remain anonymous, thus encouraging them to answer all the survey questions more truthfully. In the survey questionnaire form, there was an opening statement that explained the type of information that would be asked, how the data would be used, and the protocol used for storing the data. They were requested to sign off the consent form if they agreed to participate electronically. Finally, after indicating their agreement, the participants were given sufficient time to complete and submit the questionnaire forms.

E. Findings and Discussion

Table 1 summarizes the computed overall internal consistency coefficient (α) and the internal consistency coefficients of the three sub-scales of the research instrument based on the three research questions.

Table 1. The internal consistency coefficients of the three dimensions of the research instrument

Research question	No. of items	Cronbach's α
1. How flexible and adaptable is the current cybersecurity framework to respond to emerging cybersecurity needs in the UAE's oil and gas industry?	12	.87
2. How can the current cybersecurity framework provide long-term cyber security for the UAE's oil and gas industry?	13	.86
3. How effective is the current cybersecurity framework in establishing superior cyber security in the UAE's oil and gas industry?	15	.87
Overall	40	.95

As summarized, the internal consistency coefficient, α, of the 12 questionnaire items pertaining to the flexibility and adaptability of the current cyber security framework of the respondents' organizations to respond to emerging cyber security needs based on the first research questions was .87. The internal consistency coefficient of the 13 questionnaire items pertaining to the ability of the framework to establish long-term cyber security was .86. Also, the internal consistency coefficient of the 15 questionnaire items relating to the effectiveness of the framework was .87. Overall, the internal consistency coefficient of all items of the research instrument was .95, which was well above the threshold value of .70 [21], signifying that the research instrument is highly reliable.

Table 2 summarizes the distribution of the respondents based on gender, work experience, academic qualification, and work location.

Table 2. The distribution of respondents based on their demographic profiles

Demography			**N**	**Demography**		**N**
Gender	Female		16	**Qualific-ation**	Diploma	10
	Male		78		Degree And Higher	84
Work Experie-nce	1-3 yr		7	**Work Location**	Main Office	27
	4-10 yr		20		Site (Off-shore/ Onshore)	67
	≥ 11 yr		67			

As shown, 78 respondents were males, who constituted an overwhelming majority, representing 82.98% of the respondents. The remaining were females, who were

represented by 16 respondents, making up 17.02% of the respondents. This finding was hardly surprising given that males tend to dominate females in the workforce in the oil and gas sector, as highlighted by a survey carried out by [22]. This finding signifies that more efforts are needed to attract more female professionals to work in this challenging but rewarding industry [23]. Moreover, having a diverse workforce with equal representation of both genders can have a huge impact on the organizations' productivity [24]. In terms of academic qualification, a majority of the respondents held higher qualifications, with 84 (89.36%) of those surveyed having a bachelor's degree or a higher degree. By contrast, the remaining 10 respondents had high school qualifications or a college diploma. This finding signifies that working in the oil and gas industry entails academically qualified personnel who are capable of coping with highly demanding tasks [25]. As highlighted, 67 (71.28%) of those surveyed had working experiences exceeding 11 years, who represented a sizeable majority of the respondents. Those whose years in service ranged from four (4) to 10 years were represented by 20 (21.28%) of the respondents. By contrast, only a handful had working experiences ranging from one (1) to three (3) years, who were represented by 7 (7.45%) of those surveyed. Such findings concur with that of [26], who observed that most workers employed in such a demanding industry were highly skilled and had many years of experience. Also, the majority of the respondents, represented by 67 (71.28%) of the respondents, worked in the onshore and offshore sites. By contrast, a relatively small fraction, made up of 27 (28.72%) of those surveyed, worked in the main offices or headquarters. This finding implies that a majority of these cybersecurity practitioners mainly work on field sites, with a relatively small minority working in offices.

Table 3 summarizes the descriptive statistics of the respondent's responses to the 12 questionnaire items relating to the first research question.

Table 3. Mean scores of the responses to the 12 questionnaire items relating to the first research question

Questionnaire item	Mean	Std. Deviation
Q06: Account Monitoring and Control: Your organization has an attestation process that actively and regularly identifies and revokes access to users and accounts with unauthorized access rights.	4.01	.86
Q11: Application Security: API security is constantly maintained using features such as API keys storage and management of API access using IP whitelisting.	3.85	.76
Q19: Data Protection: Your organization's data in all forms are protected based on the criticality, sensitivity, value, availability, and level of impact during loss.	3.97	.99
Q20: Data Protection: The current framework in place provides holistic and effective protection for the oil and gas industry.	3.88	.96
Q24: E-mail and Web Protections: All web application access using organization assets is mitigated from inherent security risks using proxies and firewalls.	4.16	.84
Q28: Incident Management: The organization has a clear reporting protocol for information security eventualities within the management structure.	4.07	.89
Q32: Privileges Access Control: There is an in-depth strategy that actively and in real-time provides a defence-in-depth strategy for protecting inherent operational networks in a way that allows authorized users and prevents unauthorized access.	3.85	.89
Q33: Privileges Access Control: The current framework provides an end-to-end understanding of the user authentication processes and modern infrastructures like SSO/TACACS (Single Sign-On/Terminal Access Controller Access-Control System).	3.81	.82
Q36: Secure Configurations: All mobile devices used for business purposes are protected by physical and technical system controls.	3.27	1.36
Q39: Security Training Assessment: Your organization has a security system in place that implements processes that manage IoT (Internet of Things) related risks in devices and assets such as network connectivity equipment, actuators, and sensors.	3.29	1.14
Q43: Vulnerability Assessment: Your organization review, update, and monitors system security programs used in all areas of the organization following ISO27001.	3.87	.94
Q44: Wireless Access Control: There is an in-depth strategy that actively provides defence for protecting inherent operational wireless networks in a way that allows authorized users and prevents unauthorized access.	3.90	.80
Overall	3.82	.62

As shown in Table 3, all the 12 questionnaire items pertaining to the first research question, which concerns the flexibility and adaptability of the current cybersecurity framework, were highly rated by the respondents, with an overall mean score of 3.82 (SD = .62). This was made evident by the high mean scores (standard deviations) of the questionnaire items, which ranged from 3.27 (1.36) to 4.16 (.84), suggesting that such a framework was highly flexible and adaptable that helped the practitioners of the UAE's oil and gas industry to put in place resilient, robust cyber security systems to eliminate any potential cyber threats from causing any serious harm or damage to their operational assets in the organizations.

Table 4 summarizes the descriptive statistics of the respondent's responses to the 13 questionnaire items relating to the second research question.

Table 4. Mean scores of the responses to the 13 questionnaire items relating to the second research question

Questionnaire item	Mean	Std. Deviation
Q05: Account Monitoring and Control: Access reviews are always conducted for terminated employees, organization assets are recovered, and system access is disabled.	4.07	.89
Q07: Analysis of Audit Logs: Your organization has processes that protect system audit records from tampering and ensures audits include information from every business segment and part of the system.	4.18	.76
Q10: Application Security: Your organization has processes that ensure effective management of system changes through proper testing, validation, and documentation.	4.16	.75
Q14: Boundary Defense: All firewalls are correctly configured, operationally active, and patched in all endpoints in the organization.	3.88	1.09
Q16: Control of Network Services: Adequate behaviour rules and procedures are established to ensure security policies and system rules applicable to information security systems are followed.	4.14	.92
Q17: Control of Network Services: Data output from installed security devices and applications are periodically reviewed. These include malware, traffic filters, IDS, and firewalls.	3.88	1.00
Q18: Data Protection: There is an elaborate process that implements physical and administrative protection for assets in case of accidental or deliberate threats to confidentiality.	3.95	.93
Q27: Incident Management: There is a clear sanction/disciplinary policy that is followed in case of policy violations by personnel or contractors.	4.28	.98
Q30: Penetration Tests: Penetration testing and red team exercises are regularly conducted within the organization.	3.23	1.26
Q34: Secure Configurations: The security policy implemented contains processes that perform scheduled maintenance promptly to prevent loss of confidentiality.	3.95	.90
Q35: Secure Configurations: Your organization has a security system that gives a framework for real-time system access decisions or requires identification based on the level of risk.	3.77	.90
Q37: Security Training Assessment: All staff members and contractors with access to sensitive and critical information have the appropriate training and educational background.	3.24	1.25
Q38: Security Training Assessment: Personnel employed in critical positions pass a thorough employment screening process to the extent permitted by the law.	3.62	1.09
Overall	3.87	.61

As shown in Table 4, all the 13 questionnaire items pertaining to the second research question, which concerns the ability of the current framework to establish long-term cybersecurity protection, were highly rated by the respondents, with an overall mean score of 3.87 (SD = .61). Evidently, the mean scores (standard deviations) of the responses to the questionnaire items were moderately high, which ranged from 3.23 (1.26) to 4.28 (.98), signifying that such a framework was able to help the practitioners to establish a reliable long-term cybersecurity mechanism to protect their important, sensitive operational assets in their organizations from cyber threats.

Table 5 summarizes the descriptive statistics of the respondent's responses to the 15 questionnaire items relating to the third research question.

Table 5. Mean scores of the responses to the 15 questionnaire items relating to the third research question

Questionnaire item	Mean	Std. Deviation
Q08: Application Security: Internal system development life cycle can be described as secure, restricted, and safe from unauthorized system access.	4.03	.84
Q09: Application Security: Some devices and programs cannot be updated or patched.	3.96	.86
Q12: Boundary Defense: All segments of the system security network have an alert system that informs relevant IT personnel of unauthorized access or unwanted behaviours.	3.87	1.02
Q13: Boundary Defense: The current framework in use contain a process that ensures adequate capacity and provides controls that limit the effectiveness of DDoS (Distributed Denial-of-Service) attacks.	3.91	.81
Q15: Control of Network Services: Your system security framework provides visibility across all users and devices across the network.	3.78	1.02
Q21: Devices inventory: Your organization uses a standard process to maintain machine-to-machine credentials and the list of inventory in use.	3.85	.78

Q22: E-mail and Web Protections: The organization is fully compliant with all the oil and gas industries and regions' cybersecurity regulations, rules, and requirements.	4.05	.87
Q23: E-mail and Web Protections: Emails and incoming information from outside networks are scanned to remove phishing attacks, spam, malware, and unwanted information.	4.38	.76
Q25: Incident Management: Your organization's system security framework provides a full-proof contingency plan that ensures continuity in case of system disruption.	4.07	.83
Q26: Incident Management: All potential system breaches have a properly-outlined incident response plan.	3.91	.95
Q29: Malware Defenses: All devices are configured with up-to-date malware protection programs in the network.	3.80	1.24
Q31: Privileges Access Control: The security framework in place allows you to monitor permission changes in user profiles and the creation of new user accounts.	3.74	1.03
Q40: Software inventory: Your organization uses a standard process to maintain credentials and the list of software inventory in use.	4.10	.71
Q41: Vulnerability Assessment: System processes that provide patch management, remediation, and vulnerability identification are regularly used in the organization.	3.85	.97
Q42: Vulnerability Assessment: Your organization have a mechanism that compares login attempts in different locations and identifies inconsistencies	3.86	.92
Overall	3.94	.55

As shown in Table 5, all the 15 questionnaire items relating to the third research question, which concerns the effectiveness of the current cybersecurity framework, were highly rated by the respondents, with an overall mean score of 3.94 (SD = .55). Clearly, the mean scores (standard deviations) of the responses to the questionnaire items were high, which ranged from 3.74 (1.03) to 4.38 (.76), indicating that such a framework was perceived by the respondents to be highly effective in helping them to institute superior cyber security in their workplace that helped provide a strong shield for their data and information assets against any potential cyber-attacks.

Overall, the above findings showed that the respondents believed that the current cybersecurity framework that they used was highly flexible, adaptable, and effective in helping them to plan and execute cybersecurity measures to deal with a host of cyberattacks, which have become a major threat to the security and safety of any equipment, types of machinery, and tools that are mainly running on the computer systems. Equally important, their feedback or opinions on this framework is critical to assessing its effectiveness in helping all the cybersecurity practitioners who are tasked to provide a high level of protection for their organizations' assets against unwarranted intrusions or security breaches.

Undeniably, given their direct involvements in the oil and gas industry, their feedback or professional opinions carry a lot of weight, which help shed a greater insight into the ability of this cybersecurity framework to guide the practitioners of such a challenging, demanding industry in putting in place all the necessary measures, notably cybersecurity systems and tools, to prevent their important, expensive assets from being made vulnerable to cyber attacks. As such, this finding provides strong evidence for all the major players in the UAE's oil and gas industry to put in extra investment in the current cybersecurity framework in their ongoing efforts to provide strong protection for the critical infrastructures against any type of cyber threats.

IV. CONCLUSION

The findings of this study showed that the current cybersecurity framework was perceived to be highly flexible, adaptable, and effective by the cybersecurity practitioners in the UAE in helping them to perform their duties or responsibilities to protect their important, complex assets against any form of cyberattacks. Arguably, the use of such a framework has enabled them to plan, strategize, develop, and deploy all the essential security measures, including relevant programs, tools, and systems, to counter the threats posed by hackers or cybercriminals by providing strong protection for all equipment and types of machinery in their organizations. As such, these promising findings help reinforce the applicability of the current cybersecurity framework as a strong industrial standard for all practitioners in cybersecurity in the oil and gas industry in the UAE, which over the long run can surely help improve the levels of protection of their critical operational assets against potential cyber threats. Ideally, in addition to the current strong protection, reinvesting in an extremely solid defence is deemed compulsory for assuring the extreme level of security by adding or blending other frameworks, such as NIST, ISA99, or ISO2700, to the current one. In summation, it must be emphasized that strong cyber resilience entails a continual process of improvement, which is surely not a one-off project, but an ongoing endeavour that may take years to carry out to reap its full benefits. Thus, companies involved in the oil and gas industry in the UAE need to keep on enhancing their cybersecurity measures by making continual improvements to their organizations' security strategies and policies.

REFERENCES

[1] W.B. United Arab Emirates GDP. World Bank, (2019).
[2] F. Hacquebord, F. and C. Pernet, Drilling Deep: A look at Cyber attacks on the Oil and Gas Industry, Trend Micro Research, (2020).
[3] A. Al Neaimi, T. Ranginya, and P. Lutaaya, A framework for the effectiveness of cyber security defences: a case of the United Arab Emirates (UAE), International Journal of Cyber-Security and Digital Forensics (IJCSDF), 4(1) (2015) 290-301.

[4] C. Pedersen, Much Ado about Cyber-space: Cyber-terrorism and the Reformation of the Cyber-security, Pepperdine Policy Review, 7.
[5] D. Kamel and J. Gnana, Middle East energy companies' cyber-security investments lag, The National, Dubai, (2019).
[6] A. GarcíaZaballos and F. González Herranz, From Cybersecurity to Cybercrime: A Framework for Analysis and Implementation, Inter-American Development Bank, (2013).
[7] I. Progoulakis, N. Nikitakos, P. Rohmeyer, B. Bunin, D. Dalaklis and S. Karamperidis, Perspectives on Cyber Security for Offshore Oil and Gas Assets, Journal of Marine Science and Engineering, 9(2) (2021) 112. [Online]. Available: 10.3390/jmse9020112.
[8] C. Haughey, Cybersecurity Framework: How To Create A Resilience Strategy, Security Intelligence, [Online]. Available: https://securityintelligence.com/articles/how-to-create-a-cybersecurity-framework/. (2020)
[9] D. Syed, T.-H. Chang, D. Svetinovic, T. Rahwan, and Z. Aung, Security for Complex Cyber-Physical and Industrial, Pacific Asia Conference on Information Systems - PACIS Proceedings, (2017) 180.
[10] E. Luiijf, K. Besseling, and P. Graaf, Nineteen National Cyber Security Strategies, International Journal of Critical Infrastructure Protection, 9 (1) (2013).
[11] M. Al Dhanhani and J. Mat Jizat, Review of Cyber Security on the Oil and Gas Industry in the United Arab Emirates: Analysis on the Effectiveness of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, 12(11)) (2021) 714-720. Available: https://turcomat.org/index.php/turkbilmat/article/view/5954/4954
[12] K. Stouffer, T. Zimmerman, C. Tang, J. Cichonski, M. Pease, N. Shah and W. Downard, Cybersecurity Framework Manufacturing Profile, 3 (2019).
[13] T. Zimmerman, Ensuring the Cybersecurity of Manufacturing Systems, NIST, (2017).
[14] R. Brooks, Top 20 Critical Security Controls for Effective Cyber Defense, Netwrix Corporation, (2018). [Online]. Available: https://blog.netwrix.com/2018/02/01/top-20-critical-security-controls-for-effective-cyber-defense/.
[15] J. Pescatore, Back to basics: Focus on the first six CIS critical security controls, SANS Analyst Program, (2018). [Online]. Available: https://wTurkish Journal of Computer and Mathematics Education,ww.dlt.com/sites/.
[16] M.E., Galligan, S. Herrygers and K. Rau, Managing cyber risk in a digital age, Committee of Sponsoring Organizations of the Treadway Commission. (2021). [Online]. Available: https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf.
[17] S. Adler, Reducing threat impact with CIS Controls, An Arctic Wolf Session Cyber Security Digital Summit, (2020). [Online]. Available: https://www.cshub.com/security-strategy/articles/reducing-threat-impact-with-cis-controls.
[18] M. Nyhuis, CIS Security Benchmarks and Compliance: What is CIS Compliance? Diligent Insights, (2020). [Online]. Available: https://insights.diligent.com/compliance/what-is-cis-compliance/
[19] T. Limba, T., Plėta, K. Agafonov, and M. Damkus, Cyber security management model for critical infrastructure, Entrepreneurship and Sustainability, 4(4) (2017) 559-573.
[20] T. Gruenloh, How CIS Controls v8 impacts SMBs? Dark Reading: Connecting the Information Security Community, (2021). [Online]. Available:https://www.darkreading.com/attacks-breaches/how-cis-controls-v8-impacts-smbs
[21] S. Caimi, Why implementation groups are so important to CIS Controls v8?, Cybersecurity Resilience Sponsored News, (2021). [Online]. Available: https://www.govtech.com/cybersecurity
[22] K. S. Taber, K.S., The use of Cronbach's Alpha when developing and reporting research instruments in science education. Research Science Education, 48 (2018) 273–1296.
[23] J. Scott, R. Dakin, K. Heller, and A. Eftimie, A survey and analysis of the gendered impacts of onshore oil and gas production in three developing countries, Extractive Industries for Development Series #28, (2013).
[24] R. Park, B. Metzger, and L. Foreman, Promoting gender diversity and inclusion in the oil, gas, and mining extractive industries, A Women's Human Rights Report: The Advocates for Human Rights, (2019).
[25] D. Rock and H. Grant, Why Diverse teams are smarter, Harvard Business Review, (2016). [Online]. Available: https://hbr.org/2016/11/why-diverse-teams-are-smarter
[26] R. Bozick, G.C. Gonzalez, C. Ogletree, and D.G. Carew, Developing a Skilled Workforce for the Oil and Natural Gas Industry: An Analysis of Employers and Colleges in Ohio, Pennsylvania, and West Virginia, RAND Corporation, (2017).
[27] N. Camps, An Exploratory Study of Skills Shortages within the Oil and Gas Industry in Scotland, International Journal of Management and Applied Research, 2(3) (2015) 130-143.