Turkish Journal of Computer and Mathematics Education Vol.12 No.11 (2021), 714-720

Research Article

Review of Cyber Security on Oil and Gas Industry in United Arab Emirates: Analysis on the Effectiveness of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework

Mohamed Jumah ALDhanhani[1], Jessnor Elmy Mat Jizat[2]

[1]Faculty of Management & Economics Universiti Pendidikan Sultan Idris 35900 Tanjong Malim, Perak, Malaysia
[2]Senior Lecturer Department of Business Management & Entrepreneurship Faculty of Management & Economics Universiti Pendidikan Sultan Idris 35900 Tanjong Malim, Perak, Malaysia
[1]drmjuae@gmail.com, [2]jessnor@fpe.upsi.edu.my

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: In view of increasing cyber attacks, the adoption of an effective security framework is essential for any organization involved in critical sectors, such as the oil and gas sector, to ensure the highest level of security and compliance. In this regard, as one of the major oil producers and exporters, the United Arab Emirates (UAE) needs to employ an effective security framework to protect the critical infrastructures of its oil and gas sector. As such, this study iscarried out to examine the potential harms of cyber attacks by focusing on the elements of the cybersecurity framework of the National Institute of Standards and Technology. The research methodology used in this research is based on a systematic review of the current literature on cyber security and frameworks. The review revealsthat NIST's cybersecurity framework has certain features that apparently make it more effective than others. Essentially, this framework has three main components, namely the framework core, implementation tiers, and profile, which are defined based on an organization's business. Specifically, the framework core has five functions, namely identify, protect, detect, respond, and recover. The findings of this research can help guide policy makers in the UAE's oil and gas industry to make informed decisions on how to best mitigate cyber threats against oil companies. In particular, the findings can assist policy makers to determine whether the NIST's cybersecurity framework can play an essential role in strengthening cyber security in the UAE's oil and gas sector. Moreover, the findings can help practitioners to recommend appropriate practical measures to strengthen the preparedness and responses of oil and gas companies in the UAE to cyber attacks.

Keywords: Cyber attacks, cybersecurity framework, oil and gas industry, safety, and security measures.

1. Introduction

The United Arab Emirates (UAE), made up of seven emirates, was created in 1971. Its landscape is dominated by a vast land mass of sand where huge oil reserves have been found, making it one of the wealthiest nations in the world, which is exemplified by its increasing Gross Domestic Products (GDP) in recent years. For example, its gross domestic product (GDP) in 2018 stood at 414.18 billion dollars (World Bank, 2019). Naturally, the UAE's oil and gas sector has been making significant contributions to its vibrant economy. After the discovery of oil reserves three decades ago, the UAE has undergone a massive transformation that has catapulted it into one of the fast-developing nations in the world (Mohamed &Meddas, 2019). In the last few years, cyber attacks on its oil and gas sector has become more intense (Al Neaimi, Ranginya, &Lutaaya, 2015). In recent times, such attacks have become more and more aggressive, sophisticated, and frequent. Given the broad range of technologies used in its oil and gas sector, such attacks have caused serious damage to many critical infrastructure in several production and processing facilities.

Typically, many of the cyber attacks were targeted at working environments in which information technology is used for a wide range of services, including customer data, web service, accounting systems, and email systems (Pedersen, 2014). However, in recent years, cyber attackers have been targeting technology-enabled operations, including industrial control systems and SCADA. A study conducted by Al Neaim, Ranginya, and Lutaaya (2015) revealed that 50% of cyber attacks in the UAE were directed toward its oil and gas industry. Similarly, the Middle East region has not been spared by such attacks, as 75% of oil and gas firms had experienced a minimum of one security breach that disrupted operations or caused a huge loss of confidential data (Kamel & Gnana, 2019).

The frequent incidences of cyber attacks have prompted many security experts to argue that the cybersecurity National Institute of Standards and Technology (NIST) framework, which is highly adaptable and flexible, could serve as a cost-effective solution for oil and gas companies in the UAE to deal with cybersecurity threats, which when implemented nationwide can boost cybersecurity compliance (Al Neaimi, Ranginya, &Lutaaya, 2015). Particularly, they contended that the NIST's cybersecurity framework could play an essential role in strengthening

cyber security in the UAE's oil and gas sector. Against such a backdrop, the researchers carried out this study with the following objectives:

(a) To review issues of cyber security in the oil and gas industry.
(b) To examine the elements of the NIST's cybersecurity framework.
(c) To propose the development of an effective cybersecurity program.

2. Cyber Security for the Oil and Gas Industry

In general, oil and gas production involves multiple processes of producing, transporting, and distributing oil and gas, as shown in Figure 1. These oil production processes rely on several automation control systems to enhance their precision and accuracy. Specifically, SCADA and industrial control systems are commonly used in the UAE's oil and gas industry, the primary objective of which is to provide effective, efficient control over oil and gas production processes. Due to complex, continuous processes and operations (which characterize the production of oil and gas), constant monitoring and control are required. The automation systems utilized in the industry enable technical personnel to examine whether such processes are performing as expected.

In addition, these systems may perform other related tasks, such as the provision of corrective measures, the determination of quality disparities and the identification of the occurrence of errors for operators. While systems greatly increase the efficiency and productivity of oil and gas companies, they are highly vulnerable to cyber attacks. Therefore, well-established cybersecurity frameworks can be used to strengthen the cyber security of the critical infrastructures of oil and gas companies in the UAE (Al Restar, 2019). More importantly, due to the increasing sophistication and flexibility of cyber-criminals, oil and gas companies need to have the adaptability and agility to effectively respond to working environments that are constantly under cyber-threats. Figure 1 shows the oil and gas production process.

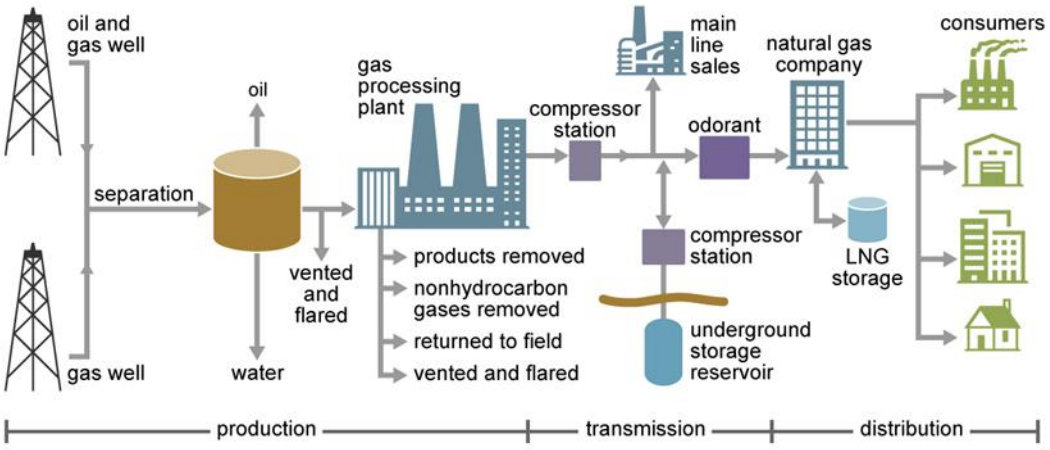

Figure 1:The oil and gas production process. Adapted from
Source: U.S. Energy Information Administration, 2019

As can be seen, oil and gas production involves the integration of numerous technologies to ensure effective and efficient control and measurement. As such, oil and gas companies need to have analyzers, load-monitoring systems, fire-monitoring systems, vibration-monitoring systems, SCADA, among other essential systems, entailing extensive expertise not only in the design but also in the configuration of control, electrical, and instrumentation systems as well as data systems and associated networks. More difficult still, the extraction and processing of oil and gas requires tight margins, stringent quality standards, high product performance, hazardous materials, and complex processes. As a result, oil and gas companies need highly functional and reliable automation systems that can provide close control, high performance, and product coherence (Ismail, Sitnikova, & Slay, 2014).

The process architecture adopted by oil and gas organizations in the UAE is based on industrial control systems that use both information technology and operational technology, with interconnected systems running the extraction and processing of oil and gas. The complexity and interconnectivity of these systems is a significant area for data security breaches, and other forms of cyber attacks. As such, the stability, robustness, reliability, as well as safety of industrial control systems, are key factors to the success of oil and gas companies. Unfortunately,

these systems are fraught with inherent weaknesses, such as the use of old operating systems, a lack of standardized software, and vulnerabilities to threats posed by the Internet of Things (IoT).

Oil and gas companies with robust technology to analyze, monitor, and optimize regulatory control systems can certainly improve the cost-effectiveness and safety of extraction and processing operations. In particular, many government regulations require oil and gas companies to comply with emission requirements, requiring effective emission control systems to reduce excessive emissions. This compliance is essential, as keeping toxic gas emissions within allowable limits can help minimize the harmful effects of global warming.

Moreover, stability control systems play a key role in ensuring that there is no significant variation that can negatively affect the performance of the distillation and separation processes. Besides, the automation systems used in the oil and gas industry can improve the reliability of processes and equipment by managing and scheduling the maintenance of critical equipment, effectively helping companies to avoid unplanned downtime. In this regard, automated systems are critical to managing maintenance timelines that can help eliminate unnecessary outages (Malek, 2019), as process controls can be properly calibrated by such systems to minimize the wear and tear of important, expensive equipment.

Clearly, the oil and gas industry in the UAE needs to emphasize the importance of cyber security by employing safety and security measures to protect the operational technology and industrial control systems. The need for such measures has become more pressing as many operations of oil and gas companies have become easy targets for sophisticated cyber attacks, which can threaten the viability of an entire organization (Al-Sati, 2019). These businesses must therefore seek and implement effective and efficient approaches that can help them achieve a high level of safety. Specifically, these companies may consider implementing multidimensional programs, systematic risk management, and robust government structures related to cyber security. In this respect, it is important to investigate whether the NIST's cybersecurity framework can serve as a suitable methodology for oil and gas companies in the UAE to strengthen their responses and improve their preparedness against cyber threats.

3. NIST's Cybersecurity Framework

In recent years, cyber attacks have become a contentious global concern among many nations, particularly among oil-producing countries, prompting many of their leaders to take several precautionary measures. For example, on February 12, 2013, the then President of the United States of America (USA), Barrack Obama, issued the Executive Order 16636, which sought to improve the critical infrastructure of cyber security. Since then, other governments, including the UAE, have embraced a similar approach to protect themselves from cyber attacks (Luiijf, Besseling, & Graaf, 2013). In the UAE, its government has taken an active role in the identification of strategies to enhance the performance of cyber security and counter cyber attacks. In this regard, the NIST's cybersecurity framework has certain features that distinguish it from previous versions of VCS, many of which were not effective in countering cyber attacks. In principle, the NIST's cybersecurity framework has three main components: the framework core, implementation tiers, and profile, which are defined based on an organization's business. Specifically, the framework core has five functions, namely identify, protect, detect, respond, and recover. Figure 2 shows the components of the NIST's cybersecurity framework and their respective functions.

Figure 2: The NIST's cybersecurity framework. Adapted from
Source: NIST, 2018

The framework's infrastructure contains both physical and virtual systems and assets that have a profound impact on the performance of the oil and gas industry (NIST, 2018). Given the continually changing nature and complexity of both internal and external threats, the UAE's telecommunication authority has taken several proactive approaches in reviewing cyber-infrastructures to ensure consistent and uniform procedures of identifying, assessing, and managing cyber attacks are put in place (Amazon Web Services, Inc, 2019). In this respect, the NIST's approach is well-suited for the UAE's oil and gas sector as it can handle numerous transactions and information related to the industry with ease without causing any data breaches. Interestingly, NIST's cybersecurity framework is technology-neutral to ensure the framework can be extended to capture new features to limit cyber attacks by incorporating new technical innovations. Previous technologies were deemed ineffective due to their rigid structures that prohibited any form of improvements. Such rigidity makes these technologies virtually almost absolute, as cyber attacks continually keep on improving, thus necessitating the need to have systems that are also continually evolving to deal with new threats (Zimmerman, 2017).

Essentially, the elements of NIST's cybersecurity framework have been heavily borrowed from several international standards, guidelines, and practices, which have been carefully developed to manage the operations of the oil and gas industry without affecting its performance. The integration of existing and emerging standards enables economies of scale and drives the development of effective information technology practices (Luiijf, Besseling, & Graaf, 2013). Lately, many oil and gas companies have ventured into the customization of products based on the NIST's cybersecurity framework, the competition of which has enabled a faster diffusion of technology to all players within the oil and gas sector.

In principle, the NIST's cybersecurity framework provides a shared structure and mechanism for the oil and gas sector to highlight their vulnerabilities against cyber attacks. The framework provides the foundational knowledge for the players of the industry to review available resources that they can rely on to counter cyber attacks. The structure further provides a mechanism for assessing cyber attackers' abilities and preparedness to launch attacks that can potentially compromise the safety of information technology systems (Stouffer, et al., 2019). The NIST's cybersecurity framework has also been adopted by many companies to support and monitor the progress made by major players in the oil and gas industry in ensuring their information technology systems are moving in the desired direction. Moreover, the structure of this framework provides a means of informing stakeholders of the oil and gas industry of imminent cyber attacks and what can be effectively done to counter such attacks. Admittedly, NIST's cybersecurity framework can only complement the industry's risk management processes; it can neither replace such processes nor inhibit the enforcement of laws to curb cyber attacks (Schatz, Bashroush, & Wall, 2017). Furthermore, the framework is not industry-specific, making it ineffective in dealing with specific issues related to the oil and gas sector.

Each section of the NIST's cybersecurity framework seeks to enhance the connection between operations of the oil and gas sector and cybersecurity activities (Conkle, 2018). Essentially, its framework core is a collection of cybersecurity undertakings, desired results, and relevant references, which are similar across critical telecommunication infrastructure units. In addition, the framework core consists of standards relating to the oil and gas industry to guide the generation, storage, and dissemination of information and to guide the development, review, and implantation of cybersecurity initiatives from the executive level or the sector head to the operational level (Stouffer, et al., 2019).

Aligned with one another, the functions of the framework core can help enhance the strategic understanding of the life cycle of how the oil and gas sector identify, prepare against, and counter cyber attacks. In addition, the framework core helps to establish the primary units and sub-units of each function by linking them with related informative references, such as current standards, guidelines, and practices, in dealing with cyber attacks (NIST, 2018). The second component of the framework is the implementation tier consisting of four levels, as shown in Figure 3.

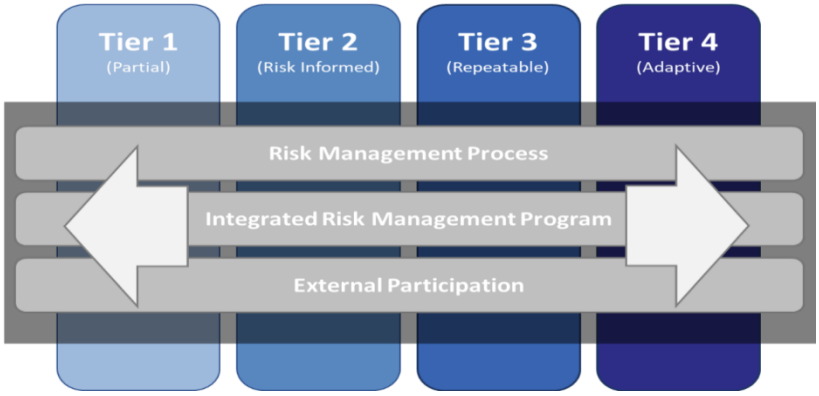

Figure 3: The tiers of the NIST's cybersecurity framework. Adapted from
Source: NIST, 2018

A tier offers a means of contextualizing the entire information technology system to understand cybersecurity risks and put in place appropriate measures to counter imminent cyber attacks (Ferron, 2018). Essentially, a tier defines the features of a framework, such as its resilience against potential cyber attacks and its ability to incorporate new features, among others. Each level indicates the evolution from informal counter-practices to the reactive responses and finally to intelligent approaches that are agile and well-prepared to counter potential risks (Al Neaimi, Ranginya, &Lutaaya, 2015). In the selection process of tiers, oil and gas companies have to consider their prevailing risk management practices, the frequency and nature of threats, and legal and regulatory guidelines to counter cyber attacks (NIST, 2018).

The profile of the NIST's cybersecurity framework characterizes results based on the business needs that the oil and gas sector has chosen from the framework units and sub-units. An active profile is categorized based on the congruence or convergence of standards, guidelines, and practices in relation to the framework core in a specific execution case (Zimmerman, 2017). If the oil and gas sector wishes to adopt such a framework, it must review all units and sub-units based on drivers and risk evaluation prior to establishing the most crucial feature to be added to the threat mitigation strategy. Based on a current profile, the sector must also consider other issues by selecting and evaluating appropriate technology to use in countering cyber attacks in terms of its implementation cost and its ability to be modified.

4. Tiers of the NIST's Cybersecurity Framework

The first tier, Tier 1, is a risk management process, the unit of which deems the oil and gas sector has no formal cybersecurity policies and features. This component also incorporates risk management programs and allows for external engagement. In addition, the unit points to a limited understanding of cybersecurity risks within an organization (Sangani& Vijayakumar, 2012).

The second tier, Tier 2, indicates that the players are informed of the risk of cyber attacks. This tier includes an elaborate risk management process that is endorsed by specific authorities. It also has an integrated risk management program to promote cybersecurity risk awareness within an organization. For instance, a company that deals with the distribution and sale of oil may incorporate the risk management plan into its operations (Reback& Costello, 2014). Additionally, this tier supports external engagement, where stakeholders can be actively involved in formulating risk mitigation plans.

The third tier, Tier 3, means that the risk management process should be formally approved and adopted as a policy. This tier ensures that risk management processes are regularly updated to reflect emerging trends in cybercrime. In addition to the risk management program, the tier assists in implementing well-defined risk-informed policies, processes, and procedures (NIST, 2018). With respect to external participation, an organization may recognize other parties that rely on its expertise to ensure the safety of their systems. As such, this tier fosters close partnerships and the constant exchange of information to facilitate better decision-making processes.

The fourth tier, Tier 4, is where an organization embraces cybersecurity practices based on lessons learned from previous attacks and simulation activities that permit the analysis of indicators of possible future attacks based on past and current cybersecurity activities. With respect to risk management programs, a tier-four

organization can implement a comprehensive approach to managing cyber attacks (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016). In many cases, tier-four organizations have adopted organizational cultures that allow them to quickly identify cyber attacks and then react with the most effective method.

5. Development of an Effective Cybersecurity Program

The NIST's cybersecurity framework has radically altered the approach to dealing with cyber security threats by establishing strategies to improve thecyber security plan. Essentially, the NIST's cybersecurity framework aims to enhance the capability of a counterattack mechanism by establishing priorities and defining the scope of cyber-attacks (Conkle, 2018). Companies in the oil and gas industry in the UAE can benefit from this framework such that they can identify how their business objectives can be targeted by cyber attacks, thus enabling them to establish high-level priorities.

Most preferably, the players in this sector should have up-to-date, accurate information that can enable them to make appropriate strategic decisions that help enhance their ability to counter cyber attacks (Amazon Web Services, Inc, 2019). Following the prioritization and scope of the cyber security framework, the next step is to comply with the regulatory provisions to guide the process. As such, stakeholders within the relevant department should be able to identify systems that are compliant with regulatory requirements that support cyber security (Lubell, 2016). In particular, organizations in this sector should be able to identify cyber threats and vulnerabilities that can have a negative impact on the available assets.

The third step in developing the NIST's cybersecurity framework is to create a current profile. Basically, a profile shows the results of the units and sub-units of the core framework. Following the creation of the framework, an assessment must be completed to determine the effectiveness of the overall risk management strategy (Hathaway &Klimburg, 2012). As such, an organization should be able to analyze the entire process and determine its capacity to counter cyber attacks based on the creation of a target profile. In essence, creating a target profile of an organization should take into consideration the influences and requirements imposed by external stakeholders, such as decision-makers and clients, among others.

The final step involves determining, analyzing, and prioritizing gaps by comparing the current profile and the target profile that helps highlight potential loopholes, which can easily be exploited by cyber attackers. As a result, a priority plan is created to address deficiencies that help make the system more efficient (Amazon Web Services, Inc, 2019). It is also recommended that a cost analysis be conducted to assist in determining the cost to implement such a system. Finally, the action plan of the NIST's cybersecurity framework is implemented to assist an organization in determining the appropriate steps for implementing the system.

6. Conclusion

As highlighted, the oil and gas industry in the UAE is highly vulnerable to cyber attacks, entailing the stakeholders to employ the best technology available to safeguard the security of critical information. Over recent years, the NIST's cybersecurity framework has emerged as one of the best technologies that has been adopted by many leading players in the industry throughout the world in countering cyber attacks. As cyber attacks become increasingly sophisticated, the effectiveness of technologies to counter such attacks must also be improved. In this regard, NIST's cybersecurity framework provides an effective approach to combatting cybercrime, given its flexibility that fosters continuous improvement. In particular, the structure of this framework can help stakeholders to identify potential threats and subsequently implement measures to safeguard the security of the information systems. Arguably, the effectiveness of this framework can be further enhanced or improved by examining its inherent weaknesses, which was the focus of this study that aimed to make such a framework more foolproof against any form of cyber attacks. In addition, the findings of this study can help industry players in many oil-exporting nations, including the UAE, to redesign the structure of such a framework by enhancing its components, which collectively make information security more robust and resilient.

References

1. Abdullahi, S. . (2020). Measuring Co-Movements and Linkages between Nigeria and the
2. UAE Stock Exchanges: Is there Opportunity for Portfolio Building?. Journal of Advanced Research in Economics and Administrative Sciences, 1(2), 106-122. https://doi.org/10.47631/jareas.v1i2.124
3. Al Neaimi, A., Ranginya, T., &Lutaaya, P. (2015). A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE). International Journal of Cyber-Security and Digital Forensics (IJCSDF), 4(1), 290-301.

4. Al Restar. (2019). Half Of The Cyber Attacks In The Middle East Targeted Oil And Gas Companies. Z6 Mag. Retrieved Dec 03, 2019, from https://z6mag.com/2019/06/18/middle-east-hackers-targets-oil-companies/
5. Al-Sati, Z. (2019). The biggest oil and gas threat isn't drones. It's cyber.Arabianbusiness. Retrieved 12 01, 2019, from https://www.arabianbusiness.com/technology/428319-the-biggest-oil-gas-threat-isnt-drones-its-cyber
6. Amazon Web Services, Inc. (2019). NIST Cybersecurity Framework (CSF). Amazon Web Services, Inc. Retrieved 12 01, 2019, from https://www.nist.gov/cyberframework
7. Conkle, T. (2018). NIST Cybersecurity Framework. Retrieved 12 01, 2019, fromhttps://www.nist.gov/cyberframework/new-framework
8. Ferron, J. (2018). The NIST Cybersecurity Framework. Retrieved March 20, 2018, from http://www.interactivesecuritytraining.com/index.html
9. Hathaway, &Klimburg, A. (2012). National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.
10. Ismail, S., Sitnikova, E., & Slay, J. (2014). Towards Developing SCADA Systems Security Measures for Critical Infrastructures against Cyber-Terrorist Attacks. ICT Systems Security and Privacy Protection IFIP Advances in Information and Communication Technology, 242-249. DOI:10.1007/978-3-642-55415-5_20
11. Kamel , D., & Gnana, J. (2019). Middle East energy companies' cyber-security investments lag. Dubai: The National.
12. Lubell, J. (2016). Baseline Tailor Software-aided Security Control Selection. NIST Engineering Laboratory.
13. Luiijf, E., Besseling, K., & Graaf, P. (2013). Nineteen National Cyber Security Strategies. International Journal of Critical Infrastructure Protection, 9(1). DOI:10.1504/IJCIS.2013.051608.
14. Malek, C. (2019). Counting the cost of Middle East cyberattacks. ArabNews. Retrieved Dec 03, 2019, from https://www.arabnews.com/node/1551171/middle-east.
15. Mohamed, K., &Meddas, O. (2019). Excellent Model of economic diversification from UAE,Economic, Business and Management Sciences Institute Journal,3(1), 21-36.
16. NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology. DOI:10.6028/nist.cswp.04162018
17. Pernik, P., Wojtkowiak, J., & Verschoor-Kirss, A. (2016). National cybersecurity organization: United States. NATO Cooperative Cyber Defence Centre of Excellence: Tallinn.
18. Reback, S., & Costello, T. (2014). Deconstructing the Internet of Things. Bloomberg Finance.
19. Sangani, K., N., & Vijayakumar, B. (2012). Cyber security scenarios and control for small and medium enterprises. Informatica Economica,, 16(2), 58.
20. Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Defifinition of Cyber Security. Journal of Digital Forensics, Security and Law, 12(2). DOI:https://doi.org/10.15394/jdfsl.2017.1476
21. Stouffer, K., Zimmerman, T., Tang, C., Cichonski, J., Pease, M., Shah, N., &Downard, W. (2019). Cybersecurity Framework Manufacturing Profile. National Institute of Standards and Technology Internal Report 8183A, Volume 3. DOI:10.6028/NIST.IR.8183A-3
22. Tirupathi, A., Banerjee, A., & Riaz, S. . (2020). Factors Leading to Sustained Growth of
23. SMES in the U.A.E: A Concept Paper. Journal of Advanced Research in Economics and Administrative Sciences, 1(2), 91-105. https://doi.org/10.47631/jareas.v1i2.85
24. World Bank. (2019). United Arab Emirates GDP. World Bank. Retrieved 12 01, 2019, from https://tradingeconomics.com/united-arab-emirates/gdp.
25. Zimmerman, T. (2017). Ensuring the Cybersecurity of Manufacturing Systems. NIST. Retrieved Dec. 4, 2019, from https://www.nist.gov/blogs/taking-measure/ensuring-cybersecurity-manufacturing-systems.