EVALUATION OF THE AGILITY, ABILITY, AND EFFECTIVENESS OF THE CURRENT CYBERSECURITY FRAMEWORK FOR THE OIL AND GAS INDUSTRY IN THE UNITED ARAB EMIRATES

MOHAMED JUMAH MOHAMED ALI ALDHANHANI

SULTAN IDRIS EDUCATION UNIVERSITY

2024

EVALUATION OF THE AGILITY, ABILITY, AND EFFECTIVENESS OF THE CURRENT CYBERSECURITY FRAMEWORK FOR THE OIL AND GAS INDUSTRY IN THE UNITED ARAB EMIRATES

MOHAMED JUMAH MOHAMED ALI ALDHANHANI

05-4506832 pustaka.upsi.edu.my Perpustakaan Tuanku Bainun Kampus Sultan Abdul Jalil Shah PustakaTBainun ptbupsi

THESIS PRESENTED TO QUALIFY FOR A DOCTOR OF PHILOSOPHY

FACULTY OF MANAGEMENT & ECONOMICS
SULTAN IDRIS EDUCATION UNIVERSITY

2024

05-4506832 pustaka.upsi.edu.my Perpustakaan Tuanku Bainun Kampus Sultan Abdul Jalil Shah PustakaTBainun ptbupsi

UNIVERSITI PENDIDIKAN SULTAN IDRIS
SULTAN IDRIS EDUCATION UNIVERSITY

Please tick (√)	
Project Paper	
Masters by Research	
Master by Mixed Mode	
PhD	✓

INSTITUTE OF GRADUATE STUDIES

DECLARATION OF ORIGINAL WORK

This declaration is made on the **13TH AUGUST 2024**

i. Student's Declaration:

I, **MOHAMED JUMAH MOHAMED ALI ALDHANHANI (P20171001249) FACULTY OF MANAGEMENT AND ECONOMICS** (PLEASE INDICATE STUDENT'S NAME, MATRIC NO. AND FACULTY) hereby declare that the work entitled **EVALUATION OF THE AGILITY, ABILITY, AND EFFECTIVENESS OF THE CURRENT CYBERSECURITY FRAMEWORK FOR THE OIL AND GAS INDUSTRY IN THE UNITED ARAB EMIRATES** is my original work. I have not copied from any other students' work or from any other sources exceptwhere due reference or acknowledgement is made explicitly in the text, nor has any part been written for me by another person.

Signature of the student

ii. Supervisor's Declaration:

I **DR. JESSNOR ELMY BINTI MAT JIZAT** (SUPERVISOR'S NAME) hereby certifies that the work entitled **EVALUATION OF THE AGILITY, ABILITY, AND EFFECTIVENESS OF THE CURRENT CYBERSECURITY FRAMEWORK FOR THE OIL AND GAS INDUSTRY IN THE UNITED ARAB EMIRATES** (TITLE) was prepared by the above named student, and was submitted to the Institute of Graduate Studies as a * partial/full fulfillment for the conferment of **DOCTOR OF PHILOSOPHY** (PLEASE INDICATE THE DEGREE), and the aforementioned work, to the best of my knowledge, is the said student'swork.

17 September 2024
Date

Dr. Jessnor Elmy Mat Jizat
Pensyarah Kanan
Fakulti Pengurusan dan Ekonomi
Universiti Pendidikan Sultan Idris

Signature of the Supervisor

UNIVERSITI PENDIDIKAN SULTAN IDRIS
SULTAN IDRIS EDUCATION UNIVERSITY

INSTITUT PENGAJIAN SISWAZAH /
INSTITUTE OF GRADUATE STUDIES

BORANG PENGESAHAN PENYERAHAN TESIS/DISERTASI/LAPORAN KERTAS PROJEK
DECLARATION OF THESIS/DISSERTATION/PROJECT PAPER FORM

Tajuk / *Title*: EVALUATION OF THE AGILITY, ABILITY, AND EFFECTIVENESS OF THE CURRENT CYBERSECURITY FRAMEWORK FOR THE OIL AND GAS INDUSTRY IN THE UNITED ARAB EMIRATES

No. Matrik /*Matric's No.*: P20171001249

Saya / *I* : MOHAMED JUMAH MOHAMED ALI ALDHANHANI
(Nama pelajar / *Student's Name*)

mengaku membenarkan Tesis/Disertasi/Laporan Kertas Projek (Kedoktoran/Sarjana)* ini disimpan di Universiti Pendidikan Sultan Idris (Perpustakaan Tuanku Bainun) dengan syarat-syarat kegunaan seperti berikut:-
acknowledged that Universiti Pendidikan Sultan Idris (Tuanku Bainun Library) reserves the right as follows:-

1. Tesis/Disertasi/Laporan Kertas Projek ini adalah hak milik UPSI.
   The thesis is the property of Universiti Pendidikan Sultan Idris
2. Perpustakaan Tuanku Bainun dibenarkan membuat salinan untuk tujuan rujukan dan penyelidikan.
   Tuanku Bainun Library has the right to make copies for the purpose of reference and research.
3. Perpustakaan dibenarkan membuat salinan Tesis/Disertasi ini sebagai bahan pertukaran antara Institusi Pengajian Tinggi.
   The Library has the right to make copies of the thesis for academic exchange.
4. Sila tandakan (√) bagi pilihan kategori di bawah */ Please tick (√) for category below:-*

☐	**SULIT/*CONFIDENTIAL***	Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub dalam Akta Rahsia Rasmi 1972. / Contains confidential information under the Official Secret Act 1972
☐	**TERHAD/*RESTRICTED***	Mengandungi maklumat terhad yang telah ditentukan oleh organisasi/badan di mana penyelidikan ini dijalankan. / *Contains restircted information as specified by the organization where research was done*
☑	**TIDAK TERHAD/*OPEN ACCESS***	

(Tandatangan Pelajar/ Signature)

Dr. Jessnor Elmy Mat Jizat
Pensyarah Kanan
Fakulti Pengurusan dan Ekonomi
Universiti Pendidikan Sultan Idris

(Tandatangan Penyelia / *Signature of Supervisor*)
& (Nama & Cop Rasmi / *Name & Official Stamp*)

Tarikh: 17 September 2024

Catatan: Jika Tesis/Disertasi ini **SULIT** @ **TERHAD**, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaandengan menyatakan sekali sebab dan tempoh laporan ini perlu dikelaskan sebagai **SULIT** dan **TERHAD**.
Notes: If the thesis is CONFIDENTAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction.

ACKNOWLEDGMENT

In the name of Allah, the Most Beneficent, the Most Merciful. I would like to sincerely thank my mother, father, wife, friends, supervisors, co-workers, and examiners for their unceasing encouragement and support. Thank you very much for all the assistance that helped me remain steadfastly passionate about undertaking this challenging academic endeavour and its successful completion. It was an incredible and fulfilling journey of exploring new knowledge, the success of which owed to the kindness, caring, and understanding of all the above individuals.

ABSTRACT

The objective of this study was to assess the agility, ability, and effectiveness of the current cybersecurity framework used by oil and gas companies in the UAE to safeguard their critical data and assets from cyber threats. A quantitative approach was employed, and an online survey was administered to 94 cybersecurity practitioners, who were involved in the planning, development, and deployment of cybersecurity measures in 12 oil and gas companies in the UAE and chosen via stratified random sampling. For the descriptive data analysis (RQ1, RQ2 and RQ3), the mean score of items relating to the agility of the current cybersecurity framework was 3.83 (SD = 0.94), mean score for the ability of the framework was 3.87 (SD = 0.98), and mean score for the effectiveness of the framework was 3.94 (SD = 0.91). This indicated that the cybersecurity framework used in the oil and gas industry in the UAE was highly agile, capable, and effective in protecting important assets and data from potential cyber-attacks. Inferential statistical analyses, including t-tests and ANOVA, showed no significant differences in framework evaluation based on gender, academic qualifications, or work experience. However, significant differences were noted in perceptions of the framework's agility, ability, and effectiveness between employees at the main offices (agility: M = 4.01, SD = 0.57; ability: M = 4.14, SD = 0.55 and effectiveness: M = 4.14, SD = 0.53), versus those working on sites (agility: M = 3.75, SD = 0.63; ability: M = 3.76, SD = 0.61 and effectiveness: M = 3.86, SD = 0.55). Overall, the study highlights the importance of a strong cybersecurity framework in guiding practitioners to establish long-term cybersecurity for companies involved in a challenging industry and provides practical implications for influential leaders to support and improve their organizations' cybersecurity systems.

PENILAIAN KETANGKASAN, KEBOLEHAN DAN KEBERKESANAN RANGKA KERJA KESELAMATAN SIBER SEMASA UNTUK INDUSTRI MINYAK DAN GAS DI EMIRAT ARAB BERSATU

ABSTRAK

Objektif kajian ini adalah untuk menilai ketangkasan, keupayaan dan keberkesanan rangka kerja keselamatan siber semasa yang digunakan oleh syarikat minyak dan gas di UAE untuk melindungi data dan aset kritikal mereka daripada ancaman siber. Pendekatan kuantitatif telah digunakan, dan tinjauan dalam talian telah diberikan kepada 94 pengamal keselamatan siber, yang terlibat dalam perancangan, pembangunan dan penggunaan langkah keselamatan siber di 12 syarikat minyak dan gas di UAE dan dipilih melalui persampelan rawak berstrata. Untuk analisis data deskriptif (RQ1, RQ2 dan RQ3), skor min bagi item yang berkaitan dengan ketangkasan rangka kerja keselamatan siber semasa ialah 3.83 (SD = 0.94), skor min untuk keupayaan rangka kerja ialah 3.87 (SD = .98), dan skor min bagi keberkesanan rangka kerja ialah 3.94 (SD = 0.91). Ini menunjukkan bahawa rangka kerja keselamatan siber yang digunakan dalam industri minyak dan gas di UAE adalah sangat tangkas, berkebolehan dan berkesan dalam melindungi aset dan data penting daripada kemungkinan serangan siber. Analisis statistik inferens, termasuk ujian-t dan ANOVA, tidak menunjukkan perbezaan yang signifikan dalam penilaian rangka kerja berdasarkan jantina, kelayakan akademik atau pengalaman kerja. Walau bagaimanapun, perbezaan yang ketara telah dicatat dalam persepsi ketangkasan, keupayaan dan keberkesanan rangka kerja antara pekerja di pejabat utama (ketangkasan: M = 4.01, SD = 0.57; keupayaan : M = 4.14, SD = 0.55 dan keberkesanan : M = 4.14, SD = 0.53), berbanding mereka yang bekerja di tapak (ketangkasan: M = 3.75, SD = 0.63; keupayaan : M = 3.76, SD = 0.61 dan keberkesanan : M = 3.86, SD = 0.55). Secara keseluruhannya, kajian itu menyerlahkan kepentingan rangka kerja keselamatan siber yang kukuh dalam membimbing pengamal untuk mewujudkan keselamatan siber jangka panjang untuk syarikat yang terlibat dalam industri yang mencabar dan memberikan implikasi praktikal untuk pemimpin yang berpengaruh untuk menyokong dan menambah baik sistem keselamatan siber organisasi mereka.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

802.1X	IEEE 802.1X standard for port-based Network Access Control
AAA	Authentication, Authorization, and Accounting
ADSIC	Abu Dhabi Systems and Information Centre
AI	Artificial Intelligence
ANOVA	Analysis of Variance
API	Application Programming Interface
BASH	Bourne-Again Shell
C1	Construct 1 (Agility)
C2	Construct 2 (Ability)
C3	Construct 3 (Effectiveness)
CCPA	California Consumer Privacy Act
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CIS	Center for Internet Security
CIS Controls	Center for Internet Security Controls
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technology
COVID-19	Coronavirus Disease 2019
CSF	Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
CSP	Cloud Service Provider
CVE	Common Vulnerabilities and Exposures

CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DDoS	Distributed Denial of Service
df	Degrees of Freedom
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
DOI	Diffusion of Innovations
EDR	Endpoint Detection and Response
EFA	Exploratory Factor Analysis
FISMA	Federal Information Security Modernization Act
GCC	Gulf Cooperation Council
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GRC	Governance Risk and Compliance
HA1	Research Hypothesis 1
HA2	Research Hypothesis 2
HA3	Research Hypothesis 3
HA4	Research Hypothesis 4
HIPAA	Health Insurance Portability and Accountability Act
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance
IAS	Information Assurance Standards
ICS	Industrial Control Systems
ICT	Information and Communication Technology

IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IG	Implementation Group
IG1	Implementation Group 1
IG2	Implementation Group 2
IG3	Implementation Group 3
IoT	Internet of Things
IP	Infrastructure Protection
IPS	Intrusion Prevention System
ISA	International Society of Automation
ISA99	International Society of Automation Standard 99
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO27001	International Organization for Standardization 27001
IT	Information Technology
KMO	Kaiser-Meyer-Olkin
Likert	Likert Scale
MFA	Multi-Factor Authentication
MSP	Managed Service Provider
NaaS	Network-as-a-service
NCRMF	National Cyber Risk Management Framework
NERC	North American Electric Reliability Corporation
NESA	National Electronic Security Authority
NIAF	National Information Assurance Framework
NIDS	Network Intrusion Detection System

NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards and Technology
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
NVD	National Vulnerability Database
O&G	Oil and Gas
OT	Operational Technology
P1-P4	Priority Tiers 1 to 4
PaaS	Platform as a Service
PCA	Principal Component Analysis
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PCI-DSS	Payment Card Industry Data Security Standard
PDCA	Plan-Do-Check-Act cycle
Ph.D.	Doctor of Philosophy
PowerShell	Microsoft PowerShell
RBV	Resource-Based View Theory
SaaS	Software as a Service
SANS	System Administration, Networking, and Security
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SD	Standard Deviation
SIEM	Security Information and Event Management
Sig.	Significance Level
SIP	System Integrity Protection
SME	Subject Matter Experts
SMEs	Subject Matter Experts

SOC	Security Operation Center
SOC 2	Service Organization Control 2
SOHO	Small or Home Office
SOX	Sarbanes-Oxley Act
SPF	Sender Policy Framework
SPSS	Statistical Package for the Social Sciences
SQL	Structured Query Language
SSDF	Secure Software Development Framework
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
TAM	Technology Acceptance Model
TCAS	Trusted Computing Base Access Control System
TLS	Transport Layer Security
UAE	United Arab Emirates
UAE IAS	UAE Information Assurance Standards
UTAUT	Unified Theory of Acceptance and Use of Technology
VDBIR	Verizon Data Breach Investigations Report
VPN	Virtual Private Network
WDEG	Windows Defender Exploit Guard
WPA2	Wi-Fi Protected Access II

APPENDIX LIST

CHAPTER 1

INTRODUCTION

1.1 Introduction

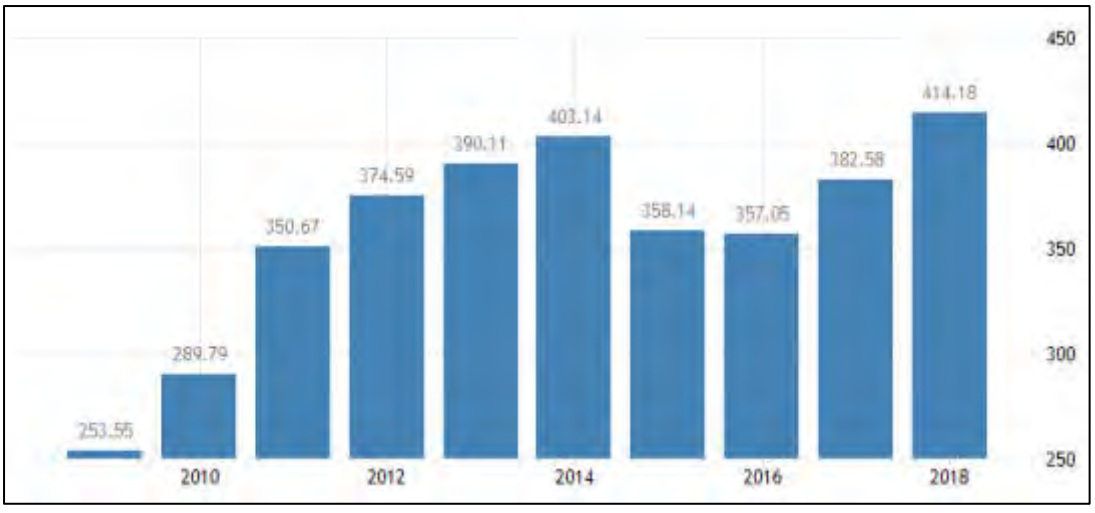
This chapter introduces a research study on cybersecurity in the oil and gas industry, beginning with a detailed exploration of the research background and the pressing cybersecurity challenges the industry faces. The study's purpose and objectives are outlined, followed by the presentation of guiding research questions and formulated hypotheses. The significance of the research is emphasized through its academic and practical contributions. Potential limitations are acknowledged to ensure a comprehensive understanding. Key terms are operationally defined for clarity, and the chapter concludes with an overview of the thesis organization, providing a roadmap for the subsequent chapters.

1.2 Research Background

The United Arab Emirates (UAE), which consists of seven emirates, was established in 1971. Geographically, it shares its borders with Saudi Arabia, Oman, and Qatar (Rossel, 2019) and a member of the Gulf Cooperation Council (GCC) (Al-Khouri A. , 2012). Its capital is Abu Dhabi, and the official language and currency of the UAE is Arabic and Dirham, respectively. Geographically, a vast network of deserts dominates this emerging wealthy nation, in which oil and gas have been discovered in huge amounts, thus contributing to its increasing economic growth. This is made evidently clear by its increasing gross domestic products (GDPs) over the recent years (World Bank, 2019), as highlighted in Figure 1.1. In terms of governance, the UAE has a federal system of government, with each of the seven emirates having its own ruler.

Figure 1.1

The United Arab Emirates' GDPs



Clearly, the UAE's vibrant economy has been driven by its oil and gas sector. Lately, it is focusing on diversifying its economy in other sectors as well as a way to

stop over-relying on oil and gas revenues. After the discovery of oil reserves in the UAE 30 years ago, the country transformed its deserts into an urban developed nation (Mohamed & Meddas, 2019). Of late, like many other nations, issues relating to cyber-attacks on its oil and gas sector has become a major concern (Al Neaimi, Ranginya, & Lutaaya, 2015). Increasingly, such attacks have become more intense, sophisticated, and frequent. Because the oil and gas sector in the UAE has heavily adopted a wide spectrum of technologies, it is highly vulnerable to cyber-attacks where hackers can implant malware on critical infrastructure used by the oil and gas sector.

Several decades ago, most of cyber-attacks were aimed at the information technology (IT) infrastructure of business entities that provided a wide range of services, including customer data, web service, accounting systems, and email systems (Pedersen, 2014). Lately, cyber-attacks have shifted to targeting technology-driven operations, including industrial control systems and Supervisory Control and Data Acquisition (SCADA). A case in point is best highlighted by a study conducted by Al Neaimi, Ranginya, and Lutaaya (2015), who discovered about 50% of cyber-attacks in the UAE were aimed at its oil and gas industry. Regionally, such attacks have become increasingly intense in the Middle East, with 75% of its oil and gas companies experiencing at least a minimum of one security breach that caused severe operational breakdowns, which incurred massive losses of important sensitive data (Kamel & Gnana, 2019).

Considering the increasing cyber threats, numerous experts have advised UAE's oil and gas companies to implement the National Institute of Standards and Technology (NIST) cybersecurity framework, highlighting its adaptability, agility, and cost-

effective nature as factors that could boost cybersecurity compliance (Al Neaimi, Ranginya, & Lutaaya, 2015). Specifically, the current cybersecurity framework employed in the UAE oil and gas sector is the National Electronic Security Authority (NESA). However, the experts argue that adopting the NIST framework could significantly fortify the cybersecurity posture of these organizations. Grounded in this context, this study aims to assess the efficacy of the existing cybersecurity framework embraced by organizations within the UAE's oil and gas sector, with a focus on providing robust security safeguards against detrimental cyber-attacks.

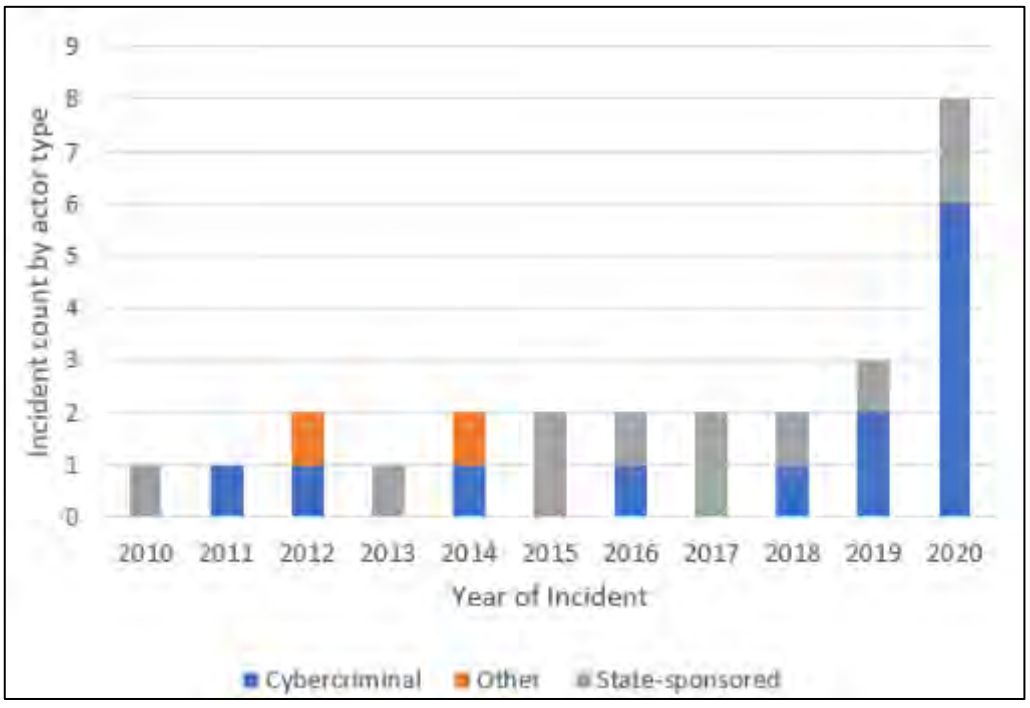
1.3 Problem Statement

Of late, the oil and gas industry in the UAE has become increasingly vulnerable to cyber-attacks by hackers. In this respect, many aspects of the sector's value chain are highly exposed to cyber-attacks, as the traditional defenses against such attacks are not fully effective. Particularly vulnerable are the industrial control systems employed in the oil and gas sector (Syed, Chang, Svetinovic, Rahwan, & Aung, 2017), which makes such attacks devastating because these systems provide essential links in the sector's value chain from transportation pipelines, depots, and refineries to oil production platforms and exploration submersibles. Unfortunately, many of the control systems put in place to manage and control critical oil and gas infrastructure have not been designed to provide maximum protection against malicious cyber-attacks (Basamh, Qudaih, & Bin Ibrahim, 2014).

To make matters worse, the continually improving Internet connectivity has escalated cyber threats to a higher level, as cyber-criminals can stealthily send malicious software online; as shown in Figure 1.2 below (CCCS, 2021), to penetrate control systems of organizations in this important industry. It is, therefore, not surprising to see such attacks have become more frequent in the industry lately (Efthymiopoulos, 2016). For example, in April 2019, a malware code linked to the Russian government was used to attack an oil facility. Earlier, in August 2017, the same malware code had been used to attack another oil facility. This malware, code-named as Triton, was designed to penetrate the networks of target organizations that could compromise the safety of their industrial control systems (Help Net Security, 2018).

Figure 1.2

The Publicly reported cyber incidents targeting Oil & Gas, by actor type



Likewise, the oil and gas infrastructure in the UAE has become a target for numerous attacks, with many of the coordinated attacks being targeted at its oil and gas companies. Typically, cyber-attacks have been directed at the oil and gas companies in the downstream, midstream, or upstream sector of the industry. Sometimes, hackers can attack these three oil streams of an oil and gas company simultaneously, making its operational technology systems and information technology vulnerable to breach of security. Usually, the objective of an attack depends on the hacker' intention, which includes causing safety violations, violating compliance regulations, facilitating illegal tapping of pipelines, preventing discovery of oil spills, interfering with product quality, disrupting production or utilities, damaging machinery, and destroying equipment. Surely, attacks targeting computing systems can cause a complete shutdown of operations, incurring massive losses of revenues (Gorkowienko A. , 2019). Even more damaging, attacks targeting industrial control systems and SCADA in the oil and gas sector, particularly burner management systems can cause fatalities in addition to adversely impacting oil and gas processing, interrupting production as well as damaging storage equipment.

Typically, the oil and gas companies use control systems to control a wide range of operations. In principle, such systems help control and monitor processes associated with the movement, storage, and processing of oil and gas in plants. Unfortunately, in recent years, hacking activities and other related attacks have adversely affected several important operations of control systems in the UAE. Without sufficient protection, hackers will be able to easily attack oil and gas companies with malicious malware, causing untold damage to their production networks and controls of critical equipment. Undeniably, cyber-attacks pose a significant threat to control systems in the oil and gas

industry because they can adversely compromise the operational reliability of such systems (The National & ADNOC, 2019).

Usually, many of the control systems used in the oil and gas industry are connected to the Internet via the companies' networks, rendering them susceptible to cyber-attacks. Even without any external network connectivity, these systems can become easy prey to cyber-attackers. For instance, an attack against the control systems in an oil and gas company can make certain equipment to operate at speeds far exceeding their permissible limits, while providing a false report to operators that the equipment is working at normal speeds. Therefore, such an attack can cause huge losses resulting in serious damage to equipment and low yield of quality products. Potentially, such attacks on control systems can take place when hackers send malicious software to a company's computing systems when they are online or through removable media (such as a USB device) that are being connected to the computing systems (Farwell & Rafal, 2011).

Certainly, existing vulnerabilities of control systems make it easy for hackers to attack a company's network using simple methods. For example, attackers may distribute malicious software using primary methods, such as waterholing attacks, spear-phishing, and compromising SCADA program updates. In particular, they perform waterholing attacks on frequently visited websites by introducing malicious codes, which may compromise the security of such websites where updates of manufacture control systems are normally stored. As such, the attackers can replace genuine software updates with illegitimate copies that carry malicious codes, which

subsequently infect control systems during the installation of software updates (TECH, 2018).

It is important to note that this technique of cyber-attack would still be menacing even if a control system being targeted is not connected to the Internet or to any other external networks. On the other hand, spear-phishing involves sending email messages that contain malicious attachments or links to a target oil and gas company. Typically, hackers may send such emails to specific individuals with whom they are familiar. Often, such emails may be creatively written to look legitimate and innocuous (DarkMatter, 2019). When these individuals click a malicious link contained on an email, they will be directed to an infested website with malicious codes that attack computer systems of a targeted oil and gas companies.

Therefore, the oil and gas industry must prioritize cybersecurity to safeguard the integrity of vital business assets. Admittedly, providing full protection in the oil and gas industry is a daunting task, given the complex structures of operating systems used in the processing and supply of petroleum products. The imperative to have a strong shield against cyber-attacks has become more urgent as the UAE's oil and gas sector is undergoing a major digital transformation in recent decades. With rapidly increasing paces of digitization and advancement of technology, inevitably many machines and equipment in the oil and gas industry will be connected to external networks, including the Internet (Malek, 2019), enabling engineers and other technical personnel not only to analyze production data but also to maintain equipment remotely.

Equally important, such digital transformation in the oil and gas industry helps enhance operational efficiencies through big data, data analytics, and the automation of sensitive tasks. The digital transformation, however, may introduce a broad range of cyber threats to operating systems of oil and gas companies (Menachery, 2017). Given that most of the systems used by oil and gas companies are relatively old, cybercriminals can easily hack such systems without too much effort. Moreover, the oil-refining process that relies on many types of equipment and control systems further exacerbates the problem, as there will be many gateways that can be exploited by cyber-attackers to enable them to gain access to the internal network of a target company.

Consequently, this can cause a serious breach of security, virtually grinding all critical operations of an oil and gas company to a halt. Put simply, a well-executed cyber-attack can cause a complete shutdown of critical control systems in an oil and gas company (Peat, 2018). As many of such organizations rely heavily on advanced digital technology, disruptions of their services and control systems can cause major reputational damage, huge financial losses, and a breach of sensitive company data.

To mitigate such damaging impacts, the Center for Internet Security (CIS) (a non-profit community-driven organization that publishes highly established best practices for protecting IT systems and data) spearheads the efforts taken by the international community of IT professionals to continually develop cybersecurity standards to help safeguard IT products and services against emerging threats. Through such collaborative efforts, they developed a number of security safeguards, known as the CIS Controls, to help organizations establish a robust, resilient cyber defense.

Ideally, organizations seeking to improve their cybersecurity resilience need to identify and utilize any cybersecurity framework that provides the agility (flexibility and adaptability) to respond to emerging cybersecurity needs, the ability to establish long-term cybersecurity protection, and the effectiveness to establish superior cybersecurity program (Hult & Sivanesan, 2014). In principle, such a cybersecurity framework should provide a set of "best practices" for determining risk tolerance and setting controls. However, determining which one is best for a particular organization can be difficult and challenging. It would, therefore, take a meticulous effort by cybersecurity practitioners to understand and embrace each framework's underlying principles that best serve their organization's security needs.

Nevertheless, this is extremely challenging given the changing landscape of cybersecurity realm that witnesses a rich diversity in terms of practitioners' demography, such as gender, work experience, work location, and academic qualification (Fatokun, Hamid, Norman, & Fatokun, 2019); (Gratian, Bandi, Cukier, Dykstra, & Ginther, 2018). Together, such demographic factors would have significant influences over the way in which practitioners view the importance of cybersecurity in their organization, which in turn shape their level of willingness to adopt a specific cybersecurity framework to improve their practices (Ismail, Masrom, Sidek, & Hamzah, 2010).

It is important to acknowledge that the majority of research studies exploring aspects such as agility, ability, and effectiveness of cybersecurity frameworks tend to focus on developed nations and large corporations. Unfortunately, there is a significant gap in research related to developing nations like the UAE, particularly in the context

of the oil and gas industry (ALDhanhani, 2021). This research deficit prompted the present study, which aims to understand the influence of various factors on the adoption and implementation of cybersecurity frameworks among practitioners in the UAE's oil and gas sector.

Considering factors such as gender, work experience, work location, and academic qualification is vital in understanding the dynamics of cybersecurity framework adoption. Firstly, examining gender diversity in cybersecurity can provide insights into potential differences in perspectives and approaches, which may impact the overall effectiveness and adaptability of cybersecurity frameworks. Secondly, work experience is an essential factor as it can offer insights into how practitioners with different levels of experience approach and adapt to cybersecurity challenges. Thirdly, work location can reveal how regional and cultural differences influence the implementation of cybersecurity measures. Lastly, analyzing academic qualifications can help identify the influence of different educational and training pathways on the effectiveness of cybersecurity frameworks in the industry.

By studying these factors in relation to the agility, ability, and effectiveness of cybersecurity frameworks, this research seeks to contribute valuable insights into the adoption and implementation of such frameworks within the UAE's oil and gas sector. This information can help organizations identify areas for improvement, as well as inform future research and policy decisions in the realm of cybersecurity.

1.4 Purpose of the Study

The purpose of this study is to ascertain whether the cybersecurity framework now in use by oil and gas businesses in the UAE can provide an effective methodology for the management of cybersecurity risks in the oil and gas industry. The findings of the research will enable policymakers in the industry to identify components of current processes that need improvements and to determine and implement new risk-mitigation methods and processes.

1.5 Objectives of the Study

Due to the constant threats of cybersecurity attacks against the critical industry in the UAE, many companies in the oil and gas sector must take all necessary measures to mitigate such threats by safeguarding their critical information infrastructure. As such, this study aims to help relevant policymakers understand and utilize the current cybersecurity framework in developing effective risk management processes and cybersecurity programs for companies in this oil-rich nation.

To guide the research, four objectives were developed as follows:

1. To determine the level of agility of the current cybersecurity framework in addressing new cybersecurity threats in the oil and gas sector in the UAE.
2. To determine the level of ability of the current cybersecurity framework to provide long-term cybersecurity for the UAE's oil and gas industry.

3. To determine the level of effectiveness of the current cybersecurity framework in establishing strong cybersecurity in the UAE's oil and gas industry.
4. To evaluate the perceptions of the framework's agility to deal with new cybersecurity needs, its ability to provide lasting cybersecurity, and its effectiveness in establishing superior cybersecurity based on gender, work experience, academic qualification, and work location.

1.6 Research Questions

To help address the above objectives, four research questions were formulated accordingly as follows:

1. What is the level of agility of the current cybersecurity framework in addressing new cybersecurity threats in the oil and gas sector in the UAE?
2. What is the level of ability of the current cybersecurity framework to provide long-term cybersecurity for the UAE's oil and gas industry?
3. What is the level of effectiveness of the current cybersecurity framework in establishing strong cybersecurity in the UAE's oil and gas industry?
4. Are there any differences in perceptions on the framework's agility to deal with new cybersecurity needs, its ability to provide lasting cybersecurity, and its effectiveness in establishing superior cybersecurity based on gender, work experience, academic qualification, and work location?

1.7 Research Hypotheses

Accordingly, four research hypotheses were formulated based on research question number four (RQ4) for this study as follows:

H_A1: There is a significant difference in perceptions of the framework's agility to deal with new cybersecurity needs, its ability to provide lasting cybersecurity, and its effectiveness in establishing superior cybersecurity based on the respondent's gender.

H_A2: There is a significant difference in perceptions of the framework's agility to deal with new cybersecurity needs, its ability to provide lasting cybersecurity, and its effectiveness in establishing superior cybersecurity based on respondent's work experience.

H_A3: There is a significant difference in perceptions of the framework's agility to deal with new cybersecurity needs, its ability to provide lasting cybersecurity, and its effectiveness in establishing superior cybersecurity based on the respondent's academic qualification.

H_A4: There is a significant difference in perceptions of the framework's agility to deal with new cybersecurity needs, its ability to provide lasting cybersecurity, and its effectiveness in establishing superior cybersecurity based on the respondent's work location.

1.8 Importance of the Study

1.8.1 Contribution to knowledge and methodology

This research paves the way for deeper insights into the efficacy of cybersecurity frameworks within the UAE's oil and gas industry, setting a precedent for future studies. The assurance it provides to cybersecurity experts in the UAE underscores the adaptability and robustness of the current systems in place. From a theoretical perspective, the study sets the stage for further exploration of how specific factors, like work location, can influence the applicability of cybersecurity frameworks. As for the methodological contribution, the adoption of a quantitative approach, considering varied demographic parameters, presents a model for future investigations to ensure structured, rigorous data analysis. The depth and implications of these findings will be elaborated upon in Chapter 7.

1.8.2 Contribution to practice

This research highlights the crucial role of cybersecurity frameworks in strengthening the UAE's oil and gas sector. The study's findings emphasize the resilience and agility of the existing cybersecurity framework to vital stakeholders, such as directors and managers. Notably, the findings aid authorities in the UAE's oil and gas sector in making informed decisions to optimally thwart cyber threats. Moreover, they provide

policymakers with insights on the potential of the current framework as an essential tool for elevating cybersecurity measures.

From a practical standpoint, this study offers a robust assurance to professionals in the cybersecurity domain, showcasing the framework's effectiveness. It propels organizational leaders to further support their cybersecurity units with necessary resources, emphasizing the growing need for proactive adaptation to escalating cyber threats. The importance of routinely evaluating protective strategies is also underscored.

The study further sheds light on the adaptable nature of cybersecurity frameworks. They vary in their application range, from organization-specific to spanning international boundaries. The type of data an organization aims to protect determines its cybersecurity stance, making a tailored framework essential. The existing framework in the UAE's oil and gas sector, as indicated by this research, proficiently matches the sector's distinct demands, amalgamating human skill, advanced processes, and state-of-the-art technology.

Furthermore, the research aids researchers in proposing actionable steps to boost the UAE's oil and gas industry's resilience and responsiveness to cyber threats. In summary, this study enhances the conversation around cybersecurity frameworks in the oil and gas sector, emphasizing the importance of solid, knowledgeable leadership in intensifying cybersecurity initiatives. These insights will be explored more comprehensively in Chapter 7.

1.9 Limitations of the Study

In this study, the research data were only gathered through an on online survey involving a number of cybersecurity practitioners, such as information technology officers, network administrators, system analysts, and security engineers, who worked in several organizations in the UAE's oil and gas industry. In view of the ongoing pandemic gripping many nations throughout the world, interviews, which were planned earlier, had to be ruled out due to health and safety concerns. Given this setback, the online survey was carried out with extreme care by using valid questionnaire items to ensure data elicited from the respondents were as reliable as possible.

1.10 Operational Definitions

The following are the operational definitions and terms used in this dissertation:

1.10.1 Cybersecurity

Cyber refers to a form of computers and information technology connected to a local private or public network. On the other hand, cybersecurity refers to the protection of programs, networks, and systems from digital attacks (Albuquerque, Villalba, Orozco, Sousa Júnior, & Kim, 2016). In this research, this term refers to the protection of networks and systems of industrial facilities from any source of digital attacks.

1.10.2 Cybersecurity Framework

Essentially, a cybersecurity framework is a set of documents describing relevant guidelines, standards, and best practices designed for cybersecurity risk management. In principle, such a framework is entailed to help organizations minimize their inherent weaknesses or vulnerabilities that hackers and other cyber criminals may exploit.

1.10.3 NIST' CSF

The National Institute of Standards and Technology (NIST) refers to the physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. The NIST Cybersecurity Framework (NIST CSF) refers to a set of guidelines, best practices, and standards developed by the (NIST) to help organizations manage and reduce cybersecurity risk. The NIST CSF provides a comprehensive approach for organizations to assess, develop, and implement cybersecurity measures in critical infrastructure industries, including the oil and gas sector. In the context of this research, the NIST CSF refers specifically to the NIST's Cybersecurity Framework.

1.10.3.1 Work Experience

Work experience refers to the number of years the participants have spent working in their respective fields or industries. This variable is used to explore the influence of professional experience on the dependent variables.

1.10.3.2 Academic Qualification

Academic qualification refers to the highest level of formal education completed by the participants, including degrees and certifications. In this study, academic qualification is considered an independent variable to investigate the potential effects of education on the dependent variables.

1.10.3.3 Work Location

Work location refers to the geographical area where the participants perform their job duties. In this research, work location is used as an independent variable to determine if there is a relationship between the physical work environment and the dependent variables.

1.10.3.4 Agility

In this study, "agility" refers to the combined attributes of flexibility and adaptability, encapsulating the participants' capacity to adjust their thoughts, behaviors, and actions in response to changing circumstances or requirements within the cybersecurity framework. Specifically, agility is measured as a dependent variable to investigate its relationships with various independent variables.

1.10.3.5 Ability

Ability as a dependent variable, refers to the participants' competence in performing their job-related tasks, including technical and interpersonal skills. This variable is used to assess how the independent variables may influence the participants' abilities in their professional roles.

1.10.3.6 Effectiveness

In this research, effectiveness is a dependent variable that measures the extent to which the participants achieve their work-related goals and objectives. Effectiveness is used to examine the potential impact of the independent variables on the participants' ability to perform successfully in their roles.

1.11 Thesis Organization

The thesis is structured into seven comprehensive chapters, each addressing specific aspects of the research on cybersecurity in the oil and gas industry. Chapter 1 serves as an introduction, setting the stage for the research by presenting the background, problem statement, purpose, and objectives of the study. This chapter also outlines the research questions, hypotheses, and the study's significance. It concludes by discussing the study's limitations, providing operational definitions for key terms, and offering an overview of the thesis organization. Chapter 2 delves into the realm of cybersecurity,

specifically in the context of the UAE. It provides an introduction to various cybersecurity frameworks, including NIST, ISO27001, NESA, ISA/IEC 62443, COBIT, the Common Weakness Enumeration, and the Center for Internet Security (CIS) Controls. Each framework is explored in detail, highlighting its background, objectives, controls, and relevance to the study. Chapter 3 offers a literature review, presenting a background on cybersecurity and benchmarking its implementation across various sectors and regions. The chapter also discusses the agility, ability, and effectiveness of current cybersecurity frameworks, underpinned by relevant theories.

Chapter 4 introduces the conceptual framework and hypothesis development. It elaborates on the constructs of the conceptual framework, such as agility, ability, and effectiveness. The chapter also delves into the theoretical foundations of these constructs and culminates in the development of research hypotheses. Chapter 5 outlines the research methodology, detailing the research design, target population, sampling technique, and the research instrument. This chapter also discusses the reliability, validity, and pilot testing of the research instrument, procedure for data collection, data preparation, and analysis of missing data & outliers. Chapter 6, "Discussion of Findings," details the implementation of the online survey and presents findings from missing data analysis and statistical assumption tests. It examines respondents' demographic profiles by gender, work experience, academic qualification, and location. The chapter analyzes both descriptive and inferential statistics, focusing on the agility, ability, and effectiveness of the current cybersecurity framework. It also investigates differences in perceptions across respondent demographics and discusses the framework's response to emerging threats, long-term security, and overall effectiveness, concluding with discussions on related hypotheses.

Chapter 7 encapsulates the contributions of the research and offers recommendations for future studies. It highlights the study's contributions to knowledge, methodology, and practice. The chapter concludes by suggesting areas for future research in the domain of cybersecurity.

The thesis concludes with a comprehensive list of references, providing sources for all the information and data presented. Additionally, an appendix is included, offering supplementary information and data relevant to the study.