CYBERSECURITY FRAMEWORKS GLOBALLY AND SAUDI ARABIA

Faysal A.Ghauri [#1]

EC-Council University, USA

[1] iam@faysalghauri.com

***Abstract*— The history of incremental internet users in Saudi Arabia defined the basis of threats posed to the country and the region. After setting up the aim, objectives, and research questions, I moved to start finding the issue and how it impacts the national economy of Saudi Arabia. Covered several cybersecurity frameworks and practices globally. The benefits and challenges of the cybersecurity framework and its impacts on the IoT and blockchain industry are apparent. Agent-based modeling simulation technique is also used in this report alongside the CIMF framework's importance, which is an essential aspect of cybersecurity.**

I. Introduction & Background

Introduction

The globalized age of modern civilization and industrialization has indeed introduced ample networking opportunities to business entities worldwide. People can now access anything on the internet, and the growth of the internet has reached such a point that almost no business operation could be conducted without it. In Saudi Arabia, the number of internet users is increasing, and simultaneously, the number of cyber threat incidents is also following a rampage of enhancement. This project report will shed light on how Saudi Arabian businesses are suffering due to a lack of cybersecurity frameworks in their business infrastructure.

Research-Background

It has been previously discovered that data security awareness education and training framework is relatively poor in Saudi Arabia. As a result, many eminent business enterprises of the country have been affected due to the cyber threats imposed on them, and their business operations were disrupted in the process. The rate of data breaching reached such a high peak that in 2019 almost 44% of Saudi Arabians were convinced that their professional information would likely be leaked on the internet. In 2018 only, through the Facebook data breach in Saudi Arabia, almost 29 million datasets of users were dumped on the internet, and it hampered the lives of many people [1]. There is no proper training given to the school and university students, colleagues, and office employees on cybersecurity frameworks to learn to remain protected from such threats. It was also discovered that almost 92% of Saudi Arabians never received any data security management training, so they face a high vulnerability rate in such adverse exposures [2]. Lack of anti-cybercrime law is also smoothening hackers' process to attack the citizens and business firms online, so researching this topic has become quite important.

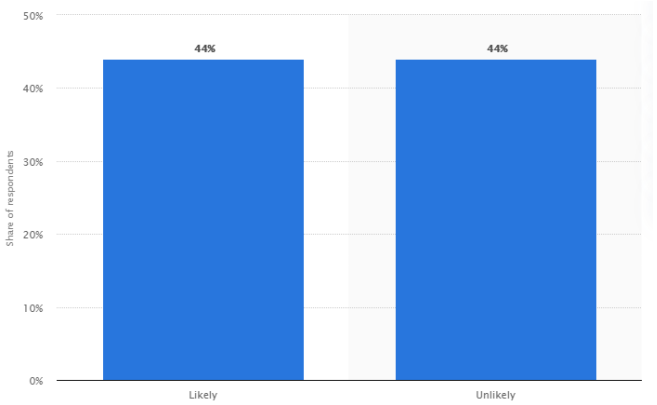


Figure 1: Saudi Arabians at Risk of Cybersecurity Breaches [3].

II. Problem Statement

Due to the rise of digital devices, cybersecurity threats in Saudi Arabia are increasing. Lack of information and data security awareness among the end-users has increased cybercrime rates in the country. The hackers have been able to erase the complete hard drive of a computer and destroy any sensitive information that has given rise to more politics and terrorism affairs. The number of internet users in the country was estimated as 22.4 million by the end of 2019. The increasing cybersecurity rate could affect these people and the e-commerce companies who operate entirely virtually with their customers.

In 2016, it was found out that their internal cybersecurity threats impact almost 40% of Saudi Arabian companies, and the most significant single cause of data loss is due to employee negligence only. In 2012, an oil company in Saudi Arabia was affected by an internal Information security incident, and a virus was sent to the computer through a USB drive [4]. Even in 2015, a study conducted by the Kaspersky

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Lab revealed that a Middle Eastern espionage firm named Dessert Falcon targeted most Saudi Arabian MNCs. The aim was to use the phishing attack and send ransomware emails to their website to increase their shoulders' malicious payload. As a result, many Saudi Arabian companies and customers' potential data were lost. Even the hard drives of their machines were erased in some cases, making it utterly difficult for them to restart their business operations. The business enterprises and the King Saud University website were hacked recently, and the personal information of 812 students was released on the internet. Therefore, it needs to be fixed so that both human malicious and non-human malicious threats could be reduced in the nation and their business infrastructure could be more trustworthy.

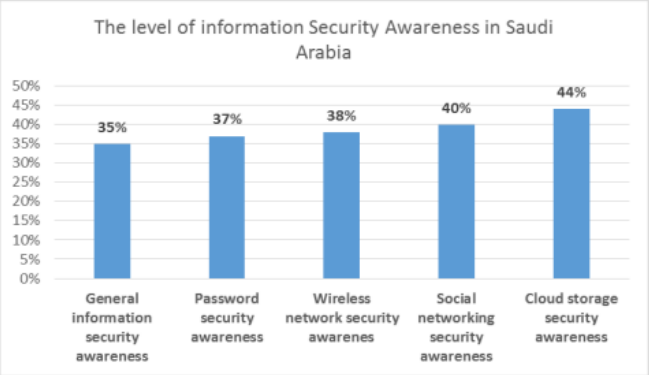


Figure 2: Cybersecurity Awareness in Saudi People [5]

Similar studies have also shown that most Saudi Arabia people are not aware of detailed information of these cybersecurity threats, so most of them only use antivirus software. It has been found out that 74.59% of Saudis use antivirus software, 12.32% use anti-phishing software, and 11.87% use anti-spam software without knowing their utilities and consequences [6]. Since the year 2012, cybersecurity threats had engulfed Saudi Arabia when the Aramco network was attacked for the first time. Almost 30,000 hard drives were erased from the computer, hindering their operational flow.

The cyberattacks must be stopped because it adversely impacts the business enterprises or on the individuals, but it hampers the national economy potentially. In Saudi Arabia only, the entire peninsula's largest economy is the oil economy, which accounts for approximately 60% of their GDP. Since the economic system is so poorly diversified, it is natural that the increasing cyber threats can destroy the national economy notably [7]. Cyberattacks can cause electrical blackouts, cause failure in military equipment, and breach national security secrets. Thus, there is a huge probability that these attacks can cause a lump sum amount of general chaos. The cyberattack boom even increased noticeably in the pandemic period. According to a research report published by Mimecast's Threat Centre, malware threats increased by 22%, and spam threats increased by 36%. Almost 95% of Saudi Arabian businesses were hit last year by cybersecurity threat incidents when the Covid19 pandemic was at its peak, and the nation was undergoing lockdown restrictions [8]. Since most businesses were operating online during that time, the rate of such attacks increased, which is why to make the e-commerce business platform more credible and trustworthy in Saudi Arabia, these attacks must be stopped.

III. Objectives

This research aims to identify the credibility of cybersecurity frameworks in Saudi Arabian business organizations.
Its objectives are;

- To identify the concept of cybersecurity framework and the vast array of categories this phenomenon has
- To explore the impact and benefits of cybersecurity framework on Saudi Arabian business infrastructure
- To discover the challenges that companies come across while implementing cybersecurity frameworks
- To recommend some probable mitigation strategies for eliminating the challenges

Thus, the research question would be;
What is the credibility of the cybersecurity framework in Saudi Arabian business companies, and how impactful is it in their existing business infrastructure?

IV. Literature Review

Concept and Types of the Cybersecurity Framework

A cybersecurity framework could be defined as the series of documents that denotes the best possible practices for a company to follow to manage its cybersecurity risks to lower the company's vulnerabilities to such exposure. In this age of modernization, companies face immense challenges every day to ensure their critical data and system's security and privacy. To address and mitigate these issues, a firm certainly needs a well-thought and structured cybersecurity plan so that their information technology details could be protected from unauthorized access [9]. There is ample cybersecurity framework guidance available in the business environment. When business leaders look into these, they become more capable of managing the IT security risks in their business infrastructure. Considering an already existing cyber-security framework or developing one internally for solely protecting the company data in the intranet, in both cases, cybersecurity frameworks could be used. There are several kinds of cybersecurity frameworks available in the market, such as;

HIPAA: It is especially applicable for the healthcare industry and those companies who work with the healthcare industries to protect health information in their system to ensure that data's confidentiality.
NIST SP 800-53: This cybersecurity framework is mainly used in federal government agencies. When a substantial

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

amount of sensitive data flows through the network system, this security framework sheds light on all the required control mechanisms to keep in place for all entities supporting these systems [10].

NIST Cybersecurity Framework: It is the most cost-effective and easy-to-use cybersecurity framework, and due to its flexible nature, it can be used in many sectors. It uses easy language so that business leaders do not need to hire an external specialist and elevate cyber-security standards for companies who do not even know how to begin protecting their datasets.

HITRUST: This is another type of cybersecurity framework applicable only for the healthcare industries and since many IT systems are fragmented. Hence, the cybersecurity measures are not consistently implemented properly, which is why HITRUST can protect those from threats of malware.
ISO 27000 Series: It is primarily used in private sector companies, and there are several standards available for this framework like ISO800-12, ISO800-14, ISO800-26, ISO800-37, and ISO800-53.
NERC1300: This framework is only applicable to bulk power supply companies. Since the power system is an essential phenomenon to modern people, this framework evaluates when the power can be lost and how long it can remain lost.
ANSI/ISA 62443: Industrial automation and control system companies use this security framework. The four-stepped framework helps the organizations check whether they are correctly adhering to the security system's requirements.

NIST Cybersecurity Framework Functions

Almost 30% of the US organizations use the NIST cybersecurity framework, and even for a structured clinical infrastructure in Saudi Arabia, the NIST framework is used. A prominent Saudi Arabian company named Saudi Aramco uses this framework to ensure a high state of governance in the overall cybersecurity approach in all the country's business organizations [11]. The National Institute of Standards and Technology provides a set of guidelines that the private sector companies can abide by for identifying, detecting, and responding to cybersecurity threats. There are five primary functions of this security framework, and they are;

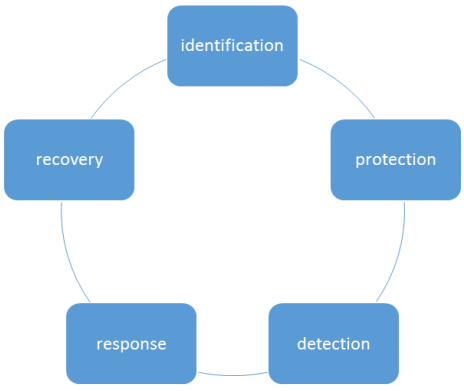


Figure 3: NIST Framework Function

Identification: Business organizations primarily should understand their internal and external environments in order to manage the cybersecurity risks in their assessments, datasets, systems, and capabilities.
Protection: The organizations then need to develop a certain amount of suitable safeguarding frameworks to limit the impact of probable cybersecurity threats.
Detection: Organisations must also apply the proper procedures for identifying and detecting the cybersecurity threats in their network as soon as possible [12].
Response: To contain the response plan of cybersecurity incidents, the companies should also develop response plans.
Recovery: There have to be effective methods for restoring the services or datasets that were hampered in the cyber threat incident.

Benefits of the Cybersecurity Framework

The cybersecurity framework provides a common language that empowers all levels of employees in their supply chain departments to understand a shared language of their cybersecurity risks. The benefits of this framework are;

1. It can protect sensitive information and confidential data from unauthorized access. It is helpful because it can protect both the company's and customers' datasets secure so that the threat to a data breach can never occur in the organization. Thus the threats of ransomware or malware could be avoided.
2. Business continuity management and security could be improved with the help of a cybersecurity framework [13]. When a cyber-threat occurs in a company, their services and datasets are disrupted, at least for a momentary time. So with an appropriate cybersecurity framework, business services would never be ceased.
3. Stakeholder confidence could be improved in the company's information security management. It is an essential spectrum because if stakeholders always fear data breaching, they would not disclose any relevant details to the company managers. So a proper security framework could increase their confidence and decrease their fears of data loss.
4. With proper security controls in place, business infrastructure and company credentials are also improved. It can enable the business to be operated in a much smoother manner, never to disrupt the workflow.
5. In case of a security breach event, the datasets could be recovered faster and efficiently, and thus a greater resilience would be achieved in the cybersecurity landscape. Despite the advanced security frameworks, companies often face malware threats. If the virus can break the firewall, then potential information could be lost, which could be recovered if a cybersecurity framework is put in place.
6. Cybersecurity requirements could be quickly and more efficiently communicated with stakeholders,

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

and thus a collective understanding could be accomplished of the company's security status [14].

7. An established cybersecurity program could help identify new opportunities for revised security standards. It would help the companies remain updated about the revised standards to obtain new customers and stakeholders through their improved data security management system.
8. It can protect the company from all kinds of threats like fraud, espionage, vandalism, or sabotage, and thus a company could get diverse solutions in their data security platform. Starting from best practice management system to testing physical infrastructure, all could be achieved by implementing a single cybersecurity framework.

Challenges of the Cybersecurity Framework

In a world where everything is accessible through the internet, the biggest challenge, government, business companies, and individuals is to keep their data safe online. There are several types of challenges in the application of cybersecurity framework such as;

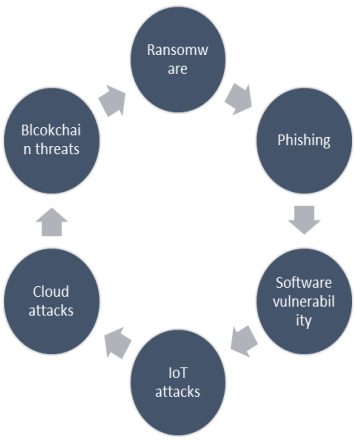


Figure 4: Challenges in Data Security

Ransomware Threats

They are the most popular ones in cybersecurity threats. It means hacking into users' data and preventing them from accessing it until a certain amount of ransom is plaid anonymously to hackers [15]. More than individuals, the business enterprises face this challenge more, and, in most cases, the hackers do not even release the data even after the ransom is paid to them.

IoT Attacks

According to IoT analytics, IoT devices like laptops, desktop phones, and intelligent security devices can transmit a large amount of data virtually over a network. With the increasing adoption of IoT devices, the rate of IoT attacks has also increased. Since it is easy to access, so the rate is higher than any other cybersecurity threat.

Cloud Attacks

Cloud services are used by many people today for both their personal and professional requirements, and the infamous iCloud attack is the most prevalent cybersecurity threat that has leaked private photos of people and most celebrities. It could pose a massive malicious threat to an organization and could also lead to their untimely collapse [16].

Phishing Attacks

It is a kind of social engineering used by hackers to steal the login credentials or credit card numbers of an individual. In this kind of attack, the hackers exploit the user's credit card until they are made aware of it, and by that time, a lump sum amount of money could get lost in thin air.

Cryptocurrency and Blockchain Attacks

Cryptocurrency and blockchain technology is used in many enterprises nowadays. As mentioned earlier, when hackers conduct the attack, then customer data and business operations could be disrupted significantly. Organizations that use these technologies would have to be more cautious because they have not yet reached their ultimate security stage.

Software Vulnerabilities

Not updating software with its latest available version could cause software vulnerabilities and weaken the system firewall, making it easier for attackers to breach the firewall and steal user data. Even the older software versions often contain lax security patches that developers fix in the newer version [17].

Cybersecurity Framework in the IoT Industry

The Internet of Things (IoT) industry is deployed in the recently developed intelligent grid infrastructure, and as a reason for that cybersecurity framework is growing. The Energy Internet (EI) is an important phenomenon because it inherits all the security vulnerabilities of an existing smart grid. The smart grid's security structure is not quite adequate for meeting the cybersecurity energy needs required by 21st-century citizens. That is why the cybersecurity framework must be so that it can provide ample privacy and security and support the EI in effective energy management [18]. Suppose an identity-based security mechanism (I-ICAAAN) can be used alongside a secured communication protocol and an Intelligent Security System for Energy Management (ISSEM). In that case, privacy and security could be certified in the IoT. In terms of the game theory, it is seen that the Nash equilibrium solution could be applicable in the ISSEM phenomenon in order to evaluate its efficiency regarding the allocations of security events. There is undoubtedly a theoretical analysis and a formal verification applied for providing the required security and data privacy to improve cyber security-based IoT.

With the help of cybersecurity, IoT's omnipresent phenomenon can enable dynamic real-time sensing and spur digital transformation to unlock the digital government's potential. It can also be used for enabling the government to become a data-driven competent government, and the policies and practices beneficial to public value and interest would be easier to provide and monitor [19]. However, the IoT policy is

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

often filled with challenges that can make the IoT policies and practices questionable. According to IoT cybersecurity policy, it can be found out that some of the major governmental agencies of the world were forwards thinking and strategic in terms of partnering and funding with sub-national governments for eradicating the IoT security challenges.

Agent-Based Modelling in Cybersecurity

To judge complex adaptive systems' behaviours, the Agent-Based Modelling (ABM) simulation technique is used. Some artificial or virtual agents represent the groups or individuals interacting with each other in the complex system, and they follow a predefined set of rules. Cyber systems are the interconnections between two or more software modules, logical circuit wiring, microchip, and between the internet and its users. These actors and interactions could be technically simulated in a model for performing the "what-if" analysis, and thus the impact of changing parameters could be predicted [20]. This model can also be utilized for analyzing the efficiency of response systems to cybersecurity threats by studying user behaviour and application characteristics for a certain period. Since in the real world, an attacker's experience could evolve with experience, so this aspect of agents' behaviour is considered in the genetic engineering algorithms. This phenomenon is helpful because the IT leaders could identify potential attackers' behaviour without evaluating all the use cases and user journeys they have hampered in the past but only through a few mutations and crossovers.

Application of Blockchain Decentralized Cybersecurity Framework

For ages, people have been struggling with exchanging information and transferring cash and other properties via internet web transfers, each of which involves a trustworthy agent. These entities shall ensure a safe exchange and be liable for any errors or violations of confidentiality. During a shift in the web transfer parameter, blockchain technology removes some central authority's need by introducing an immutable and decentralized public ledger. In the process, executing the data transactions and financial transactions becomes easier between multiple parties without any probable cause of security breaches [21]. The transactions are also verified more than once by consensus mechanisms and predefined validation, and that without the affirmation from any central authoritative intermediatory. This public directory is a hierarchical database shared between all participants of the network. It guards the manipulation of all transactions between the parties, it is cryptographically safe, and it is a permanent record of the financial or data transactions [22]. One can access the transactions when one wants. However, if they already have authenticated and linked the transactions to a blockchain, it cannot be undone or altered, making the blockchain technology irreversible and immutable. The cost is reduced in this decentralized cybersecurity framework. However, the rate of data loss is potentially reduced because a singular copy of the information is available in the system network, synchronized among all the participants.

Importance of Cybersecurity Incident Management Framework (CIMF)

There are three major components in the cybersecurity incident management framework: the technological infrastructure, the security operations centre, and the computer emergency response centre. The objectives of CIMF are to eliminate the potential cyber threats before they can occur and minimize the impact of a cybersecurity incident for achieving integrity, confidentiality, and availability of the industry's operations, activities, services, and informative assets. The appropriate implementation of CIMF at the workplace can reduce the danger of a security threat [23]. Cybersecurity incident coordination and management could be better improved in the industry where it is applied. Both direct and indirect costs associated with the cybersecurity incidents could be reduced if a CIMF is put in place. Even the detection of threats and reporting it to the executive management becomes more manageable. Its purpose is to put a consolidated nation mechanism to the management, including the coordination of potential cyber threats with the data security system [24]. It sets out diverse roles and responsibilities to the people who attempt to implement them in the workplace. The business stakeholders and the governmental agencies, critical infrastructure owners, public and private sector partners, and operators any others with whom a company connects are responsible for following the guidelines set by CIMF. Therefore, it is of much significance that the CIMF platform must enable the business enterprises to participate in a coordinated national cyber incident response fully.

V. Methodology Adopted

Methodology in research could be referred to as discussing methods applied systematically by the researcher to collect research data. This chapter occupies a pivotal role in collecting accurate data through the implementation of practical techniques and tools. It is essential to use accurate research methods to reach the desired conclusion and meet pre-identified research objectives.

Research Method

This segment of the current chapter highlights all the tools which have been applied in this study. The table below displays all the research methods used to complete this study

RESEARCH METHODS	TOOLS USED
RESEARCH PHILOSOPHY	Positivism Philosophy
RESEARCH APPROACH	Deductive Approach
RESEARCH DESIGN	Descriptive design

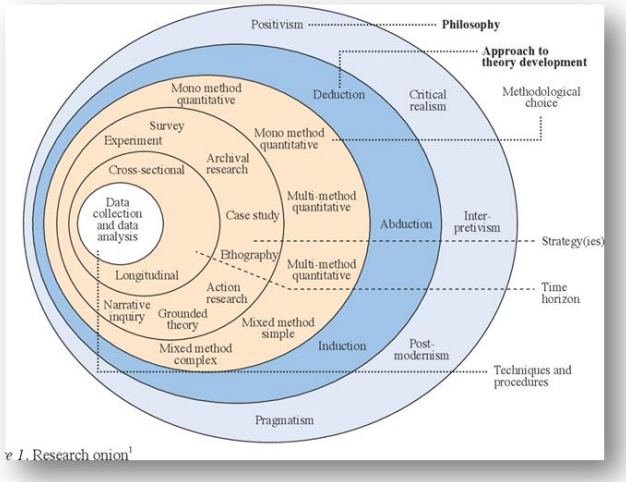
https://sites.google.com/site/ijcsis/
ISSN 1947-5500

RESEARCH STRATEGY	Thematic analysis
METHOD OF DATA COLLECTION	Qualitative Data Collection
DATA SOURCES	Secondary (books, articles, journals, and websites)
SAMPLING METHOD	Purposive Sampling
SAMPLE SIZE	Ten literary sources, including books, articles, websites

Table 1: Research Methods Used in the Study

Research Onion

Research onion being introduced by Saunders aims to elaborate various stages developing a research study. From the inside of the model to the outside, each layer explains methods adopted for the entire research process. The first and foremost benefit of research onion is that it creates a series of steps under which wide data collection methods can be understood effectively. Different stages depicted in research onion are research philosophy, research design, research approach, data collection method, and others,



e 1. Research onion[1]

Figure 5: Research Onion [25]

Research Philosophy

Research philosophy believes how data about any particular topic or phenomenon shall be collected, analyzed, and applied. From the perceptions of various scholars, research philosophy is all about developing ideas and knowledge in an efficient way that is intense while moving along various stages of the research topic. In addition to this, it also ensures accurate identification of the core research principles. Among the four basic types of research philosophies; Interpretivism, positivism, post-positivism, and realism, the researcher has selected the positivism approach.

The Rationale for Selecting this Philosophy: Positivism philosophy has been chosen by rejecting the remaining paradigms. Positivism allows exploring real-life aspects through a series of critical discussions for investigating and interpreting accumulated data. It has become possible for the researcher to conduct this scientific study of Cyber Security Frameworks through the logical extraction of ideas from relevant sources.

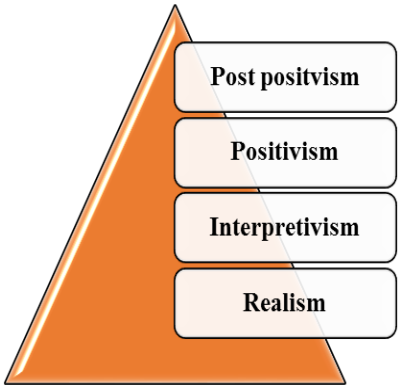


Figure 6: Research Philosophies

Research Approach

Research approaches are procedures and plans for research that span the research steps from broad assumptions to detailed data analysis procedures, collection, and interpretation. Mainly two types of research approaches are used by the researchers while conducting research studies. Under the inductive approach, the premises are viewed through some relevant evidence but without full assurance of the conclusion's truth [26]. On the other hand, the deductive approach revolves around theories, and it involves testing those existing theories.

The Rationale for Selecting this Philosophy: In the current study, the researcher has selected the deductive approach by ignoring the inductive one. Using this, he has become able to reach a logical conclusion. From different analysts' opinions, deductive reasoning goes in the similar pathway as that of the conditionals and connects research premises with a conclusion [27].

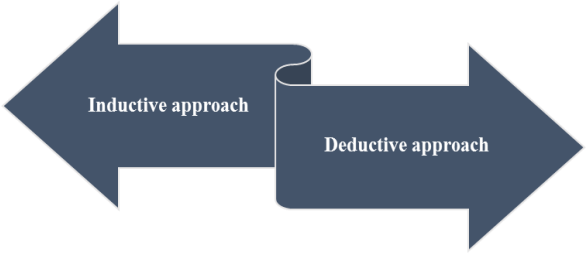


Figure 7: Research Approach

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Research Design
Research design is a framework of overall research strategies utilized for carrying out research studies. This defines a logical and succinct plan to tackle established research questions and objectives through data accumulation, interpretation, analysis, and discussion. As per research scientists' comments, selecting appropriate research designs helps researchers synchronize various components concerning the topic [28]. In the current study, the researcher has selected an Explanatory research design as it provides a functional explanation and solution to the problem, which demands priorities.

The Rationale for Selecting this Design: The researcher has chosen exploratory design because it has focused on a detailed explanation of various aspects of the topic, Cyber Security framework. By adopting exploratory design, the researcher has gathered a wide range of conceptual information to answer the research questions through requirement fulfillment and suitable solutions.

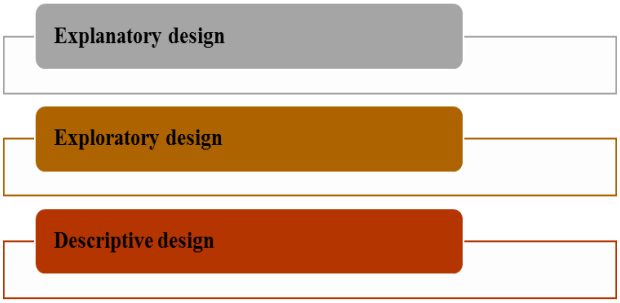


Figure 8: Research Design

Data Analysis Method
Data analysis methods are specific procedures used to identify, select and analyze information about a given topic. It is the pathway through which the researchers conduct their research and evaluate the research problems. Regarding the research topic, research philosophy, and design, the researcher has developed the paper based on qualitative data analysis. Qualitative research mainly relies on observation, visual or textual analysis. The research has found this method highly effective in demonstrating rich, intuitive secondary data to answer the research question and accomplish the aim. One key advantage of qualitative data collection is that it requires minimum financial resources, whereas the primary disadvantage is that this method raises questions about the research's credibility.

The Rationale for Selecting this Method: The researcher in the current study has chosen the qualitative data analysis method because it contributes to content analysis. As the study has been based on explanatory research design, content analysis from textual or visual sources is exceptionally relevant in this case. Moreover, this method would enable the researcher to complete the study within the stipulated time frame.

Data Sources
By considering the research topic and objectives, the researcher has selected a secondary data collection method for assimilating accurate information. Insightful secondary data have been gathered from different secondary data sources such as online articles, journals, books, and websites regarding several Cyber Security framework dimensions. In a more detailed manner, the researcher has used various researchers' existing literary works on the current topic to examine the research questions specifically.

Sampling Method
In research, the sample represents a population to ensure that the findings can be generalized from the sample to the entire population. As the present study is based on secondary qualitative data, the researcher has opted for ***Purposive sampling*** under Non-probability sampling. According to a wide range of research specialists, Purposeful sampling is used in qualitative research papers to select and identify the information-rich cases about the phenomenon of interest. The researcher has used existing judgments of various other experts to analyze the collected data. One of the critical advantages of purposive sampling is that it does not involve real-time data collection procedures. Thus it is one of the most time effective and cost-effective sampling methods.

Ethical Issues
Research ethics mainly govern the necessary standards to conduct scientific studies. Discussion of ethical principles of justice, beneficence, and autonomy are central pillars to the ethical review. It is crucial to adhere to the ethical principles for safeguarding the research components' rights, dignity, and welfare. For the present research study, the knowledge collected from different secondary data sources has not been used commercially. The articles, books, and journals used to jot down relevant data have been accumulated from verified sources. It can be said that the researcher has complied with the standards of the Data Protection Act 1998 in order to avoid social and ethical issues.

Timetable Chart
The research timetable is presented in the form of a Gantt chart.
[Refer to appendix]

Research Limitation
While conducting the research study of Cyber Security Frameworks, the researcher has experienced certain obstacles that have reduced the study's quality and efficiency. There has been a lack of optimum authentic information about the main topic. Apart from these, throughout the entire study, the researcher has faced inadequate financial resources, which is one of the primary reasons for the shortage of information. Additionally, the given time frame has also been inadequate to

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

complete the topic in a scrutinized way. All these aspects have prohibited the researcher from conducting quantitative data analysis, making the research more feasible.

This chapter mainly exhibits various analytical tools and methods that have enabled the researcher to analyze the topic accurately. By implying practical research philosophy, design, method, and approach, the researcher has developed a logical conclusion. On the contrary, the researcher has come across particular challenges like lack of financial resources and time, which have acted as impediments for successfully elucidating the research topic.

VI. Results – Finding of the Project

The research study's present segment deals with in-depth analysis of the accumulated data using the secondary qualitative data analysis method. In this regard, the researcher has developed perceptive themes on different Cyber Security Frameworks genres through which the information gathered has been elucidated on a critical note. Different textual and visual sources have been utilized to make the data analysis more reliable and credible. Below are presented the data on Cyber Security frameworks in the form of themes:

Cybersecurity is showing emerging importance to the Health Services of Saudi Arabia

Saudi Arabia is one of the fastest-growing countries in the Middle East in terms of technological progress. It can be found that the health and social care (HSC) system of Saudi Arabia has come across enormous developments over the last ten years, including the use of Information technology (IT). On a detailed note, increasing information technology use has made the healthcare IT infrastructure vulnerable to potential risks like data theft and unauthorized information access. In this aspect, cybersecurity has occupied a pivotal role in the Health and rescue services in Saudi Arabia. By aligning cybersecurity and patient safety initiatives, the Saudi Arabian HSC organizations are promoting patient safety and privacy [29]. In addition to all these, the application of cybersecurity frameworks like HIPAA, GDPR, and FISMA in HSC also ensures continuity in delivering high-quality care services. Some renowned health care organizations in Saudi Arabia, such as King Faisal Specialist Hospital and Research Centre, National Guard Health Affairs, The Public Institution for Social Security, are using application security, antispyware software, firewalls, monitored network access, and two-step authentication system for improving their Cyber Security systems. In addition to this, by providing frequent training to the IT staff, the HSC entities in Saudi Arabia have established a security culture within the health and social care system.

Cybersecurity is Implemented in Smart Grids

To improve reliability and efficiency, Saudi Arabia's government has made a notable investment in developing a more innovative and automated power system using Cyber Security tools. Through Information Communications Technology (ICT), the power system operators can now control tasks based on data received from remote facilities in the country [30]. Smart grid cybersecurity is a recently developed digital infrastructure that sites above the existing electrical grids. Supervisory control and data acquisition (SCADA) systems have been introduced in different industries of Saudi Arabia (especially oil and gas industries) to send control commands to the switching devices for online monitoring and operations. However, the energy industries in Saudi Arabia are regulated heavily at multiple levels regarding IT use. Thus, protection circuits, synchronization systems, and control systems are applied to ensure cyber safety, performance, and operational efficiency. Thus, Saudi Arabian Energy industries are indulged in cybersecurity research and development to stabilize smart grids.

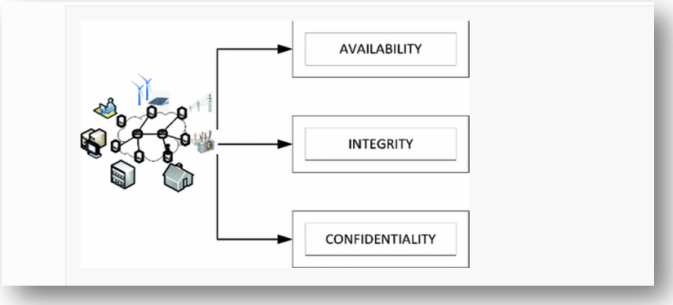


Figure 9: Objectives of Cybersecurity in Smart Grid [31]

There exist vulnerabilities in the cybersecurity infrastructures of Saudi Arabian companies

In computer security infrastructures, vulnerability can be recognized as the weakness exploited by threat actors like attackers, malware, or ransomware. The IT sector, energy sector, and healthcare sector in Saudi Arabia have been adopting security measures for protecting their cyber networks from unauthorized access. For a country like Saudi Arabia, potential threats and risks posed to cyberspace mainly revolve around state-sponsored attacks, cybercrimes, cyber terrorism, and digital data interception. Cyber in the country is rising faster because of the increasing use of digital services, lack of optimum information security knowledge, weak cybersecurity infrastructure, and employee errors. Below are highlighted some of the very cybersecurity vulnerabilities prevalent in Saudi Arabia:

1. Inaccurate Input Validation: In cybersecurity networks, input validation is an effective technique to add an extra security layer for preventing attackers' access. However, inaccurate input validation leads to illegitimate data into the cyber system of IT and energy companies in Saudi Arabia.

2. Buffer Overflow: Because of accurate input validation, the system experiences buffer overflow vulnerabilities, which may arise due to programming errors. Moreover, this gives rise to more vulnerabilities like heap-based or stack-based buffer overflow, allowing remote code execution on the host network [32].

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

3. Lack of Bound Checking: The absence of proper bound checking results in crashed and misbehaving programs. On the other hand, results due to invalid inputs are inserted into the array, causing the programs' interrupted service [33]. This allows the attackers to inject unexpected data and modification of the program execution.

4. Poor Quality of Coding: It has been found that several attacker groups in Saudi Arabia have become successful in penetrating the weak cybersecurity infrastructures of companies because of their poor coding quality. This makes the programs vulnerable because good programming practices and network maintenance practices are not followed. Additionally, the malformed input vulnerabilities caused due to poor coding practices create Null Pointer Dereference where the pointer is NULL, although it is expected to be valid [34].

5. Improper Authentication: Cyber-attacks happen in Saudi Arabian business entities, particularly educational, IT, and energy companies, because of vulnerabilities like faulty authentication mechanisms. The software allows other methods for bypassing authentication, and the attackers exploit this to receive unauthorized access to the network. In this way, vital information and business intellectual properties can be extracted by modifying the client credentials [35].

6. Poor Network Design: A poorly designed network that does not deploy in-depth defense strategies can be regarded as another significant vulnerability to Saudi Arabian companies' poor cyber network infrastructures. These types of networks do not deploy multiple security layers and use relatively flat networks without any zones, perimeters and port security. It widens the pathways for the attackers to invade and steal sensitive data.

7. Firewall issues: Improperly configured firewalls allow unauthorized data to move among multiple networks without proper checks. The attackers use this opportunity and allow the malware to be spread across the networks. Non - existent firewalls cause leakage of confidential business information which unauthorized individuals' access.

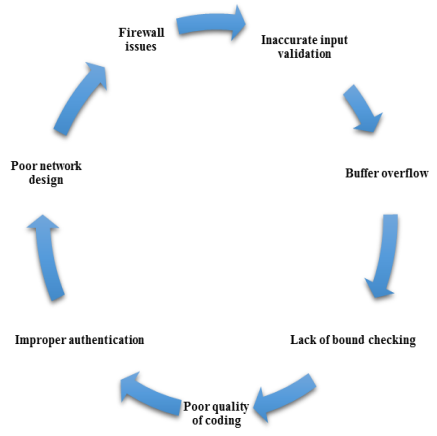


Figure 10: Common Cybersecurity Vulnerabilities that occur in Saudi Arabia

Known Cyberattacks in Saudi Arabia

Over recent years, some of the highest numbers of cyber threat incidents have been found in Saudi Arabia. In 2015, over 5500 IT specialists from 26 different countries worldwide had identified that Cybersecurity incidents have severely impacted 40% of companies in Saudi Arabia. On the other hand, in 2012, Saudi Arabian Oil Company's (Saudi Aramco) computer network had been compromised the malware was inserted into the organization's network through a flash drive [36]. This attack had erased the hard drives of the systems and also destroyed enormous essential data. In addition to this, during 2015, Kaspersky Lab discovered cyber espionage named Desert Falcons, whose primary aim was to target Middle East countries with a particular focus on Saudi Arabia to be its activity platforms in Saudi. In this case, phishing attacks via social networks and e-mails were used for sending malicious payloads.

Furthermore, King Saud University's (KSU) official website got hacked by unknown groups of hackers. A robust database of 812 students was hacked at first and then leaked on the internet. The country is becoming a significant target of cyber-attacks, including 'Shamoon Virus', which destroys computers by removing disks. This has posed a significant hit in both the petrochemical firms and government ministries in 2017. Recently, with the Corona Virus boom in 2021, Saudi Arabia has visualized a surge in cyber-attacks due to improper maintenance of computer networks because of company lockdown. There has been a sharp rise in malware (37%) and ransomware (29%) in the Middle East, particularly in Saudi Arabia. According to several IT specialists of the country, the need for scalable and resilient cloud solutions has exponentially increased since March 2020 as several organizations are managing remote work conditions in an unprepared manner. Thus, most Saudi Arabian companies are non - compliant with frameworks like ISO 27001, ISO 27002, SOC2, HIPAA, HITRUST, and NERC1300. It can be commented that with an increase in the numbers of internet users in Saudi Arabia, the chances of cybersecurity threats have been increasing in leaps and bounds.

The chapter is based on qualitative data analysis, where various perspectives of other scholars have been taken into account to analyze the topic. The accumulated qualitative data from different literary sources have been explained in short informative themes for collecting core elements of the research topic. In this way, it has become easier for the researcher to answer the framed research question persuasively.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

VII. RECOMMENDATIONS

SMART Recommendation 1: Creating Secured Cyber Ecosystem

Specific	Measurable	Achievable	Realistic	Time Bound
This reccomm-endation is specific because it would allow the companies to have a robust cyber-security method-ology where the cyber devices will work with each other for preventing future cyber attacks	It is measurable because a robust cyber ecosystem exhibits three symbiotic structures using which the companies can measure their cybersecurity performance; Authentication, Interoperability and Automation	This strategy is easily achieved by implementing advanced security measures like Blockchain technology, solid firewalls, and high-quality coding.	This recommendation is realistic because it is possible to be achieved quickly and would enhance cyber resilience and decision-making procedures.	The time limit for implementing this strategy is two months

Table 2: Recommendation 1

SMART Recommendation 2: Providing Intensive Training to IT Employees of Saudi Arabian Companies

Specific	Measurable	Achievable	Realistic	Time Bound
This recommendation is specific because it would increase the cybersecurity awareness and skills among employees through proper education and mentoring	It is measurable because the post-optimized skills and increased efficiency gained by employees after training in developing advanced security methods will strengthen the existing cybersecurity strategies.	It is achievable by frequent coaching sessions with peers and leaders, information sharing, in-depth learning, and continuous monitoring	It is a hyper-realistic strategy because providing cybersecurity training to employees is feasible to prevent a data breach, intellectual property disclosure, and information leakage.	The time limit for implementing this strategy is three months

Table 3: Recommendation 2

SMART Recommendation 3: Strengthening Regulatory Strategies

Specific	Measurable	Achievable	Realistic	Time Bound
This strategy is specific because it directly impacts compliance with regulatory standards (ISO 27001, ISO 27002, SOC2, HIPAA, HITRUST, and NERC1300) by addressing the non-compliances in various entities.	It is measurable because by ensuring cyber regulatory strategies, the business entities can comply with the necessary cybersecurity frameworks.	This strategy can be efficiently achieved by introducing inter-business policies, standards, and governing rules	It is realistic because companies can formulate rules and regulations concerning cybersecurity frameworks for achieving resilient cyber programs	The time limit for implementing this strategy is 1.5 month

Table 4: Recommendation 3

VIII. CONCLUSION

From the study above, it could be concluded that ensuring a robust Cyber Security Framework is a highly essential business practice that contemporary organizations need to follow for managing cyber threats. It has been found that such frameworks (ISO 27001, ISO 27002, SOC2, HIPAA, HITRUST, NERC1300) upgrade the ethical standards of a business entity by reducing the exposure to series of vulnerabilities. In a country like Saudi Arabia, where the use of information technology has become prevalent in almost all aspects of life and with the growth of companies has tripled, Saudi Regulatory bodies (SAMA, NCA, MCIT & CMA) came up with regulatory and cybersecurity frameworks which are an abstract of NIST & CIS to address several threats. It can be identified that the internet security awareness among the IT employees of Saudi Arabian companies is considerably low but better than most of the other nations, and thus they lack organized threats. Some specific sectors in the country, including energy, education, financial, and healthcare, can be identified as top-notch targets for the attackers. In this context, various cybersecurity threats that need to be addressed

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

immediately are phishing, cloud attacks, IoT attacks, ransomware threats, and software crashes. Through secondary qualitative data analysis, it can be known that the prevailing vulnerabilities to the Cyberinfrastructure of Saudi Arabian entities are inauthentic input validation, poor coding practices, weak network designs, firewall issues, buffer overflow, and others. The COVID 19 scenario was challenging across the globe for almost all companies to accommodate work from home securely. This has uplifted the cybersecurity attacks because of un-strategic working conditions in some companies, thereby leading to the disclosure of credential information, intellectual properties, confidential data to unknown groups. Continuous training, regulatory strategies, and the cyber ecosystem can upgrade the cybersecurity performance of companies efficaciously.

IX. References

[1]. Alassafi, M. O., Alharthi, A., Walters, R. J., & Wills, G. B. (2017). A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies. *Telematics and Informatics*, *34*(7), 996-1010.
Retrieved From:
https://eprints.soton.ac.uk/412432/1/A_framework_for_critical_security_factors_that_influence_the_decision_of_cloud_adoption_by_Saudi_government_agencies_003_.pdf

[2].Statista (2021) *Respondents in risk of data loss*
Retrieved From:
https://www.statista.com/statistics/1041552/saudi-arabia-likelihood-breach-personal-data

[3]. Statista (2021) *Respondents in risk of data loss*
Retrieved from:
https://www.statista.com/statistics/1041552/saudi-arabia-likelihood-breach-personal-data

[4]. Research gate (2021) *Saudi Aramco cyber-attacks*
Retrieved from:
https://www.researchgate.net/publication/326975373_Cyber_Attack_on_Saudi_Aramco

[5]. IJCSI (2021) *Cyber security detailed knowledge in Saudi Arabians*
Retrieved from:

https://www.ijcsi.org/papers/IJCSI-13-6-129-135.pdf

[6]. Core (2021) *Cybersecurity incidents in Saudi Arabia*
Retrieved from:
https://core.ac.uk/download/pdf/322474772.pdf

[7]. Mawgoud, A. A., Taha, M. H. N., Khalifa, N. E. M., & Loey, M. (2019, October). Cyber security risks in MENA region: threats, challenges and countermeasures.
In *International Conference on Advanced Intelligent Systems and Informatics* (pp. 912-921). Springer, Cham.
Retrieved from:
https://www.researchgate.net/profile/Ahmed_A_Mawgoud/publication/336219647_Cyber_Security_Risks_in_MENA_Region_Threats_Challenges_and_Countermeasures/links/5fb379fe299bf10c3686141a/Cyber-Security-Risks-in-MENA-Region-Threats-Challenges-and-Countermeasures.pdf

[8]. Computer Weekly (2021) *Cybersecurity attacks increase during pandemic*
Retrieved from:
https://www.computerweekly.com/news/252489175/Saudi-Arabia-sees-cyber-security-boom-as-coronavirus-bites#:~:text=As%20the%20virus%20ramped%20up,started%20spreading%20in%20the%20region

[9]. Sohal, A. S., Sandhu, R., Sood, S. K., & Chang, V. (2018). A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Computers & Security*, *74*, 340-354.
Retrieved from:
https://research.tees.ac.uk/ws/files/16202354/cybersecurity_CandS_accepted.pdf

[10]. Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178-188.
Retrieved from:
https://www.researchgate.net/profile/Srinivas_Jangirala/publication/328183318_Government_regulations_in_cyber_security_Framework_standards_and_recommendations/links/5c1d53d892851c22a33d339e/Government-regulations-in-cyber-security-Framework-standards-and-recommendations.pdf

[11]. Barrett, M. P. (2018). Framework for improving critical infrastructure cybersecurity. *National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep*.
Retrieved from:
http://isawaterwastewater.com/wp-content/uploads/2018/08/WWAC-2018-NIST-Barrett_final.pdf

[12]. Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: a case study. *The Journal of Supercomputing*, *74*(10), 5171-5186.
Retrieved from:
https://link.springer.com/article/10.1007/s11227-018-2479-2

[13]. Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Information Segmentation and Investing in Cybersecurity. *Journal of Information Security*, *12*(1), 115-136.
Retrieved from:
https://academic.oup.com/cybersecurity/article-pdf/6/1/tyaa005/32979473/tyaa005.pdf

[14]. Zhang, Z. J., He, W., Li, W., & Abdous, M. H. (2021). Cybersecurity awareness training programs: a cost–benefit analysis framework. *Industrial Management & Data Systems*. Retrieved from: https://www.emerald.com/insight/content/doi/10.1108/IMDS-08-2020-0462/full/html

[15]. Ghafur, S., Grass, E., Jennings, N. R., & Darzi, A. (2019). The challenges of cybersecurity in health care: the UK National Health Service as a case study. *The Lancet Digital Health*, *1*(1), e10-e12. Retrieved from: https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30005-6/fulltext

[16]. Mantha, B. R., & de Soto, B. G. (2019). Cyber security challenges and vulnerability assessment in the construction industry. In *Creative Construction Conference 2019* (pp. 29-37). Budapest University of Technology and Economics. Retrieved from: https://repozitorium.omikk.bme.hu/bitstream/handle/10890/13197/CCC2019-005.pdf?sequence=1

[17]. Mendhurwar, S., & Mishra, R. (2019). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. *Enterprise Information Systems*, 1-20. Retrieved from: https://www.tandfonline.com/doi/abs/10.1080/17517575.2019.1600041

[18]. Mozzaquatro, B. A., Agostinho, C., Goncalves, D., Martins, J., & Jardim-Goncalves, R. (2018). An ontology-based cybersecurity framework for the internet of things. *Sensors*, *18*(9), 3053. Retrieved from: https://www.mdpi.com/1424-8220/18/9/3053/pdf

[19]. Radanliev, P., Montalvo, R. M., Cannady, S., Nicolescu, R., De Roure, D., Nurse, J. R., & Huth, M. (2019). Cyber Security Framework for the Internet-of-Things in Industry 4.0. Retrieved from: https://www.preprints.org/manuscript/201903.0111/download/final_file

[20]. Thompson, B., & Morris-King, J. (2018). An agent-based modeling framework for cybersecurity in mobile tactical networks. *The Journal of Defense Modeling and Simulation*, *15*(2), 205-218. Retrieved from: https://journals.sagepub.com/doi/pdf/10.1177/1548512917738858

[21]. Han, Y., Wang, Z., Ruan, Q., & Fang, B. (2018). Sapiens chain: a blockchain-based cybersecurity framework. *arXiv preprint arXiv:1811.10868*. Retrieved from: https://arxiv.org/pdf/1811.10868

[22]. Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine*, *7*(2), 18-21. Retrieved from: http://www.smohanty.org/Publications_Journals/2018/Mohanty_IEEE-CEM_2018-Mar_The-Blockchain.pdf

[23]. Onwubiko, C., & Ouazzane, K. (2020). SOTER: A playbook for cybersecurity incident management. *IEEE Transactions on Engineering Management*. Retrieved from: http://repository.londonmet.ac.uk/5358/1/TEM%20paper%20on%20SOTER_Camera_Ready%20Version_1.5_Nov2019.pdf

[24]. Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems*, *143*, 113476. Retrieved from: https://www.sciencedirect.com/science/article/pii/S0167923620302311

[25]. Saunders, M. N., Lewis, P., Thornhill, A., & Bristow, A. (2015). Understanding research philosophy and approaches to theory development. Retrieved on 18th March 2021 from: http://oro.open.ac.uk/53393

[26]. Ørngreen, R., & Levinsen, K. (2017). Workshops as a Research Methodology. *Electronic Journal of E-learning*, *15*(1), 70-81. Retrieved on 18th March 2021 from: https://files.eric.ed.gov/fulltext/EJ1140102.pdf

[27]. da Silva, C. S. R. (2017). Research design-the new perspective of research methodology. *Journal of Education, Society and Behavioural Science*, 1-12. Retrieved on 18th March 2021 from: http://journaljesbs.com/index.php/JESBS/article/download/16285/30216'

[28]. Cuervo-Cazurra, A., Mudambi, R., Pedersen, T., & Piscitello, L. (2017). Research methodology in global strategy research. *Global Strategy Journal*, *7*(3), 233-240. Retrieved on 18th March 2021 from: http://centaur.reading.ac.uk/84151/3/CuervoMudambiPedersenPiscitello_Method_23May.pdf

[29]. Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, *14*(1), 129. Retrieved on 18th March 2021 from: https://www.academia.edu/21451805/Comparative_Analysis_of_Various_National_Cyber_Security_Strategies

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

[30]. Sun, C. C., Hahn, A., & Liu, C. C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, *99*, 45-56. Retrieved on 18th March 2021 from: http://credc.com/sites/default/files/papers/2017_Q4_ContMonitor_published.pdf

[31]. Bîrleanu F.G., Anghelescu P., Bizon N., & Pricop E. (2019). Cyber Security Objectives and Requirements for Smart Grid. In: Kabalci E., Kabalci Y. (eds) Smart Grids and Their Communication Systems. Energy Systems in Electrical Engineering. Springer, Singapore. Retrieved on 18th March 2021 from: https://doi.org/10.1007/978-981-13-1768-2_17

[32]. Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32-74. Retrieved on 18th March 2021 from: https://www.tandfonline.com/doi/pdf/10.1080/23742917.2016.1252211

[33]. Khan, S. R., & Gouvia, L. B. (2017). Cybersecurity attacks: Common vulnerabilities in the critical infrastructure. *PASJ International Journal of Computer Science (IIJCS)*, *5*(6), 7-14. Retrieved on 18th March 2021 from: https://www.researchgate.net/profile/Luis_Borges_Gouveia/publication/319800931_Cybersecurity_Attacks_Common_Vulnerabilities_in_the_Critical_Infrastructure/links/5db861154585151435d15c7b/Cybersecurity-Attacks-Common-Vulnerabilities-in-the-Critical-Infrastructure.pdf

[34]. Ogie, R. I. (2017, February). Cyber security incidents on critical infrastructure and industrial networks. In *Proceedings of the 9th International Conference on Computer and Automation Engineering* (pp. 254-258). Retrieved on 18th March 2021 from: http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1217&context=smartpapers

[35]. Khan, S. R., & Gouvia, L. B. (2017). Cybersecurity attacks: Common vulnerabilities in the critical infrastructure. *PASJ International Journal of Computer Science (IIJCS)*, *5*(6), 7-14. Retrieved on 18th March 2021 from: https://www.researchgate.net/profile/Luis_Borges_Gouveia/publication/319800931_Cybersecurity_Attacks_Common_Vulnerabilities_in_the_Critical_Infrastructure/links/5db861154585151435d15c7b/Cybersecurity-Attacks-Common-Vulnerabilities-in-the-Critical-Infrastructure.pdf

[36]. Alzahrani, A. and Alomar, K., 2016. Information security issues and threats in Saudi Arabia: A research survey. *International Journal of Computer Science Issues (IJCSI)*, *13*(6), p.129. Retrieved on 18th March 2021 from: https://www.ijcsi.org/papers/IJCSI-13-6-129-135.pdf

X. Appendix

Research Timeline

Activities	**1st to 2nd week**	**3rd to 4th weeks**	**5th to 6th weeks**	**7th to 8th week**	**9th to 10th week**	**11th week**
Topic selection						
Research structure						
Literature review						
Primary/Secondary data collection						
Formation of the research plan						
Recognition of the research technique						
Data analysis						
Conclusion and recommendation						
Submission of the research report						

https://sites.google.com/site/ijcsis/
ISSN 1947-5500