Sana'a University Journal of Applied Sciences and Technology https://journals.su.edu.ye/index.php/jast
Vol. 1 | No. 3 | Page 234 – 252 | 2023 | ISSN : 2958-9568
Doi:10.59628/jast.v1i3.248

Suggestion Cybersecurity Framework (CSF) for Reducing Cyber-Attacks on Information Systems

Abdulkarem Yahya Abohatem [1,*], Fadl M.M. Ba-Alwi[2], Abdualmajed Ahmed G. Al-Khulaidi [3]
[1,2] Information System Department, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen.
[3] Software Engineering, Department of Computer Science, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen.
*Correspond author: *Abdulkareem.abohatem@ptc.gov.ye*

ARTICLE INFO
Article history:
Received: February 19, 2023
Accepted: July 29, 2023
Published:, August, 2023

KEYWORDS
1. Cybersecurity
2. (CSF) Cybersecurity Framework
3. (CA)Cyber-Attack

ABSTRACT
This study conducts a comprehensive analysis of different standards frameworks in cybersecurity to identify best practices and international standards. The primary objective is to propose an appropriate cybersecurity framework that aligns with global standards, effectively reducing the risks of cyberattacks and threats to data, information, networks, and devices within institutions. By enhancing cybersecurity, the framework aims to safeguard infrastructure. It further contributes to improved management of cybersecurity risks by incorporating the best global practices and local cybersecurity legislation. Through an examination of various cybersecurity frameworks, including NIST 800-53Ar4, COBIT, and ISO27002, the study finds that NIST 800-53Ar4 is the most effective framework. The researcher recommended adopting a hybrid approach that combines elements from multiple frameworks and standards

CONTENTS

1. Introduction:

The technological revolution has proved to be a boon, on the other hand, the internet and its users have become more vulnerable to cyberattacks. This has created a greater need for cybersecurity awareness to protect users from online fraud and cybercrime. Many government organizations have been managing cybersecurity without a defined process.

Critical infrastructure (Pekka N., 2022) is the most important threat to cyberinfrastructure (CI). In recent years, attacks against critical infrastructure, critical information infrastructure, and the Internet have become ever more frequent, complex, and targeted because perpetrators have become more professional.

Attackers can inflict damage to or disrupt physical infrastructure by infiltrating digital systems that control physical processes,

damaging specialized equipment and disrupting vital services without physical attack. These threats continue to evolve in complexity and sophistication.

(Yuchong Li & Qinghui Liu, 2021) At present, most of the economic, commercial, cultural, social and governmental activities and interactions of countries, at all levels, including individuals, non-governmental organizations and government and governmental institutions, are carried out in cyberspace.

Recently, many private companies and government organizations worldwide have been facing the problem of cyberattacks and the danger of wireless communication technologies. In today's highly technology-dependent world, safeguarding electronic data from cyberattacks has become an extremely challenging issue. To this end, various organizations have used various solutions to prevent damage caused by cyberattacks.

Cybersecurity follows real-time information on the latest IT data.

Thus, Maurice and Doris and Francisco and Mónica D. 2021) stated that organizations will design cybersecurity processes to provide structures and methodologies for protecting important systems, data, information, networks, and devices from external security threats.

Businesses rely on data to survive in a competitive market, and data is constantly in danger of loss or theft. The loss of valuable data leads to negative consequences for both individuals and organizations. Cybersecurity is the process of protecting sensitive data from damage and theft. A range of procedures and standards should be followed to successfully achieve the objectives of implementing cybersecurity at different levels.

Satisfactory cybersecurity protection encompassing all data security solutions can only be achieved by adopting a cybersecurity framework that provides a structure and methodology for protecting critical digital assets.

Reviewing the experiences of other businesses in the industry helps organizations adopt the most relevant cybersecurity standards and frameworks.

(The D. E. F. D., 2021) cybersecurity framework (CSF) helps indicate procedures to manage cybersecurity risk and align policy, business, and technological approaches across all parts of the organization.

The cybersecurity framework has been proven to provide the best practices for building security infrastructure and organizational systems.

(Gaganjot K S.& Malka N. Halgamuge & others, January 2020) the authors determined that the government sector is the main application area in cybersecurity and is more susceptible to cyberattacks.

They described cybersecurity issues and solutions and demonstrated that the majority of applications in this area are from the government and public sector (17%), whereas transportation and other areas have a minor percentage (6%).

2. Materials and Methods

Comparative analysis of cybersecurity capability maturity model literature. Comparative document analysis helped identify gaps in the existing information systems and a literature survey of Yemen Telecom.

1. Studies on different standards frameworks.
2. Theoretical analysis of applying cybersecurity.
3. Suggestion of optimal framework.
4. Analysis propose of a framework of newly modified.

3. Literature review

3.1 Cybersecurity

(Mohammed. I. Alghamdi, April 2021) Cybersecurity can be partially described as solving problems and partially mitigating risks. In addition to network attacks, such as PC viruses, knowledge breaks, Distributed Denial of Service (DDoS), and numerous other assault vectors.

(YuchongLi & QinghuiLiu, 3 September 2021) Cyber security is an important issue in the infrastructure of every company and

organization. In short, a company or organization based on cybersecurity can achieve high status and countless successes because this success is the result of the company's capability to protect private and customer data against a competitor. The organizations and competitors of customers and individuals are abusive.

A company or organization must first and foremost provide this security in the best way to establish and develop itself.

(Maurice F. D.& Doris E.& Francisco F.& Mónica D., 2021) The National Institute of Standards and Technology (NIST) define cybersecurity as "The process of protecting information by preventing, detecting and responding to attacks".

'Cybersecurity,' also written as 'cyber security' is main the domain of studying and implementing methods against cyberattacks, and often includes references to protecting networks and devices.

(Amy Mahn & Daniel Topper & Stephen Quinn &Jeffrey Marron&, August 2021) Cybersecurity is an important and amplifying component of an organization's overall risk management process.

(Adamu Abdullahi Garba, February 2021) Cybersecurity is a method of protecting organization assets, through the identification of threats that can compromise the critical information stored in the organization's systems, it also involves the protection, identification, and response to threats.

Cybersecurity includes the ability to detect, mitigate, and stop vulnerabilities, risks, or attacks on devices, networks, and data. It also includes knowing how to respond in the event of an attack.

Cybersecurity is a proactive and reactive measure for the protection of critical data and infrastructure from attacks, damage, and unauthorized access, which is the top priority for the nation.

The field of cybersecurity is concerned with creating and sustaining processes that identify emerging threats and provide the most practical and cost-effective countermeasures.

Cybersecurity plays an important role in the field of information technology. Securing information and transactions has emerged as one of the biggest challenges in recent times.

3.2 Critical Infrastructure

(Martti L. & Pekka N.,2022) CI encompasses the structures and functions that are vital to society's uninterrupted functioning. It comprises physical facilities and structures as well as electronic functions and services. Critical infrastructure systems (CISs) comprise a heterogeneous mixture of dynamic, interactive, and nonlinear elements.

The United Kingdom States that critical infrastructure consists of facilities, systems, sites, information, people, networks, and processes necessary for a country to function and upon which daily life depends. It also includes some functions, sites, and organizations that are not critical to the maintenance of essential services, but that need protection due to the potential dangers they could pose to the public in the event of an emergency.

(Siegfried M., 2022) Critical Infrastructures and Key Assets (the Strategy) takes steps to reduce the nation's vulnerability by protecting its critical infrastructures and key assets from physical attack. Critical infrastructures are systems and assets, both physical and virtual.

(Petri V. Martti L. & Antti K., 2022) Critical infrastructure (CI) is a vital asset for the economy and society's functioning, covering sectors such as energy, finance, healthcare, transport, and water supply.

Governments around the world have invested considerable effort in the continuous operation, maintenance, performance, protection, reliability, and safety of Cl. However, the vulnerability of the CI to cyberattacks and technical failures has become a concern.

(Divine S. A., March 2018) from NIST, defined Critical Infrastructure (CI): All systems and assets, both physical and virtual, which are vital to the normal social function of a nation in a way such that incapacitating them in some way

will cause a debilitating impact on security, national economic security, national public health or safety, or any combination of these outcomes.

In telecommunications, Critical Infrastructure is divided into two sectors: Critical Telecom Infrastructure and Critical Telecom Data. (Pakistan Telecommunication Authority, 2022) is defined as:

3.2.1 CTI (Critical Telecom Infrastructure)

CTI refers to equipment/assets, whether physical or virtual, that are vital for the provision of telecom-licensed services and for storing, processing, and transferring data. National interests include violation of conventions and treaties, adverse damage to the reputation of the country, diplomatic relations and political affiliations, operational efficiency of the security or intelligence operations of military forces, national economy, national infrastructure, and government functions. It is imperative to mention here that any system including the intermediator system that is used to process Critical Data can be classified as a Critical Telecom Infrastructure.

3.2.2 CTD (Critical Telecom Data)

CTD refers to personal data, licensee users/customers, secret customer data belonging to government agencies or institutions, which are retained by the telecom licensee, and information that is critical for the operations, confidentiality, and security of the licensee telecom systems, including voice/data communication of its users/customers being handled by the telecom licensee.

Furthermore, any data can result in a financial loss that leads to the inability of organizations to perform their duties, a major loss of competitive abilities, or a combination thereof, and/or can also be classified as Critical Telecom Data (CTD).

3.3 Cybersecurity Framework (CSF)

According to the NIST website (www.nist.gov), The Cybersecurity Framework is based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk.

The framework helps organizations manage and reduce risks for those processes, information, and systems directly involved in the delivery of critical infrastructure services, and fosters risk and cybersecurity management communications among both internal and external organizational stakeholders.

Gabriel Kabanda, 2018) from Zimbabwe, stated that the lack of a framework to provide direction, focus, guidance, and a standardized way of addressing cybersecurity issues in Zimbabwe is one of the challenges facing the ICT industry. With no cybersecurity framework in place, dealing with cybersecurity issues becomes problematic, as there is no guidance and direction on how to prevent, respond, and reduce cybersecurity breaches and risks, as well as improve personnel awareness. Therefore, a cybersecurity framework that will support a cybersecurity culture to prevent cyberattacks in Zimbabwe is required under these circumstances.

(Siegfried Moyo, 2022) The development of a cybersecurity framework that provides a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to manage cybersecurity risk.

The need to implement effective cybersecurity frameworks is growing. Cybercriminals continuously derive sophisticated techniques to execute attacks.

This has led to the development of various cybersecurity frameworks to assist organizations in achieving robust cybersecurity programs. Therefore, businesses should understand the top cybersecurity framework to enhance their security posture.

The framework includes a methodology for addressing the privacy implications of cybersecurity activities. This framework helps organizations assess and improve their cybersecurity programs. Information privacy and security professionals have already begun to use this framework to assess and improve their cybersecurity programs.

3.4 Framework for Critical Infrastructure

Critical infrastructure is defined as: "Systems and assets, whether physical or virtual, so vital to the countries that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters.

Organizations use this framework in various ways. Many have found it helpful in raising awareness and communicating with stakeholders within their organizations, including executive leadership. The Framework also improves communication across organizations, allowing cybersecurity expectations to be shared with business partners, suppliers, and among sectors.

By mapping the framework to current cybersecurity management approaches, organizations learn and demonstrate how they match the framework's standards, guidelines, and best practices. Some parties use the framework to reconcile and deconflict internal policy with legislation, regulations, and industry best practices.

The Framework is also used as a strategic planning tool to assess risks and current practices.

3.5 The Components of a Cybersecurity Framework

Cybersecurity frameworks differ from one company to another, and every cybersecurity framework differs. Thus, each describes the core components in its manner. That said, they are all built on similar principles and are used to achieve similar cybersecurity goals. While a Pacific cybersecurity framework goes into far greater detail in how it is constructed and designed, it loosely revolves around a continuous lifecycle process consisting of the following four key stages.

3.5.1. Identify and document cybersecurity goals.

This component is used to identify the cybersecurity goals that an organization wants to achieve. The identified goals are different for each organization. They are mostly dependent on the business's level of cybersecurity competency, overall business intent, and whether the organization must meet specific goals owing to regulatory requirements.

3.5.2. Set guidelines designed to achieve cybersecurity goals.

In this stage of a cybersecurity framework, a detailed list of functions, processes, and actions is created that serve to achieve the goals outlined in the identification stage. This stage should also contain steps to prioritize goals and define the roles and responsibilities for each defined objective.

3.5.3. Implement cybersecurity processes.

In the action stage of the framework, each goal is implemented within the enterprise infrastructure. Communication is crucial in this stage because applied cybersecurity processes often involve multiple areas or departments.

3.5.4. Monitor and communicate results.

Finally, the implemented objectives were monitored, documented, and reviewed to ensure that the cybersecurity framework processes were effective.

The results are appropriately communicated to the organization, and steps are taken to continuously improve the existing processes and objectives.

3.6 Cybersecurity Threats and Cyber Attacks

(Yuchong Li & Qinghui Liu, 2021) The purpose of cyberattacks is to harm companies financially. In other cases, cyberattacks can have military or political purposes. Some of these damages are PC viruses, knowledge breaks, data distribution services (DDS), and other assault vectors.

To this end, various organizations have used various solutions to prevent damage caused by cyberattacks. Cybersecurity follows real-time information on the latest IT data.

As (Maurice F. D.& Doris E.& Francisco F.& Mónica D., 2021) similar to financial and

reputational risks, cybersecurity risks can lead to higher costs and impact on revenues and returns. It also harms the organization's ability to innovate, acquire, and maintain customers.

(Martti Lehto & Pekka Neittaanmäki,2022) the vulnerability of CI to cyberattacks and technical failures has become a major concern nowadays. Sophisticated and novel cyberattacks, such as adversarial attacks, may deceive physical security controls, providing a perpetrator with an illicit entry to the smart critical facility.

(Martti Lehto & Pekka Neittaanmäki,2022) they add, the critical infrastructure can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents, computer hacking, criminal activity and malicious behavior. National critical infrastructure can be targeted by hostile states, cyber criminals, terrorists, or criminals for disruption, espionage, and/or financial gain.

(P.S.Seemma, S.Nandhini, M.Sowmiya, November 2018) Globally, the demands of society have resulted in the development of ever-more complex technological systems which operate in and support, almost all aspects of modern life. Such systems rely on the use of information technology, and can therefore be vulnerable to attacks based on the malicious use of software-based techniques. Recent experience has illustrated a wide range of targets for such attacks, including central state-operated administrative functions, such as financial and healthcare services, as well as critical national infrastructure, such as energy, water, and transportation networks.

In more detail (Wumi A.& Obi I.& Taiwo O.& Madewa M.,2022) typed the threats to

Cyberattacks are exponentially increasing [Grab your reader's attention with a great quote from the document or use this space to emphasize a key point. To place this text box anywhere on the page, just drag it.].
daily with the advancements of technology.

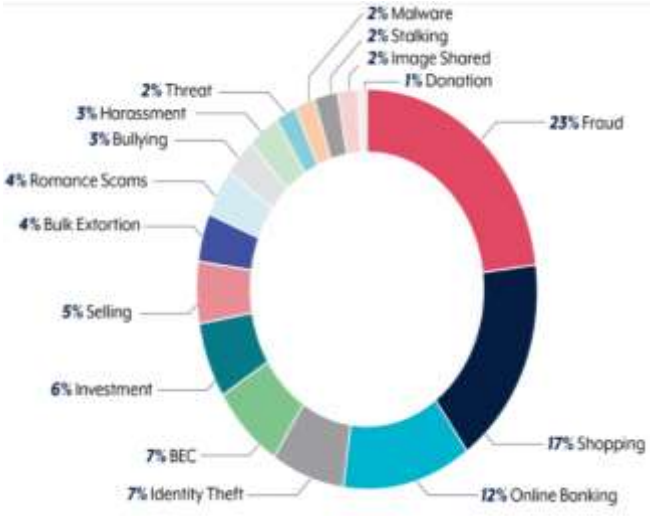

Figure 3.6.1: The ACSC Annual Cyber Threat Report 2020–21.

Therefore, the detection and prediction of cyberattacks are important for every organization that deals with sensitive data for business purposes.

Md A. R., Yeslam A., & Tanveer Z. (November 09, 2020) presented a framework on cyber security using a data mining technique to predict cyberattacks that can help takes proper interventions to reduce cyberattacks. The two main components of the framework are the detection and prediction of cyber-attacks. The framework first extracts patterns related to cyberattacks from historical data using J48 decision tree algorithm tasks provided by the Canadian Institute of Cybersecurity.

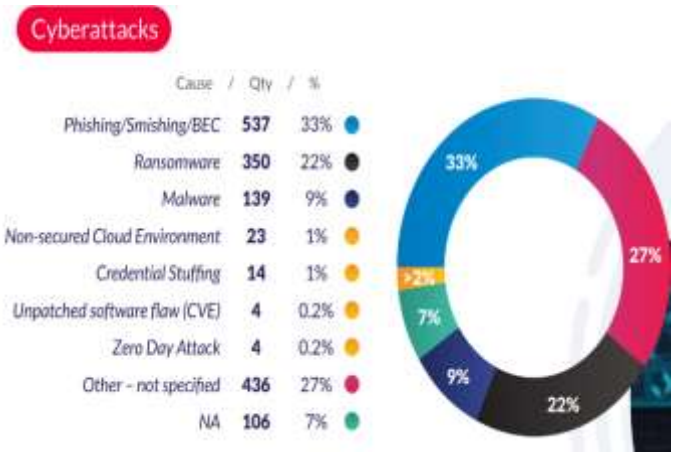

Figure 3.6.2 Root Cause of Compromises

In the datasets, several types of cyberattacks were presented, including DDoS, Port Scan, Bot, Brute Force, SQL Injection, and Heartbleed. The proposed framework correctly detects cyberattacks and provides patterns related to them. The overall accuracy of the proposed prediction model for detecting cyberattacks is approximately 99%. The extracted patterns of the prediction model based on historical data can be applied to predict future cyber-attacks. The experimental results of the prediction model indicate its superiority in detecting future cyberattacks.

(Michelle Moore) wrote an article about the top cybersecurity threats in 2022:

1. Phishing Gets More Sophisticated

Phishing attacks, in which carefully targeted digital messages are transmitted to fool people into clicking on a link that can then install malware or expose sensitive data, are becoming increasingly sophisticated.

Now that employees in most organizations are more aware of the dangers of email phishing or clicking on suspicious-looking links, hackers are upping the ante — for example, using machine learning to craft and distribute convincing fake messages in the hopes that recipients will unwittingly compromise their organization's networks and systems. Such attacks enable hackers to steal user logins, credit card credentials, and other types of personal financial information as well as gain access to private databases.

2. Ransomware Strategies Evolve

Ransomware attacks are believed to cost victims billions of dollars every year, as hackers deploy technologies that enable them to kidnap an individual or organization's databases and hold all of the information for ransom. The rise of cryptocurrencies such as Bitcoin is credited with helping fuel ransomware attacks by allowing ransom demands to be paid anonymously.

As companies continue to focus on building stronger defenses to guard against ransomware breaches, some experts believe that hackers will increasingly target other potentially profitable ransomware victims such as high-net-worth individuals.

3. Crypto-jacking

Cryptocurrency movement also affects cybersecurity in other ways. For example, crypto-jacking is a trend that involves cybercriminals hijacking third-party homes or work computers to "mine" cryptocurrency. Because mining for a cryptocurrency (e.g., Bitcoin) requires immense amounts of computer processing power, hackers can make money by secretly piggybacking on someone else's systems.

For businesses, crypto-jacking systems can cause serious performance issues and costly downtime, as IT works to track down and resolve the issue.

4. Cyber-Physical Attacks

The same technology that has enabled us to modernize and computerize critical infrastructure also brings about risks. The ongoing threat of hacks targeting electrical grids, transportation systems, and water treatment facilities represents a major vulnerability. According to a recent report in The New York Times, even America's multibillion-dollar military systems are at risk of high-tech foul play.

5. State-Sponsored Attacks

Beyond hackers looking to make a profit by stealing individual and corporate data, all nation-states are now using their cyber skills to infiltrate other governments and attack critical infrastructure. Cybercrime today is a major threat not just to the private sector and to individuals, but also to the government and the nation as a whole. As we move to 2022, state-sponsored attacks are expected to increase, with attacks on critical infrastructures of particular concern.

Many such attacks target government-run systems and infrastructure, but private sector organizations are also at risk. According to a

report from Thomson Reuters Labs, state-sponsored cyberattacks are an emerging and significant risk to private enterprises that will increasingly challenge those sectors of the business world that provide convenient targets for settling geopolitical grievances."

6. IoT Attacks

The Internet of Things is becoming more ubiquitous by the day (according to Statista.com, the number of devices connected to the IoT is expected to reach 75 billion by 2025). It includes laptops and tablets, routers, webcams, household appliances, smart watches, medical devices, manufacturing equipment, automobiles, and home security systems.

Connected devices are convenient for consumers, and many companies now use them to save money by gathering immense amounts of insightful data and streamlining business processes. However, more connected devices mean greater risk, making IoT networks more vulnerable to cyber invasion and infections. Once controlled by hackers, IoT devices can be used to create havoc, overload networks, or lock down essential equipment for financial gains.

7. Smart Medical Devices and Electronic Medical Records (EMRs)

The healthcare industry continues to evolve as most patient medical records have now moved online, and medical professionals have realized the benefits of advancements in smart medical devices. However, as the healthcare industry has adapted to the digital age, there are many concerns about privacy, safety, and cybersecurity threats.

According to the Software Engineering Institute of Carnegie Mellon University, "As more devices are connected to hospital and clinic networks, patient data and information become increasingly vulnerable. Even more concerning is the risk of remote compromise of a device directly connected to the patient. An attacker could theoretically increase or decrease dosages, send electrical signals to a patient, or disable vital sign monitoring".

With hospitals and medical facilities still adapting to the digitalization of patient medical records, hackers are exploiting many vulnerabilities in their security defenses. Since patient medical records are almost entirely online, they are a prime target for hackers because of the sensitive information they contain.

8. Third Parties (Vendors, Contractors, Partners)

Third parties such as vendors and contractors pose a huge risk to corporations, the majority of which have no secure system or dedicated teams in place to manage these third-party employees.

As cyber criminals become increasingly sophisticated and cybersecurity threats continue to rise, organizations are becoming increasingly aware of the potential threats posed by third parties. However, the risk is still high; U.S. Customs and Border Protection joined the list of high-profile victims in 2021.

A report on "Security Risks of Third-Party Vendor Relationships" published by Risk ManagementMonitor.com includes an infographic estimating that 60% of data breaches involve a third party and that only 52% of companies have security standards in place regarding third-party vendors and contractors.

9. Connected Cars and Semi-Autonomous Vehicles

While the driverless car is close, but not yet here, the connected car is. A connected car utilizes onboard sensors to optimize the operation and comfort of the passengers. This is typically achieved through embedded, tethered, or smartphone integration.

As technology evolves, connected cars are becoming increasingly prevalent; by 2020, an estimated 90 per cent of new cars will be connected to the Internet, according to a report titled "7 Connected Car Trends Fueling the Future."

For hackers, this evolution in automobile manufacturing and design provides yet another opportunity to exploit vulnerabilities in insecure

systems and steal sensitive data and/or harm drivers. In addition to safety concerns, connected cars also pose serious privacy concerns.

(Wumi A.; Obi I.; Taiwo O.; Madewa M.,2022) identified Mitigation Methods for providing cyber security, they said we cannot over-emphasize the importance of a strategic plan when it comes to mitigating against malicious threats or actors. The first step in guarding against most cybersecurity threats is to carefully draft an organizational security policy. Defining security policies as clear instructions that provide the blueprint for employee behavior concerning protecting information, they are also basic building blocks in creating effective controls to guard against potential security threats, which can only be implemented by empowering employees with training using well-articulated policies and procedures. Security is about providing answers to a single question: How do you give people access to the correct systems for the correct amount of time while keeping the wrong people out? To drastically reduce the potential risk of remote unauthorized access to organizations, some key steps need to be taken.

1. Identity and access management
2. Vulnerability management (technology exposure)
3. Third- and fourth-party risk
4. Email Security
5. Web Security

To guard against these threats, particularly phishing- and web-based attacks, a rock-solid strategy will include the following:

a) Continuous Infrastructure Awareness

b) Server Hardening

c) Aggressive threat hunting.

Every organization is getting online for its business survival and placing its important resources on web servers that are openly available through the HTTP interface. To make these resources secure, every organization must follow security standards or guidelines. Unfortunately, security solutions are mostly signature-based and static (i.e., if a signature is present, malicious activity can be detected otherwise). Hence, there is a need for a dynamic solution to cater to upcoming vulnerabilities daily. Moreover, there is a need for a semantic solution that can understand the context of the vulnerabilities before fixing them.

(IBM security, Cost of a Data Breach Report 2022) distribution of the sample by industry. According to IBM, a comparison of threats or attacks by sector (technical health education).

The largest samples of industries were in these sectors

Figure 3.6.3 Types of Cyber Attack

1- Industrial 12% Chemical processing, engineering and manufacturing companies.
2- Technology 11% Software and hardware companies.
3- Services 12% Professional services such as legal, accounting and consulting firms.
4- Financial 16% Banking, insurance, investment companies.

It concludes the extent to which the technical sector represents, compared to the rest of the sectors targeted by the attacks according to the sector.

3.7 Cybersecurity Challenges

(Dr Sameh A., 2017) Ensuring cybersecurity is an emerging challenge that

interlinks with other political challenges in the Middle East, such as critical socio-economic challenges; regional and transnational terrorism; and education, awareness and capacity-building.

due to ideological differences in the various approaches.

(Michael D. Farber, 2018) In addition to obstacles from the federal perspective, his study identified four other challenges to Framework adoption that were reported by the entities that were surveyed:

3.7.1 Limited ability to commit necessary resources toward Framework adoption.

While large entities, in some cases, have larger teams and more than sufficient resources to address cybersecurity, smaller businesses in the supply chain are often unable to dedicate staff to voluntarily implementing the framework.

3.7.2 Lack of the necessary knowledge and skills to effectively implement a Framework.

Despite efforts to introduce and promote the use of the NIST Framework by SSAs, SCCs, and other federal agencies, several organizations are still uncertain about whether and how to apply the framework to their business model.

3.7.3. Existing regulatory, industry or other requirements inhibit Framework adoption.

At least five of the 16 sectors are heavily regulated by state, federal, and sometimes local authorities, thereby creating a patchwork of overlapping and sometimes conflicting obligations that, in turn, create a disincentive to voluntarily add framework adoption to an already crowded field of priorities.

3.7.4. Other priorities take precedence over conducting cyber-related risk management or adopting the Framework.

Owing to the vast differences in size, type, function, and location of critical infrastructure assets and the resources available to protect these assets, seven SCCs indicated that companies are forced to prioritize physical security, natural disaster response, and insider threats over cybersecurity. Smaller organizations are still not convinced that they are a viable target for an attack and therefore see little benefit in voluntarily adopting the framework to address an incident with a low or zero risk of occurrence.

3.8. The Types of Cybersecurity Frameworks

Businesses should understand cybersecurity frameworks for enhancing organizational security.

The cybersecurity framework is a structure that an organization needs to protect against cyberattacks. Some cybersecurity frameworks are mandatory and others are often strongly encouraged by regulators.

Thus, frameworks guide organizations in the implementation process to meet standard requirements. The main goal of a cybersecurity framework is to reduce the risk of cyber threats by learning from best practices. The most popular and frequently used cybersecurity frameworks are as follows.

3.8.1. ISO/IEC 27002

Is the international standard that specifies the requirements for an information security management system (ISMS). An ISMS is a framework of policies and processes that helps organizations secure confidential information. The standard is designed to be adaptable to any organization, regardless of its size or sector. It can be used by all types of businesses, including manufacturers, retailers, banks, and government agencies. By implementing ISO/IEC 27002, organizations can benefit from improved security and decreased risk of data breaches, improved security posture, reduced risk of data breaches, and increased customer confidence, meet compliance obligations, and help organizations protect their data and systems from unauthorized access, use, or disclosure. The standard provides a framework for managing information security and can be

applied to any type of organization, regardless of size or industry.

3.8.2. NIST Cybersecurity Framework (NIST CSF)

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is a set of voluntary guidelines that provide a high-level taxonomy of cybersecurity outcomes and a methodology for assessing and managing those outcomes. It is intended to help private sector organizations that provide critical infrastructure with guidance on how to protect it, along with relevant protection for privacy and civil liberties. The NIST CSF has many benefits, including the fact that it is technology agnostic, which means it can be implemented regardless of an organization's technological choices; it is also scalable, so it can be tailored to meet the specific needs of any organization; and, perhaps most importantly, it provides a common language for discussing cybersecurity, which can help facilitate communication and collaboration between different organizations.

The framework was created in response to the growing threat of cyberattacks and provides a comprehensive approach to cybersecurity. It comprises three main components: identification, protection, and detection. The first step helps businesses to identify their assets and vulnerabilities. The second step, protecting, helps businesses implement security controls to protect their assets. Finally, the third step, detection, helps businesses to detect and respond to cyber incidents. By following the NIST Cybersecurity Framework, businesses can improve their cybersecurity posture and defend themselves from attacks.

On February 12, 2013, Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity charged the National Institute of Standards and Technology (NIST) to create a framework for reducing risk to critical infrastructure and the Department of Homeland Security (DHS) to help critical infrastructure use and understand the framework. One year later, NIST released the Cybersecurity Framework to help critical infrastructure sectors and organizations reduce and manage their cyber risk regardless of size or cybersecurity sophistication.

The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations improve their ability to prevent, detect, and respond to cyberattacks, and can be used to help identify and prioritize actions for reducing cybersecurity risk; it is a tool for aligning policy, business, and technological approaches to managing that risk. This framework can be expressed as follows:

- Align cybersecurity decisions to mission objectives;
- Organize security requirements originating from legislation, regulations, policies, and industry best practices
- Communicate cybersecurity requirements with stakeholders, including partners and suppliers;
- Integrate privacy and civil liberties risk management into cybersecurity activities;
- Measure current state and express the desired state;
- Prioritize cybersecurity resources and activities; and
- Analyze trade-offs between expenditure and risk.

Table 3.8.1 Evaluation of Standers NIST

Standard(s)	Evaluation
NIST 800-53Ar4	Security of IT systems
NIST SP 800-115	Security of IT products
NIST SP 800-161	Risk management in supply chains
NIST IR 8062	Privacy risk management in federal systems

3.8.3. PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from major card schemes. The PCI Standard is mandated by card brands but administered by the Payment Card Industry Security Standards Council. This standard was

created to increase controls around cardholder data to reduce credit card fraud.

The PCI Standard is mandated by card brands but administered by the Payment Card Industry Security Standards Council. A standard was created to increase the controls around the cardholder data. Implementing the PCI DSS can be beneficial to organizations by decreasing the chance of a data breach, thus reducing the number of damages that could be associated with such an incident. In addition, being PCI DSS compliant may help improve an organization's reputation. Organizations that handle credit cards are expected to comply with the PCI DSS and those that do not face penalties from card brands. Thus, taking steps to become compliant can help protect the organization's bottom line.

3.8.4. COBIT

COBIT was developed in the mid-1990s by ISACA, an independent organization of IT governance professionals. ISACA offers a well-known Certified Information Systems Auditor and Certified Information Security Manager certifications.

COBIT originally focused on reducing IT risk. COBIT 5, released in 2012, includes new technology and business trends to help organizations balance IT and business goals. The current version is the COBIT 2019.

It is designed to help individuals and organizations manage their IT resources in a manner that aligns with their business objectives. COBIT can help organizations improve their overall performance by providing a clear and concise set of guidelines for managing IT resources.

3.8.5. CIS 18

The Center for Internet Security (CIS) Critical Security Controls is a set of best practices for cybersecurity. Version 8 was released in January 2020, and includes updates for handling cloud computing and IoT devices. These controls are designed to help organizations protect their data and systems from cyberattacks.

There are 18 CIS controls, divided into three categories: basic, foundational, and organizational. CIS controls can benefit any organization, but they are particularly well-suited for small businesses that may not have the same resources as larger organizations. Implementing CIS controls can help small businesses protect their data and systems from cyberattacks. The benefits of implementing CIS Critical Security Controls include improved security posture, reduced risk of data breaches, and compliance with regulatory requirements. These controls can help organizations quickly identify and respond to security incidents.

3.8.6. HITRUST Common Security Framework

The HITRUST Common Security Framework includes risk analysis and risk management frameworks along with operational requirements. The framework has 14 different control categories and can be applied to almost any organization, including healthcare.

HITRUST is a massive undertaking for any organization because of the heavy weight given to documentation and processes. As a result, many organizations have ended up scoping smaller areas of focus for HITRUST.

The HITRUST Common Security Framework includes both a risk analysis and risk management framework, as well as operational requirements. This makes it an ideal tool for organizations of all sizes that are looking to improve their security posture. One of the benefits of the HITRUST Common Security Framework is that it helps organizations manage risk holistically.

This helps organizations ensure that their security controls are effective and meet the industry’s best practices.

The HITRUST Common Security Framework also includes operational requirements designed to help organizations reduce their cybersecurity risks. The HITRUST Common Security Framework is also being used by healthcare organizations worldwide to

improve cybersecurity programs. Implementing the HITRUST Common Security Framework can help organizations in any industry reduce cybersecurity risks and improve their overall security posture.

3.8.7. OWASP Top 10

OWASP is a nonprofit organization that regularly publishes the top 10 security issues of web applications, mobile services, web services, etc. Most security auditing organizations follow these top ten security issues to categorize security vulnerabilities.

The benefit of using OWASP's top 10 list is that it provides a common language for discussing and ranking security risks. The Top 10 list is an important tool for any organization that wants to improve the security of its web applications.

3.8.8. SOC 2

The American Institute of Certified Public Accountants (AICPA) developed the SOC 2 framework. This framework enables organizations to collect and store personal customer information in cloud services to maintain proper security.

The framework also provides SaaS companies with guidelines and requirements to mitigate data breach risks and strengthen their cybersecurity postures. In addition, the SOC 2 framework details the security requirements that vendors and third parties must conform to. These requirements guide them in conducting both external and internal threat analyses to identify potential cybersecurity threats.

The framework helps ensure that companies that use cloud services have proper security measures in place to prevent data breaches. By following the guidelines and requirements outlined in the framework, SaaS companies can help mitigate the risks of data breaches and protect customer information.

3.8.9. FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a framework designed for government agencies. The framework provides standardized guidelines that can enable federal agencies to evaluate cyber threats and risks to different infrastructure platforms, cloud-based services, and software solutions.

Furthermore, the framework permits the reuse of existing security packages and assessments by various governmental agencies.

The framework is also based on continuous monitoring of IT infrastructure and cloud products to facilitate real-time cybersecurity programs. More importantly, FedRAMP focuses on shifting from tedious, tethered, and insecure IT to secure mobile and rapid IT. The aim is to ensure that federal agencies have access to modern and reliable technologies, without compromising their security. To achieve the desired security levels, FedRAMP collaborates with cloud and cybersecurity experts to maintain the other security frameworks. These include the NSA, DoD, NIST, GSA, OMB, and other private sector groups.

3.8.10. Defense Federal Acquisition Regulation Supplement (DFARS)

The Defense Federal Acquisition Regulation Supplement (DFARS) is a set of regulations that governs the acquisition of goods and services by the United States Department of Defense (DOD). DFARS provides specific requirements for the acquisition of goods and services by the DOD, including requirements for contracting small businesses and for the use of commercial items. DFARS also prescribes methods for acquiring supplies and services that support national defense.

DFARS also establishes minimum standards for security, health, and safety. In addition, DFARS requires contractors to comply with federal laws and regulations, including those about labor and employment laws.

The benefits of DFARS include the fact that it helps to improve the security of defense information and systems. It does this by establishing standards for contractors and other entities that access or handle defense

information. DFARS also requires contractors to report any cyber incidents so that the government can properly investigate and address them.

(Žiga T.& Muammer S. S. & Robert K., 22 September 2020) they added

3.8.11. Global Technology Audit Guide (GTAG)

Assessing Cybersecurity Risk: Roles of the Three Lines of Defense The guide from the Institute of Internal Auditors (IIA) addresses cybersecurity risks and threats for all types of organizations and provides an approach to conducting cybersecurity risk assessments. This highlights the importance of ensuring the robust operation of each of the three lines of defense. The first line of defense covers the management of risks, data, processes, and controls; the second line of defense ensures the effectiveness of the first line of defense; and the third line of defense assesses the effectiveness of the first and second lines of defense. This guide presents a framework for the risk assessment of cybersecurity. The framework comprises six components: Cybersecurity Governance, Inventory of Information Assets, Standard Security Configurations, Information Access Management, Prompt Response and Remediation, and Ongoing Monitoring. Suggestions were made for each component of the framework, rather than providing a checklist for conducting a risk assessment.

3.8.12. National Cybersecurity Centre (NCSC) – Cyber Assessment Framework

This comprehensive framework of the United Kingdom's NCSC is designed to be used by organizations themselves or by third parties to assess the cybersecurity functions of organizations. The assessment structure is built around four main objectives: managing security risks, protecting against cyberattacks, detecting cybersecurity events, and minimizing the impact of cybersecurity incidents. In total, there are 14 principles under four main objectives, and these principles are grouped into thirty-nine contributing outcomes for a detailed assessment. For each contributing outcome, a set of good practice indicators is listed in tables to assess whether the contributing outcome is achieved, partially achieved, or not achieved by the organization. Good practice indicators are presented as clear statements in the form of a checklist, making them easier and more convenient to use.

3.9. Using cybersecurity framework for protection from threats

(Maurice, Doris, 2021) propose the use of a methodology based on the NIST Framework for the adequate management of cybersecurity in government organizations within the framework of the delivery of digital services. Many government organizations have been managing cybersecurity without a defined process, which means that management is deficient and without indicators. Whether they are implementing the methodology based on the NIST cybersecurity framework.

In conclusion, it was shown that the use of the methodology based on the NIST cybersecurity framework influences cybersecurity management in government organizations, and it is clear that they are currently not using it, which causes a relatively poor level of leadership in the implementation of security measures concerning cybersecurity management.

Divine Sufor Anye (2018) categorized the threat posed by terrorist organizations to Cameroon's telecommunications critical infrastructure (TCI) using the Generic Threat Matrix (GTM). GTM suggests that understanding the overall impact of threats entails that the categorization of threat attributes is essential.

When used, it allows the private and government sectors to operate in a secured partnership without compromising the confidentiality, integrity, and availability of each collaborating entity.

(Halima I. & Shareeful I.& Haralambos M., January 14, 2022) proposed an integrated cyber security risk management framework (I-CSRM) that adopts various existing standards and cyber threat intelligence data for risk management. I-CSRM also includes machine learning (ML) models to predict risk types so that organizations can undertake the necessary proactive measures to tackle the risks. The framework also includes tool support to automate some risk management activities.

Finally, I-CSRM is applied in a CI-based industrial context, and the results of applying the framework are promising.

Specifically, the context was able to identify and assess risks using I-CSRM and determine the right level of control for overall business continuity.

The participants' observation was that I-CSRM is a practical approach to risk management, and integration of the CTI makes risk management activities more effective.

We believe that the proposed I-CSRM framework, its process, and supporting tool will significantly impact the cybersecurity domain and the state of the art in general.

The I-CSRM framework focuses only on the supervised learning method, which requires a labelled dataset.

(Samer Okour,2019) identifying the impact of the application of IT governance represented by (Planning and Organization, Possessiveness and Implementation, Support and Delivery, Monitoring and Evaluation, and Guidance and Control), using (COBIT 5) framework to reduce the risks associated with cloud computing (Identity and Access Management, Data protection, Virtual operating risk, IT support, and organization) in Jordanian industrial companies' public shareholding from the perspective of Jordanian Certified Public Accountants.

He followed sequential procedures as a strategy for the mixed methods that have been applied. Qualitative data were collected and quantitatively analyzed.

A questionnaire was used to assess the purpose of this study. The study population included all external accountants practicing auditing in Jordan, who numbered up to the end of 2017 (384); a simple random sample was drawn, and the sample included (192) auditors.

His study concluded that all decisions of the (COBIT5) Committee, including Planning and Organization, Possessiveness and Implementation, Support and Delivery, Monitoring and Evaluation, and Guidance and Control, affect the reduction of the risk of cloud computing in terms of identity and Access Management, Data protection, virtual operating risk, IT support, and Organization the Jordanian industrial companies' public shareholding from the perspective of Jordanian Certified Public Accountants.

Based on the findings of the study, the researcher recommends that Jordanian industrial companies activate the role of security controls and increase the level of application against the environmental risks surrounding the company likely to occur as a result of the application of cloud computing. It is also necessary to update and develop information technologies, particularly those related to technology.

(Yusuf D.& Yuliza C.& Djoko S.& others, August 2017) evaluated the application system TULIS in the Main Library of UIN Syarif Hidayatulllah Jakarta using Control Objectives for Information and Related Technologies.

(COBIT 5) framework focuses on the process of managing security (APO13) and managed security services to know the gap and provide recommendations to the top management of the library.

In this study, Likert scale calculations were used. The results of this study are as score value for APO13 was 0.65 and for DSS05 was 0.87 which indicated that both were at the level of capability 1 (Performed Process) but the security governance standard has not been well implemented yet.

Moreover, the value for APO13 was 1.65 and DSS05 was 0.87, which indicated that both were in capability level 2. In addition to upgrading the system, a high-standard security policy was among the recommendations to overcome these problems.

The firewall and Secure Socket Layer (SSL) need to be implemented in the system to protect against attacks.

(Ziga T. & Borja G. & Bharadwaj R.K. & Abel M. & Alexandru G.,2022) The construction industry is specific and needs a specialized framework that would assist in understanding and managing cybersecurity. We developed an original framework that identifies three types of wrongful activities: stealing, lying down, and harming. It identifies four elements that can be affected by wrongful activities: information assets, material assets, people, and systems. Cybersecurity is defined as the absence of three wrongs across the four elements. The framework is construction-specific and, as such, a useful tool for senior management to understand security problems and organize security processes.

(Melwin S. &Siti R. S. &Nurul A. Z.) Protecting organizations from cyber threats while demonstrating compliance with laws and standards is seen as extremely complex due to the difficulty of choosing the appropriate standard to be used. Moreover, a lack of knowledge of the elements offered by the standard leads to the problem of identifying the starting point where the protection will begin. Therefore, the literature and analysis are presented in identify the elements of cybersecurity standards and frameworks that can facilitate the organization or government in choosing the appropriate standard and framework to be used and utilized.

(Amy Mahn & Daniel Topper & Stephen Quinn &Jeffrey Marron&, August 2021) provided direction and guidance to organizations seeking to improve cybersecurity risk management by utilizing the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework or the Framework). The Framework enables organizations to apply the principles and best practices of risk management to improve security and resilience, regardless of the size, degree of cybersecurity risk, or cybersecurity sophistication. Through the implementation of the framework, organizations can better identify, assess, and manage their cybersecurity risks in the context of their broader mission and business objectives.

(2022 IEEE Delhi Section Conference (DELCON), February 2022) The Framework is the guideline for the organizations. There are different specialized frameworks for the use of organizations. Organizations implement them in their environment to become more secure, easy to handle workloads and minimize cyber-space risks. The NIST Cybersecurity Framework and Secure Control Framework cover five functions: identification, protection, detection, pond, and over. The Secure Control Framework has more subdomains than the NIST Cybersecurity Framework does. Before implementation, each function requires well-organized plans and continuous actions. CSF have a wide scope in Information Technology, Cyber-Physical Systems, Industrial Control Systems, and the Internet of Things. The protection of Critical Infrastructure is more important for governments; they develop the National Cyber Governance Bureau and try to keep them safer from cyberattacks.

(Adamu A. G., February 2021) Cybersecurity is a method of protecting organization assets, through the identification of threats that can compromise the critical information stored in the organization’s systems, it also involves the protection, identification, and respond to threats. This paper aims to provide a detailed review of the current cybersecurity frameworks that can serve as a guideline for organizations in selecting the appropriate framework for their organization and as a benchmark for future cybersecurity framework design.

Table -4.1 Evaluation of Standers NIST

Threats \CSF types	Malware	Ransomware	Web-based attacks	Mobile threats	Denial of service	Botnets	Identity theft	Data breaches	Cloud service abuse	Information leakage	Insider threats	Phishing	spam	Personal data breach
ISO/IEC 27002	x	x	x		x		X	X		x	x	x	x	
NIST SP 800-37	x	x	x	x	x	x	X	X	x	x	x			
NIST SP 800-53r4	x	x	x	x	x	x	X	X	x	x	x	x	x	
NIST SP 800-121 Revision								X		x				
NIST SP 800-122					x		X	X		x				
NIST SP 800-126 Revision	x			x				X				x		
NIST SP 800-144							X	X	x	x				
NIST SP 800-150							X	X		x				
NIST- Framework for Improving Critical Infrastructure Cybersecurity	x	X	x	x	x	x	X	X	x	x	x	x	x	x
COBIT			x				X	X		x	x	x	x	

4. Results Discussion

By collecting data and comparisons from the above information about threats and their sources, we find that most frameworks address specific protection, as shown in the table above. Therefore, there is no optimal framework, but the frameworks are complementary, and we need most of them to propose an optimal cyber framework.

5. Conclusion

In conclusion, this study conducted a comprehensive analysis of different standards frameworks in the field of cybersecurity, including NIST 800-53Ar4, COBIT, and ISO27002. It has provided valuable insights into the best practices and international standards for ensuring data security against cyber threats.

It is essential to acknowledge that no single standard can fully address the security demands of an organization. Therefore, adopting a combination of standards is recommended to effectively mitigate cyber threats and protect against data loss. Among the examined frameworks, NIST 800-53Ar4 has been

identified as the most effective. However, given the evolving nature of cyber threats, a hybrid approach incorporating elements from multiple frameworks and standards is crucial. This approach enables organizations to develop a tailored cybersecurity framework that aligns with specific needs and industrial requirements.

This study underscores the importance of adhering to global best practices and local cybersecurity legislation to enhance the management of cybersecurity risks.

Establishing and maintaining information security standards within organizations is crucial for ensuring compliance and reducing the risk of non-conformity.

In summary, organizations can significantly benefit from adopting a cybersecurity framework that combines the strengths of

various standard frameworks, such as NIST 800-53Ar4, COBIT, and ISO27002. This approach enables the effective mitigation of cyber risks and enhances infrastructure protection. By implementing these recommendations, organizations can strengthen their cybersecurity posture and protect their data and systems from evolving cyber threats.

References: -

[1] M. Lehto, "Cyber-attacks against critical infrastructure," in Cyber Security: Critical Infrastructure Protection: Springer, 2022, pp. 3-42.

[2] Y. Li and Q. J. E. R. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," vol. 7, pp. 8176-8186, 2021.

[3] M. F. Delgado, D. Esenarro, F. F. J. Regalado, and M. D. J. c. T. c. d. d. a. a. l. T. Reátegui, "Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations," vol. 10, no. 2, pp. 123-141, 2021.

[4] G. K. Saini, M. N. Halgamuge, P. Sharma, J. S. J. C. W. Purkis, M. Terrorism: Concepts, Tools,, and Applications, "A Review on Cyberattacks: Security Threats and Solution Techniques for Different Applications," pp. 98-126, 2020.

[5] M. I. Alghamdie, "WITHDRAWN: A novel study of preventing the cyber security threats," ed: Elsevier, 2021.

[6] A. Mahn, D. Topper, S. Quinn and J. Marron, "Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide," 2021.

[7] A. A. Garba, A. M. J. I. J. o. I. S. Bade, and R. Technology, "An investigation on recent cyber security frameworks as guidelines for organizations adoption," vol. 6, no. 2, pp. 103-110, 2021.

[8] S. Moyo, Executive's Guide to Cyber Risk: Securing the Future Today. John Wiley & Sons, 2022.

[9] P. Vähäkainu, M. Lehto, and A. Kariluoto, "Cyberattacks Against Critical Infrastructure Facilities and Corresponding Countermeasures," in Cyber Security: Critical Infrastructure Protection: Springer, 2022, pp. 255-292.

[10] B. C. H. Barte et al., "Level of Preparedness of the School Security Personnel and Their Qualifications Towards Institutional Security," vol. 6, no. 2, pp. 85-102, 2022.

[11] [G. J. A. J. o. M. Kabanda, Engineering and C. Science, "A Cybersecurity culture framework and its impact on Zimbabwean organizations," vol. 3, no. 4, pp. 17-34, 2018.

[12] P. Seemma, S. Nandhini, M. J. I. J. o. A. R. i. C. Sowmiya and C. Engineering, "Overview of Cyber Security," vol. 7, no. 11, pp. 125-128, 2018.

[13] W. AJAYI, O. Ibeto, T. Olomola, and M. J. I. J. o. A. R. I. C. S. Madewa, "Analysis Of Modern Cybersecurity Threat Techniques Andavailable Mitigating Methods," Vol. 13, No. 2, 2022.

[14] M. A. Rahman, Y. Al-Saggaf, and T. Zia, "A data mining framework to predict cyber attack for cyber security," in 2020 15th IEEE Conference on Industrial Electronics and Applications (ICIEA), 2020, pp. 207-212: IEEE.

[15] S. J. G. Aboul-Enein, "Cybersecurity challenges in the Middle East," vol. 17, pp. 5-49, 2017.

[16] Ž. Turk, M. S. Sonkor, R. J. J. o. C. E. Klinc and Management, "Cybersecurity assessment of BIM/CDE design environment using cyber assessment framework," vol. 28, no. 5, pp. 349–364-349–364, 2022.

[17] H. I. Kure, S. Islam, H. J. N. C. Mouratidis, and Applications, "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection," vol. 34, no. 18, pp. 15241-15271, 2022.

[18] S. J. M. A. S. Okour, "The Impact of the Application of IT Governance According to (COBIT 5) Framework in Reduce Cloud Computing Risks," vol. 13, no. 7, p. 25, 2019.

[19] Y. Durachman, Y. Chairunnisa, D. Soetarno, A. Setiawan, and F. Mintarsih, "IT security governance evaluation with use of COBIT 5 framework: A case study on UIN Syarif Hidayatullah library information system," in 2017 5th International Conference on Cyber and IT Service Management (CITSM), 2017, pp. 1-5: IEEE.

[20] Ž. Turk, B. G. de Soto, B. R. Mantha, A. Maciel, and A. J. A. i. C. Georgescu, "A systemic framework for addressing cybersecurity in construction," vol. 133, p. 103988, 2022.

[21] T. Welker, O. J. I. J. o. C. Abiona, Network and S. Sciences, "Improving the cybersecurity framework for future consumer networks," vol. 14, no. 04, p. 47, 2021.

[22] Dr.Michelle Moore, Top Cybersecurity Threats in 2022.
[23] https://www.statista.com/
[24] https://www.ibm.com/reports/data-breach
[25] Michael D. Farber, 2018 https://www.vnf.com/gao-reports-challenges-and-successes-in-cybersecurity-framework