East Journal of Applied Science
ISSN: 3079-9392
Volume 1, Issue 3
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss3.95

Technical and Procedural Measures to Protect Against Modern Cyber Breaches and Attacks

Mohamed Osman Mohamed GasmElseid*[1]

[1]Information Systems Department, University of Technology, Sudan, Mohamed12247823@gmail.com

*Corresponding Author.

Received: 19/04/2025, **Revised**: 03/05/2025, **Accepted**: 15/05/2025, **Published**: 17/05/2025

***Abstract*:**

The research deals with a group of problems and breakthroughs in the previous period and the largest attacks in history that caused failures in technical systems around the world. The research discussed cyber-attacks and disruptions and how to deal with them, better understand the difference, and enhance cyber security. Through the research, many examples of malfunctions, hacks, and cyber-attacks on modern global systems are discussed. The research aims to identify the basic causes, weaknesses, and methods that contribute to finding solutions security and the challenges of espionage and electronic penetration of countries through cyberspace ،it aims to clarify the various cyber challenges and risks that threaten the security of countries. The research cyber security crimes and methods and techniques for protection and security in cyberspace. Cyber-attacks addressed a set of measures and techniques and identified important points in technical protection methodsThrough research, it is explained how to identify security vulnerabilities, cybercrimes research studies one necessary measures for protection

Keywords: Cyber Security, Electronic hacking, Cyber Space.

1. Introduction

Today's most pressing research topics in cyber security go beyond password protection and firewalls. A global pandemic, geopolitical events and technological advances are also behind some key topics that are now driving cyber security research, the many devices that rely on the IoT measure and process vast amounts of data, and the networks and cloud systems that hold and share that data present a host of security risks.

Cyber security is one of the most important aspects of protecting electronic systems and data from electronic threats and attacks. It includes a set of techniques and practices that aim to protect information systems, networks, and electronic devices. Cyber security plays a major role in the era of modern technology, requiring continuous protection and advanced strategies to confront increasing threats there are many cyber security risks facing individuals, companies, and organizations. The recent period has witnessed many cyber security challenges more than any previous period, which occurred as a result of malfunctions and glitches in the systems, software, and applications used through which attacks were carried out. Therefore, it is necessary to recognize the big difference from the researcher's point of view between malfunctions, glitches, and cyber-attacks. Malfunctions are technical problems that occur due to defects in software or technology.

Through the definition and clarification of the difference, the relationship appears in that the cyber-attack exploits faults, malfunctions, loopholes and weak points in the networks or operating systems used or software by the attackers and causes damage to the systems and data.Cyber security research can shed light on issues with data protection and the tools and processes that provide it.The problem of cyber-attacks and the danger of wireless communication technologies. Today's world is highly dependent on electronic technology and protecting this data from cyber-attacks.

1.1 Research Problem

The basic Research problem is in the activities that target computer systems and important networks and exploit vulnerabilities, which constitute electronic threats that are carried out on banks, financial institutions, means of travel, airports, trains, and even media channels, and cause great harm and disrupt the interests of individuals, institutions, and countries through the studied and targeted cyber-attacks that are carried out and can be interpreted as piracy, sabotage, and harm to the interests of peoples.

1.2 Research Objectives

The important research objectives in the malfunction (faults) are technical problems that occur due to defects in software or technology without deliberate intent to cause harm. Faults are usually the result of software errors, technical problems, or increased load on systems. Understanding the difference between cyber-attacks and faults helps in dealing with each of them better and enhancing cyber security in general.

1.3 The Importance of Research

It is represented in a group of important points that have recently appeared, which is a group of malfunctions and breaches in computing systems, as airlines, airports, banks and media companies have witnessed them in the research and the effort to know the reasons that led to this and prevent breaches, electronic threats, and ensure the security of data and information and avoid them in the future for the great global impact.

1.4 Research Structure

In this paper, the research topics were divided into several aspects. The most important of winch are Explanation and clarification of the methodology followed in the research, section two importance of cyber security and Types of cyber security, cyber-attacks, types of cyber-attacks, and an explanation of the weaknesses of programs, applications, and protection measures.

2. Methodology

The research in the research methodologies is the descriptive and analytical method. The descriptive method is in explanation and description, and then the analytical method is to explain the problem and contribute to how to find many ways that help in solutions and reaching the necessary research results. The research highlights weaknesses, which are (software, network, and operating Systems). In software, there are weaknesses present in the software code that can be exploited by hackers. In the network, they are present in the network infrastructure that attackers can exploit. Weak points in Systems. Operations are these that involve an error, each type will be explained and malfunctions or violations identified through it. The research focused on cybercrimes, risks, and protection methods in cyber security for countries and institutions, as well as the problem of identifying vulnerabilities and risks, implementing technical measures, and identifying solutions and treatments that help in protection.

Through research, we note that there are numerous threats and violations facing cyber security. It is necessary to develop tools to protect against these threats, supporting protection and monitoring. Protecting operating systems and technologies used and preventing attacks and crimes targeting government agencies and state institutions.

Through research, it is explained how to identify security vulnerabilities, cybercrimes, and the necessary measures for protection. In light of the risk and potential consequences of cyber events, every mitigated risk or prevented attack strengthens the cyber security.

3. Cyber Security

we survey this large, complex, and rapidly evolving subject with the goal of giving the understanding that will enable incorporation of cyber security within an MBSE process and effective interaction with security experts, there are many crimes surrounding cyber security, these are adequately addressed and explained in this section, explain how to insure and protect, identify vulnerabilities, and clarify protection methods.

3.1 The Importance of Cyber Security

Cyber security as the protection (preservation of confidentiality, integrity and availability) of information and defense (prevention, detection and response to attacks) of networks and networked systems and software applications. This is achieved through proper execution of a comprehensive strategy outlined by policies and standards that define authorized and prohibited activities.

Cyber security is important because cyber-attacks and cybercrime have the power to disrupt damage or destroy businesses, communities and lives. Successful cyber-attacks lead to identity theft, personal and corporate extortion, loss of sensitive information and business-critical data, temporary business outages, lost business and lost customers and, in some cases, business closures [1].

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security.

The term "cyber security" applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

3.2 Types of Cyber Security

Comprehensive cyber security strategies protect all an organization's IT infrastructure layers against cyber threats and cybercrime. Some of the most important cyber security domains include the researcher explains in the form of the types and functions of each type, AI security, Network security, Cloud security and Application security [2].

A. AI Security

AI security refers to measures and technology aimed at preventing or mitigating cyber threats and cyber-attacks that target AI applications or systems or that use AI in malicious ways.

B. Network Security

Network security focuses on preventing unauthorized access to networks and network resources. It also helps ensure that authorized users have secure and reliable access to the resources and assets they need to do their jobs.

C. Cloud Security

Cloud security secures an organization's cloud-based services and assets, including applications, data, virtual servers and other infrastructure. Generally speaking, cloud security operates on the shared responsibility model. The cloud provider is responsible for securing the services that they deliver and the infrastructure that delivers them. The customer is responsible for protecting their data, code and other assets they store or run in the cloud.

D. Information Security

Information security (InfoSec) protects an organization's important information digital files and data, paper documents, physical media against unauthorized access, use or alteration.

E. Application Security

Application security helps prevent unauthorized access to and use of apps and related data. It also helps identify and mitigate flaws or vulnerabilities in application design. Modern application development methods such as DevOps and DevSecOps build security and security testing into the development process. Table 1 showing the types of electronic and automated attacks that take place.

Table 1: Definition of attacks [3]

Shortcut	Scientific Term	Definition
DDoS	Distributed Denial of Service	a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites

DoS	Denial of Service Attacks	attack is an attempt to overload a website or network, with the aim of degrading its performance or even making it completely inaccessible
Phishing	Phishing	type of cyber-attack (hackers trying to get sensitive information like passwords or numbers)

4. Research Problem Cyber-attacks and Cyber-crimes

Through research, it is explained how to identify security vulnerabilities, cybercrimes, and the necessary measures for protection.

4.1 Cyber-attacks and the Danger of Wireless Communication Technologies

Today's world is highly dependent on electronic technology, and protecting this data from cyber-attacks is a challenging issue. The purpose of cyber-attacks is to harm companies financially. In some other cases, cyber-attacks can have military or political purposes. Some of these damages are PC viruses, knowledge breaks, data distribution service (DDS) and other assault vectors.

4.2 Cyber Breaches and Attacks

There are two types: evaluation and treatment, and control and measures. The most common flaws are (software, network, operating systems). Software vulnerabilities are weaknesses in the software code that can be exploited by hackers. Network vulnerabilities are weaknesses in the network infrastructure that can be exploited by attackers. Operating systems vulnerabilities are those that involve an error, through which the faults or violation will be explained and identified [4]

4.3 Gaps and Weaknesses in Software and Applications

The most dangerous vulnerabilities in cyber security are outdated software and systems. When software and procedures are not updated regularly, they become vulnerable to attacks and hackers can exploit them to access sensitive information or install malware. To protect against this vulnerability, you must ensure that all software and systems are regularly updated with the latest updates. Especially security and important upgrades to programs and applications in the computer the scope of cyber security is illustrated by figure 1.

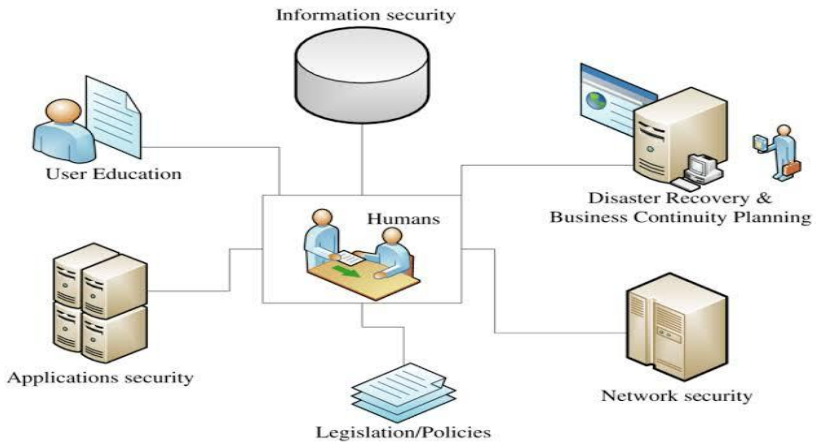

Figure1: Scope of cyber security [6]

4.4 Gaps and Weaknesses Point in Enterprise Networks

Weaknesses and malfunctions in the networks of institutional systems cause cyber-attacks and violations. The researcher addresses an important group of these malfunctions on the network side of important institutions, companies, banks, and banks in the country. Refers to weaknesses or flaws in the network infrastructure that can be exploited by malicious actors to gain unauthorized Access, disruption, or theft of information.

4.5 Network Protocol Attacks

Attack 1/51 refers to a specific type of distributed denial of service (DDOS) attack that exploits vulnerability in network protocols. It takes advantage of the way these protocols handle incoming traffic, leaving the target system with an excessive number of requests. The name "1/51" stems from the fact that for every 51 packets sent by the attacker, only one response is needed, making it effective highly resource intensive, an attacker could exploit this vulnerability. Cyber security risks in outdated software and systems include those that are not updated, automated scripts that run without virus scanning and cause malfunctions, and configuration vulnerabilities. Misconfiguration vulnerabilities in network devices or systems create security gaps. For example, leaving default passwords unchanged on network devices makes them an easy target for attackers [7]. Identify risks, assess the problem, and determine technical measures, remediation methods, and appropriate solutions for IT systems. Complete control over data elements and network access to prevent any cyber-attacks. Steps taken periodically to confront and address cyber threats by monitoring, identifying, and assessing them. In order to manage them effectively, this requires a comprehensive view of these risks and cooperation from all employees. As we delve into the intricacies of this landscape, it becomes evident that a comprehensive understanding of the diverse range of cyber threats is essential for developing effective defense Strategies. Figure 1 gives the categorization of cyber threats.

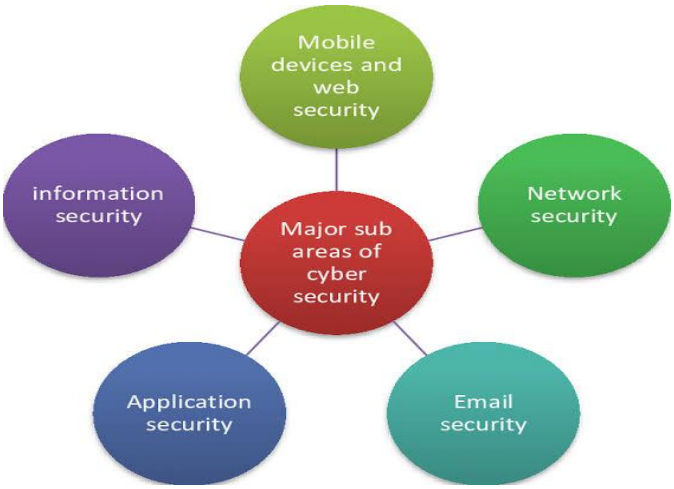

Figure 2: Schematic of classifications of cyber threats [3]

4.6 Motivations and Objectives Behind Cyber Attacks

The motivations and objectives behind cyber-attacks are diverse, reflecting the complex landscape of cyberspace and the varied interests of those involved in such activities [2]. Cyber attackers, or threat actors, may include individuals, organized crime groups, hacktivists, and even nation-states. Understanding the motivation behind cyber-attacks is crucial for developing effective cyber security strategies. Some common motivations and objectives for cyber-attacks are shown in Figure 3.

Figure 3: Schematic of Motivation and Objectives for Cyber Attacks [3]

Many cyber-attacks are financially motivated. Criminals seek to steal sensitive information, such as credit card details, banking credentials, or personal identifiable information (PII), which can be monetized on the dark web Ransom ware attacks, where attackers demand payment in exchange for restoring access to data or systems, and exemplify this motivation. Nation-states may conduct cyber espionage to gain a strategic advantage by stealing sensitive information related to military, economic, or political matters. These attacks often target government agencies, defense contractors, and critical [3].

A "drive-by" software weakness in Windows 10 and Windows 11 system that enables those systems to be hacked and access to operating device data. Print Nightmare's software problems with the Windows Print Spooler services, and even released updates for Windows 7 systems that it had stopped supporting.

While technological advancements play a crucial role in cyber security, the human element remains a pivotal factor in fortifying digital defenses Understanding and addressing human vulnerabilities [3].

4.7 Technical Measures

- Firewalls and other protective devices at the system boundary to protect against unauthorized information flows in or out of the system
- Intrusion detection devices to detect, log, and analyze unauthorized attempts to access a system, often resulting in alarms so that timely defensive measures can be taken
- Public Key Infrastructure (PKI)
- Auditing of activity logs, system configuration changes, and other events to detect and respond to suspicious or prohibited actions
- Security testing, including simulated hostile attacks, to verify the robustness of information protection and identify deficiencies that must be corrected.

- Access control mechanisms to enforce user privileges and restrict unauthorized use of resources and data [6].

5. Recommendations

As cyber threats become by leveraging advanced technologies, fostering a security-conscious culture, and preparing for future developments such as quantum computing, organizations can enhance their resilience and effectively protect their digital assets. Encryption is not an option, and security incidents are very expensive in every meaning of the word.

Research focused on cybercrimes, risks, and protection methods in cyber security for countries and institutions, as well as the problem of identifying vulnerabilities and risks, implementing technical measures, and identifying solutions and treatments that help in protection.Through research, we note that there are numerous threats and violations facing cyber security, it is necessary to develop tools to protect against these threats, supporting protection and monitoring. Protecting operating systems and technologies used and preventing attacks and crimes targeting government agencies and state institutions. Through research, it is explained how to identify security vulnerabilities, cybercrimes, and the necessary measures for protection. In light of the risk and potential consequences of cyber events, every mitigated risk or prevented attack strengthens cyber security. The comprehensive review on cyber security underscores the critical importance of staying ahead of modern threats through advanced defense strategies.

6. Conclusion

In conclusion, the comprehensive review on cyber security underscores the critical importance of staying ahead of modern threats through advanced defense strategies. As cyber threats become more sophisticated, organizations must adopt a proactive and adaptive approach to cyber security. By leveraging advanced technologies, fostering a security-conscious culture, and preparing for future developments such as quantum computing, organizations can enhance their resilience and effectively protect their digital assets. Encryption is not an option, and security incidents are very expensive in every meaning of the word. As organizations navigate the complexities of the digital age a forward-looking and strategic approach to cyber security is paramount for securing the digital future.

References

[1] Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., &Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. Electric Power Systems Research, 215, 108975.
[2] Dutta, A. (2021). Human factors affecting digital security
[3] Enebe, G.C., Ukoba, K., & Jen, T.C. (2019). Numerical modeling of effect of annealing on nanostructured CuO/TiO2 pn heterojunction solar cells using SCAPS.
[4] NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.
[5] Barth, Bradley. (2018). Monero bug that doubled coin transfer amounts allowed attackers to steal from Altex.exchange. SC magazine, 3 August 2018.
[6] Matthew, Lee. (2017). File with 1.4 Billion Hacked and Leaked Passwords Found on the Dark Web. Forbes, 11 December 2017.
[7] Matthew, Lee. (2017). File with 1.4 Billion Hacked and Leaked Passwords Found on the Dark Web. Forbes, 11 December 2017.
[8] Ahmed Jamal et al., 2021 A review on security analysis of cyber physical systems using machine learning
[9] Al-Ghamdi, 2021 Effects of knowledge of cyber security on prevention of attacks
[10] Al Shaer et al., 2020 Hydroxamate siderophores: Natural occurrence, chemical synthesis, iron binding affinity and use as Trojan horses against pathogens
[11] Alghamdi, 2021 Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia