SHIFRA
Vol. (2023), 2023, pp. 73–85
ISSN: 3078-3186

Research Article

The Evolution of Cybersecurity Threats and Strategies for Effective Protection. A review

Hasan Ahmed Salman[1,2,*], Abdulazeez Alsajri [1,3]

[1] *Department of Computer Science, University Arts, Sciences and Technology, Beirut, Lebanon.*
[2] *Computer Center, University of Nahrain, Baghdad, Iraq.*
[3] *Al-Mashahadah Municipality Directorate, Baghdad Municipalities Directorate, Baghdad Governorate, Baghdad, Iraq.*

ARTICLE INFO

Article History
Received 20 Apr 2023
Revised: 15 Jun 2023
Accepted 15 Jul 2023
Published 1 Aug 2023

Keywords
Cybersecurity,
Malware,
Phishing Attacks,
Intrusion Detection Systems (IDS),
Ransomware.

ABSTRACT

Cybersecurity has become an increasingly crucial priority for individuals, organizations, and governments due to the growing reliance on technology and internet connectivity. This paper explores the various threats posed by cyber-attacks, such as malware, ransomware, and phishing, that exploit security vulnerabilities to access sensitive information or disrupt systems. It emphasizes the need for comprehensive defense strategies to safeguard digital systems and ensure the continuity of vital processes. The paper also highlights the evolution of cyber-attacks, from simple viruses to sophisticated state-sponsored attacks, and outlines key elements for enhancing cybersecurity, including threat protection, incident response, and user awareness. The paper concludes by advocating for a proactive approach to cybersecurity through technological advancements, legal frameworks, and collaborative efforts at national and international levels.

1. INTRODUCTION

Cybersecurity has become one of the most important priorities at the level of individuals, organizations and countries. With the increasing dependence on technology and internet connectivity in all aspects of life, the threat from cyber-attacks targeting sensitive data and digital infrastructure has also increased [1].

Cyber-attacks are not just technical threats, they represent a real danger that can affect the economy, national security, and personal privacy. These threats range from malware (Malware) and viruses to ransomware (Ransomware) and phishing (phishing) attacks, all of which seek to exploit security vulnerabilities to access information or disrupt systems[2].

Understanding and realizing the importance of cybersecurity risks is an essential step to protecting digital systems and ensuring the continuation of vital processes. Without adequate insurance, the consequences can be catastrophic, ranging from the loss of sensitive financial data to the disruption of basic services on which millions of people depend.

This introduction aims to highlight the importance of cybersecurity and the challenges it faces, while emphasizing the need to develop effective defense strategies to counter the growing threats in this area. By adopting a strong security approach, we can protect information and digital assets from the threats that are constantly evolving in the cyber world[2].

2. DEFINITION OF CYBERSECURITY

Cybersecurity: - is the practice of protecting systems, networks and programs from digital attacks. These attacks are usually aimed at accessing, changing or destroying sensitive information, extorting money from users, or disrupting normal business operations [1].

Cybersecurity includes a set of preventive measures, technologies and procedures aimed at protecting systems, networks and data from cyber threats. This includes securing information stored on computers and servers, protecting data during its transfer over networks, and ensuring the security of systems from malware and other attacks [1].

2.1. cyber security includes and includes several areas, including

1. Network security: protecting networks from intrusions or attacks aimed at unauthorized access or disruption of services[3].

*Corresponding author email: has062@live.aul.edu.lb
DOI: https://doi.org/10.70470/SHIFRA/2023/009

2. Application security: securing programs and applications from potential attacks that may exploit security vulnerabilities in applications [3].
3. Information security: protection of sensitive data and information from unauthorized access, modification or leakage [3].
4. Identity management and access control: ensuring that only people who have access to systems and information have this right [3].
5. Process Security: apply and implement the necessary policies and procedures to protect digital assets and ensure that operations continue safely [3].

2.2 The concept of cyber security

It refers to a set of processes, technologies and practices designed to protect devices, networks, software and data from cyber-attacks or any type of digital threat. Cyber security includes all measures taken to ensure the security, confidentiality, safety and availability of information and systems that are exposed to threats via the internet [4].

2.3 The main goal of cyber security

Protecting digital systems from cyber threats that can range from malicious attacks such as viruses and malware to intrusion attempts, hacking, data theft, or even shutting down the service through DDoS attacks. This requires a comprehensive approach that integrates advanced technology, security policies and organizational procedures, as well as security awareness of users[1].

2.4 Key elements of the concept of cybersecurity

Threat protection: it includes protecting systems and networks from malicious attacks that may lead to unauthorized access, data corruption or theft.

Prevention: includes the development of preventive strategies and systems to prevent attacks before they occur, such as the use of firewalls, antivirus programs, and intrusion detection systems.

Incident response: develop plans and procedures for an effective response in the event of a cyberattack, including data recovery and restarting affected systems.

Recovery: securing the return of systems and services to their normal state after being attacked, ensuring that the same incidents do not recur.

Education and awareness: promoting security awareness among users and training them on how to protect themselves and their systems from cyber threats[4].

2.5 The importance of cyber security

With the ever-increasing use of technology and reliance on the internet in various aspects of life, cybersecurity has become essential to ensure the protection of sensitive information, preserve privacy and ensure the continuity of business and services.

In light of the growing cybersecurity threats, it has become necessary for organizations and individuals to be fully aware of the concept of cybersecurity and the importance of applying it comprehensively to ensure the safety and security of the digital environment[1].

3. THE EVOLUTION OF CYBER ATTACKS

the world is experiencing, cyber-attacks have evolved significantly in terms of complexity and impact. These attacks with the rapid technological progress and digital transformation are becoming more diverse and innovative, making them a serious threat to individuals, companies and governments alike. The evolution of cyber-attacks can be traced, as they have gone from relatively simple attacks to complex and organized ones, through multiple stages[5].

1- The first stage: conventional attacks:
Viruses and worms: at the beginning of the computing era, cyber-attacks were relatively simple, often focused on viruses and worms that spread through physical media such as floppy disks and then via email and the internet. This malware was intended to damage data or disrupt systems[5].

2- The second stage: organized attacks:
Phishing attacks: cyber-attacks are beginning to evolve to include more intelligent methods such as phishing, where users are tricked into revealing their personal information through fake emails that appear to be from reliable sources.
Targeted attacks: targeted attacks have appeared that target specific organizations or individuals, and these attacks are often highly sophisticated and aimed at accessing sensitive information[5].

3- Stage three: complex and funded attacks:
Advanced Malware: malware has begun to evolve to become more sophisticated, as it has become able to evade detection and disable traditional protection systems. Examples of this are attacks such as Stuxnet and flame that targeted critical infrastructure.

Ransomware: ransomware attacks have become common, where attackers encrypt victims ' files and demand a ransom in exchange for the decryption key. Attacks such as WannaCry and Petya were some of the most prominent examples that caused significant losses globally[5].

4- The fourth stage: organized and cross-border attacks:
State-orchestrated attacks: recent years have seen an increase in cyber-attacks directed by states or state-backed entities, targeting critical infrastructure, stealing industrial secrets, or influencing international elections and policies.
Cyber-attacks on supply chains (Supply Chain Attacks): attackers are targeting companies through vulnerabilities in supply chains, as happened in the SolarWinds attack that affected many companies and governments around the world[5].

5- Current stage: smart and sophisticated attacks:
AI-powered attacks: attackers have come to rely on AI technologies to improve the accuracy and effectiveness of their attacks. These attacks can quickly adapt to different environments and penetrate systems in New and unexpected ways.
Attacks on the Internet of Things (IoT): with the widespread spread of devices connected to the internet, cyber-attacks have begun to target these devices that are often weak in terms of security, making them easy targets for attacks[5].

4. THE IMPORTANCE OF CYBER PROTECTION

Cyber protection, or cybersecurity, has become a must in the modern digital world. With the increasing reliance on technology and digital communications, the risk of cyber threats targeting individuals, institutions, and governments alike is also increasing. Here are some reasons that explain the importance of cyber protection[2]:

1- Protection of sensitive data:
Personal data: cyber protection includes ensuring that unauthorized persons do not have access to personal information, such as names, addresses, phone numbers and financial information. The theft of this data can lead to identity attacks and financial theft[3].
Business data: for companies, the protection of confidential, financial and customer-related data is vital. Any leakage of this data can damage the company's reputation and lead to significant financial losses.

2- Ensuring business continuity:
Cyber-attacks such as DDoS attacks can disrupt the systems and services that companies rely on for their daily work. Cyber protection helps ensure business continuity by preventing such attacks or mitigating their effects.
Incident Response Plans: having effective cyber incident response plans ensures that a business can recover quickly after an attack, reducing the time periods in which the business is affected[2].

3- Maintaining trust and reputation:
Customers and partners: companies rely on the trust that customers and Partners place in them. Any penetration or leakage of information can lead to the loss of this trust and negatively affect business relations.
Compliance with laws and regulations: there are many regulations and laws that force companies to protect customer data, such as the General Data Protection Regulation (GDPR) in the European Union. The commitment to cyber protection ensures that companies remain compliant with these laws, which helps in avoiding fines and legal penalties[3].

4- Combating cybercrime:
Countering cyber-attacks: with the increase of cyber-crimes such as phishing, ransomware attacks, and online fraud, cyber protection has become essential to prevent and combat these crimes.
International cooperation: cybersecurity helps strengthen cooperation between countries to combat cross-border cybercrime, as attacks are often Global and target victims in different countries[3].

5- Supporting digital innovation:
Encourage innovation: in a secure environment, companies and individuals can innovate without fear of cyber threats. Cyber protection provides a secure framework within which new technologies and innovative applications can be developed[4].
Protection of critical infrastructure: many vital sectors, such as energy, water and telecommunications, rely on digital technology. Securing this infrastructure from cyber-attacks protects the essential services on which society depends.

6- Strengthening national security:
Defense against organized attacks: cyber-attacks targeting critical infrastructure, such as energy or defense systems, pose a serious threat to national security. Cyber protection contributes to the defense of this infrastructure and ensuring its safety[5].

Protecting government institutions: cyber protection helps secure government systems and sensitive information from threats that may be supported by countries or terrorist groups.

5. CURRENT CYBER THREATS

1- Ransomware attacks
In which attackers encrypt the victim's data and demand a financial ransom in exchange for re-decryption, targeting large companies and critical infrastructure.
Example: one of the most famous attacks is WannaCry and Petya, which caused significant damage globally[6].

2- Phishing
It is an attempt to deceive users to obtain sensitive information such as usernames and passwords, through fake emails or websites that appear legitimate[6].

3- Supply chain attacks
Description: these attacks target companies through vulnerabilities in their supply chains. Attackers hack through suppliers or third parties to gain access to target systems.
Example: the SolarWinds attack that affected many companies and governments was a prime example of this type of attack[6].

4- Malware
Malware that is installed on devices without the user's knowledge, and is used to steal data, monitor activity, or control the device remotely[1].
Such as malware that avoids detection or uses technologies such as artificial intelligence to disable protection systems.

5- Distributed denial of service attacks (DDoS)
Description: these attacks rely on flooding servers or networks with phony requests beyond their ability to respond, which leads to disruption of services[9].
DDoS attacks are becoming more sophisticated, with networks of compromised devices (botnets) being used to increase the size and impact of the attack.

6- State-Sponsored attacks
Description: these attacks are carried out by countries or government-backed entities for the purpose of espionage or causing damage to the sensitive infrastructure of another country.
Recent developments: these attacks focus on targeting critical infrastructure, spying on industrial secrets, or influencing elections and public policies[9].

7- Internet of Things (IoT)attacks
Description: with the wide spread of devices connected to the internet, these devices have become easy targets for cyber-attacks, especially since many of them have weak security measures[7].

8- Cloud Attacks
Description: as companies increasingly rely on cloud services, these services have become the target of cyber-attacks, as attackers seek to penetrate cloud servers and steal data, modern attacks focus on exploiting security vulnerabilities in cloud platforms or unauthorized access through APIs[6].

5.1. Types of malware

1- Viruses: programs that multiply by copying themselves to other programs or files, resulting in file corruption or information theft.
Worms: they are similar to viruses but do not need a host file to spread. Worms can cause flooding of networks and significantly increase traffic, disrupting systems.
Trojans: they look like legitimate programs, but they contain malicious functions. They are commonly used to create backdoors in systems that enable attackers to gain unauthorized access.
Ransomware: encrypts user data and demands a ransom for decryption, often targeting large organizations.
Spyware: monitors users ' activity on their devices and steals sensitive information such as passwords and financial information.
Advertising software (Adware): it displays unwanted ads on infected devices, and it can also be part of spyware.

2- Methods of spreading malware
Email: malware usually infects devices through malicious email attachments or phishing links.
Downloads from the internet: malware can be attached to programs downloaded from unreliable sources, or embedded in fake websites.
USB devices: malware can be transmitted via external storage devices such as USB modules.
Networks: malware may spread through infected networks, especially if the systems are not adequately protected.

3- Malware damage
Data theft: malware can steal sensitive information such as bank account logins or passwords.
Disruption of systems: may lead to complete disruption of systems, causing financial losses to companies and loss of productivity.

Financial extortion: as is the case with ransomware, where attackers demand a ransom to regain access to data or systems.
Spyware: spyware can collect personal information without the user's knowledge and be used for malicious purposes[6].

5.1.1 Malware protection strategies

Using antivirus software: installing and updating antivirus software regularly can provide the first line of defense against malware.
Security updates: keeping systems and software updated periodically helps fill security gaps that can be exploited by malware.
Awareness and training: training users to recognize malicious emails and safe browsing practices can reduce the risk of malware infection.
Data backup: performing regular data backups ensures data recovery in case of ransomware infection.

6. METHODS OF CYBER ATTACKS

1- Attacks on Networks (denial of Service - DoS)
Distributed denial of service (DDoS) attacks: they are aimed at flooding a network or server with massive traffic that leads to disruption of services. It is carried out using networks of hacked devices known as (Botnet).
Data Flooding: sending huge amounts of data to a specific server to disrupt its work.
Eavesdropping on the network.
Passive eavesdropping: data transmitted over the network is intercepted without being modified, often with the aim of stealing sensitive information such as passwords.
Attacks on network protocols: such as attacks on protocols such as DNS to direct users to malicious sites[9].

2- Software-Based Attacks
Exploiting Software Vulnerabilities
Zero-day attacks: exploitation of unknown software vulnerabilities by developers or users.
Code injection: such as SQL Injection, where malicious SQL commands are entered into databases via web applications.
Attacks on software interfaces (API Attacks)
Attacks on application programming interfaces (APIs): exploit vulnerabilities in APIs to gain access to unauthorized data or functions[8].

3- Identity-Based Attacks Phishing
Email phishing: sending phishing emails claiming to be from trusted sources with the aim of stealing users ' data.
Spear Phishing: a customized phishing attack targeting specific individuals or companies, with customized information included to increase the chances of success.
Password Attacks
Brute Force Attacks: try to guess passwords by trying all possible combinations.
Combined password Spraying attacks: try the same common password on many accounts before the attack is detected[6].

4- Insider Attacks
Exploitation of privileges (Privilege Escalation)
Horizontal lifting of powers: the attacker gets the powers of another user at the same level.
Vertical lifting of powers: the attacker gets higher powers, which gives him access to sensitive resources or information.
Malicious Insider
Treacherous employee: exploiting the employee's powers to steal, destroy data or disrupt the system[10].

5- Social Engineering Attacks
Phishing attacks: using phone calls to trick users into obtaining sensitive information.
Text message attacks: phishing messages that contain links that lead to malicious websites or ask for personal information Guessing attacks (Pretexting)
Impersonation: an attacker pretends to be a trusted person or organization to gain access to sensitive information[5].

6- Storage-Based Attacks
Malware on mobile devices: exploits vulnerabilities in mobile phones to access data or control the device.
Attacks on network equipment: such as attacks on routers to access or disable networks[7].

6.1 Methods of targeted attacks on individuals

She relies on psychosocial manipulations and technical techniques to achieve her goals.

1- Email phishing: attackers send emails that appear to be from a trusted source (such as a bank or a well-known company) to convince the victim to click on a malicious link or provide sensitive information such as passwords or credit card numbers.

2- Social engineering

Attacks by phone (fishing): attackers call victims by phone pretending to be representatives of a company or government institution, asking them to provide sensitive information such as bank account numbers or passwords.

Impersonation: the attacker pretends to be a trusted person, such as a co-worker or family member, to convince the victim to provide confidential information or perform a certain action.

Pretexting: the attacker creates a fake story or scenario to convince the victim to reveal sensitive information.

3- Spy software (Spyware)

Installing spyware: attackers may convince the victim to install programs that look legitimate but contain spyware that monitors their online activity and collects sensitive information.

Attacks on webcams: exploit vulnerabilities in devices to gain access to webcams and record victims without their knowledge.

3.Malware (Ransomware): a malicious program is installed on the victim's device that encrypts her files, and demands a financial ransom for decryption.

Trojan: malware that appears as a useful program but when installed, it performs malicious operations such as stealing data or opening back doors for attackers to gain access to the device.

4- Threatening to publish sensitive information: private information or photos if his financial demands are not met.

Defamation: personal or sensitive information about the victim is revealed online, such as home addresses or phone numbers, with the aim of embarrassing or harming the victim.

5- Attacks on social media

Fraud via fake accounts: pretending to be a friend or colleague of the victim, using him to extract sensitive information or to ask for money.

Account theft: targeting and stealing social media accounts to access personal information or using them to post malicious content.

6- Exploitation of public Wi-Fi networks: attackers install surveillance tools on unsecured public Wi-Fi networks to access the data of users connected to those networks.

7- Online Financial Fraud

Fraud through fake websites: creating fake websites that resemble the websites of banks or electronic stores with the aim of stealing credit card information.

Identity theft: the use of stolen personal information to carry out fraudulent operations on behalf of the victim, such as opening bank accounts or applying for loans.

8- Mobile Device Hacking

Installing malicious apps: convincing the victim to install apps that look legitimate but contain malware that steals data or tracks activity on the phone.

Bluetooth Exploits: exploit Bluetooth vulnerabilities to access phone data or install malware remotely[8,9,10].

7.THE IMPACT OF CYBER ATTACKS

It affects individuals, companies, and government institutions. These effects range from financial and Economic to social and psychological, and may lead to legal and security repercussions.

1- Financial impacts

Direct financial losses: such as ransomware and the theft of financial data to large financial losses, whether through the payment of ransomware or the loss of funds from bank accounts.

Response and recovery costs: these costs include rebuilding damaged systems, hiring security experts to investigate breaches, and compensating affected customers.

Loss of revenue: disruption of services or business operations as a result of a cyber-attack that can lead to significant financial losses as a result of loss of sales or interruption of operations.

2- Security implications

Compromising sensitive information: leads to the leakage or theft of sensitive data such as personal information or confidential government data, posing a threat to national security or personal security.

Declining trust: attacks targeting critical infrastructure (such as power grids or transportation systems) can threaten public security and lead to panic.

3- Legal and regulatory effects

Legal accountability: companies that fail to protect their customers ' data may face lawsuits and large fines, especially if they violate data protection laws such as the General Data Protection Regulation (GDPR) in the European Union.

Regulation and supervision: large-scale attacks may lead to tighter regulation and supervision by government agencies, increasing the compliance burden on companies.

4- Social and psychological influences
Psychological pressure on individuals: individuals who are exposed to attacks such as identity theft or cyber blackmail may face severe psychological pressure as a result of anxiety and fear of the repercussions of the attack.
Impact on Reputation: companies that are exposed to cyber-attacks may suffer a deterioration in their reputation, which affects the trust of customers and partners and may lead to loss of customers and revenue.

5- Economic effects
Impact on markets: large-scale cyber-attacks, such as those targeting banks or financial markets, can lead to volatility in financial markets and large-scale economic losses.
Disruption of business processes: attacks targeting supply chains or critical infrastructure can lead to disruption of economic and industrial processes, harming the economy at the macro level.

6- Impact on innovation and technology
Declining trust in technology: cyber-attacks can lead to declining trust in new technology such as the Internet of Things (IoT) or cloud services, hindering the widespread adoption of these technologies.
High costs of cybersecurity: companies may have to invest large sums in strengthening security infrastructure and cybersecurity training, which affects their investments in innovation and development[9,10]

8.TOOLS OF CYBER ATTACKS

Cyber-attacks are based on tools that attackers use to hack systems, steal data, or disrupt services. These tools must be advanced, used in attacks targeting individuals, companies or critical infrastructure.

1- Malware
Viruses: malicious software that spreads from one device to another, infects files and causes multiple damages such as deleting data or disabling systems.
Worms: malware that spreads automatically over networks without the need for user interaction, and usually causes network congestion and system damage.
Trojans: malicious software that appears to be legitimate software but opens back doors in the system to facilitate the entry of attackers.
Ransomware: software that encrypts the victim's files and demands a financial ransom in exchange for decryption.
Spyware: software that tracks user activity and collects sensitive information such as passwords without his knowledge.

2- Social engineering tools
Phishing Kits: ready-made toolkits that allow attackers to create fake web pages and emails to entice victims to provide their personal information.
Impersonation Tools: software that helps attackers impersonate trusted individuals or organizations to access sensitive information.

3- Exploit tools
Exploit kits: tools designed to detect and exploit vulnerabilities in systems and programs, commonly used in attacks on websites.
Metasploit Framework: a powerful tool used for penetration testing and vulnerability detection, but also used by attackers to exploit those vulnerabilities.
Password Cracking Tools: programs such as "John the Ripper" and "Hashcat" are used to guess or crack passwords using techniques such as brute force attack or dictionaries.

4- Network Tools
Network Scanners: like "Nmap", they are used to scan networks for connected devices, open services, and vulnerabilities.
Network eavesdropping tools (Sniffing Tools): such as "Wireshark", are used to capture and analyze data traffic over the network, enabling attackers to gain access to sensitive information such as passwords or session details.
Denial of service attack tools (DDoS Tools): such as "LOIC" and"HOIC", are used to flood servers with huge traffic, which leads to their disruption and blocking access to services.

5- System Intrusion Tools
Remote Access Tools (RATs): software that allows attackers to fully control the victim's device remotely, such as "njRAT" and"DarkComet".
Privilege Escalation Tools: used to gain higher privileges in the system once hacked, giving the attacker greater control over the device.

6- Data manipulation Tools

Encryption and decryption Tools: software used to encrypt or decrypt data, both to protect data and to hide malicious activity.
Anti-Forensic tools: used to hide or destroy forensic evidence after a cyber attack to prevent attackers from being tracked down.

7- Wireless hacking tools
Wi-Fi Cracking tools: such as "Aircrack-ng", are used to hack encrypted Wi-Fi networks to access the network.
Man-in-the-middle attack tools: used to intercept and analyze data sent between two parties in a wireless network.

8- Stealth and analysis Tools
Anonymity Tools: such as "Tor"and" VPNs", are used to hide the identity of attackers while carrying out attacks.
System Monitoring Tools: software used to monitor and analyze the activity of Target Systems and devices before or during an attack[10,11][12].

9. THE MOST IMPORTANT TECHNIQUES FOR PREVENTING CYBER ATTACKS

Countering cyber-attacks requires the use of advanced technologies and integrated strategies to enhance security and protect systems and networks.

1- Firewalls
Traditional firewall: it acts as a barrier between the internal network and the external internet, monitoring and filtering data traffic based on predefined rules.
Next-Generation Firewall (NGFW): combines the functionality of traditional firewalls with advanced features such as application scanning, identity management, and Threat Protection.

2- Intrusion detection and prevention systems (IDS/IPS)
Intrusion Detection system-IDS: monitors the network or systems for suspicious activity or security breaches and alerts administrators.
Intrusion Prevention system (IPs): it not only detects possible attacks but also prevents them by taking automatic actions to stop the threat.

3- Encryption techniques
Data-in-Transit Encryption: used to protect data as it travels over the network using protocols such as TLS / SSL.
Data-at-Rest encryption: to protect data stored on hard disks or other media using algorithms such as AES.

4- Multi-Factor Authentication (MFA)
Authentication components: multi-factor authentication requires users to provide more than one verification factor, such as a password and a code that is sent to the mobile phone, which makes hacking accounts more difficult.
Biometric: involves the use of biometric data such as fingerprint or facial recognition as part of the verification process.

5- Virtual private network (VPNs)technologies
Business VPN: used to secure remote employee communications with company intranets, where the traffic between the device and the network is encrypted.
Personal VPN: protects users ' online privacy by hiding their IP addresses and encrypting their online activities.

6- Antivirus and anti-malware software
Antivirus: scans systems and files to detect and remove viruses.
Anti-Malware: provides comprehensive protection against all types of malware such as ransomware, spyware, Trojans.

7- Backup and Recovery Solutions
Regular backup: maintain data backups regularly to ensure the ability to restore data in case of loss or attack.
Disaster Recovery Systems: plans and tools that allow systems and data to be quickly restored in the event of a cyber-attack or disaster.

8- Identity and Access management technologies (IAM)
Role-based access control (RBAC): enables the management of access rights to systems and data based on the roles of users in the organization.
Identity management systems: ensures that access is granted only to authorized users using advanced security protocols.

9- Behavior analysis techniques
User behavior analysis: monitors user activity to detect unusual patterns that may indicate malicious activity.
Entity Behavior Analysis: monitors devices and applications for any unusual behavior that may indicate internal or external threats.

10- Email protection technologies (Email Security)
Spam filtering: filters out unwanted messages and prevents them from reaching your inbox.
Phishing Detection: advanced technologies for analyzing emails and detecting phishing attempts and fraud.

11- Cloud Security Technologies
Cloud security: includes the necessary security measures to protect data and applications located in the cloud using technologies such as encryption and continuous monitoring.
Cloud Access Management (Cloud Access Security Brokers-CASB): tools that provide accurate monitoring and control of access to cloud services.

12- Security Awareness and Training
Regular training programs: training employees on the latest attack technologies and how to deal with them

Phishing simulations: organizing a phishing attack simulation to teach employees how to identify and deal with phishing attacks[13,14,15].

9.1 The firewall

Used as a first line of Defense to protect networks and systems from cyber-attacks. It acts as a security barrier between the internal network (or computer) and the outside world (the internet), monitoring and filtering traffic based on a set of predefined rules.

Types of firewalls:

1- Packet-Filtering Firewall
Examines data packets transmitted over the network and decides to allow or block their passage based on information such as IP address and ports used.

2- Application-level based firewall
Works at the application level and examines traffic related to various applications.
It can block malicious traffic based on data content and not just on addresses and ports.

9.1.1 Next-Generation Firewall-NGFW

Combines the functionality of traditional firewalls with additional features such as application scanning, identity control, protection from advanced threats.

It provides comprehensive protection against a wide range of complex cyber attacks.

Proxy Firewall:

Acts as an intermediary between users and the internet, preventing direct communication between the parties.

Redirects requests from users to the desired destination after checking them.

The role of the firewall in protecting against cyber attacks:

- prevent unauthorized access:
- prevents attackers from accessing networks and systems by filtering incoming and outgoing traffic.
- it allows only authorized users to access sensitive resources.
- protection of sensitive data.
- prevents leakage of sensitive data by setting strict rules for data transmission.
- prevents attempts to hack data during its transmission over the network.
- Preventing denial-of-service attacks (DDoS).
- detects and prevents distributed denial of service attacks by identifying abnormal traffic.
- filtering excessive requests aimed at flooding the target server.
- protection against malware.
- checking traffic for malware and preventing it from entering the network.
- prevent the download or execution of malicious software that may arrive via email or malicious websites.
- Recording and monitoring activity.
- record all activities and communications that occur on the network.
- provides logs that can be used to analyze security incidents and detect suspicious activities.[10]

10.BEST PRACTICES FOR ENHANCING CYBERSECURITY

1- Regularly update systems and software
Address newly discovered loopholes.
Modern software: use versions the latest security technologies.

2- Use strong and complex passwords that include numbers, uppercase and lowercase letters, and symbols.

3- Application of multi-factor authentication (MFA)
Multiple verification: login to sensitive accounts.
Biometric technologies: the use of technologies such as fingerprint or facial recognition as part of the verification process.

4- Regular data backup
Backup: make regular backups of important data and store them in secure locations.

Backup testing: be sure to test backups periodically to ensure the ability to restore data when needed.

5- Data encryption
Encrypt data in motion: use protocols such as TLS / SSL to encrypt data as it is transferred over networks.
Data encryption at rest: protect data stored on devices through the use of encryption.

6- Security awareness training for employees
Regular training: train employees on how to recognize cyber threats such as phishing and how to deal with them.
Simulated attacks: implement a simulation of phishing attacks to assess employee readiness and awareness.

7- Using firewalls and intrusion detection systems (IDS)
Firewalls: make sure the firewall is up to date and working properly to protect the network from attacks.
Intrusion detection systems: use intrusion detection and prevention systems to monitor the network and alert about any unusual activity.

8- Review and adjust access permissions
Limit permissions: make sure that users have only the necessary permissions to perform their tasks.
Periodic Review: Review access permissions regularly to make sure there are no unnecessary or excessive permissions.

9- Manage assets effectively
Asset identification: keep an accurate record of all hardware and software used in the organization.
Asset monitoring: continuously monitor all assets to ensure protection against any threats.

10- Planning an incident response in the event of a security breach.

11- Reduce the risk of external suppliers
They adhere to strict cybersecurity standards.
Service level agreements (SLAs): include security requirements in service level agreements with suppliers.

12- Awareness of evolving cyber threats participate in conferences and read relevant publications.

13- subscribe to security alerts: provided by recognized institutions to follow up on new threats.

11. LEGISLATION AND LAWS RELATED TO CYBERSECURITY

1- International cybersecurity laws: Budapest Convention on cybercrime(2001)
The first international treaty that seeks to combat cybercrime by coordinating national legislation and facilitating international cooperation in investigations and prosecutions.
The agreement emphasizes the protection of computer systems and data from unauthorized access and malicious attacks.
The General Data Protection Regulation (GDPR) of the European Union:
Although the GDPR is mainly focused on the protection of personal data, it has strict security requirements to protect this data.
The regulation includes strict cybersecurity standards and the imposition of large financial fines on companies that fail to protect user data.

2- National cyber security legislation:
Cybersecurity law in the United States:
The Cybersecurity Act of 2015 (Cybersecurity Act of 2015): aims to promote the exchange of information on cyber threats between the public and private sectors, and improve coordination and cooperation in the face of cyber attacks.
Critical Infrastructure Protection Act (CISA): focuses on protecting critical infrastructure systems such as energy and communications from cyber threats.
Chinese cybersecurity law:
Regulates the collection, storage and use of data in China, establishes strict requirements for the protection of personal data and cybersecurity in enterprises and organizations.
Requires foreign companies operating in China to store user data locally and provide support to the government in Security Investigations.
Cybersecurity law in the United Arab Emirates:
Within the framework of the UAE Vision 2021, several laws and decrees related to cybersecurity have been issued, such as the Cybercrime Law (2012), which punishes crimes committed using information technology.
The National Electronic Security Authority (NESA) was established to establish standards and controls for cybersecurity in vital sectors.

3- Cybersecurity legislation in the Middle East:
Kingdom of Saudi Arabia:
The kingdom has issued the law on combating information crimes (2007), which aims to protect systems and information from illegal access and cybercrime.
The National Cyber Security Authority (NCA) was established to develop national cyber security strategies.

Egypt:
The law on combating Information Technology Crimes (2018) was issued to regulate the safe use of the internet and impose penalties for cybercrime.
The law is aimed at protecting personal data, securing networks and websites.

4- Regulatory frameworks and directives:
Cybersecurity of critical infrastructure:
Many countries such as the United States, the European Union, and the Gulf states provide guidance to protect critical infrastructure such as energy, water, and telecommunications systems from cyber threats.
ISO/IEC 27001 standards:
Provides an international standard for information security management systems (ISMS), and helps organizations protect information assets from cyber threats.

5- Challenges of implementing legislation:
Adapting to evolving threats: lawmakers need to constantly update laws to keep up with changing and evolving cyber threats.
International cooperation: dealing with cybercrime requires cooperation between countries to ensure that perpetrators are prosecuted across national borders.
Privacy protection: there is a need to balance laws between protecting cybersecurity and ensuring the privacy rights of citizens[10,11].

12. THE FUTURE CHALLENGES OF CYBERSECURITY

1- The rapid development of cyber threats
Artificial intelligence and advanced attacks: the use of artificial intelligence in the development of cyber-attacks may lead to the emergence of more complex and precise attacks, making them more difficult to detect and counter.
Intelligent malware: malware evolves to be able to adapt to different security environments and circumvent protection systems.

2- Increasing the number of devices connected to the Internet (Internet of things)
The expansion of the Internet of things: as the number of devices connected to the internet (IoT) increases, the number of vulnerabilities that attackers can exploit increases.
Lack of security in IoT devices: a lot of IoT devices do not have an adequate level of security, which makes them easy targets for attacks.

3- Challenges associated with cloud computing
Security Management in cloud environments: the transfer of data and operations to the cloud increases the complexity of security management, especially with regard to data protection and Privacy.
Cloud hacks: any breach in the cloud infrastructure can have a significant impact on the stored data and services that organizations rely on.

4- Threats from within (Insider Threats)
Unreliable employees: internal threats remain one of the most serious challenges, as an unreliable employee can gain access to sensitive information and use it maliciously.
Human errors: even without bad intent, human errors can lead to significant security vulnerabilities.

5- The need for advanced laws and legislation
Disparity of laws between countries: the difference in legislation and laws related to cybersecurity between countries remains a major challenge, as attackers may exploit these legal loopholes.
Keeping up with technical changes: the evolution of current laws may not be fast enough to keep up with rapid technological advances, leaving gaps that can be exploited.

6- Attacks on critical infrastructure
Targeting national infrastructure: critical infrastructure such as electricity, water, and telecommunications have become prime targets for cyber attacks that can lead to major disruptions.
The high cost of recovery: attacks on these infrastructures may require significant resources to recover, putting enormous economic pressure on states.

7- Cyber-attacks on financial systems
Digital banks and cryptocurrencies: the increase in the use of digital financial systems and cryptocurrencies opens the door to new and complex attacks.
Sophisticated cyber fraud: attacks on financial systems may become more sophisticated and difficult to detect, exposing the global economy to significant risks.

8- Quantum computing
Current cryptographic threat: as quantum computing progresses, existing cryptographic algorithms may become ineffective, requiring the development of new cryptographic techniques resistant to quantum computing.

The impact of quantum computing on information security: quantum computing can radically change the way we protect data, creating new challenges in cybersecurity.

9- Privacy-related challenges

Personal data protection: with the increasing collection of personal data, it becomes more difficult to maintain privacy and protect it from exploitation.

Tracking users: the development of tracking and surveillance technologies raises concerns about how the data collected will be used and how it will be protected.

10- The shift towards relying on artificial intelligence in cybersecurity

Trust in automated systems: the heavy reliance on artificial intelligence to manage cybersecurity may become a challenge in itself, especially if these systems are exploited by attackers.

Lack of specialized competencies: there will still be a high demand for cybersecurity professionals who can understand and manage complex systems.

13. CONCLUSION

Cybersecurity is no longer just an option, it has become an imperative necessity for every organization or individual that relies on technology in their daily work. As cyber-attacks develop and become more complex, it requires us to adopt a proactive approach in securing digital infrastructure. Efforts should be joined at the International and domestic levels to develop laws and legislation that protect cyberspace and ensure the rights of individuals and enterprises.

- Recommendations:

1-enhancing cyber security awareness: the need to raise awareness among individuals and institutions about the risks of cyber-attacks and the importance of following best security practices.

2-organizing workshops and continuous training courses to educate employees about cyber threats and how to respond to them.

Funding:

The authors acknowledge that this research did not receive any financial backing from external agencies, commercial bodies, or research foundations. The project was completed independently.

Conflicts of Interest:

The authors report no conflicts of interest associated with this study.

Acknowledgment:

The authors are thankful to their institutions for their constant moral and professional support throughout this research.

References

[1] S. V. Amanoul, A. M. Abdulazeez, D. Q. Zeebare, and F. Y. H. Ahmed, "Intrusion Detection Systems Based on Machine Learning Algorithms," in IEEE Xplore, 2021, https://doi:10.1109/I2CACIS52118.2021.9495897 .

[2] M. E. Hathaway and A. Klimburg, "Preliminary Considerations: On National Cyber Security," in National Cyber Security: Framework Manual, A. Klimburg, Ed. Talin: NATO CCD COE Publication, 2012, pp. 1-34.

[3] Lachow, "Cyber Terrorism: Menace or Myth?" in Cyberpower and National Security, F. D. Kramer et al., Eds. Potomac Books Inc., 2009, pp. 437-463.

[4] Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," IEEE Access, vol. 10, pp. 93104-93139, 2022, https://doi:10.1109/ACCESS.2022.3204051 .

[5] P. Rosenzweig, "National Security Threats in Cyberspace," American Bar Association Standing Committee on Law and National Security and National Strategy Forum, Sep. 2009. [Online]. Available: http://afri.au.af.mil/cyber/Docs/panel1/threats_in_cyberspace.pdf. [Accessed: Mar. 29, 2013].

[6] K. Rajora and N. S. Abdulhussein, "Reviews research on applying machine learning techniques to reduce false positives for network intrusion detection systems," Babylonian Journal of Machine Learning, vol. 2023, pp. 26–30, 2023, doi: https://doi.org/10.58496/BJML/2023/005 .

[7] X. A. Larriva-Novo, M. Vega-Barbas, V. A. Villagrá, and M. S. Rodrigo, "Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies," IEEE Access, pp. 9005-9014, 2020, https://doi:10.1109/ACCESS.2019.2963407 .

[8] J. H. Allen, The CERT Guide to System and Network Security Practices. Boston, MA: Addison-Wesley, 2001.

[9] Gide and A. A. Mu'azu, "A Real-Time Intrusion Detection System for DoS/DDoS Attack Classification in IoT Networks Using KNN-Neural Network Hybrid Technique," Babylonian Journal of Internet of Things, vol. 2024, pp. 60–69, 2024, doi: https://doi.org/10.58496/BJIoT/2024/008 .

[10] J. A. Lewis, "Sovereignty and the Role of Government in Cyberspace," Center for Strategic and International Studies Journal, vol. XVI, no. II, Spring/Summer 2010.

[11] J. Cresswell, "Oxford Dictionary of Word Origins: Cybernetics," Oxford Reference Online, Oxford University Press, 2010.

[12] K. Saalbach, "Cyber War, Methods and Practice," Version 9.0, University of Osnabruck, Jun. 17, 2014.

[13] S. A. Abed, "Big Data and Artificial Intelligence on the Blockchain: A Review," Babylonian Journal of Artificial Intelligence, vol. 2023, pp. 1–4, 2023, doi: https://doi.org/10.58496/BJAI/2023/001 .

[14] Desai and M. Desai, "A Review of the State of Cybersecurity in the Healthcare Industry and Proposed Security Controls," Mesopotamian Journal of Artificial Intelligence in Healthcare, vol. 2023, pp. 82–84, 2023, doi: https://doi.org/10.58496/MJAIH/2023/016 .

[15] A.-H. Al-Mistarehi, M. Mijwil, Y. Filali, M. Bounabi, G. Ali, and M. Abotaleb, "Artificial Intelligence Solutions for Health 4.0: Overcoming Challenges and Surveying Applications," Mesopotamian Journal of Artificial Intelligence in Healthcare, vol. 2023, pp. 15–20, 2023, doi: https://doi.org/10.58496/MJAIH/2023/003 .