IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024

Cyber Security Layers and Awareness from Threats Lurk in Cyberspace for Preserving the Safety in Our Digital Environments

Kirti Saneja[1] and Dr. Ajit Kumar[2]
Research Scholar, Department of Computer Science[1]
Research Guide, Department of Computer Science[2]
Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan

Abstract: *The present paper focuses on cyber security awareness and the difficulties with cyber security maintaining the security of your data online. In the current digital era, when technology is developing quickly, cyber security is more important than ever. Cyber security is a vital field focused on protecting systems, networks, and data from digital attacks. It encompasses various practices, technologies, and processes designed to safeguard information integrity, confidentiality, and availability. The threat of cyber-attacks is increasingly global. Many worries have been raised about how it would affect the world economy. Businesses and groups, particularly those handling data pertaining to health, finances, or national security, must take precautions to safeguard their private and sensitive corporate information as the number of cyber-attacks rises. Therefore, it's necessary to consider the difficulties in enhancing citizens', customers', and employees' information security behaviours. In order to provide thorough protection, this paper examines the layers of cyber security and to ascertain the difficulties with cyber security safeguarding your data while using the internet.*

Keywords: Cyber Security, Awareness, Digital Attacks, Security Safeguarding

I. INTRODUCTION

Cyber security is the collection of tools, procedures, and methods created to guard against attacks, theft, damage, alteration, and unauthorized access to networks, devices, software, and data. This involves identifying and avoiding online scams as well as employing specialized programs to search for malicious software. You can guarantee the privacy of your data and the security of your online experiences by adopting sound cyber security practices.

We can protect ourselves from different cyber-attacks, such as phishing and DDoS attacks, by learning about cyber-attacks and cyber security. It shields your devices against malware and hackers by using techniques like firewalls and antivirus programs. The government, corporations, and healthcare facilities, among other organizations, process, store, and collect record amounts of data on computers. This data includes financial and military records as well as other potentially harmful properties like personal information. For these reasons, cyber security is essential.According to the Cyber security& Infrastructure Security Agency, cyber security is "the practice of ensuring confidentiality, integrity, and availability of information as well as the art of protecting networks, devices, and data from unauthorized access or criminal use." Every business uses information technology (IT) in some capacity; whether it's for service delivery, tracking shipments, or bookkeeping, the data must be secure. Cyber security measures make sure your company is always safe and running.

Where did it all start? We examine the development of cyber security from its inception to the present. When researcher Bob Thomas developed computer software named Creeper in the 1970s, it was able to traverse the ARPANET network and leave a breadcrumb trail in its wake. This marked the beginning of cyber security. Email's creator, Ray Tomlinson, created the program Reaper, which tracked down and eliminated Creeper. Reaper was the first computer worm ever, as well as the first instance of self-replicating software and antivirus software.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024

1.1 History of Cyber Security

1980s: The commercial antiviral industry began.

Commercial antivirus software was first introduced in 1987, despite conflicting reports over who invented the original antivirus program.

1987, Ultimate Virus Killer, the first antivirus program created by Andreas Lüning and Kai Figge, was also launched for the Atari ST. In the same year that three Czechoslovaks developed the initial iteration of the NOD antivirus, John McAfee established McAfee and launched Virus Scan in the United States.

1990s: The world goes online

As more people had access to the internet, more people started posting personal information online. Organized crime groups began using the internet to steal data from individuals and governments after realizing this could be a lucrative opportunity. Threats to network security had skyrocketed by the mid-1990s, necessitating the widespread production of firewalls and antivirus software to keep the public safe.

2000s: Risks increase in variety and quantity

Beginning in the early 2000s, governments clamped down on hacking as a criminal activity and imposed considerably harsher terms on individuals found guilty. At the same time, criminal organizations began to heavily fund professional cyber-attacks. Unfortunately, viruses also expanded as internet usage increased, despite information security continuing to progress in tandem.

2021: The following cohort

The cyber security sector is still expanding at a breakneck pace. According to Statista, the size of the worldwide cyber security market is expected to reach $345.4 billion by 2026. One of the most frequent risks to the data security of any organization is Ransomware, and its prevalence is expected to rise.

1.2 Problem on hand

Due to the growing reliance on computer systems, the internet, and wireless network technologies like Bluetooth and Wi-Fi, as well as the expansion of smart gadgets and other devices that make up the "Internet of things," cyber security is becoming more and more important. One of the main issues facing the current world is cyber security because of its complexity on both a political and technological level. Data security and privacy will always be the most important security precautions that any firm takes. Nowadays, every piece of information is kept in a digital or cyber format in our environment. Users of social networking sites can engage with friends and family in a secure environment.

1.3 Benefits of Cyber Security

Defending Private Information- Data is growing in value as a result of increased digitization. Cyber security aids in preventing theft and illegal access to sensitive data, including financial, personal, and intellectual property information.

Avoidance of Cyber-attacks- Protecting sensitive data from theft and illegal access, including financial and cyber security aids in preventing theft and illegal access to sensitive data, including financial, personal, and intellectual property information.

Protecting Vital Infrastructure- Protecting sensitive data from theft and illegal access, including financial and Computer systems that are networked are essential to critical infrastructure, such as power grids, transportation networks, healthcare systems, and communication networks. In order to maintain the seamless operation of vital services and avoid any disruptions that might have an influence on national security and public safety, it is imperative that these systems be protected against cyber threats.

Sustaining Business Persistence- Protecting sensitive data from theft and illegal access, including financial and Businesses can be severely disrupted by cyber-attacks, which can lead to lost sales, reputational harm, and in extreme situations, firm closure. By preventing or lessening the effects of cyber-attacks, cyber security contributes to the maintenance of business continuity.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024

Compliance with Regulations- Protecting sensitive data from theft and illegal access, including financial and Organizations must protect sensitive data under stringent restrictions that apply to several industries. Serious fines and legal action may follow noncompliance with these regulations. Cyber security aids in ensuring adherence to laws like PCI DSS, GDPR, and HIPAA.

Defending the Nation's Security- Protecting sensitive data from theft and illegal access, including financial and Cyber-attacks that target government networks, military installations, and vital infrastructure can be used to undermine national security. Preventing cyber warfare and safeguarding national security depend heavily on cyber security.

Maintaining Confidentiality- Protecting sensitive data from theft and illegal access, including financial and In a world where personal data is being gathered, saved, and shared online more and more, cyber security is essential to maintaining privacy. Safeguarding personal information from unwanted access, monitoring, and abuse contributes to the preservation of people's right to privacy and builds confidence in digital platforms.

There are an increasing number of data breaches every year, and the global cyber threat is still evolving at a rapid pace. According to a risk based security analysis, in just the first nine months of 2019, data breaches exposed an astounding 7.9 billion records. The amount of records revealed during the same period in 2018 is less than half (112%) of this statistic.

Every year, there are more and more data breaches, and the worldwide cyber threat is still developing quickly. An amazing 7.9 billion records were exposed by data breaches in just the first nine months of 2019, according to a risk based security research. Less than half (112%) of the records disclosed during the same period in 2018 were included in this figure.

II. LITERATURE REVIEW

Maria Bada1, Angela M. Sasse2 and Jason R.C. Nurse3(2019)- In an information security program, security awareness is a component that is frequently disregarded. Normal users are the weakest link in any business since relatively little is done to raise their level of security awareness, even when organizations are expanding their usage of cutting-edge security technologies and regularly training their security professionals.

G.Nikhita Reddy1, G.J.Ugander Reddy(2014)-Modern technologies such as net banking, cloud computing, mobile computing, and e-commerce require a high degree of security.

These technologies' security has become essential as they include some very valuable information about individuals. For the sake of both national security and economic prosperity, important information infrastructures must be safeguarded and cyber security must be improved.

Fadi A. Aloul (2012) –In this paper one aspect of an information security program that is frequently disregarded is security awareness. The weakest link in any business is its regular users, who receive very little security awareness training despite organizations expanding their usage of cutting-edge security technologies and regularly training their security personnel.

Azeez Nureni Ayofe, Barry Irwin-(2010) - Online transactions are now fraught with uncertainty due to the elevated degree of insecurity on the internet. The severity and prevalence of cybercrime are rising steadily. Results from the Computer Crime and Security Survey conducted in 2002 indicate an increasing trend, indicating the necessity for a prompt evaluation of current strategies to combat this emerging issue in the information era. In this essay, we give a general review of cybercrime and offer a global viewpoint on combating it.

2.1.Objectives

- To understand the history and value of cyber security, and improve the security of information
- To study on different types of cyber security focuses on securing computer from unauthorized access, data breaches.
- To implement the cyber security layers to ensure comprehensive protection.
- To determine the challenges and implement the methods of protection cyber security keeping your data safe over the internet.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024

III. RESEARCH METHODOLOGY

Use the systematic process of collecting, analysing, and interpreting data to answer research questions. It includes the following:

- **Quantitative research methodology-** focuses on measuring and testing numerical data of differentcyber-attacks and cyber security trends.
- **Qualitative research methodology** examines the opinions, behaviours, and experiences of people. It collects and analyses words and textual data on cyber security challenges and protection method used by different techniques.
- **Design**: Include experimental, quasi-experimental, correlational, descriptive, and exploratory.
- **Data collection-**Data collected from books, sites and research papers.
- **Data analysis-**Analysis by detect, respond, impact and behaviour of different cyber security method in different environment.

IV. WHAT MAKES CYBER SECURITY CRUCIAL?

Protecting our digital assets, such as private and sensitive financial data, intellectual property, and vital infrastructure, requires cyber security. Cyber-attacks may have detrimental effects on one's finances, reputation, or even physical health. No matter how big or small a firm is, cyber security is essential. Information is becoming digital through wireless communication networks as a result of growing software and technology in a variety of industries, including government, education, healthcare, and so forth.

The goal of cyber security is to protect the very sensitive data that is stored in many businesses, such as email, Yahoo, and others, and which could harm our reputation as well as ourselves. Attackers target both big and small businesses, stealing vital records and data from them. The importance of cyber security has grown in the linked world of today. The risk of cyber-attacks has increased along with the amount of data that is being stored and delivered electronically. The technique of preventing theft, damage, or illegal access to computer systems, networks, and data is known as cyber security.

Cyber security Trends in 2024

Sr. No.	Cyber Security Trends	Approaches Works	Security	Analyse and Method
1	**Rise of AI and Machine Learning**	To detect and respond to threats faster than humans can	More cyber security tools	Analyse patterns and predict potential attacks
2	**Cloud Security**	Security protocols to protect against breaches	Ensuring this data is secure is a top priority.	strong authentication methods and regularly updating
3	**Internet of Things (IoT) Vulnerabilities:**	More devices connected to the internet, like smart home gadgets and wearable tech, there's an increased risk of cyber attacks	updated security features	Strong updated methods
4	**Zero Trust Security**	Threats could come from inside or outside the network	a standard practice to ensure a higher level of security.	Constantly verifies and monitors all access requests
5	**Cyber security Skills Gap**	for skilled cyber security professionals	protect against these threats is higher than ever	Demand for experts
6	**Regulatory Compliance**	New regulations are being introduced worldwide	To protect personal data.	To ensure they comply and avoid hefty fines.

(Table-1 Cyber security Trends in 2024 approaches work)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024

4.1 The Seven Layers of Cyber security

A single technological advancement that boosts security shouldn't be cyber security. Instead, to guarantee complete protection, it must to be a multifaceted, layered strategy. Comprehending the components of a layered strategy is crucial. There are typically seven layers of cyber security to take into account.

Mission-Critical Assets

It is vitally important to secure this data. Businesses deal with hostile forces on a regular basis, whether they choose to acknowledge it or not. How are leaders handling this kind of protection, I wonder? And what safeguards have they put in place to prevent violations?

Software for electronic medical records (EMRs) is one example of a mission-critical asset in the healthcare sector. Financial records of customers in the financial sector.

Data Security

When security measures are implemented to safeguard data storage and transit, it is known as data security. To prevent data loss, a backup security mechanism must be implemented, which calls for the usage of encryption and archiving. Due to the potentially catastrophic effects of a data breach, data security is a top priority for all businesses.

Endpoint Security

This layer of protection ensures that user device endpoints are not compromised. This covers the safeguarding of laptops, desktops, and mobile devices.

Depending on a company's demands, endpoint security systems allow for protection on a network or in the cloud.

Application Security

This involves the security features that control access to an application and that application's access to your assets. It also includes the internal security of the app itself. Most of the time, applications are designed with security measures that continue to provide protection when the app is in use.

Network Security

Here, security measures are implemented to safeguard the company network. Preventing unwanted access to the network is the aim.

It is essential to apply the required security patches, including encryption, to every system on the company network on a regular basis. Disabling unneeded interfaces is always recommended to increase security against potential threats.

Perimeter Security

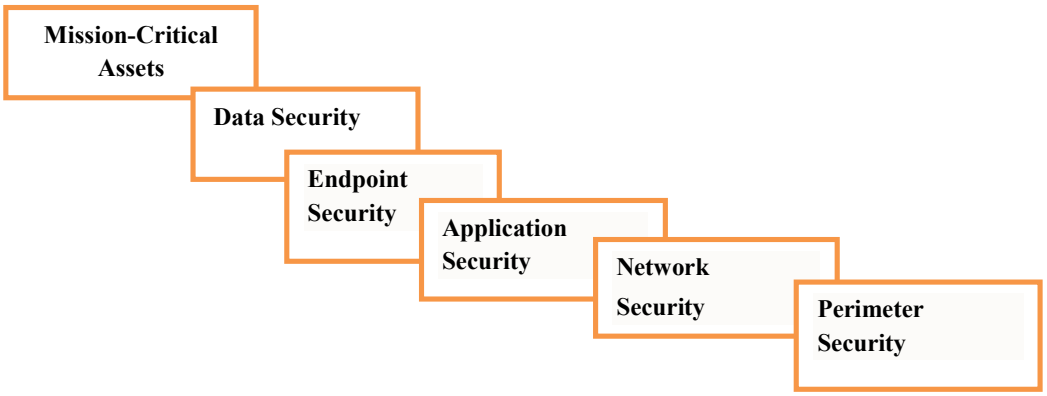
This layer of security guarantees that an organization is fully protected by both digital and physical security measures. It consists of devices like firewalls that guard the company network from outside threats.

The Human Layer

The human layer is a crucial component of the security chain, despite being seen as the weakest link. As an example, it integrates phishing simulations and management controls.

The goal of these human management controls is to safeguard the most important security elements for a corporation. This encompasses the very real risk that a firm faces from people, hackers, and hostile users.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024



(Fig.1.1 Seven Layers of Cyber Security)

4.2 Types of Cyber Security

- **Network security**-keeps an eye on network traffic to spot and stop possible threats. Network protocols, wireless access points, firewalls, hosts, and servers are a few examples.
- **Cloud security**-protects cloud data while it's in use, traveling, and resting by encrypting it. Additionally, it finds and corrects erroneous security configurations and vulnerabilities.
- **Endpoint security-** safeguards computers, including workstations and servers, against viruses, illegal access, and flaws in operating systems and browsers.
- **Application security-** shields applications from dangers such as software vulnerability exploitation, network attacks, and web application attacks. Additionally, it checks software programs for vulnerabilities as they are being developed and tested.
- **Internet of Things (IoT) security-** helps increase visibility and security for Internet of Things (IoT) devices, which are frequently used to hold sensitive data but aren't usually designed with security in mind.
- **Threat intelligence-** provides additional context for security events by combining data from numerous feeds on threat actors and attack signatures.
- **Physical security-** Regulates the physical access to computers and gadgets.

4.3 Challenges of Cyber Security

Some of the challenges of cyber security include:

- **Phishing:** The most prevalent kind of cybercrime, phishing entails an attacker posing as a representative of a respectable organization in order to obtain private data.
- **Ransomware**: Ransomware assaults remain a significant concern, and increasingly sophisticated attack techniques are compelling victims to make payments.
- **Data breaches**: These days, it's a big deal when firms like American Airlines, Microsoft, and Twitter get hacked.
- **IoT assaults**: One of the current issues facing cyber security is IoT attacks. Cloud and AI attacks: One of the current issues facing cyber security is cloud and AI assaults.
- **Advanced Persistent Threats (APTs)**: are persistent, targeted attacks that are frequently carried out by organizations with state sponsorship. APTs frequently go months without being caught in order to steal data or interfere with activities over a long period of time.

Cyber-Crime Increases Year Wise

Sr. No	Year	Most cyber crime	Increases
1	2020	**Malware** phishing	98%
2	2021	Phishing	80%
3	2022	Data breaches	38%

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024

4	2023	Ransomware attacks.	72%
5	2024	Phishing and spear-phishing attacks	55%

(Table 2- Cyber-crime increases year wise)

4.4 Ways to Stop Cyber-attacks.

To halt online assaults combines administrative, technical, and pedagogical strategies. Some of the best strategies for preventing cyber-attacks are listed below.

- **Utilizing software for antivirus and anti-malware**- Software for viruses and malware removal is crucial for shielding your computer from online dangers like Ransomware, spyware, and viruses.
- **Continual Updates for Software**- Security patches are frequently included in software upgrades and address identified vulnerabilities. Make sure you update all of your software on a regular basis, including your web browser, operating system, and other apps.
- **Using multi-factor authentication and strong passwords**:- Multi-factor authentication and strong passwords can aid in preventing unwanted access to your accounts. Make sure your passwords contain a mix of capital and lowercase characters, numbers, and symbols. Make sure that multi-factor authentication is enabled for all accounts that support it.
- **Individuals and organizations**–It can recognize possible cyber dangers and take the appropriate safeguards with the aid of cyber security education and awareness.

V. RESULTS AND DISCUSSION

The study revealed that methods to avoid Cyber-attacks, Cyber security firms are becoming more involved in the protection of different enterprises as a result of the estimated $8 trillion in worldwide expenditures associated with cybercrime in 2023 and the potential for that amount to reach $10.5 trillion in 2025.

It goes without saying that modern cyber security services are more important than ever, and businesses are prepared to take the necessary steps to implement them.

There are an increasing number of data breaches every year, and the global cyber threat is still evolving at a rapid pace. According to a risk based Security analysis, in just the first nine months of 2019, data breaches exposed an astounding 7.9 billion records. The amount of records revealed during the same period in 2018 is less than half (112%) of this statistic.

Every year, there are more and more data breaches, and the worldwide cyber threat is still developing quickly. An amazing 7.9 billion records were exposed by data breaches in just the first nine months of 2019, according to a risk based security research. Less than half (112%) of the records disclosed during the same period in 2018 were included in this figure.

VI. LIMITATIONS

In this paper research only cyber security layers and challenges and notdefined proper new advanced tools.

- **Costly**-Cyber security implementation can be costly and necessitates continuing education and resources. It could be difficult for small enterprises to cover these expenses.
- **Evolving threats**: Organizations must adapt as cybercriminals are always coming up with new ways to breach security.
- **Inconvenience to users**: Users may find cyber security to be inconvenient.

VII. CONCLUSION

It is now crucial to treat cyber security seriously due to the rise in cyber-attacks and data breaches. Cyber-attacks can target sensitive data, including intellectual property, financial information, and personal data. Cyber security safeguards aid in preventing illegal access, alteration, or destruction of this data. Organizations are required by a number of laws and regulations, including PCI DSS, GDPR, and HIPAA, to secure their networks and data from cyber-attack. Customers and stakeholders may stop doing business with a company as a result of a cyber-attack seriously harming its

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, September 2024

reputation. Cyber security is essential for averting and lessening these disruptions, protecting a business's continuity and stability from online attacks. Using antivirus software, upgrading software frequently, creating strong passwords and multi-factor authentication, and spreading cyber security knowledge and education are further recommended practices that can help avoid cyber-attacks. We can contribute to ensuring the security and resilience of our digital environments, protecting sensitive data, and upholding the integrity and trust of our systems in a world where connectivity is growing by adopting a proactive approach to cyber security.

REFERENCES

[1]. "Emirates vulnerable to internet attacks", The National, 2008. Available at: http://www.thenational.ae/apps /pbcs.dll/article?AID=/20080814/NATIONAL/420302377 &SearchID=73402849474210.

[2]. Information Security Forum (ISF): From Promoting Awareness to Embedding Behaviours, Secure by choice not by chance, February 2014. https://www.securityforum.org/shop/p-71-170

[3]. Kirlappos, I., Parkin, S., Sasse, M. A.: Learning from Shadow Security: Why understanding non-compliance provides the basis for effective security. *Workshop on Usable Security,* 2014.

[4]. National Institute of Standards and Technology - NIST: Building an Information Technology Security Awareness and Training Program. Wilson, M. and Hash, J. Computer Security Division Information Technology Laboratory.

[5]. October 2003. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

[6]. "Phishing raid empties bank accounts", The National, 2010. Available at: http://www.thenational.ae/apps/pbcs .dll/article?AID=/201 00405/NATIONAL/704049912&SearchID=733987396980 56.

[7]. https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html

[8]. https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html