Article Review : Using Cyber security In digital World

Assist. Teacher Malik Qasim Mohamme

Ministry of Education

albahadily@yahoo.com

Abstract

Global communication and information technology are becoming more and more important to modern society. The network, information security, the information society, and its members are all fundamentally threatened by the continuous dependency as well as a number of new and emerging dangers. The integrity of important national information infrastructures, notably with regard to personal information and child security, is negatively impacted by the expanding criminal exploitation of computer networks. Any national security strategy must now include cybersecurity. It is well known that national defense strategists in the United States of America, the European Union, Russia, China, India, and other nations have prioritized cybersecurity challenges in their strategies. Additionally, a lot of nations have made announcements about how their national security teams would be divided up into divisions and scenarios for cyberwarfare. To tackle cybercrime, e-fraud, and other cybersecurity-related issues, all of these initiatives are made in addition to the usual security measures.

Keywords : Cyber security , Cyber Crime , Cyber Threat

الملخص

تعتمد المجتمعات الحديثة بشكل متزايد على الاتصالات العالمية وتكنولوجيا المعلومات ومع ذلك ، فإن هذا الاعتماد المستمر يرافقه مجموعة من التهديدات الناشئة والمحتملة التي تهدد بشكل أساسي الشبكة وأمن المعلومات ومجتمع المعلومات وأعضائه ، إن تزايد إساءة استخدام الشبكات الإلكترونية لأغراض إجرامية يؤثر سلبًا على سلامة المعلومات الوطنية الحساسة للبنى التحتية ، وخاصة المعلومات الشخصية وأمن الأطفال ، اذ اصبح الأمن السيبراني جزءًا لا يتجزأ من أي سياسة للأمن القومي فقد أصبح معروفًا أن صانعي السياسات في الولايات

المتحدة الأمريكية والاتحاد الأوروبي وروسيا والصين والهند ودول أخرى قد صنفوا قضايا الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية بالإضافة إلى ذلك فقد أعلنت العديد من الدول حول العالم عن تخصيص أقسام واماكن ضمن فرق الأمن القومي تضاف هذه الجهود إلى الجهود الأمنية التقليدية لمكافحة الجرائم الإلكترونية والاحتيال الإلكتروني والجوانب الأخرى للأمن السيبراني .

الكلمات المفتاحية: الأمن السيبراني ، الجريمة الإلكترونية ، التهديد السيبراني

1) ntroduction

Since computer systems are more integrated or interconnected and there are more cyberattacks every day, cyberthreats are becoming more and more complicated. As a result, there is a growing sense of urgency for new security policies, rules, and procedures to combat cyber-risks globally.Cyberthreats continue to exist and become more complicated and worse , it is predicted that as computer systems become more integrated and information and communication technologies increase our society's interdependence will only become worse[1].

When the internet originally came into existence in the 1960s, it was only accessible to a select group of scientists, researchers, and members of the military. Online users have undergone fast transformation. At initially, computer crimes were confined to causing physical harm to computers and related devices. Around the 1980s, the emphasis switched from purposefully causing physical harm to computers to using malicious software, or "viruses," to purposely break them. The influence was not as widespread since up until that moment, only military bases, significant multinational firms, and academic groups had access to the internet. When the public first had access to the internet in 1996, it gained popularity swiftly, and people's reliance on it progressively expanded to the point where it changed the way they lived.Because of how nicely the GUI (Graphics User Interface) is developed, consumers don't need to bother about how the internet functions. No need to worry about where the data is kept, how it is transmitted over the Internet, whether it is reachs to other people, whether it can connect to the Internet, be called, or whether data packets sent over the Internet can be examined

and moderated—all you have to do is click a hyperlink or enter the information you need where you need it. [2]

1.1 Research problem

Without cybersecurity, digital process operation is impossible. Numerous businesses are investing in the security of their operations as a result of this realization. So why do hackers keep getting past their defenses? It goes beyond the usage of security technology alone. This research aiming to focus on the vulnerabilities and the threats that arises and deal with it to discover some solutions for theses problems which are:

- How does malware function?
- Application security in three steps
- How crucial network security is
- The significance of end-user training
- Can information be protected with strong passwords?
- Is critical infrastructure security important?

1.2 Review Aim

Cybercriminals are using their methods to make some changing in environment and the developing market. Important enterprises are being disrupted by cybercriminals using ransomware assaults these supply chain attacks have an impact on the entire planet, rather than staying in the background, they are adjusting their tactics to a workforce that is increasingly mobile and cloud centric, and other fields. The main objective of cybersecurity is to keep data safe from theft or compromise and there are a few methods to do this and keep these goals in mind such are :

- Spotting potential threats.
- Arranging the resources in order of relevance and priority. The ones that matter the most are always kept secure.
- Selecting the most effective security guard deployment method for every danger
- Modifying risk management practices in light of past assessments.

- preserving both data in motion and data at rest, and monitoring for possible intrusions.
- Constant maintenance and solving any issues that pop up.

1.3 Background facts

The use of methods, procedures, and controls to defend against cyberattacks on systems, networks, programs, devices, and data is known as cybersecurity. It is made to lower the threat of cyberattacks and stop unlawful use of systems, networks, and technology. When computers or other computing devices—such as smartphones, tablets, personal digital assistants (PDAs), etc.—are used as tools or targets in an unlawful action, that conduct is referred to as cybercrime. People with destructive and criminal mindsets who are driven by retaliation, money, or a desire of adventure are often those who perpetrate it.[3]

2) Related Work

Cybersecurity is a subset of IT security , networks, computers, and other electronic equipment are safeguarded by cyber security against illegal access, assault, and destruction. Cybersecurity guards the digital data on your networks, computers, and devices from unwanted access, assault, and destruction whereas IT security safeguards both physical and digital data. In this part, a brief description would be discussed :

The initial approach for developing criteria for evaluating criminality that originates in cyberspace is described by Brenner [4]. Although acknowledging that it is highly difficult to construct metrics and scales for cybercrime because to challenges with apprehension, scale, and proof, she presents a straightforward taxonomy of damages that divides them into three primary categories: individual, systemic, and other. Using a similar approach to Laube et al. [5], Kshetri wants to build a cost-benefit analysis. yet he concentrates on the attacker's perspective. He contends that interaction between these three categories of individuals causes cybercrime to escalate out of hand. He explains the traits of cybercriminals, cybercrime victims, and law enforcement authorities. He creates a formula that weighs the benefits and expenses of an attacker as

well as the case for or against a cybercrime. This work [6] use interruption detection together with information-digging techniques for digital inquiry. Cybercrime is frequently described in terms of the crime triangle [7], which asserts that three elements must be present for a cybercrime to take place: a victim, a motive, and an opportunity. The person who will be assaulted is the victim. The reason why the crime will be done is the motivation, and the time will be the opportunity (e.g., it can be an innate vulnerability in the system or an unprotected device).

It could be challenging to identify which forum has legal authority when a case spans many jurisdictions. This subject and the situation of Internet jurisdiction legislation are covered by Chertoff et al. in their article from 2008 [8]. They offer four possible wordings for establishing the prevailing jurisdiction equitably and explicitly in diverse situations. These laws are based on the citizenship of the person who was the subject of the unlawful information, data, or system, the location where the harm occurred, the citizenship of the person who created the data, or the citizenship of the person who has or is in charge of the data. According to Mathieu and Guy [9], a high-quality solitary literature review offers trustworthy information and insights on prior research, enabling other researchers to pursue new directions on related areas of interest. The results of this study can also be used as a basis for future research or as references in related subjects.

3) <u>CybersScurity Importance</u> [10]

- Cyberattacks are getting increasingly advanced. Attackers are using a wider range of strategies in more sophisticated cyber operations. These include ransomware, malware, and social engineering.

- The price of cybersecurity incidents is rising. Organizations that experience cybersecurity breaches may be subject to significant fines. Non-financial expenses must also be taken into account, such as B. Reputational harm.

- Assuming that online criminals are uninterested in you is a mistake. Cybersecurity is necessary for everyone who uses the internet. This is so because the majority of cyberattacks are automated and meant

to target broad security flaws rather than particular companies or websites .

- Crime online is a huge industry. According to a CSIS and 2020 McAfee research based on information gathered by V Bourne, cybercrime costs the global economy more than $1 trillion per year.

- At the board level, cybersecurity is a major concern. Monitoring cybersecurity threats is difficult due to new reporting rules and laws. The board wants management's guarantees that its cyber risk management approach lowers attack risk and minimizes the impact on finances and operations.

4) <u>Cyber Threats Types</u> Common cyber threats include:[11]

- Remote access-enabling backdoors.

- Formjacking, in which malicious code is injected into internet forms.
- 3. Malware, which includes Trojans, viruses, worms, spyware, rootkits, bootkits, ransomware, botnet software, and RATs (remote access Trojans).

- The DNS (Domain Name System) is susceptible to poisoning attacks, which cause traffic to be redirected to fake websites.

- Cryptojacking, which entails downloading and running unauthorized bitcoin mining software .

- Distributed Denial of Service (DDoS) attacks: they attempt to bring down servers, networks, and systems by overburdening them with traffic.

5) Cyber Security Key Measures [12]

- First, network security Network security entails patching flaws in network topologies and operating systems, such as servers, hosts, wireless access points, and firewalls.

- Internet of Things , Security IoT security includes securing networks and intelligent devices linked to the IoT. Smart fire alarms, lights, thermostats, and other appliances are examples of IoT devices. These items automatically connect to the Internet.

- Protection of important infrastructure from cyberattacks Since SCADA (Supervisory Control and Data Acquisition) systems frequently employ outdated software and are governed by NIS rules, critical infrastructure businesses are frequently more susceptible than others. Regulations mandate that businesses manage their security risks by implementing the necessary organizational and technical controls.
- SafeGuarding apps Application security is the process of addressing flaws resulting from hazardous development practices when developing, coding, and publishing software or a website.
- Cloud Safety Protecting data, apps, and infrastructure in the cloud is part of cloud security.

6) Classification of Cyber Crimes

The organization that is the target of the cyberattack may have internal or foreign cybercriminals. This fact allows for the classification of cybercrime into two categories:[2]

1) **External Assault**: An external attack occurs when an outsider or an employee of the firm hires the attacker. An organization that is the victim of a cyberattack experiences reputational harm in addition to financial loss. The attacker often scans and collects data because they are not an organization member. Because it is possible to spot external dangers by carefully reviewing these firewall logs, a skilled network/security administrator keeps a close eye on them. Systems for detecting intrusions are also put up to keep an eye on any dangers from outside.

2) **Insider Threat:** Insider attacks are committed by someone who have been given access to a network or computer system. Internal employees or contractors who are irate or dissatisfied frequently commit it. The motive for the insider strike might be revenge or avarice. Given that he is aware with the security system's rules, practices, IT architecture, and strength, an insider may execute a cyberattack quite effortlessly. The hacker also has access to the network. As a result, it is quite easy for an insider attacker to take crucial data. An insider attack typically happens when an individual is fired or given a new job within a company that is not outlined in the IT standards. This gives the attacker a window of verifiability. A company's internal intrusion detection system (IDS) may be able to thwart an insider attack.

6.1 Reasons of Cyber Crimes

The expansion of cybercrime is fueled by a variety of factors. Several of the primary causes are:[2]

- **Money**: People who commit cybercrime are motivated by a desire to make quick, easy money.
- **Retaliation**: Some people seek vengeance through harming the reputation of another person, group, organization, caste, or religion or by causing them physical or financial harm. This is considered a kind of online terrorism.
- **Fun**: Amateurs engage in cybercrime for amusement. They only want to evaluate the most recent gadget they have come across.
- **Recognition**: It is seen with pride when someone manages to breach highly protected networks, such as defense websites or networks.
- **Anonymity:** Often, the ability to stay anonymous in a cyberspace environment promotes cybercrime since it is more easier to do than in the real world. In the virtual environment as opposed to the physical one, it is far simpler to get away with criminal activities. There is a pervasive sense of anonymity that might tempt normally moral people to compromise their moral principles in the name of self-interest.

- **Cyber Espionage:** On occasion, the government engages in cyber trespassing to monitor another individual, network, or nation. The motive might be driven by politics, the economy, or social issues..

6.2 Computer Hacking

It entails modifying computer software and hardware to accomplish goals different than those for which they were first created. It is possible to hack a computer system for a number of reasons, including testing one's technical prowess or securing, modifying, or wiping data in order to further social, economic, or political goals. Corporations are increasingly actively seeking hackers, or people who intentionally attack networks, in order to find and fix security holes.

These categories of hackers include[13]:

- **White Hat Hackers** are individuals who breach a system to find security holes and notify the company so that preventative actions may be taken to secure the system from outside hackers.

- **Black Hat**: Unlike white hats, black hats attack the system with malicious intent. They could attempt to hack the system for social, political, or financial motivations.

- **Grey Hat**: Security weaknesses are found by grey hat hackers, notify site managers, and provide a patch for the security fault in exchange for consulting fees.

- **Blue Hat**: A blue hat hacker is an independent computer security consultant that tests a system for bugs before it is released in order to find exploits that can be fixed.

7) Results and Desscussion

The scope of cyber security, which very much encompasses the whole foundation of contemporary civilization, includes any intelligence device that may transfer data to one or more other devices (either over a network or not). All people need to be aware of cyber security, cybercrimes, and the slight seriousness of security in relation to online, social, and other activities through which the chance of danger is increased. Data is lost,

modified, and vital information like passwords for bank accounts or email accounts are removed. Also, people may be aware of cyberlaws, laws against cybercrime, upcoming actions, and methods for combating crimes. There are a lot of strategies and some methods that will be consider solutions and defenses against cyber vulnerabilities such are these following factors as shown in figure 1 and table 1 .

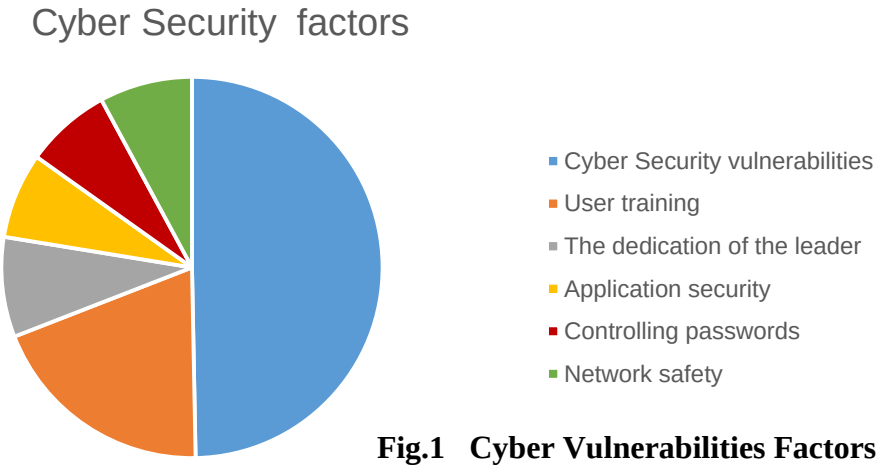

Fig.1 Cyber Vulnerabilities Factors

Table 1 disscussed various methods and approches against cyber threats and vulnerabilities , each of which is essential and necessary part to achive the rubost against cyber threats .

Table 1 Disscussion of Factors That Impact Cyber Threats		
	Solutions & strategies	The Description
1	Network safety	The process of adopting network security aims to safeguard the usefulness and integrity of your network and data. By doing a network penetration test, which assesses your network for security faults and vulnerabilities, you may achieve this.
2	User training	Human error is the main factor that leads to data breaches. We must thus arm personnel with the knowledge necessary to thwart dangers. Staff awareness training teaches employees how security risks affect them as well as how to apply best practice recommendations to real-world situations.

3	The dedication of the leader	Leadership dedication is necessary for cyber resilience. Without it, it is difficult to establish or execute effective processes. smart management must be prepared to commit the required funds for resources like cyber security awareness campaigns.
4	Application security	Since online applications are increasingly crucial to businesses, security must be given high importance. Web application weaknesses are a common entrance point for hackers.
5	Controlling passwords	The most popular passwords in the UK are "password," or "123456," and "qwerty." We should put in place a password management policy to direct creating secure passwords and maintaining them.

8) Conclusions

Cybersecurity is a matter of utmost importance as the world becomes more and more linked via numerous networks. The goal of a cyber security management program is to recognize the dangers, understand their likelihood and possible consequences on the business, and then put security defenses in place that decrease the threats to an acceptable level for the establishments.

The issue of cyber security should be addressed by a number of important parties. Cybercriminals are well-equipped, knowledgeable foes who specialize in stealing secrets and intellectual property. Due to a number of factors, most notably the associated financial rewards, crime is becoming more complicated and prevalent. Internet users, including organizations, people, organizations, governments, and companies, are growing quickly, creating a baseline of potential targets. Following the rise of cloud computing, social networking, and mobile devices, the way individuals share information and communicate online has radically changed. Before cybercriminals turn into a widespread menace that is difficult to eradicate, there are many different crimes that have negative

consequences in terms of money losses and the theft of personal information.

9) References

[1] Rafael R.(2018) **Governing Cyber Security through Networks:** An Analysis of Cyber Security Coordination in Belgium International Journal of Cyber Criminology – June 2018. Vol. 12 .

[2] Dr. Jeetendra P.(2017) **Introduction to cyber security** , Uttarakhand Open University, Haldwani .

[3] Shruti A, Aditi N(2021) , **Cyber Security : Techniques and Perspectives on Transforming -A Review** , International Journal of Scientific Research in Science and Technology .

[4] Brenner SW. **Cybercrime metrics: old wine, new bottles?** Va. JL & Tech, 9:13–13, 2004 .

[5] Kshetri N. **The simple economics of cybercrimes,** IEEE Secur Priv, 4, pp. 33–39, 2006

[6] Maloof, M. A. (Ed.), **Machine learning and data mining for computer security: methods and applications.** Springer Science Business Media, 2006

[7] N. Dhanjani, B. Rios, and B. Hardin, Hacking: **The Next Generation: The Next Generation.** O" Reilly Media, Inc., 2009

[8] M. Chertoff and P. Rosenzweig. (Mar. 1, 2015). **A Primer on Globally Harmonizing Internet Jurisdiction and Regulations, accessed** on oct. 15, 2015.

[9] Mathieu, T. & Guy, P., **"A Framework for Guiding and Evaluating Literature reviews", Communications of the Association for Inf**. System, 37(6), pp 6, 2015

[10] Shivani G, Akshada P, Prof. Rashmi L,(2020) **Importance of Cyber Security International Journal of Engineering Research & Technology** (IJERT) .

[11] R.S Weerasuriya, S.M.D.E Fernando , P.A.H.S Gunasekara , **Cyber Security: An analysis on awareness on cyber security among youth in Sri Lanka .**

[12] Awais R ,Howard C ,George D ,Emil L, Andrew M, (2019) **The Cyber Security Body of Knowledge .**

[13] Gray H, Erin W, (2016), **Computer Hacking ,Security Testing, Penetration Testing And Basic Security**