KARACHI INSTITUTE OF ECONOMICS & TECHNOLOGY

Data Networking And Communication

(*DCN*)

Project Report

Project Title: The Cyber Security (Report)

CLASS ID: 107933

Project Title: Cyber Security

Project Members:

1) 11508 Muzamil Khan
2) 11200 Muhammad Ahmed
3) 11515 Zain Zahid

CYBER SECURITY

TABLE OF CONTENTS

INTRODUCTION

Cyber security is the use of technology, procedures, and policies to defend against cyber assaults on systems, networks, programs, devices, and data. Its goal is to limit the risk of cyber assaults and to safeguard against unauthorized use of systems, networks, and technology. A cyber security degree can be challenging when compared to other degrees, but it typically does not need advanced math or intense laboratories or practical's, making the courses considerably more accessible.

Cyber security is a rapidly expanding area, and cyber security professionals are in high demand. People with the proper combination of talents, knowledge, and experience have strong career chances. Typically, you'll begin in an entry-level or junior cyber security position. This report deals with the cyber security, its types, importance, awareness of cyber security education system, career and challenges and measures [1]. This report also highlights the cyber security in Pakistan. The field is growing more important as people's reliance on computer systems, the Internet, and wireless network standards grows. The number of "smart" gadgets that utilize internet networks is increasing. In today's world, cyber security is critical for data protection.

DISCUSION

CYBER SECURITY

Since the birth of the Internet and the digital revolution that has occurred in recent years, the notion of cybersecurity has become commonplace in both our professional and personal life. Cybersecurity and cyber threats have been a constant throughout the preceding 50 years of technological growth [1]. Computer security was primarily restricted to academics in the 1970s and 1980s, until the invention of the Internet, when, with expanded connection, computer viruses and network intrusions began to proliferate. Following the rise of viruses in the 1990s, the decade of the 2000s saw the institutionalization of cyber risks and cybersecurity.

CYER SECURITY CATEGORIES

Cybersecurity is the process of putting in place various security measures to safeguard your network, computer systems, cloud infrastructure, and online personal data against cyber-attacks. Cyber assaults are designed to steal personal information such as credit card information, passwords, social security numbers, and other sensitive information [2]. The phrase cybersecurity pertains to both personal and commercial internet-connected gadgets.

Cyber security is divided into different categories:

NETWORK SECURITY

This form of security refers to the safeguarding of your computer network against threats both within and outside the network. It utilizes a variety of approaches to avoid malicious malware or other data breaches. Network security employs a variety of protocols to prevent attacks while allowing authorized users access to the secure network.

Firewall is the most important software that does not allow suspicious and unauthorized activity that is shown to be threat to the computer network. Firewall is able to control the traffic of networks that goes in and out of the system. the activity of computers and networks that follows the rule are allowed by the firewall and others who does not follows the rules are not allowed to access the network [3]. It is becoming preferable and famous among the companies because it protects the computer network and data by its latest methods.

APPLICATION SECURITY

This is the process of safeguarding sensitive data at the application level. The bulk of these security practices must be in place order to launch the application. Application security may include measures such as requiring the user to enter a strong password.

CLOUD SECURITY

Most of the data of companies, schools, college and big organization, the data in stored in cloud. This is one of the good data storage facility. So most of the secure data could be found in the clouds. There must be some sort of security that should be given to the cloud [3]. Cloud security is the one which plays this role. This cloud storage can include micro soft one drive, google drive and Apple icloud [4]. Cloud security provides protection the data that is stored in clouds.

OPERATIONAL SECURITY

The risk management procedure for all internal cybersecurity is referred to by this phrase. This sort of management often employs a number of risk management officers to guarantee that a backup plan is in place in the event that a user's data is hacked. Employees must be taught on the best practices for keeping personal and commercial information safe as part of operational security [5].

NECESSITY CYBER SECURITY

Cybersecurity is the procedure of making preparations for computerized attacks on frameworks, organizations, and projects [4]. These cyberattacks are regularly planned to get sufficiently close to, change, or erase delicate data; coerce cash from clients; or upset routine corporate exercises. As far as an individual, agreeable area, state, and country, data is the most valuable resource. Exclusively, the spaces of concern are as per the following:

1. Protecting the system's resources from illegal access, disclosure, and alteration.
2. Protection for online transactions such as shopping, banking, train bookings, and stock market trading.
3. Account security while using long range interpersonal communication destinations against account commandeering
4. One fundamental to improving network safety is a superior comprehension of the risk and the vectors used by the aggressor to overcome digital protections.
5. There is a need for a distinct entity to handle the organization's security.
6. Different groups or missions attract various sorts of enemies with varying agendas, necessitating varying levels of readiness.

AWARENESS OF CYBER SECURITY EDUCATION SYSTEM

Kids in the instruction framework should be made mindful of the many types of attacks and intruders [6]. They should likewise be comfortable with words, for example, Hardware/Desktop Security, Wi-Fi Security, wired Security, Password Protection/(File/Folder) level Security, Social Networking Attack Security, and Malicious Software:

- Phishing and hoaxes
- Spyware, Malware, Viruses, Worms
- Trojans, Zombie and Botnet, Spyware, Adware

The fact that students are learning information technology skills calls into question instructors' capacities to ensure that healthy online behavior patterns are established [7]. The instructor providing security information, on the other hand, lacks understanding and up-to-date information regarding Cyber awareness issues, notably security. Teacher technology training is required for skill development and awareness.

CYBER SECURITY ACCORDING TO SOME AUTHORS

According to Hansen and Neissenbaum in 2010

"The first true battle in cyberspace" assaulted Estonia ten years ago, putting the country in "a national security emergency [3]."

According to Dunn Cavelty in 2010

Nowadays, cyber security is a daily concern that can be found everywhere, from the news reporting spam, scams, frauds, and identity theft to scholarly studies discussing cyber warfare, cyber espionage, and cyber defenses [3].

According to Dunn Cavelty in 2013

How we might interpret of digital protection will have impacted on the grounds that it's not just by what we accept is generally significant in our regular day to day existences, yet additionally by the public authority's and other central participants' points of view. The relationship of political discourse to different digital dangers [1]. In reality, network protection includes a more extensive extent of examination and more troublesome issues. She further classifies it as 'three covering network protection talks,' which incorporate 'specialized talk' that incorporates 'infections, worms, and different blemishes,' a 'wrongdoing undercover work talk' including 'digital hoodlums and computerized spies,' and 'military-common safeguards talk,' which incorporates the subject of 'cyber(ed) clashes and critical framework security [3].'

According to Dewar in 2014

He emphasizes that "the purpose of cyber security is to enable activities in cyberspace free of danger of physical or digital damage." How countries see the buildup of interplays among securitization aspects in cyber security issues and the attribution problem causes their cyber security strategy and policy to differ from one another.

CAREER IN CYBER SECURITY

Cyber security experts, also known as information security analysts, have a wide range of tasks, but the most important aspect of their work is to keep internet data secure. As more of our personal information is kept online, it becomes increasingly vital to strengthen security. Because of the frequency of cyber assaults, job opportunities abound, and competent individuals are in high demand.

Work will most likely be done in an office, and you will most likely be utilizing a computer for lengthy periods of time. However, if the cyber security specialist is a consultant, he may be required to travel in order to meet with customers. For seasoned individuals, self-employment is an opportunity. People might start their own cyber security firm or work as a freelance cyber security expert [2]. They might also work as a contractor for a company. Some jobs will need employees to get security clearance, especially if they work for a government agency or a commercial company that deals with extremely sensitive material. Employees may also be limited in what they may say about their jobs.

There is a greater concentration of jobs in big cities, with many jobs situated in the South East of England. Many jobs in Scotland may be found in Edinburgh and Glasgow. Duties in Wales are most often found in Cardiff, Swansea, and Newport. However, as a consultant for a corporation, a cyber-security specialist must travel both inside the UK and maybe worldwide. Independent consultants can work from any location and travel to meet with customers. In my opinion cyber security is a good job that can give you more income and profit than other degrees.

ISSUES WITH CYBER SECURITY

Every application and every field has some sort of issues. Cyber security has also some issues for example:

- **Mobile phones and mobile applications:**

  The remarkable multiplication of Mobile gadgets creates the dramatic development of safety concerns [4]. Each new advanced cell, \Tablet, or other Mobile gadget adds another powerless passageway to networks, making the way for a digital attack. The intermittent issue of lost and taken devices will be extended to cover these new and old innovation that recently cruised under the radar of network safety procedure.
- **Networking on Social media:**

The increased usage of social media will exacerbate personal cyber dangers. The use of social media by businesses is increasing, as is the risk of an assault [9]. Organizations should anticipate to see a rise in the usage of social media accounts as a conduit for social engineering strategies in 2012.

- **Cloud computing:**

  Cloud figuring will be utilized by an expanding number of organizations. The colossal expense decreases and benefits of distributed computing are empowering organizations to move to the cloud. As cloud use fills in 2012, new break cases will represent the issues these administrations deal to scientific examination and episode reaction, and cloud security will at last get the consideration it merits [5].

COUNTER MEASURE ON ISSUES OF CYBER SECURITY

INTRUSION DETECTION SYSTEM

Computer infrastructure attacks are becoming a more serious problem [4]. An invasion is any series of acts designed to compromise the integrity, confidentiality, or availability of a resource. As a result, intrusion detection is required as an additional barrier to safeguard systems.

DISTRIBUTEDINTURSION DETECTION SYSTEM

In Distributed IDS, conventional interruption recognition frameworks (IDS) are installed inside insightful specialists and sent over an enormous organization (DIDS). In a conveyed climate, IDS specialists speak with each other or with a focal server [5]. Conveyed checking empowers network chairmen to identify arranged and composed assaults early, permitting them to go to preventive lengths.

SUBSCRIBER IDENTITY AUTHENTICATION

At the point when a mobile client looks to interface with the organization, he should initially confirm his personality to it. Client validation shields against unapproved use and assurances precise invoicing. GPRS utilizes a similar verification strategy as GSM, with similar calculations for confirmation and key creation, just as a similar mystery key [1]. The verification instrument utilized in Grasso displays a few flimsy spots in regards to security. All the more explicitly, the

verification method is single direction, and, in this way, it doesn't guarantee that a portable client is associated with a real serving network [7]. This reality empowers dynamic assaults utilizing a bogus base station personality

CYBER SECURITY IN PAKISTAN

Rapid digitalization and the widespread adoption of Information and Communication Technologies (ICTs) have exposed nations to new and growing cybersecurity risks. Data and network security has become a must-have for governments. While many responsible nations have devised comprehensive policies and measures to combat oncoming cyber threats, Pakistan has struggled to build a coordinated national cybersecurity policy or plan [10]. Although cybersecurity and governance guidelines for specific sectors (such as banking and defenses) were in existence, a comprehensive national-level strategy to cybersecurity was lacking [10]. The Federal Cabinet adopted Pakistan's first National Cyber Security Policy for data protection and cybercrime prevention on July 27, 2021, a much-anticipated document in the cybersecurity world. The policy was developed by the Ministry of Information Technology and Telecommunications in order to propose a definitive plan of action for establishing a solid legislative and institutional framework connected to cybersecurity.

POLICIES FOR CYBER SECURITY IN PAKISTAN

- ✓ The policy's goal for 2021 is to "create a secure, robust, and continually increasing nationwide digital ecosystem while ensuring responsible confidentiality, integrity, and availability of digital assets.". Its primary guiding concepts include data privacy and citizen security, giving the necessary support and system to concerned public and commercial institutions, establishing a national response structure, and, last but not least, adopting best practices to preserve national digital sovereignty [10].
- ✓ Another essential part of the program is the indigenization and development of cybersecurity solutions through research and development initiatives [10]. This, too, was a critical issue that required attention. Adequate local resources, both in terms of personnel through Centers of Excellence and HRD programs, and technology, would alleviate our over-reliance on external sources, which exacerbates the country's cyber threats. However,

authorities did not define how much money or resources would be set aside for this critical purpose.

CONCLUSION

A comprehensive cybersecurity strategy has various degrees of assurance scattered all through the PCs, organizations, applications, or information that are to be defended. Individuals, techniques, and innovation should all cooperate in an organization to build up a successful insurance against digital dangers. Online protection occupations are in incredible interest, and the requirement for greater security experts doesn't have all the earmarks of being disappearing soon. Digital attacks are developing more customary and more risky, and keeping in mind that we typically catch wind of assaults on high-profile partnerships, no firm or individual with a web presence is insusceptible to them. The desire to keep data, information, and devices private and secure drives the pertinence of network safety. Individuals in the present society keep enormous measures of information on PCs and other web associated contraptions. Organizations require network protection to defend their information, money, and licensed innovation. Network protection is worried about both the uncertainty brought about by and through this new area/space and the practices or techniques that will make it (more) safe..

REFERENCES

[1] D. Cavelty, "Cyber security meets security politics: Complex technology, fragmented politics, and networked science," *Contemporary Security Policy* , 12 October 2019.

[2] K. O'Hara, "The Future of Cybersecurity Jobs," 2021. [Online]. Available: https://www.monster.com/career-advice/article/future-of-cybersecurity-jobs.

[3] M. D. Cavelty, Cyber-security, 4th ed., 2015.

[4] A. M. Tonge, "Cyber security: challenges for society- literature review," *IOSR Journal of Computer Engineering*, vol. 12, 2013.

[5] T. Satyapanich, "CASIE: Extracting Cybersecurity Event Information from Text," *AAAI Technical Track: Natural Language Processing*, vol. 34, 2020.

[6] L. J. Farzana Quayyuma, "Cybersecurity awareness for children: A systematic literature review," *International Journal of Child-Computer Interaction*, vol. 30, December 2021.

[7] J. Jaskolka, "Cyberattacks to critical infrastructure threaten our safety and well-being," 24 October 2021.

[8] Z. A. C. •. I. L. •. J. H. Lambert, "Four domains of cybersecurity: a risk-based systems approach," 2013.

[9] M. E. O'Connell, "Cyber Security without Cyber War," *Journal of Conflict and Security Law*, vol. 17, 8 August 2012.

[10] A. Safdar, "An Overview of Pakistan's Cyber Security Policies," 23 September 2021.