**Cyber Security**

**What Does It Do**: -

Cyber security is the practice of protecting critical systems and sensitive information from digital attacks, which constitutes of a combination of facets, including physical, virtual, and philosophical technology. Also known as information technology security, Cyber security measures are designed to combat threats against networked systems and applications, whether those threats originated from inside or outside of an organization. Cyber security focuses on defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. Although Cybersecurity professionals work hard to close security gaps, attackers are always looking for new ways to escape It notice, evade defence measures and exploit emerging weaknesses. The latest Cybersecurity threats are putting a new spin of known threats taking advantage of work from home environments remote access tools and new cloud services. These evolving threats include: -

**Malware: -** The term malware refers to malicious software variants such as worms, viruses, trojans and spyware that provide unauthorized access or cause damage to a computer. Malware attacks are increasingly fileless and designed to get around familiar detection methods, such as antivirus tools, that scan for malicious attachments

**Ransomware**: -Ransomware is a type of malware that locks down files, data or system and threatens to erase or destroy the data or make private or sensitive data to the public unless a ransom is paid to the cybercriminals. Who launched the attack. Recent ransomware attacks have targeted state and local governments which are easier to breach than organizations and under pressure to pay ransom in order to restore applications and web sites on which citizens rely.

**Phishing/social engineering**: - Phishing is a form of social engineering that tricks users into providing their own PII or sensitive information such as credit card data or log in information. The FBI has noted about a surge in pandemic related phishing, tied to the growth of remote work.

**Insider Threats**: - Current or former employees, business partners, contractors or anyone who has had access to systems or anyone who has had access to systems or networks in the past can be considered as insider threat if they abuse their access permissions. Insider threats can be invisible to traditional security like firewalls and intrusion detection systems, which focus on external threats.

**Distributed denial of service(DDoS) attacks**: - A DDoS attack attempts to crash a server, website or network from multiple coordinated systems. DDoS attacks overwhelm enterprise networks via the simple network management protocol (SNMP), used for modems, printers, switches, routers and servers.

**Advance persistent Threats (APTs)**: - In an APT, an intruder or group of intruders infiltrate a system and remain undetected for an extended period of time. The intruder leaves the networks and systems intact so that intruder can spy on business activity and steal sensitive data while avoiding the activation of defensive countermeasures. The recent Solar winds breach of United States government systems is an example of an APT.

**Man-in-the-middle attacks**: - Man-in-the-middle is an eavesdropping attack where a cybercriminal intercepts and relays messages between two parties in order to steal data. For example, on an unsecure Wi-Fi network an attacker can intercept data being passed between guest’s device and network.

**Trojans**: - A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they can cause damage or collect data.

**Spyware**: - A program that secretly records what a user does so that cybercriminals can use that information such as spyware could capture credit card details.

**Botnets**: - Networks of malware infected computers which criminals use to perform tasks online without the user’s permission.

Businesses today are connected like never before. Our systems, users and data all live and operate in different environments. Perimeter based security is no longer adequate but implementing security controls within each environment creates complexity. The result in both cases is degraded protection for our most important assets. A zero-trust strategy assumes compromise and sets up controls to validate every user, device and connection into the business for authenticity and purpose.

**What is the likely impact**: -

Cybersecurity is a growing concern for both individuals and businesses alike. Not only does it pose a physical threat to our personal privacy and security, but it also has a significant economic impact. According to National Institute of Standards and technology (NIST), cybersecurity costs United States economy more than $600 billion annually. In fact, in recent study by Ponemon Institute found that companies that are proactive in addressing cyber threats can experience a 36 percent increase in profits. The following are the three ways it affects our society: -

* Cybersecurity affects our privacy in a significant way cybersecurity is all about protecting our information and privacy when hackers gain access to personal data, they can use it to steal identities, commit fraud or even spy on us. Cybersecurity can protect us from these types of attacks by ensuring that our data is secure and accessible only to those who should have access to it.
* Cybersecurity affects our security in a significant way cybersecurity also protects our security if hackers can breach our security measures, they could gain access to our personal information as well as confidential company data by implementing strong cybersecurity measures, we can protect ourselves from these types of attacks and keep businesses safe from harm.
* Cybersecurity affects our overall quality of life when we’re not able to access our email or online banking account, we feel inconvenienced and frustrated.

The impact of cyber security on society will continue to grow as the world becomes increasingly connected and reliant on technology. As such it is important for everyone including businesses, government agencies and individuals to take measures to protect themselves against online attacks. Cybersecurity is a big issue these days with so many people using the internet, business and governments are always looking for ways to keep their data safe, unfortunately this can also mean that we as citizens are at risk of our personal information being stolen or worse yet compromised as we all become more reliant on the internet it’s important to be proactive about cybersecurity and make sure that our online activities are protected.

**How will this affect us**: -

Cyber security is actually a vast field in IT sector which is unfortunately given the least importance. Everyday before leaving our homes we protect the property within by locking our doors, closing our windows or activating our security system we go to great lengths to ensure that our home have the necessary safeguards in place to thwart potential intruders and those who may try to steal it. When it comes to our confidential information however many of us use to fail to understand its importance that just like we lock our doors to protect our livelihood we hold dear, we must take decisive action to protect ourselves and our personal information from the burdensome ramifications of a cyberattack. Although many of us are aware of dangers that could result from sharing information with others, we use to often lack the knowledge that we need to protect ourselves and our families.

With ever growing information about personal information security from cyberattacks we are getting more aware of how to protect ourselves. Organizations and leader have started taking cyber security seriously and have started to develop new departments for cybersecurity. Those departments have the potential to employ more cyber security specialists who can understand weak points, learn from the past attacks and formulate strategies to deal with cyber-attacks.

As the population continues to age and more people are living with disabilities, it is important that we take steps to protect them from identity theft and other cybercrimes. A strong cybersecurity strategy has layers of protection to defend against cybercrimes and needs different skill sets such as critical infrastructure security, network security, application security, cloud security, information security, end user education disaster recovery and business continuity planning, storage security and mobile security. The most urgent need at the moment is to make people aware of risks and educate them to come out of common rather dangerous cybersecurity myths such as cybercriminals are outsiders, risks are well known, attack vectors are contained and my industry is safe.

References: -

1. [Impact of Cyber Security: An Overview(2021) (jigsawacademy.com)](https://www.jigsawacademy.com/blogs/cyber-security/impact-of-cyber-security) as viewed on 18/01/2023
2. [What is Cyber Security and How Does It Affect You? | NY State Senate (nysenate.gov)](https://www.nysenate.gov/newsroom/press-releases/michael-f-nozzolio/what-cyber-security-and-how-does-it-affect-you) as viewed on 19/01/2023
3. [What Impact Does Cyber Security Have On Our Society? - Cyber Security Career](https://cybersecuritycareer.org/what-impact-does-cyber-security-have-on-our-society/) as viewed on 18/01/2023
4. [What is Cybersecurity? | IBM](https://www.ibm.com/topics/cybersecurity) as viewed on 18/01/2023