**Cybersecurity\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**What is cyber security?**

Cyber security is the protection of computer systems from theft and damage to the hardware, software, disruption or misdirection services, data, damage, or unauthorised access.

**What does it do and why is it important?**

Cyber-attacks not only effect large scale organisations and government bodies but also small size businesses and common people like us. In today’s era, I. D thefts, credit card fraud, email internet fraud, theft of corporate data, cyber extortion, ransomware attacks etc have become so common that a report by at the University of Maryland suggests that “hackers attack a computer in the U.S every 39 seconds on an average”. As our reliance on A. I, cloud computing grows the need to protect our valuable data is more than ever. It would not only protect law-abiding citizens, small businesses as well as multinational private and public organisations from cyber-attacks that could steal personal as well as valuable customer’s information, but it would also protect top secret military and government information from being misused by hackers and terrorist organisations.

**Cyber security at present:**

Security related to the I.T sector has become a major concern for our banking, financial services, defence, and aerospace as well as other important sectors. Recent development in the A.I, machine learning sector has without a doubt revolutionised the way organisations do business and manage enormous amount of data but at the same time has exposed them to cyber-attacks.

According to a recent report by European cyber security organisation, the government of U.K invested around $2.30 B USD for the implementation of cyber security programs in defence and research sector. Furthermore, in response to the rise in intense threats and breaches governments across the world are emphasising on increasing investment in defence and research sectors to establish advanced and well protected cyber security infrastructure.

Companies in the cyber security market are adopting technologies such as IoT, machine learning and huge amount of data in their security business units. Most of the companies in the market are shifting from a “signature based” malware detection system to an IoT enabled machine learning signature less system.

Big data technology on the other hands is playing an important role by assisting big organisations understand and analyse potential risks.

Cloud computing has also played a significant role in the growth of cyber security industry. Cyber security solutions are based on complex mathematical models and often deals with handling huge amount of data. Cloud computing has offered a safe, reliable, low-cost platform to monitor this data. This has helped organisations to detect any uncertain threats quickly.

**Future of Cyber Security (Next 5 years)**

With emergence of disruptive technologies such as Artificial Intelligence, IoT, block chain and others. Cyber security sector has evolved drastically in the past 20 years. The next 5 years look quite promising for the industry and it’s predicted that the sector will keep growing as the demand to hire specialised cyber security personals to counter the increase in cyber-attacks. According to statistics global cyber security market is predicted to grow from $167.1 B USD in 2019 to $248.67 B USD by 2023.

Additionally, the adoption of cyber security technology is only expected to grow further with an increase in investments from nations like India, Spain, Canada, South Korea etc. At the same time the requirement from our healthcare, defence, aerospace, financial services and manufacturing sector has only contributed to the growth of cyber security in the recent years and it is estimated to only increase in the next 5 to 10 years.

**Impact of Cyber security on our future**

The recent developments have without a doubt revolutionised the way we interact with technology around us. On one hand A. I and machine learning has made everything so convenient that with just a voice command we can control and operate electronic equipment at our homes and in our hands. With the help of voice to text technology we can send messages, emails etc. With the help of biometrics technology such as face recognition we can make payments and authorise devices to perform important tasks on our behalf. Today A.I and machine learning algorithms can be used to automate tasks that make decisions much faster and quicker hence as a result increased productivity with a very low margin of error. In the financial services or the banking sector use of A.I to resolve most of the issues raised by customer is already proving to be effective.

On the other hand, we cannot ignore the fact that the A.I technology also create cyber security risks and machine learning algorithms can be easily manipulated by hackers .In short nobody can tell what the next major cyber-attack will be or where it will come from, and as small to medium businesses as well as common people like us are becoming aware of these threats the demand of having a strong, reliable cyber security infrastructure has only been predicted to grow higher in the near future.

The other major future impact of cyber security on our society that we may have is a growing risk of cyber war fare. The trend began in 2010 with Stuxnet. By 2017 a Russian backed hacking group was boldly going after big American corporations. As more nations become nuclear states these types of attacks are more likely to increase and combat ware to reduce. This would require stronger and much more efficient cyber security defence system, and this may trigger a race among the nations to make it a part of their defence budget and start investing int it heavily.

**Cyber Security in daily life**

With going frequency of cyber-attacks year after year the need of protecting ourselves from these attacks is more than ever. I believe students at a very early age should be educated on the risks associated with cybercrimes and should be taught basic cyber security skills.

Current projection suggests that the global market will be worth over $42 billion by 2022 however there is only so much a paid for software can do to protect businesses.

Larger security spends do not achieve anything unless they are monitored by someone with adequate information security skills.

The shortage of workers with these skills has created a huge gap in the market. A study by the global information security workplace estimated a gap of 2 million jobs by 2022.

Personally, as an individual who is passionate about cyber security and someone who’s interested in working in the industry this gives me the confidence that after graduation and after attaining the required certification the possibility of getting into the industry is quite high in the future.

As the number of attacks will keep increasing so will be the requirement of people with the skills to counter those attacks. Even if A.I is introduced in the information security there will always be a need for the professionals to protect that A.I from getting manipulated.

References:

1. Columbus, L., 2021. *2020 Roundup Of Cybersecurity Forecasts And Market Estimates*. [online] Forbes. Available at: <https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/?sh=36ecf248381d> [Accessed 15 January 2021].
2. Fortunebusinessinsights.com. 2021. *Cyber Security Market Size, Share, Growth | Trends Report, 2027*. [online] Available at: <https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165> [Accessed 15 January 2021].
3. TechRadar. 2021. *What Is the Future of Cybersecurity.* [online] Available at: <https://www.techradar.com/au/news/what-is-the-future-of-cybersecurity> [Accessed 15 January 2021].
4. Securitymagazine.com. 2021. [online] Available at: <https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds> [Accessed 15 January 2021].