

1. What does it do?

Since the explosive of the fourth industrial revolution, the role of cybersecurity and privacy in our daily life has increased significantly. To be clearer, our activities is getting digitalized and rely more on technology than ever before and this trend shows no signs of slowing down. Our sensitive information like national identification numbers, credit card, and bank account information are usually saved in cloud storage services such as Microsoft One Drive, Google Drive, and iCloud. These data could be leaked which might lead to great lost in property and honor. Every day, whether you are an individual, a small business, or a large multinational corporation, you rely on computer systems and that is one of the reasons why cybersecurity are so important in modern world.

According to a site called “Cybermagazine.com”, the beginning of internet security program was in the 1970s, when a researcher name Bob developed Creeper, a software that could roam throughout network, regenerate the way it being sent everywhere it went. Ray Tomlinson who is the inventor of email, created Reaper, a software that tracked and taken down Creeper. Reaper was the very first computer worm, as well as the first example of antivirus software and the first self-replicating program. After this event, many antivirus commercials were born and some of their products are still relevant today such as McAfee Virus Scan and Avast Antivirus.

While there are tones of antivirus software out there, what we really care about is the good one. A decent antivirus program should be able to accomplish its job: detect viruses and other dangerous software. Its purpose is to prevent, detect, and eliminate security threats like cybercrime and file infector virus. It must have a high detection rate in order to identify threats by utilizing advanced detection algorithms and methodologies. And, because more robust, undiscovered viruses emerge on a regular basis, the software should receive regular upgrades from its developers to improve its malware-suppression capabilities. Furthermore, a quality antivirus should have a rapid scanning engine that allows the user to clean his computer in a short period of time. It must have extensive

cleanup capabilities, so that it not only quarantines malware, but also assists the user in recovering lost or damaged files.

With technological improvements, hackers can take good use of them and getting better at locating gaps and fractures in corporate security systems so that they can gain access to secured files and data, creating a huge cybersecurity danger. Even when using advanced software and security system, global corporation and multinational company still face the risk of getting their system taken over by high-tech crime. Manchester United, a well-known football club in England, just had their computer systems hacked on November 20th, and their club employees still does not have access to email, and some other functionality has been affected. If the data of their fan is compromised as a result of the cyber-attack, they might face a punishment from the data regulator. To deal with the increasing number of skillful hackers, many scientists have suggested the application of AI in developing computer security in the upcoming time. We can upgrade detection to removes the breach and stops the spread of malware automatically while making sure that no data is affected. The future of cybersecurity surely focusses on authentication detection and password protection. Passwords are weak, and the future necessitates a safer replacement in the face of escalating social engineering activities. As a result, AI would be utilized in the identification of face recognition, fingerprints, retina scans, and other biometrics which make the task of storing our core data safer than the software we are currently using.

2. What is likely the impact?

As I have mentioned above, AI is a great innovation of humanity that, if correctly applied, has the potential to give a high level of sophistication to the cyber security business in tracking down viruses and preventing hacker from attacking their computer cloud. Speed and automation are two fundamental qualities that distinguish people from smart robots. When it comes to its affection on individuals, those working in big data science may be replaced by AI technology because they must spend a significant amount of time

analyzing data and gaining insights from multiple sources while machines might quickly conduct the same computations and deliver insights within a short amount of time. Corporation may put this possibility into consideration because with an IT expert who can use and develop AI alone could possess higher productivity than a group of computer scientists whose techniques are old or may even be outdated. But, in my opinion, instead of being a replacement for human employees, AI will take a role as an assistant tool in order to help cybersecurity analysts do their job better, faster, and more effectively. Of course, among information security analysts in many businesses, those who cannot keep up with the constant improvements of cybernetics will be replaced by the elite ones. Finding trained individuals to install and manage successful cybersecurity programs, on the other hand, is proving to be the most difficult challenge. According to a study conducted last year by the IT security group (ISC)², there are 2.93 million vacant cybersecurity positions globally.

Obviously, given the scarcity of knowledge and the rapid growth of technology, automation has been viewed as the answer to this skills gap. That makes sense, and because the cybersecurity solutions industry is so busy and competitive, these sorts of technologies are becoming accessible to alleviate the rising workload on current workers.

3. How will this affect you?

In my daily life, storing my personal information always makes me feel anxious because my Google account was once hacked, which is the main reason for the loss of my data on Google Drive and my Facebook account. I struggled to look up for my friend's contact when I registered a new account and it cost me so much time to find all of them.

When I opened a bank account to use a credit card in high school, I even used a USB and a hard disk to save my password as well as bank information and trust me, that was the most inconvenient act I have ever done. That is the moment where I recognized the importance of cybersecurity and my family had paid for a year-pack to use the cybersecurity services.

of Avast Premium to protect our data till now. My father also use this software for his company to prevent the leakage of inside information. It makes either my life or family life a lot more comfortable and easier because we do not need to care about data issues anymore since them has been secured by Avast and if there any problem occur, the software will take of it like separate the infected files and speedily wipe them out without our acknowledge.

Reference list:

Vikki Davies 2021, “The history of cybersecurity”, viewed 1 December,
<https://cybermagazine.com/cyber-security/history-cybersecurity#:~:text=Cybersecurity%20began%20in%20the%201970s,which%20chased%20and%20deleted%20Creeper.>

Abi Tyas Tunggal 2021, “Why is cybersecurity important?”, view 1 Dec,
<https://www.upguard.com/blog/cybersecurity-important#toc-3>

Bob Martin 2016, “5 must-have features of antivirus software”, view 1 Dec,
<https://greatlakescomputer.com/blog/5-must-have-features-of-antivirus-software>

Jyotsna 2019, “How will AI impact Cyber Security in the future”, viewed 1 December,
<https://www.jigsawacademy.com/how-will-ai-impact-cyber-security-in-the-future/>

Sky Sports 2020, “Manchester United cyber attack: UK security agency assisting as disruption continues”, view 1 December,
<https://www.skysports.com/football/news/11667/12143564/manchester-united-cyber-attack-uk-security-agency-assisting>

Joe Devanesan 2021, “Will AI replace cybersecurity teams completely?”, view Dec 1,
<https://techwireasia.com/2021/03/will-ai-replace-cybersecurity-teams-completely/>

