Name: Rakyan Satrya Adhikara

Student ID: 219548135

Cyber security and Hacking: Is it a social or a technical problem?

Computer science, one of the studies that are still developing compared to others. However, recently, its development has been grown on a very fast pace, which capture people’s interests. There are many aspects of computer science that are well-known these days and among them is Cyber security. Accordingly, Cyber security is “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organization and user’s assets” (Solms and Niekerk 2013). Thus, it is a fact that Cyber security is highly important and nothing to be underestimate. However, its development, unlike any other, is not as fast and as impactful. Accordingly, 82% of employers report a shortage of cybersecurity skills (Sobers 2020) and Hackers attack every 39 seconds, on average 2,244 times a day (Sobers 2020). Also, it has been shown that a lot of people still misjudge the true importance of cyber security. More than 13,500 reports of cybercrime that the Australian Cyber Security Centre has encountered since a new online portal opened in July 2019 (Carr-Catzel 2019) and the federal government estimates cyber security incidents cost Australian businesses $29 billion each year (Carr-Catzel 2019). In addition, almost one in three Australian adults were affected by cybercrime in 2018 (Carr-Catzel 2019). In consequence, it is safe to say that there are a huge number of people that have not recognize cyber security and how much it can make a difference. This research will tell if whether cyber security is a social or a technical problem.

To begin with, currently, cyber security is one of the biggest problems that people must face in the whole world. In correspondence, “there are 4.1 billion of reported records exposed in the first half of 2019” (Crane 2019). This number does not include data breaches that went unreported or undiscovered, meaning that potentially, there might be millions of more records were exposed that many people are not aware. Not only that, but there were 144.91 million new malware samples in 2019 and already at 38.48 million new samples in 2020 (Zaharia 2020). Now, in Australia, cyber security is a problem that people are commonly get, in form of many attacks. According to recent report from Australian Cyber Security Centre (2019), In the first three months of operation, there were 13,672 reports that are made to ReportCyber, which indicates that in average, there are 148 reports per day, or every ten minutes, there is one report. In addition, accordingly, “Victoria receiving the greatest proportion (3,023; 26.4%), followed by Queensland (2,997; 26.1%) and then New South Wales (2,930; 25.6%)” (Australia Cyber Security Centre 2019). Which as a result, is has been estimated that annual losses to cybercrime is around $328 million and more than $890,000 in reported losses each day (Australia Cyber Security Centre 2019). This indicates that people have aware how cyber security is a critical component. To support this argument, research shows that “40 percent of global respondents, including 36 percent of Australian respondents, have implemented cyber-awareness programmes as part of their cyber preparation strategy” (Telstra 2018). Which, it indicates that less than half of Australia have not implemented any cyber security strategies.

Furthermore, Australian Cyber Security Centre (2019) reports that between July and September 2019, there are five types of attack that were commonly reported to the ACSC, those are identity theft, online fraud & shopping scams, bulk extortion, online romance scams, and wire-fraud & business email compromise. In addition, Accordingly, Identity theft and online fraud are the two most commonly reported cybercrime categories, making up over 40% of reports received by the ACSC over the quarter (Australia Cyber Security Centre 2019). Which indicates that a mass number of people have no strategy to face such problems. Those kinds of problem commonly caused **social engineering attacks**, a cybercrime that using more social skills than the technical skills. People aren’t aware that cyber security is not only consists of technical issues, but also social issues. Social engineering attacks are kinds that people commonly get, such as phishing, vishing (voice phishing), shoulder surfing. Thus, it is a fact that

In conclusion, cyber security is one of many aspects of computer science that are well-known these days and it is highly important. On the other hand, there are several issues that can be found in cyber security. Its development is not as superior as other aspects. Accordingly, by 2021, it’s projected that there will be 3.5 million unfilled cybersecurity jobs globally (Sobers 2020). In addition, many people have underestimate cybercrimes in Australia. In average, there are 148 reports per day, or one every ten minutes (Australia Cyber Security Centre 2019). In addition, not many people aware how important cyber security is. Telstra (2018) states that 40 percent of global respondents, including 36 percent of Australian respondents, have implemented cyber-awareness programmes as part of their cyber preparation strategy. Furthermore, people aren’t aware that cyber security needs more than technical strategy. It also needs social strategy to face social engineering attacks and currently, it lacks of social support.

References

1. Solms, Rossouw von & Niekerk, Johan van 2013, “From information security to cyber security”, *Computer & Security*, vol. 38, pp. 97, retrieved 9th May 2020, ScienceDirect.
2. Sobers, R 2020, ‘110 Must-Know Cybersecurity Statistics for 2020’, Data Science, 15th April, retrieved 9th May 2020, <<https://www.varonis.com/blog/cybersecurity-statistics/>>
3. Carr-Catzel, J 2019, *Almost one in three Australian adults were affected by cybercrime last year*, media release, 8th October, SBS News Australia, retrieved, 9th May 2020, <<https://www.sbs.com.au/news/almost-one-in-three-australian-adults-were-affected-by-cybercrime-last-year>>
4. Crane, C 2019, ‘33 Alarming Cybercrime Statistics You Should Know in 2019’, hashedout, 14th November, retrieved 9th May 2020, <<https://www.thesslstore.com/blog/33-alarming-cybercrime-statistics-you-should-know/>>
5. Zaharia, A 2020, ‘300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2020] EDITION]’, Comparitech, 22nd April, retrieved 9th May 2020, <<https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/>>
6. Australia Cyber Security Centre 2019, *Cybercrime in Australia July to September 2019*, ACSC, Canberra
7. Telstra 2019, *Telstra Security Report 2018*, Telstra Corporation Limited, Melbourne