Topic Analysis #6 - How Does Info Security Impact All Areas Of IM?

Information security is the way to practice preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of sensitive records *(Nicholas King, 2 March 2021)*. Every organization should take this practice seriously because unless an organization never use internet, it will have chance to encounter cyber threats and lose the data. Therefore, I would like to use the next paragraphs to explain how does information security impact all areas of information management.

The global average cost of a data breach reached $4.24 million in 2021, according to the Cost of a Data Breach Report 2021 released by IBM and the Ponemon Institute, a 10% increase from the previous year *(Andrada Coos, 11 April 2022)*. How to keep information secure become an important topic. Businesses keep their information secure by many ways. First of all, the data should be well organized. Businesses only collect the data they required and nothing more. This reduced the database size that is required to store the data as well as reduce the risks for businesses and their customers. This is because if data breaches unfortunately occurred, private information of customers will lose fewer. Besides, business need to know exactly which and where data is stored. By knowing this, business can make right decision regarding the measures they need to protect the data. Also, there are plenty of cybersecurity software, such as Avast, Kaspersk, and Lastpass. Business should invest in one of the cybersecurity programs that is trustworthy. By subscribing the service, the data is protected from malware and threats. Lastly, most business will also use encryption to protect sensitive business data and secure customers' private information. This is important because many people work with their own computers and smartphones. When users need to verify identity through two or even three factors before entering the business's database, it will ensure the data inside it is more secure.

There are many ways that hackers and other cyber thieves used to acquire sensitive information, here, I will provide three ways. First, social engineering is a way that some of us have encountered. Hackers can use social media to trick you as some you are familiar with. In fact, my own aunt has been tricked to click a link on messenger and got hacked. One of the most recent famous examples is a Singaporean scammer called Ho Jun Jia, he tricked co-founder of Riot Games by social engineering *(Davina Tham, 23 Jun 2022)*. Another method is called "keylogger". It is a software and can be installed to USB, it can also send as an attachment of email *(Alexander S. Gillis, nd)*. Once it is in the computer, it will

record everything the user has typed. By doing this, the hacker can retrieve the user's passwords. The last example is public wi-fi eavesdropping. Since public Wi-Fi allow unsecured transmission of data, users' information might be exploited and unencrypted. What hackers will take advantage of this situation is by naming their own hotspot as the name of the public Wi-Fi. Once the user connected to the hacker's Wi-Fi, the hacker will be able to see everything you do and steal the user's personal information. Besides these three examples, there are many other ways hackers do to get steal information. Therefore, we should always be conscious when using our tech devices.

In a careful organization, information security affects information management in many ways. Firstly, in the field of data science, information security is used to make data protection. Before starting a new project, the data should be checked with information security. This is because malware might be hidden in the dataset. In the field of business intelligence, every important information inside the organization should be encrypted. Without decrypt method, even if hackers get the data, they will not be able to understand what it means. Also, by regularly scanning for vulnerabilities, information security can ensure the database is secured. Moreover, it can quickly identify the threat before it become critical concern. Lastly, when a data organization has implemented information security, it can verify to third parties that sensitive data is secured by the organization, by doing this, other companies will be willing to share their data to the data organization to do further analyze. Information security might affect the efficiency of information management because it has to scan through all the data that need to be managed later. However, it is all worth it. What an organization can do is to simplify or update the information security function instead of getting rid of it and put the company at risk.

In my opinion, two of the most significant information security challenges businesses will face in the future are ransomware attacks and deepfakes. Many companies and individuals have already become the victims of ransomware, however, since it is still an ongoing security attacks without solution, I believe it is still a big challenge for information security in the future. What ransomware will do is hacking into the users' account and encrypted their information. If the victims want to access their data again, they need to pay the hackers to decrypt. Moreover, there is no promise that hacker will decrypt the data after the victims paid. According to the Financial Trend Analysis report by Fincen (Financial Crime Enforcement Network), suspicious activity related to ransomware SARs in the first half of 2021 estimated $590 million exceeded the total reported for all of 2020 ($416 million). Deepfake is a new technology that use deep learning to change faces of people in

images or even videos. Hackers can use this trick to cheat people into believing they are seeing a video of someone they know. When the victims let their guards down. They might believe whatever the hackers said and scammed. To me, these are the two information security challenges that will continue affecting the world and definitely need to be solved in the future.

Reference:

Nicholas King. "The Importance of Information Security." *Vigilant Software - Compliance Software Blog*, 2 Mar. 2021, www.vigilantsoftware.co.uk/blog/the-importance-of-information-security.

Andrada Coos. "5 Ways Big Companies Protect Their Data." *Endpoint Protector Blog*, 27 Dec. 2018, www.endpointprotector.com/blog/5-ways-big-companies-protect-their-data/.

Tham, Davina. "Singaporean Jailed for Deceiving Amazon, Google into Providing S$7.6 Million Worth of Cloud Services." *CNA*, 23 June 2022, www.channelnewsasia.com/singapore/cheat-amazon-google-cloud-computing-mine-cryptocurrency-marc-merrill-2765636. Accessed 3 Nov. 2022.

Gillis, Alexander S. "What Is a Keylogger? Definition from SearchSecurity." *SearchSecurity*, www.techtarget.com/searchsecurity/definition/keylogger.