The cyber security become as big and important issue in this digital era while COVID-19 pandemic made many organizations to move online. According to (IBM, 2021), the cost of data breach due to COVID-19 pandemic and remote work were more than average while no effort made by organization, with taken remote work as a factor the cost was $1.07 million more than the remote work is not a factor.

While big-names businesses such as Microsoft, MGM resorts, Twitter, Facebook, LinkedIn and others were a victim for cyberattack this year (Bekker, 2021), therefore, small or medium business are at high risk. Invest in cyber security is crucial for businesses to keep their clients/customers data safe, unreachable for unauthorized people as well as to protect its reputation between other competitors, in addition, to remain away of financial loss.

Uber as a private company its business is to request a car by using smartphone application depends on GPS and location. Uber reported that by December 2018 have 91 million riders and 3.9 million drivers with 10 billion trips completed worldwide (Uber Newsroom, 2019). (Rasalam and Elson, 2019) highlights that there were two data breaches with Uber, the first was in 2014 and Uber was fined $20,000 because of not disclose that on the same time, the second was in 2016 were data of  57 million customers and 600,000 drivers affected, data such as names, mobile numbers and driver’s card downloaded from Uber storage. According to (Federal Trade Commission, 2018) Uber paid $100,000 to the intruders and fail to disclose the data breach to customers or federal trade commission in the same time, while the law not allowed to pay for hackers, therefore, for this violent Uber fined $41,484 in result.

For all of that, cybersecurity is a safety valve for the economy in this digital age, and business need to continue a lot of efforts to reach a secure system. However, even having a security system is not completely sufficient, but need to understand the potential risks we are facing and recognize that the data is vulnerable to breach, then we can reach a more sufficient level of protection (VanSyckel, 2018).

Bekker, E. (2021). *2021 Data Breaches - The Worst Breaches of the Year | IdentityForce®*. [online] We Aren’t Just Protecting You From Identity Theft. We Protect Who You Are. Available at: https://www.identityforce.com/blog/2021-data-breaches [Accessed 13 Aug. 2021].

Federal Trade Commission. (2018). *Uber Agrees to Expanded Settlement with FTC Related to Privacy, Security Claims*. [online] Available at: https://www.ftc.gov/news-events/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security [Accessed 15 Aug. 2021].

IBM (2021). *Cost of a Data Breach Study*. [online] Ibm.com. Available at: https://www.ibm.com/security/data-breach [Accessed 14 Aug. 2021].

Rasalam, J. and Elson, R. (2019). *CYBERSECURITY AND MANAGEMENT’S ETHICAL RESPONSIBILITIES: THE CASE OF EQUIFAX AND UBER*. [online] . Available at: https://www.igbr.org/wp-content/uploads/articles/GJBP\_Vol\_3\_No\_3\_2019-pgs-8-15.pdf [Accessed 14 Aug. 2021].

Uber Newsroom. (2019). *Company Information | Uber Newsroom Canada*. [online] Available at: https://www.uber.com/newsroom/company-info/ [Accessed 15 Aug. 2021].

VanSyckel, L. (2018). White Paper: Introducing Cybersecurity - Sealevel. *Sealevel*. [online] 22 Jan. Available at: https://www.sealevel.com/support/white-paper-introducing-cybersecurity/ [Accessed 15 Aug. 2021].