My initial post indicates the failure on preventing cyber risks on the business side. They are business operation, reputational, and legal and compliance risks. Besides the attacks and risks on the IT side, cyber risks can also harm businesses in several aspects. There were system breach incidents that happened in Yahoo!. It began in Aug 2013, and staff in Yahoo! discovered a breach of its data in late 2014 but they did not take the breach seriously including Yahoo! CEO. Over 500 million user accounts had been stolen and sold data online. Yahoo! publicly disclosed the breach in Sep 2016 (Yahoo! Inc, 2016). This data breach caused Yahoo! To lose its reputation and its value. In 2017, Verizon re-negotiated the acquisition figure from $4.8 billion to $4.48 billion. Yahoo! CEO Marissa Mayer lost her 2016 bonus (Kharpal, 2017) and resigned in Jun 2017 (Schwartz, 2017). The investigation revealed a total of 3 billion Yahoo! accounts were hacked (Perlroth, 2017). This is also shown as a good example of the business cost of Cybersecurity failure.

Thank you for the responses from Demain, Deepak, and Patricia. The cyber risks are targeting both online devices and offline devices. They raised a very good question, examples, and studies inherited and addressed from my initial post. I do agree that the cyber security measures should be included for both as a cyber security task force. The data breach in Yahoo! I mentioned also emphasizes the cost of delay of breach identification and notification discussed in Uvaraj's post. The security measure scopes should cover all the identified areas as much as possible, and perform the prevention and protection as much as we can. The incident response plan should also take into consideration and seriously.

During the first 3 units of module 1, I learned the concept of Confidentiality, Integrity, and Availability (CIA) in Cyber Security, the attack surfaces in a network, the ethical and governance frameworks, the implications of security breaches, and the approach to threat and vulnerability identifications. In the preparation for the discussion forum, those cases and researches give me a sense of the industrial practice approaches and bring me to know how the importance of cyber security awareness around information systems security and data protection acts.

Reference:

Yahoo! Inc. 2016. *Yahoo security notice December 14, 2016.* Available: https://help.yahoo.com/kb/SLN27925.html [Accessed 19 March 2022].

Kharpal, A. 2017. *Verizon completes its $4.48 billion acquisition of Yahoo; Marissa Mayer leaves with $23 million.* Available: https://www.cnbc.com/2017/06/13/verizon-completes-yahoo-acquisition-marissa-mayer-resigns.html [Accessed 19 March 2022].

Schwartz, M.J. 2017. *Yahoo CEO loses bonus over security lapses.* Available: https://www.bankinfosecurity.com/yahoo-ceo-loses-bonus-over-security-lapses-a-9748 [Accessed 19 March 2022].

Perlroth, N. 2017. *All 3 billion Yahoo accounts were affected by the 2013 attack.* Available: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html [Accessed 19 March 2022].

Swinhoe, D. 2021. *What is physical security? How to keep your facilities and devices safe from on-site attackers.* Available from: https://www.csoonline.com/article/3324614/what-is-physical-security-how-to-keep-your-facilities-and-devices-safe-from-on-site-attackers.html [Accessed 20 March 2022]