Cyber security is a global issue. From the discussion posts, we can argue that investment is imperative for businesses to manage attacks, breaches and build confidence in their reputation.

One of the most significant challenges to companies is securing data, and as companies grow, so does the risk applied to that data from threat actors. (VanSyckel, 2018:1) 'This is the rule of the data revolution: for every action to store, secure, and use data, there is an equal or greater reaction to steal data' identifies the increased risk applied to securing data and the Equifax data breach (Federal Trade Commission, 2020) in 2017 is testament to this. In the Equifax case, it is evident that the company was not in the prime position to manage and deal with such an attack effectively. Evidence suggests that months before the breach, Equifax was made aware of exploit vulnerabilities, namely Struts (Ullrich J, 2017). The team did not act by patching the issues of concern (Fruhlinger J, 2020a). The failure to act had disastrous consequences for Equifax, which began with the threat actors going undetected for many months, using encryption methods with small increments of data over approximately 76 days to avoid detection. Equifax had invested substantial amounts of money in their system and had the capabilities to prevent such infiltration; however, they had poorly managed and implemented their security design. Unpatched vulnerabilities and the tools needed became ineffective as Equifax did not renew a public key certificate (Fruhlinger J, 2020b) which would have supported the defence of the attack.

The Equifax case summarises that investment is more than having secure technical infrastructure. To aim for successful confidentiality, integrity and availability, companies need to invest in human factors such as staff expertise in dealing with software or network security. The risk posed is far greater with significant financial losses, reputational damage, business service disruption, and ultimately psychological damage to stakeholders whose data was the subject of a breach.

Federal Trade Commission. 2020. *Equifax Data Breach Settlement* [Online]. Available: **https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement** [Accessed 12 August 2021].

Fruhlinger J. 2020a. *Equifax data breach FAQ: What happened, who was affected, what was the impact?* [Online]. Available: **https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html** [Accessed 23 August 2021].

Fruhlinger J. 2020b. *What is PKI? And how it secures just about everything online* [Online]. Available: **https://www.csoonline.com/article/3400836/what-is-pki-and-how-it-secures-just-about-everything-online.html** [Accessed 23 August 2021].

Vansyckel, L. 2018. *Sealevel Systems White Paper - Introducing Cybersecurity.* [Online].

Available: **https://www.sealevel.com/support/white-paper-introducing-cybersecurity/** [Accessed 12 August 2021].