Cybersecurity is a global issue, and investment by companies is crucial if they are to build confidence, sustain their reputation and be competitive in their business markets.

In the case of Equifax, a multinational company that supports financial services to consumers (Equifax Inc., 2021a); In 2017, Equifax discovered a data breach that consequently affected 147 million people from the United States, United Kingdom and Canada. The resulting discussions with the Federal Trade Commission decided that $425 million would be settled to support people affected by this data breach (Federal Trade Commission, 2020).

Equifax collects personal data from third-party companies such as banks, insurance companies, loan brokers or financial advisors who offer financial services such as loans, investment advice and insurance (Equifax Inc., 2021b). A breach could potentially have severe consequences for companies such as Equifax and others providing a solid argument for company investment in cybersecurity. One consequence would be a decline in confidence and reputational damage. (VanSyckel, 2018) highlights that even with sufficient cybersecurity planning in place, companies need to admit that data is vulnerable with protections needed suggesting that investment is essential to be ready for potential attacks by improving current systems with new technology. It is important to note that not all breaches have negative financial consequences. In the UK, many businesses disclosed that temporary loss of access and website disruption was more common than the more significant ransomware or denial of service attacks. This trend is likely due to companies becoming more resilient to breaches or attacks and understanding that attackers behaviours can change. Attackers potentially could be organising more sophisticated attacks on a smaller number of companies. (Department for Digital Culture Media and Sport., 2019)

Therefore cybersecurity is a global issue whereby companies need to invest carefully. A data breach with material outcomes such as loss of money, assets, file loss, or staff resources damages the company's profile. It can take considerable time to recover data and allow the company to resume normal operations. Inevitably this leads to significant negative financial implications and a longer-term reduction in consumer confidence.

Department for Digital Culture Media and Sport. 2019. *Cyber Security Breaches Survey 2019: Statistical Release* [Online].
Available: **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950063/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised_V2.pdf** [Accessed 12 August 2021].

Equifax Inc. 2021a. *About us* [Online]. Available: **https://www.equifax.com/about-equifax/** [Accessed 12 August 2021].

Equifax Inc. 2021b. *Privacy Statement* [Online].
Available: **https://www.equifax.com/privacy/privacy-statement/** [Accessed 12 August 2021].

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].

Vansyckel, L. 2018. *Sealevel Systems White Paper - Introducing Cybersecurity.* [Online]. Available: **https://www.sealevel.com/support/white-paper-introducing-cybersecurity/** [Accessed 12 August 2021].