INTRODUCTION

Microsoft is one of the biggest companies in the world, with a market cap of approximately $3 trillion USD (Nasdaq, 2024). Their portfolio covers the majority of the technological landscape, from personal computing to enterprise cloud solutions. As such, they are a huge target for potential attacks, a recent example being account takeovers carried out by a state sponsored threat actor (MSRC, 2024). This post will discuss why cyber security is an important issue for Microsoft to invest in.

FINANCIAL IMPLICATIONS

The financial implications of a cyber attack will be a concern for any company, with the median cost of a targeted attack being approximately $16,000 USD (Hiscox, 2023). For a company the size of Microsoft, this could be seen as small. However, in the EU Microsoft still has to comply with the General Data Protection Regulation (GDPR). Any data breach in the EU could lead Microsoft to be fined up to four percent of their worldwide annual turnover (European Parliament, 2016). With a yearly revenue of $211 billion USD (Microsoft, 2023), this is a significant amount, and highlights the importance of regulatory compliance. In order to avoid the financial consequences of a breach, investment in employee cyber security training and the hardening of network architecture is an ideal solution.

REPUTATIONAL DAMAGE

Not only could a data breach or attack be expensive, but it would also cause consumers to lose trust in the security of Microsoft’s products. A series of security issues plagued Microsoft products, such as IIS, in the early 2000s. Consumers were advised to avoid them, which damaged their reputation and naturally harmed their competitiveness in the market. As a result, Microsoft had to invest more time in product development. Microsoft delayed their products until they underwent thorough testing and they prioritised consumer trust, leading to fewer security vulnerabilities in their later products (Wiliams, 2019).

CONCLUSION

While the financial cost of a cyber security attack is minute compared to Microsoft’s market cap, any breach of data will lead to significant fines. It will also lead to damage to their reputation and loss of competitiveness. Microsoft has suffered from security issues in the past, which led to new secure development practices. Without a heavy investment in cyber security, Microsoft would not be the global company it is today.

References

European Parliament. No. 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> [Accessed 03 May 2024].

Hiscox. (2023) *Hiscox Cyber Readiness Report.* Available from: <https://www.hiscoxgroup.com/sites/group/files/documents/2023-10/Hiscox-Cyber-Readiness-Report-2023.pdf> [Accessed 18 April 2024].

Microsoft. (2023) *Annual Report*. Available from: <https://www.microsoft.com/investor/reports/ar23/index.html> [Accessed 03 May 2024].

# MSRC. (2024) Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard. Available from: <https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/> [Accessed 04 May 2024].

Nasdaq. (2024) Microsoft Corporation Common Stock (MSFT). Available from: <https://www.nasdaq.com/market-activity/stocks/msft> [Accessed 03 May 2024].

Williams, L. (2019) Secure Software Lifecycle Knowledge Area. Available from: <https://www.cybok.org/media/downloads/Secure_Software_Lifecycle_issue_1.0.pdf> [Accessed 03 May 2024].