**Summary Post**

The peer responses appeared to largely agree with my post, however they suggested exploring Microsoft’s current strategies, business needs and security posture compared to their rivals. This post will summarise our discussion.

**Business Needs**

Arguably, Microsoft see security low in their business needs if there is no return on investment. In 2023, Microsoft faced backlash when federal departments that used their systems were hacked (Guardian, 2023). Security features were paid add-ons (Jones, 2023), as opposed to defaults which their own team advocates (Howard & LeBlanc, 2014). This backlash also emphasises my original point about reputational damage and data breaches harming trust. An increase in investment in the development cycle could have prevented the criticism.

**Industry Rivals**

Paid add-ons were clearly a financial decision, and in stark contrast to their rival Apple who appear to prioritise security. For example, when the FBI requested access to a terrorist’s iPhone, Apple refused, stating it would damage consumer trust and put all iPhone users at risk (Mishra, 2020). Microsoft could have avoided the criticism from the aforementioned hack had they taken the same stance and moral investment in cyber security as Apple. There is also a danger of rivals taking market share should Microsoft have a lax security posture compared to their rivals.

**Current Strategies**

Microsoft ensure their security methods are up-to-date through collaboration, research and investment. This approach is heavily outlined in the *Microsoft Digital Defense Report* and is seen with Microsoft assisting Ukraine in combatting Russian “cyber weapons” (Microsoft, 2023). The company is also enhancing its security posture by investing in areas such as Artificial Intelligence. This investment will aid Microsoft in achieving their predicted 2025 cyber security revenue of $35 billion USD (Krause, 2023).

**Conclusion**

To summarise, Microsoft have struggled with security in the past. However, they must maintain investment in cyber security. Failure to do so will result in reputational damage, loss of consumer trust and damage to their market share compared to more security conscious rivals.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**References**

Guardian. (2023) US Reprimands Microsoft for security failures that allowed Chinese hack. Available from: <https://www.theguardian.com/technology/2024/apr/03/microsoft-errors-security-chinese-hack> [Accessed 19 May 2024].

Howard, M. & LeBlanc, D. *Writing Secure Code: Practical Strategies and Proven Techniques for Building Secure Applications in a Networked World.* Redmond: Microsoft Press. Available from: <https://ebookcentral.proquest.com/lib/universityofessex-ebooks/reader.action?docID=540974> [Accessed 19 May 2024].

Jones, D. (2023) Microsoft offers free security logs amid backlash from State Department hack. Available from: <https://www.cybersecuritydive.com/news/microsoft-free-security-logs-Outlook-email-hack-backlash/688388/> [Accessed 18 May 2024].

Krause, R. (2023) Microsoft’s Cybersecurity Business is Booming. Critics Say It’s The Problem. Available from: <https://www.investors.com/news/technology/microsoft-stock-cybersecurity-business-booms-critics-say-its-the-problem/> [Accessed 19 May 2024].

Microsoft. (2023) *Microsoft Digital Defense Report 2023.* Available from: <https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023> [Accessed 18 May 2024].

Mishra, A. (2020) The Intricacies of Trust in Technology: A Study of the Clash Between Apple and the FBI. *Journal of Cases on Information Technology* 22(4): 32. DOI: [10.4018/JCIT.2020100102](https://dx.doi.org/10.4018/JCIT.2020100102)