Review 1 - **Turnitin ID: 2631289403**

The essay presents an analytical examination of the human factors that impact cybersecurity in startups, delivering substantial insights into the specific challenges encountered by these organisations. A notable strength is the incorporation of scholarly literature, specifically referencing Butschek (2024) and the compliance budget concept introduced by Beautement and Sasse (2009), which helps to elucidate the conflicts between security compliance and operational flexibility. Additionally, the discussion of the 'trust paradox' is particularly effective, emphasising the challenges startups encounter in balancing operational efficiency with security obligations.

There is potential to improve the analysis. The essay references cognitive biases (Alnifie and Kim, 2023) and ineffective awareness strategies (Renaud and Weir, 2018). However, offering concrete recommendations for how startups can effectively tackle these challenges would enhance the argument. Furthermore, although the discussion on insider threats is comprehensive, including a few practical interventions that startups could feasibly adopt would be beneficial to the essay.

The essay is structurally cohesive and has been proofread effectively, which greatly improves its readability.

The analysis effectively identifies significant vulnerabilities; however, incorporating actionable recommendations specifically adapted to the constraints faced by startups would enhance the practical relevance of the essay.

References

Alnifie, G. and Kim, S. (2023) ‘Cognitive biases in cybersecurity decision-making among startup employees’, *Journal of Cyber Risk Management*, 4(2), pp. 101–114.

Beautement, A. and Sasse, M.A. (2009) ‘The compliance budget: managing security behaviour in organisations’, *Financial Cryptography and Data Security*, 4(1), pp. 40–48.

Butschek, T. (2024) ‘Examining cybersecurity challenges for startups: a human factors approach’, *International Journal of Cyber Studies*, 8(3), pp. 115–129.

Renaud, K. and Weir, G.R.S. (2018) ‘User engagement in cybersecurity training: an ineffective approach?’, *Information & Computer Security*, 26(2), pp. 246–259.

Review 2 - **Turnitin ID: 2629003232**

The essay provides a comprehensive analysis of key human factors influencing cybersecurity within a local startup, emphasising Insider Threats, Human Error, and Security Awareness and Training. It effectively situates these factors within an academic context by referencing relevant literature such as Sasse et al. (2021) and Rohan (2022).

A notable strength is the detailed examination of insider threats, clearly distinguishing between deliberate and accidental risks, supported by examples from Gartner (2024), CybSafe (2019), and Fortinet (2025). The inclusion of real-world incidents, such as those involving SolarWinds (Microsoft, 2021) and Tesla (Handelsblatt, 2023), demonstrates practical significance.

Human error is recognised as a significant risk, substantiated by findings from IBM (2023) and KnowBe4 (2024). Nonetheless, the analysis could be enhanced by providing clear, practical recommendations specifically tailored for startups. Additionally, the Security Awareness and Training section effectively links inadequate training to cybersecurity breaches, exemplified by the Twitter incident (FBI, 2020). However, incorporating more explicit training strategies for startups would strengthen this argument.

Overall, the analysis effectively identifies critical vulnerabilities, yet the inclusion of specific, actionable recommendations could significantly improve its practical applicability.

References

CybSafe (2019) *Human error to blame for 9 in 10 UK cyber data breaches in 2019*. Available at: https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/ (Accessed: 7 April 2025).

FBI (2020) *Twitter Bitcoin Scam*. Available at: https://www.fbi.gov/news/stories/twitter-bitcoin-scam-072020 (Accessed: 7 April 2025).

Fortinet (2025) *What Is an Insider Threat? Definition, Types, and Prevention*. Available at: https://www.fortinet.com/resources/cyberglossary/insider-threats (Accessed: 7 April 2025).

Gartner (2024) *Market Guide for Insider Risk Management Solutions*. Stamford, CT: Gartner, Inc.

Handelsblatt (2023) 'Tesla data leak exposes safety complaints', *Handelsblatt*, 28 April. Available at: https://www.handelsblatt.com/ (Accessed: 7 April 2025).

IBM (2023) *Cost of a Data Breach Report 2023*. Armonk, NY: IBM Corporation. Available at: https://www.ibm.com/reports/data-breach (Accessed: 7 April 2025).

KnowBe4 (2024) *Phishing by Industry Benchmarking Report*. Clearwater, FL: KnowBe4 Research. Available at: https://www.knowbe4.com/ (Accessed: 7 April 2025).

Microsoft (2021) 'Sunburst Attack Analysis'. Available at: https://www.microsoft.com/security/blog/2021/01/05/sunburst-attack-analysis/ (Accessed: 7 April 2025).

Rohan, R. (2022) 'Understanding of Human Factors in Cybersecurity: A Systematic Literature Review', *IEEE ComPE*, 53109, 9752358. Available at: https://doi.org/10.1109/ComPE53109.2021.9752358 (Accessed: 7 April 2025).

Sasse, M.A. et al. (2021) 'Human factors in cybersecurity: Emerging threats and mitigation strategies', *Computers & Security*, 104, p. 102221. Available at: https://doi.org/10.1016/j.cose.2021.102221 (Accessed: 7 April 2025).