**Review 1:** Reviewed Essay Turnitin ID: 2631148490

James Edney’s essay provides a well-developed critical analysis of three key factors influencing cybersecurity in start-up environments: human error, organisational culture, and insider threats. A key strength lies in the nuanced treatment of human error, which avoids oversimplified attribution to individual negligence. Instead, the essay appropriately acknowledges the influence of cognitive load, leadership expectations, and system unfamiliarity—concepts consistent with El-Bably’s (2021) and Kosta’s (2022) research.

The analysis of organisational culture is similarly strong, effectively linking theoretical frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework (Edwards, 2025) to the challenges faced by new businesses. The Capital One case study adds valuable real-world context, reinforcing the importance of a security-first mindset.

However, the essay could be strengthened by offering more integration across the three factors. The conclusion would benefit from more apparent synthesis, emphasising how poor organisational culture can cause human error and heighten insider threats. The insider threat section could also be more robust by including further peer-reviewed sources to deepen the analysis and provide a broader academic foundation.

Overall, the work is coherent, well-researched, and well-communicated, with constructive opportunities to enhance the depth of argument and evidence.

**Word Count: 190**

**Review 2**: Reviewed Essay Turnitin ID: 2631247337

Peter Osifo’s essay thoughtfully analyses three significant human factors in cybersecurity: user behaviour, insider threats, and organisational culture. The introduction sets the stage by referencing Schneier (2015), establishing the importance of human vulnerabilities in start-up environments with limited structure and resources.

The discussion of user behaviour is particularly effective. It is well-supported with evidence from Verizon (2021), Triplett (2022), and Maglaras et al. (2016) and successfully draws attention to the role of leadership in shaping cybersecurity practices. This area is often underexplored in similar discussions. This section effectively connects individual errors to organisational oversight.

The insider threat section provides good insight into psychological and environmental factors, referencing Bishop et al. (2009) and Greitzer and Frincke (2010). However, the section could benefit from more specific examples or industry case studies to enhance real-world relevance. Similarly, the discussion of organisational culture is intense, particularly in its critique of innovation-driven risk tolerance, supported by Xenikou (2022) and Ashenden and Lawrence (2016).

While the essay synthesises themes, the conclusion might be strengthened by reinforcing how these factors interrelate. Overall, the essay demonstrates coherent structure, sound critical engagement, and good use of academic sources to support its key arguments.

**Word Count: 194**

**References**

Ashenden, D. and Lawrence, D. (2016) Can We Sell Security Like Soap? A New Approach to Behaviour Change. New Security Paradigms Workshop (NSPW). https://doi.org/10.1145/3011883.3011889

Bishop, M., et al. (2009) Insider Threat Identification in Cyber Security: Concepts, Methods, and Technologies. Advances in Information Security.

Department for Science, Innovation & Technology (2024) Cyber Security Breaches Survey 2024. Available from: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024

Edwards, J. (2025) A Comprehensive Guide to the NIST Cybersecurity Framework 2.0: Strategies, Implementation, and Best Practice. Hoboken, NJ: Wiley.

El-Bably, A.Y. (2021) Overview of the Impact of Human Error on Cybersecurity Based on ISO/IEC 27001 Information Security Management. Journal of Information Security and Cybercrimes Research, 4(1), pp. 95–102. https://doi.org/10.26735/WLPW6121

Greitzer, F.L. and Frincke, D.A. (2010) Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modelling for Insider Threat Mitigation. Insider Threats in Cyber Security.

Kosta, E., Leenes, R. and Kamara, I. (2022) Research Handbook on EU Data Protection Law. Northampton, MA: Edward Elgar Publishing.

Maglaras, L., He, Y., Janicke, H. and Evans, M. (2016) Human Behavior as an Aspect of Cybersecurity Assurance. Security and Communication Networks, 9(17), pp. 4667–4679.

Schneier, B. (2015) Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton & Company.

Triplett, W.J. (2022) Addressing Human Factors in Cybersecurity Leadership. Journal of Cybersecurity and Privacy, 2(3), pp.573–586. https://doi.org/10.3390/jcp2030029

Verizon (2021) 2021 Data Breach Investigations Report. Available from: https://www.verizon.com/business/resources/reports/dbir/

Xenikou, A. (2022) Leadership and Organisational Culture. In: Handbook of Research Methods for Organisational Culture. Cheltenham: Edward Elgar Publishing, pp. 23–38.