Peer Review - Essay Posting for Review -> Individual Essay

1.0 Introduction:

It is crucial to highlight that people play a vital role in the framework of cybersecurity, particularly if the goal is to safeguard information systems in the highly challenging environment of a local start-up. Through human error, insider threats and concerns regarding security awareness and training programmes, start-ups suffer high rates of security threats due to their constricted budgets, fewer employees, and massive growth. Therefore, this article considers these three human factors of enterprise IT security seriously for their importance to a startup firm. Startups should perhaps be able to navigate the challenges of maintaining effective and robust cybersecurity measures in a dynamic and constrained environment if they are aware of these vulnerabilities.

2.0 Employee Awareness and Training:

However, it is crucial for start-ups especially since in such organisations the security posture of the organisation is entirely in the hands of one individual to incorporate awareness and training in cybersecurity. "Employee awareness" refers to ensuring the employees have adequate information regarding cybersecurity threats and how they can be averted (Wong *et al*., 2022). One of the typical obstacles for an official training program is the intensity of a start-up's schedule, the scarcity of funds, and personnel.

Startups can be at a high risk of security threats due to low training. Business owners neglect security education because startups focus on velocity and flexibility, which result in data theft, monetary loss, and brand image deterioration. This issue is more apparent in young organizations that have not had the time to institutionalize their practices. Further, lack of managerial control in the flat hierarchy and uncontrolled communication in organizations can result in the circulation of inadequate security standards (Van der Vyver, 2020). Employees with such minimal knowledge and training are even more vulnerable and can hardly be updated on possible security risks.

3.0 Insider Threats:

Insider threats are a major risk in start-up organisations, especially if they are small and lack defined structures. These threats can be of intentional type where the attack is planned and executed with a certain goal in mind, or accidental where employees do not know what they are doing and are careless. Small compact groups often foster negative attitudes to security and complacency and these insiders can perform many destructive actions without being noticed. High employee turnover rates also contribute to the danger of insider threats because any specific person who decides to quit the company still possesses access to information (Klein, 2023). Small teams are less formal, and this can result in the development of wrong attitude and complacency this makes it easy for insiders to operate without being detected.

The factors that start-ups must address include how open they should be as well as how much security they should apply to it. Insider threats pose a significant risk with immense financial and reputational repercussions, especially in the beginning phases of a start-up company when a single vulnerability is capable of causing significant losses.

4.0 Human Error:

Organizational cyber threats include bad password habits, configuration issues and accidental leakage of data. However, human error still dominates as a leading risk, especially in emerging startups, unlike the advances in technology. One of the reasons for high levels of employee mistakes in start-ups is the overload of work, short time limits for tasks, and the absence of qualified security personnel. This can lead to supervision and burnout. The structure of start-ups is less rigid and less formal compared to the structure of other companies and organizations, so they are also more vulnerable to security threats. The misconfiguration of these key systems puts them in a position where software releases are hasty and vulnerable to hacks. Consequently, the various risks affecting startups include having insecure applications since the software is deployed hurriedly.

These errors can have serious consequences for a startup, jeopardizing data, system availability, and, most importantly, client trust. It is specially so for start-ups whereas little mistakes could mean a lot more since they don't have the capacity and resources to recover quickly from a setback such as this. Cost constraints are especially a can of worms for start-ups because they do not have adequate funds to put in place elaborate error check mechanisms like an extensive testing and review process. This security hole goes on to explain why it is important for a startup's IT security measures to consider the errors made by employees.

5.0 Conclusion:

The cybersecurity of a local startup presupposes the training of its employees and places emphasis on recognizing insider threats and minimizing human errors. These interconnected human factors constitute the organization's security position. If a startup is not cautious in any of these areas, the security may be compromised, and this will be costly to its operations and reputation. Therefore, it can be stated that for start-ups that have a strategic mission of development in the long term in the conditions of an increasingly dangerous digital environment, it is not only justified but mandatory to include human factors in the IT security plan. Focusing on these areas will enrich the foundation upon which the startup and its safety and success depend upon.

References:

Kessler, M., Arlinghaus, J.C., Rosca, E. and Zimmermann, M., 2022. Curse or Blessing? Exploring risk factors of digital technologies in industrial operations. *International Journal of Production Economics*, *243*, p.108323. **https://research.rug.nl/files/192304368/1_s2.0_S0925527321002991_main.pdf**

Klein, J., 2023. Information Security Officers Perceptions of How to Implement Successful Information Security Programs in Health Sciences Center Environments. **https://ttu-ir.tdl.org/bitstreams/a5cd8b96-fa6f-4c11-be1e-214303a91053/download**

Van der Vyver, J., 2020. *A conceptual communication model to mitigate reputational risk within a higher education institution* (Doctoral dissertation, North-West University (South Africa)). **https://repository.nwu.ac.za/bitstream/handle/10394/36488/20556683%20VD%20Vyver%20J.pdf?sequence=1**

Wong, L.W., Lee, V.H., Tan, G.W.H., Ooi, K.B. and Sohal, A., 2022. The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*, p.102520. **https://www.sciencedirect.com/science/article/pii/S0268401222000548**