|  |
| --- |
| Close-up image showing the leaf-sides of two oversized books side-by-side on a bookshelf, with additional books in soft focus background |
| Critical Analysis of Three Human Factors in Cyber Security for a Local Start-Up |
| |  |  |  | | --- | --- | --- | | Milad Chowdhury | 3/28/25 | The Human Factor - March 2025 | |

Contents

[Introduction 2](#_Toc194051253)

[1. Social Engineering Susceptibility 2](#_Toc194051254)

[2. Insider Threats 2](#_Toc194051255)

[3. Security Awareness and Training 3](#_Toc194051256)

[Conclusion 3](#_Toc194051257)

[References 4](#_Toc194051258)

## Introduction

Human behaviour is central to cybersecurity. While technology offers robust defences, it is often the actions of individuals that introduce the most significant risks. For start-ups, the situation is intensified by resource constraints, informal structures, and fast growth. This essay critically examines three major human factors: social engineering susceptibility, insider threats, and security awareness and training, focusing on their implications for start-ups. The assessment brief intentionally excludes solutions.

## 1. Social Engineering Susceptibility

Social engineering manipulates human psychology to bypass technical controls. It includes tactics such as phishing, pretexting, and baiting (Hadnagy, 2018). In a start-up context, where trust and informality are typical, employees are particularly vulnerable to deception.

The *UK Cyber Security Breaches Survey 2019* found that **80% of attacks on UK businesses involved phishing**, highlighting how pervasive such threats are (UK DCMS, 2019). Start-ups are prime targets due to minimal investment in preventative tools and lack of structured training. Employees often lack awareness of verification protocols and may unknowingly disclose sensitive information.

Hughes-Lartey et al. (2021) also noted that organisations deploying IoT devices without robust human oversight increase the attack surface. Employees may fail to change default passwords or connect insecure devices, inadvertently allowing access to internal systems. For start-ups, such breaches can result in operational downtime, data theft, and reputational damage—potentially threatening their market entry or survival.

## 2. Insider Threats

Insider threats stem from individuals within an organisation who deliberately or accidentally compromise security. Malicious insiders may steal data for profit or sabotage systems, while negligent insiders contribute to breaches through carelessness (CERT Insider Threat Team, 2013).

Start-ups often operate with overlapping responsibilities and informal access controls. Employees frequently have wide-ranging permissions, which increases the risk of misuse. Moustafa, Bello and Maurushat (2021) argue that this lack of segmentation heightens exposure to internal risks. For example, a marketing employee with unnecessary access to customer databases could leak sensitive data intentionally or through poor data handling practices.

According to CERT (2013), **around 50% of insider incidents are unintentional**, driven by human error such as misconfigurations or lost devices. Start-ups typically lack comprehensive onboarding and offboarding procedures, so former employees may retain access, posing additional risks. Without monitoring tools or behavioural baselines, insider actions—incredibly negligent ones—often go undetected until damage is done.

Greitzer et al. (2019) further argue that insider risk is more than just a technical issue—it is behavioural. Rapid changes in start-up environments make it difficult to establish ‘normal’ patterns, which complicates the detection of anomalies. The consequences include financial loss, intellectual property theft, and regulatory non-compliance.

## 3. Security Awareness and Training

Cybersecurity training is essential yet often overlooked in start-ups. With competing priorities, such as product development and funding, training may be deprioritised or absent altogether. This leaves employees unaware of risks or how to respond to them.

Legrand (2022) notes that while people are often labelled the “weakest link,” they can be a critical defence when adequately informed. However, Schatz, Bashroush and Wall (2021) found that organisations without regular training are significantly more vulnerable to breaches from simple errors, like clicking on malicious links or failing to recognise fake login pages.

Johnson (2021) explains that security protocols must be aligned with user needs. If systems are too complex or inconvenient, users may circumvent them—for instance, by reusing passwords or saving credentials in browsers. This is particularly relevant in start-ups, where speed and ease of use often take priority over secure practices.

Employees are prone to cognitive overload in high-stress or multitasking environments. Hughes-Lartey et al. (2021) demonstrate that such environments increase the likelihood of human oversight, such as failing to spot phishing emails or mismanaging data access. These individual lapses can collectively weaken the entire organisation’s security posture.

The broader implication is cultural. Without leadership's emphasis on security, employees may not perceive it as a shared responsibility. Over time, this can embed poor habits into the organisational culture—habits that become more difficult to correct as the company grows.

## Conclusion

This essay has critically analysed three key human factors affecting cybersecurity in local start-ups: susceptibility to social engineering, insider threats, and security awareness gaps. These factors significantly influence risk exposure, especially in fast-moving, resource-limited environments. By understanding the behavioural roots and systemic implications of these vulnerabilities, start-ups can begin assessing their readiness and resilience while recognising that addressing solutions lies beyond the scope of this analysis. A comprehensive view of human behaviour in cybersecurity is essential to reducing future incidents and building long-term organisational security. Moreover, acknowledging the interplay between human decision-making, organisational culture, and technical infrastructure is crucial for anticipating emerging risks. As start-ups evolve, a failure to consider these dynamics may institutionalise poor security practices. Therefore, integrating human factors into strategic planning is not optional but foundational for sustainable and secure growth in a complex threat landscape.

## References

CERT Insider Threat Team. (2013) *Unintentional Insider Threats: A Foundational Study*. Social Engineering Institute.

Greitzer, F. L., Strozer, J. R., Cohen, S. A., Moore, A. P. and Mundie, D. (2019) ‘Insider threat indicators: Lessons learned from analysis of malicious and non-malicious insiders’, *Cybersecurity: A Systems Approach*, 29(3), pp. 45–60.

Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. John Wiley & Sons.

Hughes-Lartey, K. et al. (2021) ‘Human factor, a critical weak point in the information security of an organisation's Internet of things’, *Heliyon*, 7(3).

Johnson, J. (2021) *Designing with the Mind in Mind: Simple Guide to Understanding User Interface Design Guidelines*, 3rd edn. Waltham, MA: Morgan Kaufmann.

Legrand, J. (2022) ‘Humans and Cybersecurity—The Weakest Link or the Best Defense?’, *ICASA*.

Moustafa, A.A., Bello, A. and Maurushat, A. (2021) ‘The role of user behaviour in improving cybersecurity management’, *Frontiers in Psychology*, 12.

Schatz, D., Bashroush, R. and Wall, J. (2021) ‘The impact of security training on cybersecurity awareness and behaviour: An empirical study’, *Computers & Security*, 102(3), 1–17.

UK Department for Digital, Culture, Media and Sport. (2019) *Cyber Security Breaches Survey 2019: Statistical Release*.