**A Local Start-Up Company's Critical Analysis of Human Factors in IT Security**

## **Introduction**

Information system security depends significantly on human aspects as well as technology, with human factors playing a crucial role in cybersecurity. (Regnier, 2022). Addressing these human elements is essential for obtaining the highest level of cybersecurity in the setting of a small local startup business. Three human aspects that are crucial for the IT security strategy of a local start-up organization will be critically examined in this essay. These elements include insider threats, social engineering attacks, and staff awareness and training.

## **Employee Awareness and Training**

Fundamental components of cybersecurity in any firm, especially for start-ups, include employee education and awareness. (Katarina Kertysova, 2018). Employee awareness and knowledge play a significant role in the security posture of the firm because they are frequently the first line of defense against cyber threats (Regnier, 2022).

### **Critical Analysis:**

1. **Lack of Awareness**: Employees in a start-up with little experience might not completely understand the importance of cybersecurity. This ignorance may result in careless actions like unintentionally clicking on dubious links or revealing critical information. (CorpSecurity, 2023).
2. **Insufficient Training**: Startups frequently have limited funding; therefore, they might not put enough money into cybersecurity training programs. Employees may be unable to recognize and respond to cyber threats efficiently because of this flaw.
3. **Human Error**: Even highly skilled workers can make blunders. Pressure to fulfill deadlines in a quick-paced start-up setting could result in mistakes such as configuration problems or unintentional data exposures.

### **Implications:**

* Lack of knowledge and instruction makes the business more susceptible to cyberattacks.
* • Cybersecurity incidents brought on by staff mistakes can be expensive and detrimental to the reputation of the business.
* To reduce these hazards, employers must take a proactive stance regarding staff education and awareness.

## **Social Engineering Attacks**

Attacks on social engineering use psychological tricks to trick workers into disclosing private information or engaging in security-compromising behavior. Because trust and collaboration are frequently high in start-ups, these attacks are especially harmful. (Murtaza Ahmed Siddiqi, 2022).

### **Critical Analysis:**

1. **Phishing**: Employees who are not properly taught to spot odd requests might easily be duped by phishing assaults, such as email or phone fraud. Startups may not have strong email filtering systems, which leaves them more open to phishing attacks.
2. **Trust-Based Culture**: Startups frequently promote a culture of cooperation and trust. Although this is advantageous for teamwork, attackers who pose as dependable coworkers can make use of it to access critical data.
3. **Overconfidence**: Employees at startups could relax their guard and be less cautious when exchanging information or opening links because they believe they are immune to cyber risks.

### **Implications:**

* Data breaches, financial losses, and reputational harm can all be caused by social engineering attacks.
* Attackers may take advantage of the trust-based culture in startups if there are no effective defenses in place.
* To combat social engineering, a combination of staff education and technical safeguards is needed.

## **Insider Threat**

Insider threats occur when current or former workers, contractors, or business partners abuse their access to the organization to cause harm. Addressing it is essential for security resilience because startups are not immune to this risk. (Forte, 2019).

### **Critical Analysis:**

1. **Employee Discontent**: Employees may encounter stress, unhappiness, or conflicts in the fast-paced environment of a start-up. These feelings may give rise to insider threats like sabotage or data theft.
2. **Inadequate Access Control**: Start-ups could lack reliable access control systems, giving staff members more access to information than necessary. Insider data breaches are now more likely because of this.
3. **Lack of Monitoring**: Because start-ups typically lack ongoing monitoring, insiders can take advantage of this weakness to conceal their malevolent behavior until damage has already been done.

### **Implications:**

* Insider threats can have serious repercussions, such as the theft of intellectual property, legal troubles, and loss of investor and client trust.
* To lessen these risks, startups must employ strict access control and monitoring mechanisms.
* Resolving employee complaints and dissatisfaction is essential for preventing insider threats.

## **Conclusion**

In conclusion, human elements are crucial to the cybersecurity of local start-up businesses and necessitate a comprehensive strategy. Insider threats, social engineering attacks, and employee awareness and training programs are three crucial elements that must be carefully considered. To create a successful IT security strategy, a thorough grasp of these elements and their ramifications is necessary. Although most of this essay was devoted to analysis and implications, dealing with these issues demands a comprehensive strategy that incorporates technology, education, and a security-conscious organizational culture.

# References

CorpSecurity. (2023, 07 6). *CorpSecurity.* Retrieved 07 06, 2023, from https://corpsecurity.org/the-role-of-human-factor-in-corporate-security/

Forte, L. (2019). *RED GOAT CYBER SECURITY INSIDER THREAT REPORT 2019.* Bristol: RED GOAT CYBER SECURITY.

Katarina Kertysova, E. F. (2018). *Ensuringawarenessandresilienceoftheprivatesector acrossEuropeinfaceofmountingcyberrisks.* The Netherlands: European Economic and Social Committee.

Murtaza Ahmed Siddiqi, W. P. (2022). A Study on the Psychology of Social Engineering-based Cyberattacks and Existing Countermeasures. *MQPI - Applied Sciences, 1*(2), 1-19.

Regnier, E. (2022). *ASISONLINE*. Retrieved October 01, 2022, from https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2022/october/employees-the-first-line-of-defense-against-cyberattacks/