Seminar 2
Question 2: Blog Post

Task:

Some say that people are the biggest risk of cyber security.

Select five terms from ISO/IEC Standard 27000 Section 3 Terms and Definitions and write a 300-word blog post on how people can be managed to overcome cyber security attacks from the inside.

There will also be an opportunity to review your team's progress during the seminar.

Answer:

The human element is often considered the primary vulnerability in cybersecurity, accounting for a substantial portion of security breaches. However, organizations can effectively address and minimize these risks by implementing strategies based on ISO/IEC Standard 27000 Section 3, particularly through the establishment of well-defined protocols and the promotion of security awareness. The following five key concepts from ISO/IEC 27000 can be utilized to strengthen internal security measures.

1. **Access Control:** Limiting access to assets based on specific criteria is vital for reducing unauthorized entry (ISO/IEC 27000: 3.56). By restricting employee access to only the data essential for their job functions, companies can substantially decrease internal security risks. Periodic reviews of access rights,

especially during role changes, ensure that staff members do not retain unnecessary access to confidential information.

2. **Audit:** Systematic and documented evaluations are crucial for assessing the efficacy of an organization's security measures (ISO/IEC 27000: 3.3). Conducting regular audits enables companies to identify policy violations and potential vulnerabilities before they can be exploited. These audits can also cultivate a security-conscious environment, as employees are aware that their activities are being monitored, encouraging adherence to best practices.
3. **Authentication:** Robust authentication processes confirm the identity of individuals accessing systems, verifying that users are who they claim to be (ISO/IEC 27000: 3.5). The implementation of multi-factor authentication (MFA) requires users to provide additional verification, making it challenging for unauthorized individuals to gain access even if credentials are compromised.
4. **Threat Awareness:** Instructing employees about cyber threats, such as phishing attempts and malicious software, is crucial for establishing a proactive defence (ISO/IEC 27000: 3.74). Training programs can equip staff members with the skills to recognize and respond to suspicious activities, thereby reducing the likelihood of successful attacks due to human error.
5. **Confidentiality:** Maintaining confidentiality by ensuring that sensitive information is accessible only to authorized personnel minimizes the risk of data breaches (ISO/IEC 27000: 3.10). Organizations should clearly outline confidentiality policies and ensure that employees understand their responsibilities in safeguarding sensitive data, thus fostering a culture of accountability and responsibility.

By focusing on these principles, organizations can effectively manage the human factor in cybersecurity. Through ongoing education, strict access protocols, and regular audits, employees can be transformed from potential liabilities into proactive defenders against cyber threats.

References

ISO/IEC (2018) ISO/IEC Standard 27000 Section 3. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en [Accessed: 30 October 2024].