While technology plays a very important role in cybersecurity, human behavior remains a significant vulnerability (Matthews, 2017). In this blog post five key terms from the ISO/IEC 27000 standard (ISO/IEC 27000, 2018) are explored with notes on how organizations can leverage them to manage human risk and prevent internal cyber threats.

1. Access Control (Section 3.1):

- Definition: Limiting access to assets based on business needs and security requirements.
- Human Risk Mitigation: Implement strong access controls to ensure individuals only have access to the information and resources they need to perform their duties. This includes role-based access control, multi-factor authentication, and regular password changes.

2. Attack (Section 3.2):

- Definition: Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
- Human Risk Mitigation: Hackers mostly use social engineering tactics against employees (Grimes, 2024), so train employees to recognize and avoid common social engineering tactics like phishing emails, phone scams, and pretexting. There should be organization-wide security awareness programs to educate them about these threats and best practices for protecting sensitive information.

3. Security Implementation Standard(Section 3.73):

- Definition: Document specifying authorized ways for realizing security.
- Human Risk Mitigation: Organizations should have security implementation standards that demonstrate compliance with relevant security frameworks and regulations such as ISO/IEC 27000 and GDPR.

4. Threat (Section 3.74):

- Definition: Potential cause of an unwanted incident, which can result in harm to a system or organization.
- Human Risk Mitigation: Due to prevalence of insider threats, organizations should implement strong background checks for new hires and conduct security clearance reviews periodically.

5. Vulnerability (Section 3.77):

- Definition: Weakness of an asset or control that can be exploited by one or more threats.
- Human Risk Mitigation: Regularly assess systems and processes for vulnerabilities that could be exploited by attackers. This includes outdated software, weak passwords, and insecure configurations. Address vulnerabilities promptly to minimize the attack surface.

REFERENCES:

Matthews, E. D. (2017) The Weakest Link in Security Chain Is People, Not Technology. *Signal*. 71 (8), 64-.

ISO/IEC 27000. (2018) Information technology — Security techniques — Information security management systems — Overview and vocabulary. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en [Accessed 26 August 2024].

Grimes, R. A. (2024) *Fighting Phishing : Everything You Can Do to Fight Social Engineering and Phishing.* 1st ed. Newark: John Wiley & Sons, Incorporated.