Unit 2 Seminar: Blog Post

Task: Some say that people are the most significant cyber security risk.

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.

The posts made in this blog tool will be visible to all participants in this module. Comments from student peers and the tutor are encouraged.

My Post:

Disterer (2013) states that effective information security measures are critical in today's technology-driven world. Organisations must safeguard physical and digital assets, and security standards like ISO/IEC 27000, 27001, and 27002 provide guidelines for developing and maintaining an information security management system (ISMS).

The importance of human aspects in an organisation's cybersecurity posture must be acknowledged in the current digital environment, where cyber threats are pervasive. A thorough foundation for information security management is provided by ISO/IEC Standard 27000 (Kosutic, 2023).

Several terms and definitions in Section 3 provide insight into effectively managing people to resist cyber security attacks. The following are the five I have select:

1. **3.29 Information security continuity**

When a disaster or crisis occurs, information security continuity refers to a set of integrated rules, procedures, and processes that ensure a predetermined level of security remains intact. Continuity is achieved by identifying potential risks and

vulnerabilities, assessing their impact, and taking action to increase organisational resilience (Praxiom, N.D.).

2. **3.30 Information security event**

According to Praxiom (N.D.), an "information security event" is any state, condition, or occurrence that suggests a compromise of information security, a breach of security policy, or a failure of control.

3. **3.31 Information security incident**

An unplanned information security event could harm data security or disrupt business operations (Praxiom, N.D.).

3.32 Information Security Incident Management

Organisations use incident management procedures for detecting, reporting, evaluating, reacting to, and learning from information security incidents (Praxiom, N.D.).

3.33 Information security management system (ISMS) professional

Organisations use information security management systems (ISMS) to safeguard data, manage and control security risks, and accomplish business goals. The ISMS includes policies, procedures, records, agreements, contracts, guidelines, practices, methods, activities, roles, and responsibilities. It is a constituent of an organisation's more comprehensive management system (Praxiom, N.D.).

References:

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, [online] 04(02), pp.92–100. doi:https://doi.org/10.4236/jis.2013.42011.

Kosutic, D. (2023). *ISO 27001 Risk Assessment & Risk Treatment: The Complete Guide*. [online] advisera.com. Available at: https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/.

Praxiom (N.D.). *ISO IEC 27000 2014 Information Security Definitions*. [online] Available at: https://www.praxiom.com/iso-27000-definitions.htm#Information_security_continuity [Accessed 20 Aug. 2023].