J. Irvine Secure Software Development

Blog Post: Question 2
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.

Remember to record your results, ideas and team discussions in your e-portfolio.

Learning Outcomes
Identify and manage security risks as part of a software development project.
Critically analyse development problems and determine appropriate methodologies, tools and techniques (including program design and development) to solve them.

ISO/IEC Standard 27000 Section 3 Terms and Definitions is a list of terms and definitions used in the Information Security Management System (ISMS) family of standards (Disterer, 2013). Some research has identified that people are the biggest risk of cyber security (Budzak, 2016). I have chosen five that could help people manage cyber security attacks from the inside.

3.1 Access control is a security measure restricting a person's access to resources unless they have the required authorisation. Access controls should be implemented and enforced by the organisation to make sure those who do not have the clearance or authority cannot access sensitive or other information.

3.28 Information security is vital and training and can help employees understand its importance and ensure appropriate measures are taken to protect it, for instance locking your computer when you leave your desk. Information security should be robust and embedded in organisational culture, this could be through training, and awareness campaigns, enforced policies and procedures, and consequences for failing to comply.

3.3 Auditing: should be highly effective and robustly monitored to detect irregular behaviours or policy violations. The organisation should frequently review logs and analyse their systems activity in order to detect possible insider threats. Employment of security technologies e.g., behaviour analytics, could help detect abnormal patterns that indicate insider attacks. Regular audits may enable early detection and minimise threats, and limit the potential damage caused.

3.39 Level of Risk
This involves identifying, assessing, and managing risks to information assets. It is important to have a risk management framework in place that includes risk assessment, risk treatment, and risk monitoring.

3.13 Continual Improvement is critical as cyber security threats evolve constantly, so ongoing education and training is essential to keep employees up to date with the latest best practices. Organisations should conduct evaluations to assess the effectiveness of security measures and identify areas for improvement as well as encouraging employees to give suggestions and feedback.

References

Budzak, D., 2016. Information security–The people Issue. Business Information Review, 33(2), pp.85-89.

Disterer, G., 2013. ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4 (2).

International Organisation for Standardisation and International Electrotechnical Commission (2018) ISO/IEC Standard 27000:2018(E), Section 3, pages 1 -11