Unit 2 Blog Post

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.

Our collective understanding of “cyber security” has expanded over time to encompass practically all facets of everyday life. Where in the 1990s, the immediate concern remained with equipping our computers with firewalls and exercising caution when opening e-mail attachments, organisations currently see a rise in increasingly sophisticated cyber threats, however, the threat of the insider, whether malicious or accidental, has been present throughout. An insider may be an employee,

Assessing top-to-bottom, it is critical that **top management** prioritise cyber security and invest accordingly in a proactive, long-term strategy. Additionally, the **governing body** which in some instances may be the board of directors must also be prepared to deal with cyber security issues. For example, in 2013 after the theft of over 60 million records of Target customers, the company directors and officers were sued due to failing to insist on adequate controls (Rothrock et al, 2018). Shaikh & Siponen (2023) discovered that high costs of security breaches directly result in higher attention to cyber security by top management. Additionally, this also then causes an increased likelihood in investing in an information security **risk assessment**. Risk assessment covers areas of risk identification, risk analysis and risk evaluation.

The National Protective Security Authority (NPSA) has created a risk assessment model specifically designed to manage insider threats within an organisation (NPSA, 2023). A with all risk assessments, it involves the assessment of **likelihood** of the insider threat and the respective impact, on a scale from 1 to 5. A real-life example of an insider attack is stealing of company-sensitive information of a departing employee from Yahoo (Ostendorf, 2023). The company discovered information had been stolen weeks later. Had the company had heightened **monitoring** practices, this might have been discovered and dealt with earlier. McCue (2008, as cited in Colwill, 2009) highlight that 90% of company efforts are focused on monitoring external threats.

In summary, insider attacks continue to pose threat to businesses and are expected to become more sophisticated given the current working climates. It is imperative that sufficient cyber security practices are driven from top-down and that organisations manage risks effectively, by firstly conducting thorough risk assessments.

References:

Colwill, C. (2009) Human factors in information security: The insider threat–Who can you trust these days?. *Information security technical report*, *14*(4): 186-196.

McCue, A. (2008) Beware the insider security threat. *CIO Jury*.

NPSA (2023) Insider Risk Assessment. *National Protective Security Authority*. Available from: https://www.npsa.gov.uk/insider-risk-assessment [Accessed 3 November]

Ostendorf, C. (2023) 11 Real-Life Insider Threat Examples. *Code 42*. Available from: https://www.code42.com/blog/insider-threat-examples-in-real-life/ [Accessed 3 November]

Rothrock, R.A., Kaplan, J. & Van Der Oord, F. (2018) The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, *59*(2): 12-15.

Shaikh, F.A. & Siponen, M. (2023) Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*: 102974.