Question 2: Blog Post

Managing People to Overcome Insider Cybersecurity Threats

In cybersecurity, people are often considered as most significant risks due to their susceptibility to threats like phishing, unauthorized access, and accidental data leaks. However, organizations can turn this vulnerability into a strength with proactive strategies. Here are five crucial terms from the ISO/IEC 27000 standard that highlight how people can be managed to strengthen cybersecurity efforts (ISO/IEC, 2018):

Access Control: Access control ensures only authorized individuals can access specific assets. By implementing role-based access control (RBAC), employees gain access only to the information required for their role, minimizing the chance of unintentional data exposure. Consistently updating permissions and conducting access reviews is essential to maintaining this control.

Authentication: Authentication ensures that a claimed identity is valid and combats identity theft and unauthorized access. Multi-factor authentication (MFA) is a suitable method that adds a layer to password verification. Training employees to recognize and report attempts to bypass MFA reinforces security and reduces internal threats.

Audit: Regular audits are a systematic approach to assessing compliance with cybersecurity policies. Internal audits help identify non-compliance or suspicious activity within the organization, while external audits provide an independent evaluation. Encouraging employees to comply with these policies through awareness programs. This fosters a culture of accountability and transparency.

Risk Management: Risk management involves identifying, assessing, and mitigating organizational vulnerabilities. Regularly updating employees on emerging cyber threats and adapting risk management policies accordingly helps them stay proactive.

Vulnerability: A vulnerability is any weakness that threats can exploit. Organizations can address human-related vulnerabilities by educating employees on recognizing security and phishing tactics. Regular security training sessions and simulated phishing exercises are ways to protect against human vulnerabilities.

(ISO/IEC, 2018)

Organizations can effectively manage internal risks by integrating these strategies and by aligning employee practices with ISO standards. This can transform the “people factor” from a cybersecurity liability into a valuable defense asset (ISO/IEC, 2018).

References

ISO/IEC (2018) ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. Available at: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27000:ed-5:v1:en [Accessed: 9 November 2024].