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.

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

New Journal Entry

Managing People to Mitigate Insider Cybersecurity Threats

Monday, 4 November 2024, 10:55 AM

by Oi Lam Siu

Visible to participants on this course

Insider threats, often due to human error, are a significant risk in cybersecurity. Managing these threats requires a strategic approach based on the ISO/IEC 27000:2018 standard. I have chosen the following terms from ISO/IEC Standard 27000 Section 3 Terms and Definitions to explore how they can help overcome cybersecurity attacks from inside.

3.1 Access Control

ISO (2018) defines this as:

"means to ensure that access to assets is authorized and restricted based on business and security requirements (3.56)"

By granting employees only the access necessary for their job functions, organizations adhere to the principle of least privilege. This minimizes the risk of unauthorized access leading to data breaches or misuse of information by insiders.

3.9 Competence

ISO (2018) defines this as:

"ability to apply knowledge and skills to achieve intended results"

Ensuring that all personnel have the necessary skills to perform their roles securely is vital. Organizations should invest in continuous education, such as cybersecurity awareness training. Enhancing employee competence promotes thoughtful and secure behavior, reducing the likelihood of mistakes that could compromise security.

3.10 Confidentiality

ISO (2018) defines this as:

"property that information is not made available or disclosed to unauthorized individuals, entities, or processes (3.54)"

Employees must understand the importance of safeguarding sensitive information and the potential consequences of unauthorized disclosure. By fostering a culture that values confidentiality, organizations can reduce the risk of accidental leaks and ensure appropri handling of information. Methods to enforce confidentiality include data classification, encryption, and clear policies on data handling, aligning closely with access control (3.1) measures.

3.14 Control

ISO (2018) defines this as:

“measure that is modifying risk (3.61)”

Establishing robust controls, such as segregation of duties, regular audits, monitoring systems, and incident response procedures helps detect and prevent malicious or inadvertent activities within the organization. Regularly reviewing and adjusting these controls ensures their continued effectiveness against evolving threats.

3.23 Governance of Information Security

ISO (2018) defines this as:

“system by which an organization’s (3.50)information security (3.28) activities are directed and controlled”

Effective governance ensures that security strategies align with business objectives and are embedded throughout the organization. By establishing clear leadership, roles, and responsibilities, organizations create an environment where information security is everyone’s responsibility. This top-down approach reinforces the importance of security policies and procedures, leading to better adherence and accountability at all levels.

Conclusion

By focusing on these key areas defined in the ISO/IEC 27000:2018 standard, organizations can effectively mitigate risks posed by internal actors. Empowering employees with knowledge, restricting access appropriately, safeguarding sensitive information, implementing risk-modifying controls, and strategically directing security activities are all critical steps in strengthening an organization’s overall security posture.

References

ISO. (2018) 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:term:3.50 [Accessed 4 November 2024].

Bibliography

Kemp, CL. & Theoharidou, M. (2010). Insider Threat and Information Security Management. DOI: 10.1007/978-1-4419-7133-3_3

Tags: cybersecurity, insider threats, iso/iec standard 27000

Permalink Edit Delete Add your comment

Managing Insider Threats

Sunday, 3 November 2024, 11:19 PM

by Anda Ziemele

Visible to participants on this course

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.

Tags: iso/iec standard 27000, monitoring, top management, governing body, likelihood, risk assessment

Permalink Add your comment

ISO/IEC Standard 27000 terms

Wednesday, 30 October 2024, 9:58 PM

by Andrius Busilas

Visible to participants on this course

The human element is often considered the primary vulnerability in cybersecurity, accounting for a substantial portion of security breaches. However, organizations can effectively address and minimize these risks by implementing strategies based on ISO/IEC Standard 27000 Section 3, particularly through the establishment of well-defined protocols and the promotion of security awareness. The following five key concepts from ISO/IEC 27000 can be utilized to strengthen internal security measures.

1. **Access Control:** Limiting access to assets based on specific criteria is vital for reducing unauthorized entry (ISO/IEC 27000: 3.56). By restricting employee access to only the data essential for their job functions, companies can substantially decrease internal security risks. Periodic reviews of access rights, especially during role changes, ensure that staff members do not retain unnecessary access to confidential information.
2. **Audit:** Systematic and documented evaluations are crucial for assessing the efficacy of an organization's security measures (ISO/IEC 27000: 3.3). Conducting regular audits enables companies to identify policy violations and potential vulnerabilities before they can be

exploited. These audits can also cultivate a security-conscious environment, as employees are aware that their activities are being monitored, encouraging adherence to best practices.

3. **Authentication:** Robust authentication processes confirm the identity of individuals accessing systems, verifying that users are who they claim to be (ISO/IEC 27000: 3.5). The implementation of multi-factor authentication (MFA) requires users to provide additional verification, making it challenging for unauthorized individuals to gain access even if credentials are compromised.
4. **Threat Awareness:** Instructing employees about cyber threats, such as phishing attempts and malicious software, is crucial for establishing a proactive defence (ISO/IEC 27000: 3.74). Training programs can equip staff members with the skills to recognize and respond to suspicious activities, thereby reducing the likelihood of successful attacks due to human error.
5. **Confidentiality:** Maintaining confidentiality by ensuring that sensitive information is accessible only to authorized personnel minimizes the risk of data breaches (ISO/IEC 27000: 3.10). Organizations should clearly outline confidentiality policies and ensure that employees understand their responsibilities in safeguarding sensitive data, thus fostering a culture of accountability and responsibility.

By focusing on these principles, organizations can effectively manage the human factor in cybersecurity. Through ongoing education, strict access protocols, and regular audits, employees can be transformed from potential liabilities into proactive defenders against cyber threats.

References

ISO/IEC (2018) ISO/IEC Standard 27000 Section 3. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en [Accessed: 30 October 2024].

Tags: iso/iec standard 27000

Permalink Add your comment

Export to portfolio all currently visible posts and their comments.