Information security management

Information security management (**ISM**) defines and manages controls that an organization needs to implement to ensure that it is sensibly protecting the confidentiality, availability, and integrity of assets from threats and vulnerabilities. The core of ISM includes information risk management, a process that involves the assessment of the risks an organization must deal with in the management and protection of assets, as well as the dissemination of the risks to all appropriate stakeholders.[1] This requires proper asset identification and valuation steps, including evaluating the value of confidentiality, integrity, availability, and replacement of assets.[2] As part of information security management, an organization may implement an information security management system and other best practices found in the ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27035 standards on information security.[3][4]

Risk management and mitigation

Managing information security in essence means managing and mitigating the various threats and vulnerabilities to assets, while at the same time balancing the management effort expended on potential threats and vulnerabilities by gauging the probability of them actually occurring.[1][5][6] A meteorite crashing into a server room is certainly a threat, for example, but an information security officer will likely put little effort into preparing for such a threat.

After appropriate asset identification and valuation have occurred,[2] risk management and mitigation of risks to those assets involves the analysis of the following issues:[5][6][7]

- Threats: Unwanted events that could cause the deliberate or accidental loss, damage, or misuse of information assets
- Vulnerabilities: How susceptible information assets and associated controls are to exploitation by one or more threats
- Impact and likelihood: The magnitude of potential damage to information assets from threats and vulnerabilities and how serious of a risk they pose to the assets; cost–benefit analysis may also be part of the impact assessment or separate from it
- Mitigation: The proposed method(s) for minimizing the impact and likelihood of potential threats and vulnerabilities

Once a threat and/or vulnerability has been identified and assessed as having sufficient impact/likelihood on information assets, a mitigation plan can be enacted. The mitigation method is chosen largely depends on which of the seven information technology (IT) domains the threat and/or vulnerability resides in. The threat of user apathy toward security policies (the user domain) will require a much different mitigation plan than the one used to limit the threat of unauthorized probing and scanning of a network (the LAN-to-WAN domain).[7]

Information security management system

An information security management system (ISMS) represents the collation of all the interrelated/interacting information security elements of an organization so as to ensure policies, procedures, and objectives can be created, implemented, communicated, and evaluated to better guarantee an organization's overall information security. This system is typically influenced by organization's needs, objectives, security requirements, size, and processes.[8] An ISMS includes and lends to effective risk management and mitigation strategies. Additionally, an organization's adoption of an ISMS largely indicates that it is systematically identifying, assessing, and managing information security risks and "will be capable of successfully addressing information confidentiality, integrity, and availability requirements."[9] However, the human factors associated with ISMS development, implementation, and practice (the user domain[7]) must also be considered to best ensure the ISMS' ultimate success.[10]

Implementation and education strategy components

Implementing an effective information security management (including risk management and mitigation) requires a management strategy that takes note of the following:[11]

- Upper-level management must strongly support information security initiatives, allowing information security officers the opportunity "to obtain the resources necessary to have a fully functional and effective education program" and, by extension, information security management system.
- Information security strategy and training must be integrated into and communicated through departmental strategies to ensure all personnel is positively affected by the organization's information security plan.
- A privacy training and awareness "risk assessment" can help an organization identify critical gaps in stakeholder knowledge and attitude towards security.
- Proper evaluation methods for "measuring the overall effectiveness of the training and awareness program" ensure policies, procedures, and training materials remain relevant.
- Policies and procedures that are appropriately developed, implemented, communicated, and enforced "mitigate risk and ensure not only risk reduction, but also ongoing compliance with applicable laws, regulations, standards, and policies."
- Milestones and timelines for all aspects of information security management help ensure future success.

Without sufficient budgetary considerations for all the above—in addition to the money allotted to standard regulatory, IT, privacy, and security issues—an information security management plan/system can not fully succeed.

Relevant standards

Standards that are available to assist organizations with implementing the appropriate programs and controls to mitigate threats and vulnerabilities include the ISO/IEC 27000 family of standards, the ITIL framework, the COBIT framework, and O-ISM3 2.0. The ISO/IEC 27000 family represents some of the most well-known standards governing information security management and the ISMS and are based on global expert opinion. They lay out the requirements for best "establishing, implementing, deploying, monitoring, reviewing, maintaining, updating, and improving information security management systems."[3][4] ITIL acts as a collection of concepts, policies, and best practices for the effective management of information technology infrastructure, service, and security, differing from ISO/IEC 27001 in only a few ways.[12][13]

COBIT, developed by ISACA, is a framework for helping information security personnel develop and implement strategies for information management and governance while minimizing negative impacts and controlling information security and risk management,[4][12][14] and O-ISM3 (https://www.ism3.com) 2.0 is The Open Group's technology-neutral information security model for enterprise.[15]

See also

- Certified Information Systems Security Professional
- Chief information security officer
- Security information management

References

1. *Campbell, T. (2016). "Chapter 1: Evolution of a Profession". Practical Information Security Management: A Complete Guide to Planning and Implementation (https://books.google.com/books?id=sbWiDQAAQBAJ&pg=PA1) . APress. pp. 1–14. ISBN 9781484216859.*
2. *Tipton, H.F.; Krause, M. (2003). Information Security Management Handbook (5th ed.). CRC Press. pp. 810–11. ISBN 9780203325438.*
3. *Humphreys, E. (2016). "Chapter 2: ISO/IEC 27001 ISMS Family". Implementing the ISO/IEC 27001:2013 ISMS Standard (https://books.google.com/books?id=Yy6pCwAAQBAJ&pg=PA11) . Artech House. pp. 11–26. ISBN 9781608079315.*
4. *Campbell, T. (2016). "Chapter 6: Standards, Frameworks, Guidelines, and Legislation". Practical Information Security Management: A Complete Guide to Planning and Implementation (https://books.google.com/books?id=sbWiDQAAQBAJ) . APress. pp. 71–94. ISBN 9781484216859.*
5. *Watts, S. (21 June 2017). "IT Security Vulnerability vs Threat vs Risk: What's the Difference?" (http://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/) . BMC Blogs. BMC Software, Inc. Retrieved 16 June 2018.*
6. *Campbell, T. (2016). "Chapter 4: Organizational Security". Practical Information Security Management: A Complete Guide to Planning and Implementation (https://books.google.com/books?id=sbWiDQAAQBAJ) . APress. pp. 43–61. ISBN 9781484216859.*
7. *Kim, D.; Solomon, M.G. (2016). "Chapter 1: Information Systems Security". Fundamentals of Information Systems Security (https://books.google.com/books?id=kvBCDQAAQBAJ&pg=PA2) . Jones & Bartlett Learning. pp. 2–46. ISBN 9781284128239.*

8. *Terroza, A.K.S. (12 May 2015). "Information Security Management System (ISMS) Overview" (https://web.archive.org/web/20160807021631/https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20(ISMS)%20Overview.pdf) (PDF). The Institute of Internal Auditors. Archived from the original (https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20(ISMS)%20Overview.pdf) (PDF) on 7 August 2016. Retrieved 16 June 2018.*
9. *"Need: The Need for ISMS" (https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/need) . Threat and Risk Management. European Union Agency for Network and Information Security. Retrieved 16 June 2018.*
10. *Alavi, R.; Islam, S.; Mouratidis, H. (2014). "A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations". Proceedings of the Second International Conference on Human Aspects of Information Security, Privacy, and Trust. **8533**: 297–305. doi:10.1007/978-3-319-07620-1_26 (https://doi.org/10.1007%2F978-3-319-07620-1_26) .*
11. *Tipton, H.F.; Krause, M. (2010). Information Security Management Handbook (https://books.google.com/books?id=S5RyW9jqxnEC&pg=PA100) . Vol. 3 (6th ed.). CRC Press. pp. 100–02. ISBN 9781420090956.*
12. *Kim, D.; Solomon, M.G. (2016). Fundamentals of Information Systems Security (https://books.google.com/books?id=kvBCDQAAQBAJ) . Jones & Bartlett Learning. p. 225. ISBN 9781284128239.*
13. *Leal, R. (7 March 2016). "ISO 27001 vs. ITIL: Similarities and differences" (https://advisera.com/27001academy/blog/2016/03/07/iso-27001-vs-itil-similarities-and-differences/) . The ISO 27001 & ISO 22301 Blog. Advisera Expert Solutions Ltd. Retrieved 16 June 2018.*
14. *White, S.K. (22 December 2017). "What is COBIT? A framework for alignment and governance" (https://www.cio.com/article/3243684/methodology-frameworks/what-is-cobit-a-framework-for-alignment-and-governance.html) . CIO. IDG Communications, Inc. Retrieved 16 June 2018.*
15. *"Open Information Security Management Maturity Model (O-ISM3), Version 2.0" (https://publications.opengroup.org/c17b) . The Open Group. 21 September 2017. Retrieved 16 June 2018.*

External links

- ISACA (http://www.isaca.org/)
- The Open Group (http://www.opengroup.org/)