Unit 7: Risks and Standards

Objectives:

- Review what is meant by risk within the context of Information Security Management.
- Discuss how to gather, analyze and mitigate risks from a security audit/ review/ planning session.
- Review business continuity and disaster recovery standards.
- Explore industry specific security standards and directives.

Outcomes:

- Describe the purpose of risk assessment.
- Explain how to mitigate risks.
- Describe the difference between business continuity and disaster recovery.
- List common security standards and select the appropriate one(s) for a given situation.

Reflection:

The word “information security risk” relates to the impact that strikes on IT infrastructure can create. IT risk spans many possible occurrences involving data theft, legal civil penalties, economic burdens, reputation loss, etc.Information security risk management is an important integration of management plans, processes, and techniques to the task of setting the framework, discovering, assessing, evaluating, managing, monitoring, and conveying cybersecurity risks. Analyze dangers, then eliminate or reduce the likelihood of that risk by implementing countermeasures, if needed, as part of the risk assessment process. As a result, your workplace is now healthier and safer (Government of Canada, C.C. for O.H. and S. 2020b).

Information Security Monitoring can be effectively achieved with an appropriate information security risk management approach. Appropriate security mechanisms in applications are outlined during a risk management. It also aims to avoid security weaknesses in application security (Yaacoub et al., 2020).

A risk analysis provides a comprehensive view of the application portfolio—from the attacker's point of view—for a company (Bhatt, D. 2018).

For mitigation of risk, we follow following steps:

- Set network access rules, install proxy servers and anti-virus programs, and evaluate the risk.
- Establish a patch management strategy, then follow it.

- Examine the network traffic in real-time,
- Create a plan of action in the event of an emergency.

Finally, disaster recovery deals with how data and infrastructure are recovered after an incident that has damaged them. If a company's technology fails or goes down, its capacity to continue operating is called business continuity. Also known as an ERP, a BCP specifies how a company will keep going in the event of a crisis (able, N. 2020).

Security standard refers to "an established terminology that comprises a technical requirements or other specified parameters and is intended to be utilized regularly." Securing IT platforms, networks, and infrastructure networks is the ultimate purpose of security protocols. Standardization among product creators and a dependable standard for acquiring security products are provided by the well-written cybersecurity standards.

- ISO
- ISO/IEC 27000 series
- HIPPA
- FISMA

References

able, N. (2020). *Key Differences Between a Disaster Recovery Plan vs. a Business Continuity Plan*. [online] N-able. Available at: https://www.n-able.com/blog/disaster-recovery-plan-vs-business-continuity-plan#:~:text=To%20summarize%2C%20disaster%20recovery%20refers [Accessed 22 May 2022]

Bhatt, D. (2018). Modern Day Penetration Testing Distribution Open Source Platform - Kali Linux -Study Paper. *INTERNATIONAL JOURNAL of SCIENTIFIC & TECHNOLOGY RESEARCH*,*7. https://www.ijstr.org/final-print/apr2018/Modern-Day-Penetration-Testing-Distribution-Open-Source-Platform-Kali-Linux-Study-Paper.pdf* [Accessed 22 May 2022]

Franklin, S., & Bhingardeve, N. (2018). A Comparison Study of Open Source Penetration Testing Tools. *International Journal of Trend in Scientific Research and Development*, *Volume-2*(Issue-4). https://www.ijtsrd.com/computer-science/computer-security/15662/a-comparison-study-of-open-source-penetration-testing-tools/nilesh-bhingardeve [Accessed 22 May 2022]

Government of Canada, C.C. for O.H. and S. (2020b). *Risk Assessment: OSH Answers*. [online]www.ccohs.ca.

Yaacoub, J.-P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A. and Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, 77, p.103201. doi:10.1016/j.micpro.2020.103201.