Secure Software Development (Computer Science) November 2021

The Human Factor

Thursday, 18 November 2021, 7:51 PM

by Michael Botha

Visible to participants on this course

- Edited by Michael Botha, Thursday, 18 November 2021, 7:57 PM

Keywords: Continual improvement; Governance of Information Security; Policy; Process; Information Security Management System.

The Big Picture

The question of whether people are the biggest risk to Cyber Security seems rhetorical, as ultimately all inadequacies found through breeches and failures fall squarely on the omission or action of individuals and teams within a specific domain (Kapersky, N.D). Whether it be in requirements analysis, design, implementation, use, or maintenance of a particular IT system all circumstances and events need to be catered for once discovered during risk and vulnerability assessments (Nieles et al., 2017). However, if one were to make the question more specific, the rhetorical nature of it begins to fade. Consider if the question were to be posed as such: “are the actions and omissions of those lay to security principles and IT, who are merely using the systems as tools, one of the biggest risks to cyber security?”. The answer could then be “maybe”. Should not those who specialise in the provisioning of such services and the accompanying governance structures provide the necessary security? The writer would answer yes, however a culture of security will ultimately provide the best results (ACM, 2021). Even in society we observe that although the law system and its enforcement is in place, the society as a whole, committed to particular values, will ultimately facilitate victory over crime.

There are various principles that will aid in reaching the goal of providing the best security features possible to an organisation. However, the human factor needs to be addressed to better prepare designers, administrators, and lay users to practice good security hygiene with the end goal of making certain techniques habitual and producing continual improvement (Kapersky, N.D).

Governance of Information Security

The set of regulations used to try orchestrate the actions of employees and 3rd-parties is critical to the overall success of an organisation in maintaining its cyber security mandates (ISACA, 2020). Policies, which are values and intentions set out by the upper management of an organisation to aid decision making, need to be geared towards an environment facilitating secure principles (ISO, N.D). Procedures are the processes to follow to achieve certain goals aligned with policies, and need to be clear and well circulated in the organisation through awareness campaigns and the accompanying training (ACM, 2021).

International standards and best practices are essential to ensuring specialised knowledge is absorbed and used (BCS, 2011). For instance, the ISO27000:2018 is an international standard that an organisation will aim to meet, and provides an Information Security Management System as a framework to facilitate the requirements of cyber security, rather than building such from scratch within your organisation (BCS, 2011).

Conclusion

Although there are many technical controls that can be put in place to limit security vulnerabilities, the management of individuals and collectives through good IT governance, and the creation of a security

culture is paramount.

References:

ACM. (2021) Implementing Insider Defenses. Available from: https://cacm.acm.org/magazines/2021/5/252178-implementing-insider-defenses/fulltext [Accessed 18 November 2021].

BCS. (2011) Governance is Key. Available from: https://www.bcs.org/articles-opinion-and-research/governance-is-key/ [Accessed 18 November 2021]

Kapersky. (N.D) The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. Available from: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ [Accessed 18 November 2021].

ISACA. (2020) The Value of IT Governance. Available from : https://www.isaca.org/resources/news-and-trends/industry-news/2020/the-value-of-it-governance [Accessed 18 November 2021]

ISO. (N.D) ISO/IEC 27000:2018(en): 3 Terms and Definitions. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en [Accessed 16 November 2021].

Nieles, M., Dempsey, K., Pillitteri, V. (2017) An Introduction to Information Security. Revision 1. United States of America: National Institute of Standards and Technology. Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf [Accessed 17 November 2021].

Permalink Edit Delete Add your comment

Comments

Friday, 19 November 2021, 9:58 AM

by Cathryn Peoples

Thanks for posting this, Michael.

MIght it be argued that even the identification of the risks could be inflenced by the interests of the people who are identifying them. Might they keep a job if there continues to be issues? Might they be paid more highly if problems keep occurring and only some efforts are made to identify the problems? This may be a reason why some say that it can be more effective to outsource the provision of security solutions (B. Schneier, "The case for outsourcing security," in Computer, vol. 35, no. 4, pp. supl20-supl21, April 2002, doi: 10.1109/MC.2002.1012426. - an old source but are there any useful takeaways here? A more recent source - https://www.sciencedirect.com/science/article/pii/S037872061830702X - do the opinions differ?), but to what degree can outsourced solutions also be trusted? In line with Microsoft, it is best to assume Zero Trust? (https://www.microsoft.com/en-us/insidetrack/transitioning-to-modern-access-architecture-with-zero-trust#:~:text=Microsoft%20has%20adopted%20a%20modern,of%20identities%2C%20devices%20an

Excellent referencing to support your arugment, Michael. Please double-check your approach to including reference detail: In relation to reference 1, I would cite this as:

Grosse, E., Schneider, F. B., & Millett, L. L. (2021) Implementing Insider Defenses, Communications of the ACM, May 2021, Vol. 64 No. 5, Pages 60-65.

The Harvard referencing guide can be accessed at: https://www.my-course.co.uk/pluginfile.php/259810/mod_resource/content/8/Harvard%20Referencing%20Guide.pdf

Best wishes,

Cathryn

◀ Seminar 1 blog post