The Importance of Security Awareness Training for Security Development Lifecycle (SDL)

A Report by

Mark Kardash

SDEV360: Secure Software Engineering

Professor David Gabello

31 October 2023

University of Maryland Global Campus

Software development is a process comprising many steps, each with its own specific details to be considered. To ensure that such a laborious process goes smoothly, companies must implement proper security awareness training for development teams. This essay provides five

reasons for the importance of security training in software development.

In today’s highly digitalized world, computer systems are present in almost every part of life. Because of this, criminals will take every opportunity to attack or use them, either to extract information, execute financial schemes, or perform other illegal operations. Proper security awareness training will benefit developers by integrating security into the workplace culture (Osborne, 2018). This means that, when trained in it, employees will pay more attention to potential threats or bugs. For software development, and the SDL, this is especially important, as any issues must be resolved before the final product release. To implement a safety-focused workplace, it is recommended to propagate software security across the company through means like posters and emails (Osborne, 2018).

Continuing the topic of safeguarding information, a second reason for the importance of security training is the reduction of data breaches (Rees, 2022). Data breaches can occur in several ways, such as when an employee clicks on a phishing email (an email appearing to be from a legitimate company, but being, in fact, a scam). Supporting the earlier point about establishing a security culture, it has been proven that employees receiving security training are less likely to fall for phishing scams (Rees, 2022). A data breach during the software development process can be catastrophic, altogether jeopardizing the release of a new product. This employee awareness can be spread not only to data breaches, but also to cyber threats in general.

Increase in the ability to detect and prevent cyberthreats will automatically lead to greater customer trust and satisfaction, the third reason for training importance. When customers entrust a company with their sensitive data (such as financial, medical, or personal information) they want guarantees that it will be kept safe. While this may not apply as much to the security development lifecycle, ensuring that a new website or application keeps data safe will reassure those investing in it that they have made the right choice. Demonstrating high concern and care about client data will not only improve relationships with current customers, but also grant the company good reputation to attract new ones (United Security Incorporated, 2022).

Besides making a company more respectable, security awareness training can also improve its overall organization. This is because, according to indeed.com, “Businesses and organizations that provide security training can help IT departments outline procedures and standards that establish compliance policies and criteria for staff to follow.” (para.4, n.d.). In the software development process, clear steps and requirements must exist for each stage, whether design or implementation. Without these steps, developers would essentially be working blindfolded, putting product quality at risk. Therefore, having employees trained in security will help create clear paths for the company to follow, improving product quality, and making its future less uncertain.

Finally, one last reason for the importance of security awareness training is its contribution to regulation compliance. Employers and employees must adhere to many policies, rules, regulations, and government acts to ensure that they are doing their jobs properly. Examples of such regulations include the Health Insurance Portability and Accountability Act (HIPAA), as well as Sarbanes-Oxley (Osborne, 2018). For software companies, releasing a product that does not adhere to regulations could result in serious backlash, and even bankruptcy. These effects could be even more severe if the noncompliance causes violation of customer privacy (ex. The development team did not secure the website enough to protect client information). This would be a violation of the SDL itself. Through adequate security awareness training, employees can learn what is expected of them or prohibited, ensuring that they are working ethically, and within legal limits (Osborne, 2018).

There are many reasons that security awareness training is important, both in SDLC, and in many other fields. For this reason, it should be deemed as a required component of software development (or, rather, an additional component), with each team using the appropriate aspects learned from it depending on the individual project.

References

*6 reasons why security awareness training is important*. (2022). United Security Incorporated. <https://inbound.usisecurity.com/blog/6-reasons-why-security-awareness-training-is-important>

Osborne, B. (2018, August 17). *Ten benefits of security awareness training*. Infosec Resources - IT Security Training & Resources by Infosec. <https://resources.infosecinstitute.com/topics/security-awareness/10-benefits-of-security-awareness-training/>

Rees, M. (2022, September 22). *Why is security awareness training (SAT) important?* Expert Insights. <https://expertinsights.com/insights/what-is-security-awareness-training-and-why-is-it-important/>

*What is Cybersecurity Training? Definition and Importance*. (n.d.). Indeed.com. <https://www.indeed.com/career-advice/finding-a-job/cyber-security-training>