**Software Development Lifecycle (SDL) training**

**Student**: Patrick Walsh

**Date**: 3/24/2021

**School**: University of Maryland Global Campus

**Course**: SDEV 360 7380

**Professor**: Dr. Alla Webb

*Provide five reasons for the importance of security training prior to executing the Software Development Lifecycle (SDL) process.*

**1. Data breaches are extremely costly to organizations**

Organizations must pay millions of dollars per year due to data breaches which result in lost revenue, loss of public trust, and compromised customer personally identifiable information (PII). One of the major reasons why these data breaches occur is lack of security training from software developers (Microsoft, 2010). A 2006 study estimated that over 60% of data breaches were caused by human error, while 84% of organizations that provided security training credited that training with fewer data breaches (Microsoft, 2010).

**2. Security training can save organizations money by being proactive in their approach**

By waiting to implement security practices until during or postproduction, companies spend time and money reacting to software weaknesses once they are discovered, rather than being proactive and building security into the SDL process in the first place. This reactive approach to security is the equivalent of a person waiting until he or she gets sick to start eating healthy and exercising rather than practicing those habits to stay healthy. In its 2002 report, the National Institute of Standards and Technology (NIST) estimated that organizations pay 30 times more to fix a software bug after product release compared to fixing the same bug during requirements analysis or architectural design (p. 5-4).

**3. Cyber criminals have become more sophisticated**

With sophisticated attacks like zero-day exploits, mobile security attacks, and even setting up fake charity websites in the wake of natural disasters becoming more common, the need for stronger security measures has never been higher (Armstrong, 2010). In her 2010 editorial, Armstrong stressed the need for organizations to take software security more seriously, and that training needed to go beyond annual refresher courses and email reminders. Armstrong viewed (2010) comprehensive security training as a vital tool in the struggle against increasingly sophisticated cyber-attacks, and a tool which most organizations were not utilizing.

**4. Promotes software security as part of the culture of the organization**

Software security is not only the responsibility of developers. Awareness of security practices must be organization-wide and promoted from the top down. Organizational leaders need to make software security training part of the organization culture. In his commentary on NIST guidelines for avoiding data breaches, Danhieux emphasized (2019) the need for leaders to promote security practices at all level of the organization. He noted that “even if an organization is putting time and resources into training developers and other key staff members, and placing emphasis on their roles in preventing vul­nerabilities and reducing security risk, the effort can often go to waste if the security culture of an organization remains funda­mentally broken” (p.17).

**5. Training is necessary prior to putting a new skill into practice**

If organizations wait until the SDL process begins to start incorporating security, it will be difficult for developers to internalize the concepts learned and effectively use them in practice. This is another reason why it is so important to conduct security training prior to executing the SDL process. Microsoft also differentiated (2010) between education and training, stating that education was the process of learning how to do something, while training was applying that knowledge in practice.

**References**

Armstrong, I. (2010). Educating the workforce and beyond. *SC Magazine: For IT Security Professionals (15476693)*, *21*(2), 6.

Danhieux, P. (2019). The New NIST Guidelines for Avoiding a Data Breach: Why customized training is essential to create secure software. *Database Trends & Applications*, *33*(5), 16–17.

Microsoft. (2010, June 2). *Essential Software Security Training for the Microsoft SDL*. Microsoft Security Development Lifecycle. http://www.microsoft.com/sdl

National Institute of Standards and Technology (NIST). (2002, May). The Economic Impacts of Inadequate Infrastructure for Software Testing. https://www.nist.gov/system/files/documents/director/planning/report02-3.pdf