**Project: SDLC Training**

Benjamin M. Brandhorst

University of Maryland Global Campus

SDEV 360 6380 Secure Software Engineering

Professor Kevin Woodson

January 25th, 2020

Software security training is of the utmost importance for all members of a software development team. Because of the ever changing nature of the tech industry it is a constant battle to stay ahead of emerging vulnerabilities and exploitations. This paper will show five reasons for the importance of security training prior to the execution of the SDLC process.

1. **Minimize software bugs:** From 2000 to 2008 the number of software vulnerabilities cataloged by the United States Computer Emergency Response Team (CERT) grew almost eight-fold from 1,100 in 200 to around 8,000 in 2008 (Microsoft, 2010, p. 2). It stands to reason that the number of vulnerabilities has only continued to grow in the years since. Ensuring all team members are provided with an up to date security training before the software development life cycle begins ensures all players have the tools needed to save money, time and resources.
2. **Prevent breaches of personally identifiable information:** Breaches exposing PII happen at a rate faster than at any other time in history. From 2005 to 2008 the costs associated with compromised customer records grew from $138 per record to $208 (Microsoft, 2010, p. 3). Security training provides the tools and skill set necessary to mitigate against exploitations that reveal PII to malicious actors.
3. **Provide specialized knowledge:** Where education is generally broad and helps refine critical thinking skills, Microsoft tells us training should be focused on teaching skills to accomplish a task (Microsoft, 2010, p. 4). Because of this, it is also important to provide role specific security training that imparts specialized knowledge according to each person’s position on the team and their capabilities. Doing this before the SDLC process ensures buy in from all team members and also ensures everyone is equipped to contribute to security.
4. **IT security is not the same as software security:** A common misconception is that software security and security software are interchangeable terms. Software security is what enables software to continue operate as normal when under an attack (Microsoft, 2010, p. 5). Security software on the other hand, is software that assists IT security practitioners in performing their duties. It is important to have some overlap in knowledge between the two. However, software security requires role specific training to be effective.
5. **Manage risk and save money:** It is almost impossible to measure how much money was saved through the prevention of events that may or may not have happened without mitigation. However, as shown before, the stakes are higher than ever and vulnerability exploitation or PII breaches can be devastating to a business. Knowing how much is riding on preventing those things from happening, the best way to manage those risks and save the costs associated with successful attacks is through role specific training prior to the SDLC process.

References

Microsoft. (2010). *Essential software security training for the Microsoft SDL*. Retrieved from https://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=9950