Chapter 97
Measuring Developers' Software Security Skills, Usage, and Training Needs

Tosin Daniel Oyetoyan
Western Norway University of Applied Sciences, Norway

Martin Gilje Gilje Jaatun
https://orcid.org/0000-0001-7127-6694
SINTEF Digital, Norway

Daniela Soares Cruzes
SINTEF Digital, Norway

ABSTRACT

Software security does not emerge fully formed by divine intervention in deserving software development organizations; it requires that developers have the required theoretical background and practical skills to enable them to write secure software, and that the software security activities are actually performed, not just documented procedures that sit gathering dust on a shelf. In this chapter, the authors present a survey instrument that can be used to investigate software security usage, competence, and training needs in agile organizations. They present results of using this instrument in two organizations. They find that regardless of cost or benefit, skill drives the kind of activities that are performed, and secure design may be the most important training need.

INTRODUCTION

Traditional security engineering processes are often associated with additional development efforts and are likely to be unpopular among agile development teams (ben Othmane et al., 2014; Beznosov & Kruchten, 2004). A software security approach tailored to the agile mind-set thus seems necessary.

DOI: 10.4018/978-1-6684-3702-5.ch097

Some approaches have been proposed to integrate security activities into agile development, e.g., the Microsoft SDL for Agile (Microsoft, 2012). However, these approaches have been criticised for looking too similar to the traditional versions in terms of workload (e.g., performing a long list of security verification and validation tasks) (ben Othmane et al., 2014). As a result, "agile" organizations have approached software security in a way that better fits their process and practices. Thus, regardless of whether agile is perceived to be incompatible with any particular secure software development lifecycle, the major discussion we should have is how to improve security within the agile context (Bartsch, 2011). Previous studies (Ayalew et al., 2013; Baca & Carlsson, 2011) have investigated which security activities are practiced in different organizations, and which are compatible with agile practices from cost and benefit perspectives. Using a survey of software security activities among software practitioners, they identify and recommend certain security activities that are compatible with agile practices.

While these activities could be argued to be beneficial and cost effective to integrate, there are still gaps between what is "adequate" security (Allen, 2005), and what is currently practiced within several organizations. According to Allen (2005), adequate security is defined as "*The condition where the protection and sustainability strategies for an organization's critical assets and business processes are commensurate with the organization's tolerance for risk*".

BACKGROUND

Software security has existed as a distinct field of research for over a decade, and reached prominence with the publication of the book "Software Security" (Gary McGraw, 2006).

The studies by Ayalew et al. (2013), Baca and Carlsson (2011), and Morrison et al. (2017) have investigated security activities from cost and benefit dimensions to advise on frameworks and selection of security activities that can be integrated to agile software development. Jaatun et al. (2015) have used BSIMM to measure security practices but with focus on security maturity at an organisational level. Other studies not directly related to our work have looked into market skills relevant for cybersecurity jobs. For example, Potter and Vickers (2015) used a questionnaire to answer and address the question of what skills does a security professional need in the current information technology environment, and they explored this question by looking at the current state of the Australian industry. Fontenele (Fontenele, 2017) developed a conceptual model and an ontological methodology to aid a robust discovery of the fittest expertise driven by the specific needs of cyber security projects, as well as benchmarking expertise shortages.

Our work differs from these studies as we have measured developers' skills and training needs along software security activities.

Secure Software Development Lifecycles

A number of Secure Software Development Lifecycles (SSDLs) have been proposed, in the following we briefly introduce to most important ones as they relate to this paper.