2018 IEEE International Symposium on Software Reliability Engineering Workshops

The DevSecOps and Agency Theory

Jong Seok Lee
Department of Business Information & Technology
Fogelman College of Business and Economics
University of Memphis
Memphis, TN, United States of America
jslee4@memphis.edu

***Abstract*—An effective implementation of DevSecOps requires an increased focus on collaborations between different work groups or disciplines within IT (development, security, and operations/implementation). Nonetheless, different groups are still too often reluctant to trust each other, or inter-group conflicts tend to commonly occur. Against this backdrop, in this research I develop a framework based on Agency Theory that sheds light on the role of goal incongruency and information asymmetry in the DevSecOps context.**

Keywords—DevSecOps, agency theory, goal incongruency, information asymmetry, the principal-agent problem

I. Introduction

Software development practices continue to evolve due to rapid technological changes and new user demands. In recent years, agile development and DevOps have emerged as potential solutions that allow development organizations to respond quickly to technological changes and new user demands. Agile development focuses on sensing and responding to user requirements and involves self-organization and continuous adaptation [1]. Prior research has shown that agile development has potential to improve software development team performance [1]. DevOps is a newer approach that aims to combine software development and software operations [2]. The main characteristic of DevOps is to automate many aspects of software testing and integration, thus making it easy for organizations to develop and deploy new software releases frequently and seamlessly. While both Agile and DevOps have become valuable practices to the software development community, security is somewhat neglected in each approach. DevSecOps focuses introducing security earlier in the development life cycle and by doing so it aims to reduce security vulnerabilities. DevSecOps has potential to reduce the time between committing a change to a system and the change being placed into normal production, while ensuring high quality and security. An effective implementation of DevSecOps requires an increased focus on collaborations between different work groups or disciplines within IT (development, security, and operations/implementation). Nonetheless, different groups are still too often reluctant to trust each other, or inter-group conflicts tend to commonly occur. Against this backdrop, in this research I develop a framework based on Agency Theory that sheds light on the role of goal incongruency and information asymmetry in the DevSecOps context.

II. Agency theory

Agency theory is an influential theory that has been used by scholars to investigate a variety of management and business issues [3]. Agency theory is also known as the principal–agent problem and describes situations where the agent makes decisions or takes actions on behalf of the principal. The principal–agent problem is known to involve a decision dilemma as the agent is motived to take actions that are aligned with his or her best interest, and such actions may be in conflict with what is best for the principal [4]. Generally, there are two known conditions under which agents behave in a way that is contrary to best interests of principles. First, goal incongruency between the agent and the principal provides incentives for the agent to acts to pursue his or her utilities as opposed to what is best for the principle. This behavior is most likely to occur when information asymmetry between the agent and the principal exists, meaning that the agent holds private information that is not accessible by the principal [5].

III. A DevSecOps & Agency Theory Framework

The potential principal-agent problem exists in software development settings, as the development team (agent) and the customer (principal) may have different goals or interest. Further, the development team often has the private information that is not accessible by the customer, thus making it an ideal setting where the principal–agent problem is likely to occur. In DevSecOps, there are three groups that must collaborate in delivering software solutions: development, security, and operations. Each group has its own goal and may have private information that is not accessible by other groups. When the principal–agent problem occurs, each group makes decisions or choices that are beneficial for the group, but not necessarily for the customer or the entire DevSecOps team. Such behavior has potential to hurt the team performance and foster distrust within the DevSecOps team.

978-1-5386-9443-5/18/$31.00 ©2018 IEEE
DOI 10.1109/ISSREW.2018.00013

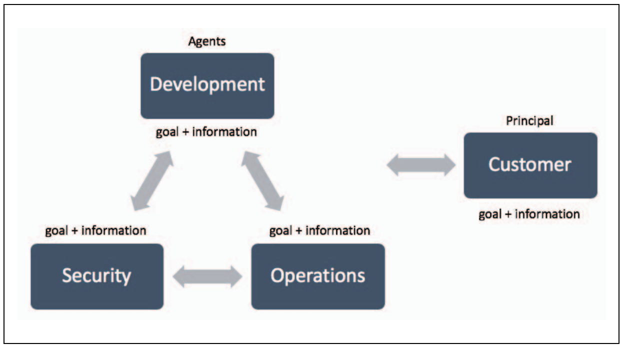

Fig. 1. A DevSecOps & Agency Theory Framework.

Proposition 1: Goal abstraction

The DevSecOps team must aim to develop and attain a goal that is common and applicable to all parties involved, including development, security, operations, and customer. While each group has its own goal, the development of a common goal can be achieved through abstraction and categorization.

Proposition 2: Information Transparency

The DevSecOps team must aim to develop a digital repository where all relevant information to all aspects of the DevSecOps team are available to all parties involved.

References

[1] Lee, G., and Xia, W. Toward agile: An integrated analysis of quantitative and qualitative field data on software development agility. MIS Quarterly, 34, 1 (2010), 87-114.

[2] Roche, J. Adopting devops practices in quality assurance. Communications of the ACM, 56, 11 (2013), 38-43.

[3] Eisenhardt, K.M. Agency theory: An assessment and review. Academy of management review, 14, 1 (1989), 57-74.

[4] Jensen, M.C., and Meckling, W.H. Theory of the firm; managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3, 4 (1976), 305-360.

[5] Baiman, S. Agency research in managerial accounting: A second look. Accounting, Organizations and Society, 15, 4 (1990), 341-371.