Chapter 15
Conceptualizing the Domain and an Empirical Analysis of Operations Security Management

Winfred Yaokumah
Pentecost University College, Ghana

ABSTRACT

Operations security management integrates the activities of all the information systems security controls. It ensures that the entire computing environment is adequately secured. This chapter conducts an in-depth review of scholarly and practitioner works to conceptualize the domain of operations security management. Drawing upon the existing information systems security literature, the chapter classifies operations security management into 10 domains. Following, the chapter performs an empirical analysis to investigate the state-of-practice of operations security management in organizations. The findings show that the maturity level of operations security management is at the Level 3 (well-defined). The maturity levels range from Level 0 (not performed) to Level 5 (continuously improving). The results indicate that operations security processes are documented, approved, and implemented organization-wide. Backup and malware management are the most applied operations security controls, while logging, auditing, monitoring, and reviewing are the least implemented controls.

INTRODUCTION

Operations security management is the day-to-day activities involved in ensuring that people, applications, computer systems, computer networks, processes, and the entire computing environment are properly and adequately secured (Gregory, 2010). It pertains to the activities that take place while keeping computing environment up and running in a secured and protected manner (Harris, 2013; Shaqrah, 2010). Operations security management integrates the activities of all the information systems security controls (Henrya, 2011). To attain a high level of operations security organizations need to put in place

DOI: 10.4018/978-1-5225-6367-9.ch015

appropriate measures that will ensure that the routine security activities are carried out in a controlled manner (Prabhu, 2013). These activities may include documenting operating procedures; ensuring that changes to information assets are carried out efficiently; protecting information resources from malware and other threats; performing backups and ensuring timely availability of information; and carrying out logging, auditing, monitoring, and reviewing user activities (Prabhu, 2013). In order to keep up with these tasks, operations security personnel (network administrators, system administrators, and database administrators) need in-depth understanding of the domain of operations security. This knowledge will help them to fully implement and adequately handle the day-to-day operations security challenges.

However, there seems to be varying views as to what constitutes the domain of operations security. According to Gregory (2010), operations security includes security monitoring, vulnerability management, change management, configuration management, and information handling procedures. Harris (2013) considers operations security as the activities involved in ensuring that physical and environmental security (such as temperature and humidity control, media reuse and disposal, and destruction of media containing sensitive information) concerns are addressed. Moreover, the International Information System Security Certification Consortium's (ISC^2) Body of Knowledge (CBK, 2017) extends operations security to cover operational support of highly available systems, fault tolerance, and mitigation of security-related cyber attacks. Also, ISO/IEC 27002 (2013) defines the scope of operations security as consisting of security procedures, roles and responsibilities; management of security in the third-party products and services; securing systems and data from malware activities; backup of data to safeguard against data lost and system corruption; and logging, monitoring, auditing, and reviewing of system activities.

Considering these different perspectives, there is the need to identify, classify, and clarify the domain of operations security for better implementation and management of operations security controls in organizations. Therefore, the objectives of this chapter are: (a) to conduct a review of scholarly and practitioner works to conceptualize the domain of operations security management, and (b) to perform an empirical analysis to ascertain the level of operations security management in organizations based on ISO/IEC 27002:2013 framework. Information security programs will be successful when measured with IT security maturity models (McFadzean, Ezingeard, & Birchall, 2011). These models are based on international standards and best practices. Information security maturity models consist of structured set of elements that describe levels of security improvement (maturity). They are often used as tools for measuring the performance of security programs in organizations (Stevanović, 2011).

Therefore, this chapter's empirical analysis of operations security management is based on the information security control objectives defined by the International Organization for Standardization/ International Electrotechnical Commission - security techniques - code of practice for information security management (ISO/IEC 27002:2013 framework). This framework is a widely accepted information technology security techniques and contains 14 security control clauses with a total of 35 main security categories and 114 controls (ISO/IEC 27002:2013, 2013). In particular, the objectives of this chapter will be achieved by answering the following three research questions:

1. What is the domain of operations security management?
2. What is the maturity level of operations security management in Ghanaian organizations?
3. Are there any significant differences among the organizations with regard to the levels of operations security management?