Chapter 14
The Role of Human Resource Management in Enhancing Organizational Information Systems Security

Peace Kumah
Ghana Education Service, Ghana

ABSTRACT

Emerging human resource management (HRM) practices are focusing on background checks, training and development, employer-employee relations, responsibility and accountability, and monitoring of information systems security resources. Information systems security ensures that appropriate resources and adequate skills exist in the organization to effectively manage information security projects. This chapter examined the role of HRM in enhancing organizational information systems security. Using importance-performance map analysis, the study found training, background checks, and monitoring as crucial HRM practices that could enhance organizational information systems security. Moreover, four indicators, consisting of training on mobile devices security; malware management; background checks; and monitoring of potential, current, and former employees recorded high importance but with rather low performance. Consequently, these indicators should be improved. On the contrary, the organizations placed excessive focus on responsibility, accountability, and employee relations.

INTRODUCTION

Human resource management (HRM) practices are day-to-day activities including recruitment and selection, performance appraisal (Khan, 2010), training and development (Katuo & Budhwar, 2006), career planning management, compensation (Ahmad & Schroeder, 2003), and internal communication (Oladipo & Adbulkadir, 2011). Human resource management plays a vital role in organizations through performance of administrative HR functions such as recruitment, training, promotion, welfare services, performance appraisal, salary administration, and collective bargaining, and retention of employees

DOI: 10.4018/978-1-6684-3698-1.ch014

(Asare-Bediako, 2011). HRM practices are strategic tools for gaining higher employee performance (Khan, 2010). For organizations to achieve their set goals, strategic plans to invest in employee knowledge, skills and abilities are crucial (Battaglio et al., 2017). Human resource management practices must be strategic in measuring current workforce capacities (Goodman et al., 2015) and in assessing the prudent use of human resources (Selden, 2009). Therefore, it is important for organizations to incorporate human capital into the organization's strategic planning by investing in the workforce (Selden, 2009).

Without strong security controls, businesses risk the possibility of financial loss, legal liability, reputation harm (Amarachi, Okolie & Ajaegbu, 2013), and the effect on national security (Okewu et al., 2018). Therefore, emerging information systems security research is discovering ways to improve organizational security by motivating employees to engage in more secure security behaviors using HRM practices (Boss et al., 2015). Information security management system is a collection of policies concerned with information technology related risks (Amarachi, Okolie & Ajaegbu, 2013). Information security management system aims at implementing the appropriate measures in order to eliminate or minimize the impact that various security related threats and vulnerabilities might have on an organization (Amarachi, Okolie, & Ajaegbu, 2013).

Human resource management practices can address the problem of the human-oriented factors. Human resource management practices of employee recruitment and selection, training and development, performance monitoring and appraisals are very important to improve organisational performance (Naz, Aftab, & Awais, 2016). Investing in training and development can motivate staff and support the growth of the organisation (Leidner & Smith, 2013). Information systems security and data privacy training can serve as critical controls for safeguarding organisation's information resources (Baxter, Holderness, & Wood, 2016). Safa et al. (2018) identify lack of employees' awareness, negligence, resistance, disobedience, apathy and mischievousness as the root causes of information security incidents in organisations. As a result, Odun-Ayo et al. (2017) propose a framework for enhancing human resources in addressing information security. Thus, to achieve the best results, security training and awareness programs should be regularly evaluated so that corrective actions can be taken (Rantos, Fysarakis & Manifavas, 2012).

In addition, employee relations are seen by employers as critical in achieving job performance through employee involvement, commitment and engagement (Radhakrishna & Raju, 2015). Moreover, employee monitoring is a significant component of employers' efforts to maintain employee productivity (Ford et al., 2015). Employee background checks are important to ascertain criminal records, character, and fitness of the employee (Sarode & Deore, 2017). Furthermore, employee's accountability can improve information security (Vance, Lowry, & Eggett, 2013). However, accountability can have both positive and negative effect on work behavior (Ossege, 2012). Enhancing information systems security by focusing on human resource management practices has not received much attention by researchers. Using Importance-Performance Map Analysis (IPMA) (Ringle & Sarstedt, 2016), this chapter aims at exploring the role of HRM practices in improving organizational information systems security. In particular, the chapter (a) discusses the use of IPMA, (b) identifies the HRM practices that can improve the performance of organisational information systems security and (c) the specific HRM indicators that can enhance organisational information systems security