

# Chapter 15

## Identifying HRM Practices for Improving Information Security Performance: An Importance–Performance Map Analysis

**Peace Kumah**

*Ghana Education Service, Accra, Ghana*

**Winfred Yaokumah**

 <https://orcid.org/0000-0001-7756-1832>

*Department of Information Technology, Pentecost University College, Accra, Ghana*

**Charles Buabeng-Andoh**

 <https://orcid.org/0000-0003-3781-684X>

*Pentecost University College, Ghana*

### ABSTRACT

*This article focuses on identifying key human resource management (HRM) practices necessary for improving information security performance from the perspective of IT professionals. The Importance-Performance Map Analysis (IPMA) via SmartPLS 3.0 was employed and 232 samples were collected from information technology (IT) professionals in 43 organizations. The analysis identified information security training, background checks and monitoring as very important HRM practices that could improve the performance of organizational information security. In particular, the study found training on mobile devices security and malware; background checks and monitoring of potential, current and former employees as of high importance but with low performance. Thus, these key areas need to be improved with top priority. Conversely, the study found accountability and employee relations as being overly emphasized by the organisations. The findings raised some useful implications and information for HR and IT leaders to consider in future information security strategy.*

DOI: 10.4018/978-1-6684-3698-1.ch015

## INTRODUCTION

Securing sensitive and critical information is a global concern (Ikenwe, Igbinoia, & Elogie, 2016; White, Hewitt, & Kruck, 2013). It involves protection of information assets from unauthorized access, accidental loss, destruction, disclosure, modification, or misuse (Tassabehji, 2005). Information security is a multi-disciplinary area involving professional activity of developing and implementing technical, organisational, human-oriented security mechanisms in order to keep information systems free from threats (Cherdantseva & Hilton, 2013). As a result of increasing dependency on information technology (IT) systems and emerging security threats and vulnerabilities relating to privacy, identity theft, and cybercrime, the role of IT professionals become crucial for maintaining security of information resources (Khao, Harris, & Hartman, 2010). Information security breaches may result in loss of sensitive information and productivity which may lead to huge financial liabilities, adversely affecting the reputation of the organisation (Abawajy, 2014). Information technology professionals are facing challenging tasks analysing, designing, and deploying solutions to protect information resources. Notwithstanding, previous studies acknowledge that human factors are the major sources of many security failures (Abawajy, 2014; Driscoll & McKee, 2007; Furnell & Thomson, 2009; Komatsu, Takagi, & Takemura, 2013). Human beings are vulnerable to a wide range of security attacks, which range from deliberate violation of security policy to circumvention of physical and technical security controls (Stewart, Tittel, & Chapple, 2005). Moreover, people underestimate the likelihood of the occurrence of security breaches (Herath & Rao, 2009).

A key area in information security research is discovering ways to motivate employee to engage in more secure behaviors (Boss et al., 2015). Human resource management (HRM) 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). IT security and data privacy training can serve as critical controls for safeguarding organisation's information resources (Baxter, Holderness, & Wood, 2016). However, 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).

Improving information security by focusing on human resource management practices has not received much attention by researchers. From the perspective of IT professionals, this current study focuses on identifying key HRM practices that can improve information security performance using Importance-Performance Map Analysis (IPMA) (Ringle & Sarstedt, 2016). Specifically, the study identifies the HRM practices that IT professionals perceive as important and whose performance is necessary to improve information security in organisations. The study answers the following research questions:

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/identifying-hrm-practices-for-improving-information-security-performance/288685](http://www.igi-global.com/chapter/identifying-hrm-practices-for-improving-information-security-performance/288685)

## Related Content

---

### Laws and Regulations Dealing with Information Security and Privacy: An Investigative Study

John A. Cassini, B.Dawn Medlinand Adriana Romaniello (2008). *International Journal of Information Security and Privacy* (pp. 70-82).

[www.irma-international.org/article/laws-regulations-dealing-information-security/2482](http://www.irma-international.org/article/laws-regulations-dealing-information-security/2482)

### Visual Watermark Identification From the Transparent Window of Currency by Using Deep Learning

Duo Tongand Wei Qi Yan (2023). *Applications of Encryption and Watermarking for Information Security* (pp. 59-77).

[www.irma-international.org/chapter/visual-watermark-identification-from-the-transparent-window-of-currency-by-using-deep-learning/320946](http://www.irma-international.org/chapter/visual-watermark-identification-from-the-transparent-window-of-currency-by-using-deep-learning/320946)

### Filtration and Classification of ECG Signals

Satya Ranjan Dash, Asim Syed Sheerazand Annapurna Samantaray (2018). *Handbook of Research on Information Security in Biomedical Signal Processing* (pp. 72-94).

[www.irma-international.org/chapter/filtration-and-classification-of-ecg-signals/203381](http://www.irma-international.org/chapter/filtration-and-classification-of-ecg-signals/203381)

### Robust Image Data Hiding Technique for Copyright Protection

Siddharth Singhand Tanveer J. Siddiqui (2013). *International Journal of Information Security and Privacy* (pp. 44-56).

[www.irma-international.org/article/robust-image-data-hiding-technique-for-copyright-protection/87414](http://www.irma-international.org/article/robust-image-data-hiding-technique-for-copyright-protection/87414)

### Securing Communication 2FA Using Post-Quantic Cryptosystem: Case of QC-MDPC- McEliece Cryptosystem

Kouraogo Yacouba, Orhanou Ghizlaneand Elhajji Said (2020). *International Journal of Information Security and Privacy* (pp. 102-115).

[www.irma-international.org/article/securing-communication-2fa-using-post-quantic-cryptosystem/247429](http://www.irma-international.org/article/securing-communication-2fa-using-post-quantic-cryptosystem/247429)