Understanding of the common methods in e-HRM data security

Yonggui Guo, Lina Cao, Xiao Gao, Xuming Lv

1 State Grid Liaoning Electric Power Co., Ltd., Shenyang, Liaoning 110006, China
xuming_lv@126.com

Abstract. Along with the development of the society, the human capital comes to the significant place in the century stage. Not only the business firms but also non-profit organizations pay lots attentions to the HRM (Human Resource Management), to get better working efficiency and lower costs. However, with the advantages of modern approaches, the developing of HRM also exposes many vital challenges, especially the data security issues. Data bear the weight of the whole HRM system and a single negligence of data may cause severe problems. This paper is going to discuss the current approaches of data security management in e-HRM. Also, some recommendations are made at the end of this paper for better applying e-HRM.

1. Introduction

The purpose of this article is to critically evaluate and discuss the relationship between HRM (Human Resource Management) and data security in modern firms. The sub focus of the article is to analyse the main benefits and limitations of data security to organisations in relation to successful provision of e-HRM programmes. Based on the critical analysis and discussion, the article will then list feasible, actionable recommendations for senior HR officials to consider when constructing new e-HRM programmes in the future.

2. Development of Data Security in HRM

Research carried out by CIPD (2018) suggests that data security concerns the process of safeguarding employees’ personal information (i.e. payment information, contract terms and career history). Data security has evolved considerably over previous years and is now a core, staple element of any successful strategy in modern HRM. Blumash (2018, p.50) explains that it is not “the need to collect information relating to hiring, promoting and firing employees” which has changed, but instead how securely this information is stored. Modern HRM can be classified as composite of the following three elements; HR actors, HR activities and HR technologies (Parry & Tyson, 2013). HR actors are the employees who are tasked with carrying out various duties and responsibilities (Strohmeier, 2018). HR activities concern the set or range of practices which add value to an organisation’s management of people in the workplace (Strohmeier, 2018).

HR technologies networking of software and hardware to facilitate the successful completion of HRM tasks (Strohmeier, 2018). Organisations need to develop strong interrelationships between each of these three elements to ensure that data security is policed effectively. Knapp (2009) further suggests that it is the role of HRM to ensure that HRIS (Human Resources Information Systems) are consistently updated and upgraded to combat the latest software threats to the integrity of employee data stores. A critical aspect of the successful evolution of HRIS and data security is the trust between managers and users (Nankervis Baird, Coffey & Shields, 2016). This is significant because most strategically effective
HRM systems in the modern business landscape operate with high levels of trust between managers and users (Nankervis et al, 2016).

The effective integration of data security with HRM practices is also of paramount importance to organisations due to the increasingly digital nature of the modern business environment. For example, on average, employees are using as much as 20 software applications every day in the workplace (Po Wan, 2017). This poses many data security issues as the integrity and security of each of these applications could be breached by malware and hackers (Po Wan, 2017). The formation of GDPR (General Data Protection Regulation) in 2018 is another example of how data security has tangibly influenced the evolution and development of HRM in recent years. GDPR was set up by the European Union to give individuals more rights in relation to personal data protection (Arden, 2017). This has impacted organisations in terms of data retention, usage, security and transparency (Arden, 2017).

3. Methodologies

3.1. Data Encryption

Data encryption is one of the main methods available to modern, contemporary organisations in improving data security in HR systems (Torres Coronas, 2008). For example, disabling infrared ports in the workplace could substantially reduce the number of hackers breaching important HR data stores (i.e. employee records etc.) (Torres Coronas, 2008). Research carried out by Condrey (2010) suggests that data encryption is especially useful for organisation’s which communicate with their employees via voice over IP (VoIP) or instant messaging (IM) as these platforms are highly susceptible to data breaches. American organisations such as Coca-Cola and KFC (Kentucky Fried Chicken) are two examples of organisations which have effectively implemented data encryption in this area to preserve the integrity of employee data and information assets (Coles & Landrum, 2011).

The increasing use of cloud software to host cross department employee communication is one of the key reasons why data encryption is used widely in the modern business world (Coffin, 2011). This is because cloud software is highly susceptible to hackers, mega breaches and cyber-attacks (Coffin, 2011). The success of deploying data encryption largely rests on training employees and using appropriate software (Coffin, 2011). Unless these items are locked in place, data encryption strategies are unlikely to add value to an organisation’s level of HRM data security. One of the main limitations with successfully implementing data encryption strategies is the skillset level of the employee base. This is because using and integrating data encryption software requires high levels of technical expertise (Condrey, 2010). Cost is a further limitation with deploying this method of data security as the software can be relatively expensive to acquire (Condrey, 2010).

3.2. GDPR (General Data Protection Regulation)

Compliance with legislation is another method by which modern organizations can combine HR practices with data security. One of the most important legislative acts for modern organizations to comply with is the GDPR (General Data Protection Regulation) which has given EU citizens more control over how their data is used by their employers (Forbes, 2018). The new GDPR legislation stipulates that organizations must secure the consent of employees when storing elements of their personal data (Forbes, 2018). Reporting of data loss is another important feature of GDPR as any data security breach must now be reported to the Information Commissioner’s Office within 72 hours of occurring (Forbes, 2018, p.1). This element of GDPR could add significant value to the integrity of modern HR systems because it will prevent hackers from using the data that they have stolen.

The new legislation also states that organizations must appoint a DPO (Data Protection Officer) to inform the employee base of their new obligations in managing data, monitor compliance and regularly report to supervisory commissions with their findings (Leatherbarrow & Fletcher, 2018). Wetherspoons is an example of an organization which has successfully complied with GDPR legislation by deleting over 700,000 customer emails (Hughes, Gray & Whicher, 2018, p.29). These emails were deleted due to their high levels of susceptibility to external breaches (Hughes et al, 2018). After the email data stores
were cleared, Wetherspoons then implemented a new data management training programme to upskill employees in how to use data ethically and legally under the new regulations (Hughes et al, 2018).

3.3. SaaS (Software as a Service)

SaaS is a system which organizations receive on a subscription basis via the internet to improve internal management of employee data (DeCenzo, Robbins, & Verhulst, 2016). Once purchased, the software is then hosted by a third-party supplier and the organization accesses it via the internet (Sun, Zhang, Chen, Zhang & Liang, 2007). UK supermarket chain Tesco is an example of an organization which has used SaaS to improve their integration of data security within their HR strategy (Flanding, Grabman & Cox, 2018). Their model of SaaS is centred on preventing unauthorized access to their network of stores and distributors (Flanding et al, 2018). This case example highlights the value adding potential of SaaS as a method of improving data security in HR systems. McDonald’s is a case example of an organization which has successfully utilized SaaS as a method of improving data security in their HR systems (Contract, 2018). SaaS is used by this organization to safely and securely deliver tasks to senior managers working from home (Contract, 2018). This would previously have been high risk for data security, but the integration of SaaS has solved this problem for McDonald’s.

One of the core benefits of this method of HRM data security is that it vastly improves the robustness of HR systems as data is logged in more reliably (Bach & Edwards, 2012). This is because the risk of human error is reduced significantly due to software supplanting humans in carrying out key tasks. SaaS is also relatively inexpensive to incorporate within existing HR systems as compared with other data security methods such as encryption (Bach & Edwards, 2012). Despite these many advantages, SaaS is not without its limitations as it can be highly complex to implement effectively, particularly if the organisation does not use third party host software (Grobler, 2005). If an organisation does use third party, host software they are then also limited in terms of internal control (Grobler, 2005).

3.4. Benefits and Limitations of HRM Data Security

A key benefit to organisations of effectively fusing data security with HRM systems is that it ensures their core employee data sets retain their integrity and usability (Leatherbarrow & Fletcher, 2018). A further benefit of HRM data security is that it significantly reduces the risk of data loss and data leaks (Lambert, 2016). This therefore prevents competitor brands from gaining access to important aspects of an organisation’s HR strategy such as structure of training and development programmes and recruitment and selection methods (Lambert, 2016). In the case of private medical organisations in India, improving HRM data security offers the following advantages; cost reduction, quality improvement in providing care to patients and promotion of the employer brand (Chakraborty, 2016). This case example highlights the many prospective benefits of successfully integrating HRM practices with data security. Additionally, data security packages are extremely beneficial for organisations which operate a BYOD (Bring Your Own Device) approach to IT in the workplace because these devices increase the susceptibility of the organisation to external threats such as hackers and malware (Nagele Piazza, 2018). Therefore, data security packages can increase the strength and robustness of the HR department’s body of private data and information.

One of the main, primary limitations facing data security in HRM is external security breaches such as hackers spreading malware (Thite, 2018). Recently, cybercriminals have begun posing as job applicants as part of a new campaign to infect online HRM systems with Golden Eye Ransomware to source personal information regarding employees (Thite, 2018). Moving forward, this poses a significant threat to the integrity of employee data stores in e-HRM portals/databases in particular. Research carried out by Rahman et al (2018) suggests that modern, contemporary employee groups are reticent about engaging with new e-HRM programmes because of data breaches like this. Important ethical issues have also arisen from the evolving role of data security in relation to HRM systems. For example, in the modern world of recruitment and selection, employers can use the social media data of job applicants to assess their suitability to the role (Holland & Jeske, 2018). This action is considered to be ethically dubious because the employer is gaining access to the applicant’s private data sets (Holland
& Jeske, 2018). The counter argument to this however is that the data is used but not stored therefore it does not contravene GDPR legislation.

4. Recommendations

A key, actionable recommendation which senior HR officials within modern organizations should consider is to provide data security training for their workforce (Po Wan, 2017). This will ensure that all employees are better educated regarding their role in keeping data sets safe and the importance of creating stronger passwords (Po Wan, 2017). This could significantly improve the security and integrity of data and information stores in modern organizations. The main limiting factor with this recommendation is cost as the training programme may require input from an external training body such as CIPD (Chartered Institute of Personnel and Development) to ensure that it is implemented effectively.

Senior HR officials should also consider developing a fully-functioning HRIS (Human Resources Information System) to improve the value adding capacity of their existing HR practices and activities (Bruce, 2014). This could improve the value adding capacity of HR practices in the following ways; reliable hosting of company-related documents, accuracy of data reporting/storage, self-service feature to minimize billable HR hours and automated reminders to enable managers to keep pace with upcoming schedule changes etc. (Bruce, 2014). The limitation with the practicability of this recommendation is cost as it can be expensive to purchase the necessary software applications such as cloud computers etc. (Bruce, 2014). Successfully implementing HRIS may also require external assistance from expert software providers.

A further important recommendation which modern, senior HR officials should consider is to implement more contingent employee offboarding strategies (Po Wan, 2017). Employee offboarding increases the risk of data leakage because employees departing the organization often feel as though they no longer have an obligation to protect the integrity of that organization’s data sets (Po Wan, 2017). These contingency strategies should be enforced in relation to high ranking employees (i.e. Chief Human Resources Officers and Chief Marketing Officers) in particular as these individuals possess the organization’s richest data sources.

5. Conclusion

In summary, this article has critically analysed and discussed the relationship between human resource management and data security in modern, contemporary organisations. One of the main, key findings streamed from the analysis and discussion carried out is that HRM has evolved considerably in recent years to become more digital-centric with e-HRM programmes supplanting older, traditional methods of storing employee data. Additionally, this article has also found that the most successful HRM systems are composite of the following three elements: HR actors, activities and technologies. Formulating a strong interrelationship between each of these three core elements is essential to effective employment management practices at modern firms.

The formation of GDPR has also had a substantial impact on how effectively each of these three core elements interrelate within modern day HR systems. The findings of this article also indicate that trust between managers and users is a key contributor to the successful operation of HRIS in contemporary organisations. This article has also found that cyber criminals pose a real threat to the integrity of data stores the in e-HRM systems of modern, contemporary organisations. This highlights why senior HR officials within modern organisations should consider administering training programmes to educate employees on the importance of creating stronger passwords.

References

[1] Atim Arden. The Impact of GDPR on HR and Personal Data. [Online] URL: https://www.hrsolutions-uk.com/impact-gdpr-hr-personal-data, 2017.

[2] Stephen Bach, Martin R. Edwards. Managing Human Resources: Human Resource Management in Transition. London: John Wiley & Sons Ltd, 2012.
[3] Stephen Bruce. HRIS: Advantages and Disadvantages. [Online] URL: https://hrdailyadvisor.blr.com/2014/01/22/hris-advantages-and-disadvantages, 2014

[4] Bulmash J. Human Resources Management and Technology[J]. Human Resources Management in Canada, 2013: 49-72

[5] Nirmalya Chakraborty, Vandna Sharma, et al. A Perceptual Study on Factors of Medical Data Security in Indian Organisations[J]. Journal of Theoretical and Applied Information Technology, 2016, 84(1): 59-78.

[6] CIPD. Data Protection. [Online] URL: https://www.cipd.co.uk/knowledge/fundamentals/emp-law/data-protection, 2018