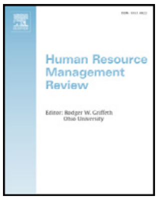
Human Resource Management Review 23 (2013) 105–113

Contents lists available at SciVerse ScienceDirect

Human Resource Management Review

journal homepage: www.elsevier.com/locate/humres



Human resource information systems: Information security concerns for organizations

Humayun Zafar *

Department of Information Systems, Kennesaw State University, 1000 Chastain Road, MD 1101, Kennesaw, GA 30144, United States.

ARTICLE INFO

Keywords:
Human resource information system
Information security
Information privacy
Security policies
Security legislation
Security architecture
Security training
Risk analysis

ABSTRACT

We explore HRIS and e-HR security by presenting information security fundamentals and how they pertain to organizations. With increasing use of enterprise systems such as HRIS and e-HR, security of such systems is an area that is worthy of further exploration. Even then, there is surprisingly little research in this area, albeit that extensive work is present in regard to HRIS privacy. While focusing on HRIS and e-HR security, we introduce aspects of HRIS and e-HR security and how it can be enhanced in organizations. A research model is also presented along with propositions that can guide future research.

1. Introduction

A human resource information system (HRIS) is an integrated computerized system used to acquire, store, manipulate, analyze, retrieve, and distribute pertinent information about an organization's human resources (Kavanagh, Gueutal, & Tannenbaum, 1990). HRIS is similar to an enterprise resource planning system, with a caveat that it focuses exclusively on the human resource (HR) functions of an organization. A comparatively recent move toward electronic human resource (e-HR) systems has allowed organizations to offer a personalized interface to individual employees. The interfaces include ability to apply for jobs, changing job-related benefits, and web-based training (Stone, Stone-Romero, & Lukaszewski, 2006). However, there is a fundamental difference between HRIS and e-HR. HRIS is directed toward the HR department itself. End users mainly include the HR staff. With e-HR, end users are not the HR staff but people outside HR as well: the employees and management. We would like to contend that e-HR is the unlocking of HRIS for all employees of an organization.

Advances in information technologies have changed the human resource (HR) functions within organizations. Today, most organizations implement an HRIS extensively to support basic HR functions, as well as to enhance administrative efficiency, decision making, and information sharing (Lengnick-Hall & Moritz, 2003). In a study conducted by Beadles, Lowery, and Johns (2005), 80% of the HR directors noted that an HRIS improved levels of usefulness of information as well as their ability to disseminate information. Moreover, 90% of the HR directors in their study reported that HRIS added value to the organization. Accordingly, HR professionals are considered to add value to organizations, since HRIS can free up their time, whereby allowing greater involvement in organizational strategic decisions (Bussler & Davis, 2002; Hussain, Wallace, & Cornelius, 2007). From these studies, it can also be interpreted that an organization's employees are its most valuable resource. The efficiencies achieved from extensive HRIS and e-HR usage allow attraction and retention of a workforce that is needed to build long-term profitability and success for a firm. Therefore, it is not a surprise to note that HRIS and e-HR are enterprise level solutions. Examples of vendors that provide HRIS and e-HR solutions include SAP, Oracle-PeopleSoft, CheckPointHR, and Epicore.

* Tel.:+1 770 420 4424; fax: +1 770 423 6731.
E-mail address: hzafar@kennesaw.edu.

1053-4822/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
doi:10.1016/j.hrmr.2012.06.010

HRIS usage does much more for a firm than eliminate manual administrative procedures, increase efficiency, and minimize costs associated with acquiring staff members and administering to all facets of their employment. It can assist in creating a more employee-centric culture (Candler, 2001), which in turn can boost satisfaction and morale, reduce turnover, and build a stronger more motivated and loyal workforce.

There is also a divergence in HRIS usage. Initially, human resource information systems were developed to replace people with software. Instead of maintaining employee records by HR clerks, data was entered into a system and updated as necessary. Later HRIS was extended to include transaction processing systems (TPS), decision support systems (DSS), communication systems, and systems including artificial intelligence (Kovach, Hughes, Fagan, & Maggitti, 2002). The evolution of HRIS from being a standalone system with limited data entry use to a more elaborate system is similar to the history of software systems. Modern day software systems exhibit a high degree of automation, as opposed to their predecessors (Mahoney, 2004). For example, there was a time when TPS catered exclusively to mainframe technologies such as airline reservation and banking systems. However, advances in networking and processing capabilities of user machines have led TPS to be incorporated in HRIS and e-HR systems. This has addressed organizational needs of handling a large number of concurrent users, updating records such as benefits instantly, and handling errors in a safe manner (Broderick & Boudreau, 1992).

As a stand-alone system, usage of HRIS is not only limited to employee record management, but also extended to compensation and benefits, recruitment of talented job applicants and retention (Stone, Lukaszewski, & Isenhour, 2005), training and development, and managing employee performance (Strohmeier, 2007). Today, HRIS and e-HR are no longer stand-alone applications but incorporated as a module to enterprise information systems such as Oracle. Thus, HR professionals have access to corporate databases and other departments can have access to HR departmental files. Accordingly, security and privacy are major concerns to ensure that only authorized personnel are allowed to have such access (Kovach et al., 2002).

While there is discussion and research on adoption, implementation, and satisfaction with HRIS, little work has been done on investigating approaches toward maintaining an HRIS while assuring security of the organization and its stakeholders. HRIS security is a pertinent area of concern for organizations. With increased implementation of HRIS as a module of enterprise systems, security is critically important. HR data often include a great deal of confidential data about employees, such as employment records, payroll and benefit data, social security numbers, test and performance appraisal data, and succession planning, etc. (DeSanctis, 1986; Kovach & Cathcart, 1999). As such, companies should be conscientious in managing this type of data.

Keeping in view the paucity of information security related research in HR information systems and information security in general (Zafar & Clark, 2009), the primary purposes of this study are to discuss (a) information security and its components in general, (b) information security related problems associated with HRIS and e-HR, (c) factors that influence HRIS and e-HR security.

2. Information security

Information security, at times referred to as computer security, is defined as the protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability (CIA) of information system resources (Stallings & Brown, 2008). Confidentiality assures that private information is kept safe from unauthorized individuals. It is critical for maintaining the privacy of the employees' personal information (Wong & Thite, 2009). Integrity assures that information and programs are created and modified in a specified and authorized manner. It is important to assure the integrity of both the data and the system. Availability assures that systems work and service is provided promptly to those who are authorized to use them. Personnel transactions and information processing are increasingly more vulnerable to security threats and risks due to the increased use and complexity of HRIS systems. Accordingly, information security should be a critically important issue of concern for today's HR personnel.

2.1. The interplay between security and privacy

While many consider information privacy as being interchangeable with information security, there are underlying differences between information security and privacy. Kang (1998) clustered privacy into three groupings. The first is concerned with physical space, or protecting an individual's territory from invasion by unwanted objects. In the second view, privacy is primarily concerned with the ability to make a choice without interference. Finally, the third cluster is concerned with the flow of personal information. Specifically, it highlights an individual's control over the acquisition, disclosure, and use of personal information.

There is a litany of research dealing with an array of issues pertaining to HR and HRIS privacy (Alge, 2001; Eddy, Stone, & Stone-Romero, 1999; Stone & Stone, 1990; Stone & Stone-Romero, 1998; Stone, Stone-Romero, & Lukaszewski, 2003; Stone-Romero, Stone, & Hyatt, 2003). However, as shown in the definition of privacy, the privacy construct deals with an expectation on part of an individual to keep information private. Information security, on the other hand, is concerned with the steps taken to keep the information secure (which is the focus of this study). These steps can vary from technical to managerial controls, and ideally should be viewed synergistically across all organizational boundaries to be implemented successfully. Due to the interplay between information security and privacy, there are several federal and state laws and regulations to safeguard information security and privacy such as the Health Insurance Portability and Accountability Act of 1966 (HIPAA), the Privacy Act of 1974, and Security Breach Notification Law (Wong & Thite, 2009).

2.2. HRIS and e-HR security

The primary purpose of a HRIS is to provide accurate and timely information to users of the system. According to Kavanagh and Thite (2009), HR information may be required by various stakeholders, such as HR professionals, managers, and employees. It may be used for strategic decision-making, identifying discrimination problems in hiring to avoid litigation, evaluating effectiveness of training programs, and/or supporting daily operations such as assisting managers monitoring time and attendance of their employees.

It can easily be argued that the data contained in a HR application needs to be well guarded by an organization. The application may include social security numbers, payroll data, performance history, medical history, and EEO related data. Confidential information may be disclosed, intentionally, by someone such as a disgruntled employee, or unintentionally, by someone who has not been properly trained in the use of a HRIS. Information can be altered or corrupted, or access to information by authorized person can be denied. Each of these security threats and/or breaches could negatively influence an organization and results in more damaging consequences such as loss of business, law suits, or even bankruptcy (Townsend & Bennett, 2003). Employees are certainly aware of the sensitive nature of the stored information, and potential threats faced. They may also perceive that if information about them is revealed, it may result in negative outcomes such as denial of employment or promotion.

3. A model of the factors contributing toward HRIS and e-HR security

Previous research has resulted in various information security oriented models in different contexts. Some of those models include security of web based applications (Joshi, Aref, Ghafoor, & Spafford, 2001), role based accessed control (Sandhu, Coyne, Feinstein, & Youman, 1996), security counter measures (D'Arcy, Hovav, & Galletta, 2009), and contingency planning (Cerullo & McDuffie, 1992). Some have argued that a more holistic approach toward security is needed, which begins with the design process (Baskerville, 1993; Hitchings, 1996).

This study modifies a conceptual model for creating security subsystems initially introduced by Clark, Beebe, Williams, and Shepherd (2009). Clark et al. (2009) posited that while complete security and privacy were not possible, systems could still attain reasonable levels of system security through integration of security principles during the system development process. This is a key point since analysts and designers invariably avoid security issues or treat them as "add-ons" to a system when security problems arise. However, the highest proportion of security attacks to systems can be attributed to poor system design (Hoglund & McGraw, 2004; McGraw, 2004). Systems such as Oracle that incorporate HRIS functionalities have been known to be suspect to security vulnerabilities due to poor system design and implementation (Maurice, 2009).

HRIS research has also mentioned that successful implementation begins with a comprehensive design (Bedell, Canniff, & Wyrick, 2008), which can significantly impact system effectiveness (Stone et al., 2003). For example, a HRIS may be less engaging than traditional HR systems, and less likely to capture an individual's attention (Stone & Lukaszewski, 2009). Though

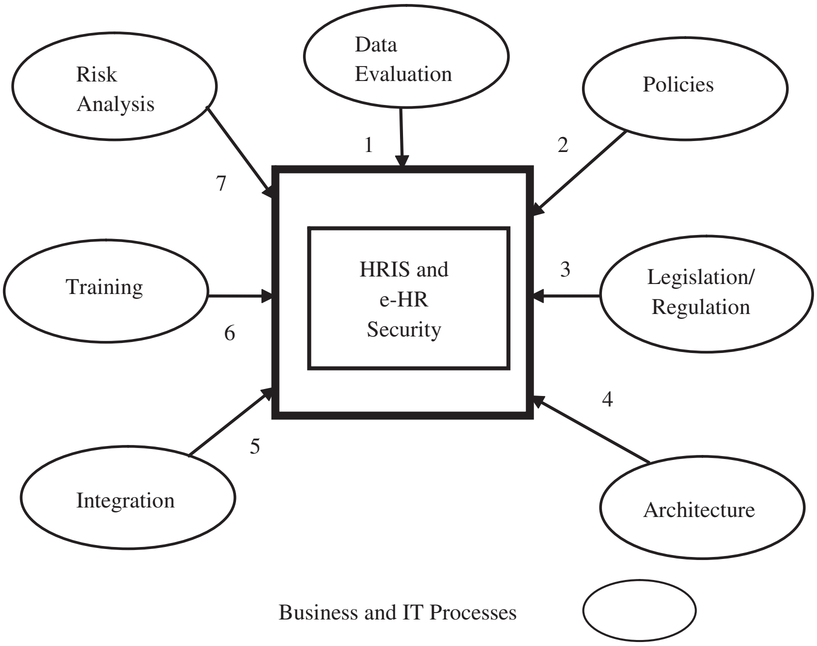


Fig. 1. Factors that contribute toward HRIS and e-HR security.

Clark et al.'s (2009) model did not specifically focus on HR issues, it can be extended to it. Clark et al.'s (2009) model mirrors the National Institute for Standards and Technology's (NIST's) system development lifecycle model (SDLC). Security adds value to the SDLC though prescriptive and proscriptive guidance and expertise in building secure software (Peterson, 2007). Security can also play a role in each phase of the SDLC. NIST develops standards and guidelines for providing adequate information security for an organization's operations and assets. The security considerations in the system development life cycle have been developed to assist in integrating an organization's essential IT security steps into their established IT infrastructure (Kissel et al., 2008). Unlike some of the comparable security models such as the International Organization for Standardization (ISO) 27000 series, NIST documents are publicly available and free. They have also been broadly reviewed by government and industry professionals, and were among the first references cited by the federal government when it decided not to select the ISO 17799 standards (Holden, 2003).

Due to their overarching nature, NIST documents are developed in a way that allows them to be extended to different domains. HR is no different. In fact, factors mentioned by Clark et al. that contribute toward HRIS security have been mentioned in past NIST documents (Stine, Kissel, Barker, Lee, & Fahlsing, 2008) and software research (Gamma, Helm, Johnson, & Vlissides, 1995; Pauli & Xu, 2005). Common examples include use of weak passwords and relative insecurity of reporting tools. Another factor to consider is the balance between security and usability/performance issues. For example, a HRIS/e-HR system may suffer from degradation of performance if unnecessarily high security settings and procedures such as enabling advanced encryption and audit trails are used. Therefore, this study presents a research model that reflects Clark et al.'s (2009) and NIST's standards as they pertain to HRIS and e-HR security (Kissel et al., 2008; Stine et al., 2008). The model is shown in Fig. 1. A brief description of each of the contributing factors is provided next, along with individual propositions derived for each.

3.1. Data evaluation

Data is saved in systems so that it can be manipulated. Individual fragments of data may seem innocuous. However when combined with other data, it may result in a security risk to an organization. For example, in most organizations, users may log into HRIS and e-HR systems with a user name that consists of the first name's initial, followed by a complete last name. However, if the password employed is relatively weak, then the entire system may be comprised via password cracking software (Zviran & Haga, 1999). For this reason, evaluating the security of stored data has been highlighted as one of the building blocks of information security (Strunk, Goodson, Scheinholtz, Soules, & Ganger, 2003). Clark et al. (2009), DeLone and McLean (2003), and Hamilton and Chervany (1981) present a series of steps regarding data evaluation:

- Determine how each data element is to be manipulated. Data manipulation refers to how data stored in a database may be altered by a user.
- Classify data according to access type. Access may be specific (private) to a particular user (e.g. role based access control to data), or available publicly to everyone.
- Based on data classification tag the data element with a security code that would highlight its risk level. In general, data that is deemed as being private will have the highest risk level, as opposed to data that is publically available.
- Document data evaluation procedures. Any procedures established should be documented so that future changes in data evaluation procedures are consistent with past approaches.

Therefore, we posit:

P1. Comprehensive data evaluation procedures will enhance HRIS and e-HR security.

3.2. Policies

Cleary articulated security policies and procedures are essential for a firm, since they represent a degree of commitment (Whitman & Mattod, 2004). Effective policies clearly articulate a body of expectations that describe acceptable and unacceptable behaviors of employees in the workplace. With respect to HRIS and e-HR, due to the nature of the information stored (social security numbers, benefits information, etc.), increased attention to privacy and security policy and procedures needs to be paid. Policies should be set such that they escalate in importance with each new application and user with direct access to personal information (Spirig, 1991). It is also critical that organizations not view security policies as static entities. Policies must be able to adapt to changes within an organization for applicability and consistency (Siponen, Baskerville, & Heikka, 2006).

Recommendations provided by previous research (Anderson, 2008; Dhillon, 2007; Spinellis, Kokolakis, & Gritzalis, 1999) in regard to security policies include:

- Determine impact of policies on stakeholders. If this is not done then policies may be a source of hindrance, which may consequently result in security lapses.
- Review and update security policies based on organizational changes. In time organizations may merge with other organizations, or go through other structural changes. In either case, policies may need to be updated due to the change.
- Distribute revised policies to all relevant stakeholders. This is important, since it would ensure that all stakeholders are aware of what the latest sets of expectations are with respect to security policies.

- Assure that third parties are aware of security policies, and any subsequent updates. Organizations may work with outside businesses, which would imply that it has extended stakeholders that need to be considered as well.
- Document policy changes. This would ensure that there is a record of all changes made to security policies and procedures.

Therefore, we posit:

P2. Clearly defined security policies will enhance HRIS and e-HR security.

3.3. Legislation/regulation

The widespread use of networked technologies such as HRIS and e-HR has introduced many windows of opportunity for the naïve person and/or the attacker. This proliferation of technology has resulted in the passage of numerous laws related to technology use and information security. Examples include the Computer Security Act of 1987 (CSA, 2008), Federal Privacy Act (FPA, 2007), and the Fair Credit Reporting Act (FCRA, 2004). Although this list is by no means exhaustive, the overall goal of these legislations is similar, that is, to establish a baseline that would guide organizations toward a level of security. For example, the Computer Security act provides for improving the security and privacy of sensitive information. The Federal Privacy Act complements the Computer Security Act by protecting an individual's privacy through multiple procedural and substantive rights in personal data. Finally, the Federal Credit Report Act among other things mandates that when credit reports are used for employment purposes, consumers should be notified if adverse decisions are based on them.

With respect to HRIS and e-HR, the above-mentioned legislations are relevant once again due to the sensitive data that is stored. If compromised, then information such as results of physical exams, and credit information may have an adverse impact on an employee's employment.

The issue of legislation and regulation is a multi-dimensional problem. For example, organizations that employ HRIS/e-HR systems may have those systems in different locations worldwide. This may lead to a situation where different legislations may apply based on the country in which the system resides. For example an organization may have to comply with both U.S. and European regulations. As a global organization, this is considered as one of the critical requirements for an organization, as it has to deal with a patchwork of disparate and over-lapping state and federal regulations, along with privacy rules laid out by individual corporate partners. Within the European Union, an organization has to contend with the data protection directive, which unlike U.S. regulations such as HIPPA or Sarbanes–Oxley acts, provides few specifics as to how these privacy requirements should be met. Therefore an organization has to focus on the need to establish a consistent set of requirements common to various U.S. and EU jurisdictions, while keeping in mind its own standards for protecting customer and supplier data. This is through enhanced security features such as encryption. This is also why, an organization may have to focus on creating in-house security tools as part of its corporate security strategy. It allows the organization to build a foundation that is both deep and broad, rather than a series of narrow solutions that address regulations on a case-by-case basis.

To ensure that organizations abide by the disparate and at times overlapping legislations, a team-based approach should be applied as part of the enterprise system design process (for example, in the case of HRIS and e-HR). The members should come from security, audit, legal, management, IT, and HRM areas as well as other functional areas if needed (Listerman & Romesberg, 2009). Team tasks could include:

- Reviewing government documents for changes in security legislation. This would ensure that an organization's security policies mirror requirements of the various security based legislation.
- Reviewing industry regulatory groups for proposed changes. This would allow for organizations to complement required legislative procedures with some of the recommendations of industry.
- Reviewing international standard groups such as ISO and NIST. This would ensure that technological and non-technological factors are applied optimally to counter threats due to viruses, Trojans, malware, and social engineering.
- Revising policies as necessary. This is especially important, since threats posed by the previously mentioned technological and non-technological threats are constantly evolving.
- Document changes. This would ensure consistency between what an organization implements as part of security legislation, and recommendations from industry counterparts.

Therefore, we posit

P3. Comprehensive implementation of legislative and regulatory policies will enhance HRIS and e-HR security.

3.4. Architecture

At point of data input, employees of an organization need to be assured that the information they enter will be secure. Security architecture is a framework that allows the development operation staff to align efforts. Employees may have an image of web based e-HR systems in which information is intercepted for malicious use by invisible third parties. This problem may not be of the highest priority for HRIS, which as stated earlier is limited to the HR department itself. If limited to a single department HRIS exhibits a high sense of physical security. Whereas e-HR systems are of a distributed nature, and there may be perceptions about them being insecure based on lack of access control levels of employees (Ward & Smith, 2002). According to Wheatman (2010), some of the roles that may need to be watched are privileged users, legitimate end users, and developers and system analysts. Privileged users have special, high-level privileges to an HRIS/e-HR, and should be subject to scrutiny from the security professionals. These users have high visibility into, and access to data and any underlying systems. Therefore, they should be subject to background checks and should be monitored and audited for potential problem activities such as addition, modification, or deletion of data, unauthorized addition or removal of employee accounts, and schema modifications.

A few other technological measures that can be used to secure enterprise technologies such as e-HR systems include encryption (Brehm & Gomez, 2010), logging capabilities for an audit trail (Accorsi, 2009), and bundling of proprietary identity management systems with an HRIS, rather than using one with open standards that interfaces with different applications (Hughes & Beer, 2007). This to some extent would ensure network and host security (Panko, 2010; Whitman, Mattord, Austin, & Holden, 2009). Network security encompasses protective mechanisms such as firewalls and intrusion detection systems. On the other hand, host security is concerned with access control to servers and workstations.

It is also important to allay employee concerns by investing in an incident response and disaster recovery plan (Whitman & Mattord, 2006). A detailed incident response and disaster recovery plan would ensure continuity of HRIS and e-HR operations in the event of an unexpected incident.

Therefore, it is pertinent to consider the following recommendations:

- Reviewing incident response and disaster recovery plans. Actions presented in these plans guide an organization in attempting to stop an incident, mitigate the impact of an incident, and provide information for recovery.
- Reviewing physical security procedures. This can include physically securing sensitive technologies such as web servers in locked rooms, providing employees with access control devices such as identification cards etc.
- Reviewing access control procedures. This is done to ensure that only the relevant stakeholders gain access to various information systems.
- Reviewing best practices of the industry. This would allow an organization to ensure that security procedures implemented are in line with what current industry requirements are.
- Documenting changes. This would predominantly feature changes made to the incident response and disaster recovery plans, as well as those made to the access control policies.

Hence, we posit:

P4. A comprehensive security architecture will enhance HRIS and e-HR security.

3.5. Integration

In organizations, HRIS and e-HR are not the only IT based systems that will be used. There may be systems designed in-house for organizational usage. System integration involves the ability to seamlessly share data and resources across all the different systems in an organization. This raises an interesting security issue, because HRIS or an e-HR system may be exposed to a vulnerability if they come in contact with a system that is not completely secure. A system is only as secure as its weakest link (Varian, 2004). For this reason, application security has become an issue of concern (Ioannidis, Bellovin, & Smith, 2002). Therefore, it is suggested (Beynon-Davies, Carne, Mackay, & Tudhope, 1999; Clark et al., 2009; Korhonen, Paavilainen, & Särelä, 2003; Lam, 2005) that organizations:

- Review integration of other systems within the organization. This would ensure that all software systems are secured to the fullest extent.
- Review potential security risks. This allows an organization to identify systems that are not secure, after which a decision would have to be made regarding either removing the flaws, or migrating that system to a different location.
- Assess degree of access. This would ensure adequacy of access to privileged users, legitimate end users, and developers and system analysts.
- Establish a record of accountability. This somewhat relates to the previous point. A record of different types of users would ensure that actions that are in contrast to the allowed policies and procedures are investigated.
- Document changes made in regard to system integration, and assessed security risks.

Therefore, we posit:

P5. Comprehensive system integration procedures will enhance HRIS and e-HR security.

3.6. Training

Training, along with education and awareness is part of an organizational educational program designed to reduce the number of security breaches that occur through a lack of employee security awareness. A high proportion of threats are from employees who either intentionally or unintentionally introduce vulnerabilities into a system (Im & Baskerville, 2005). Human error, although not deliberate, can still result in security breaches. (Werlinger, Hawkey, & Beznosov, 2009). Examples of human error include forgetting to change passwords, not logging off before leaving a workstation, or careless discarding of sensitive information (Warkentin & Willison, 2009). Case studies, scenario planning, and crisis exercises are used to create awareness, and are an effective means of changing organizational security culture (Hagen, Albrechtsen, & Hovden, 2008; Lacey, 2010). According to Johnson (2006), benefits from awareness programs mitigate overall security risks, increase reliability and correctness of information, and result in early detection of potential security incidents. Examples pertinent to HRIS and e-HR include maintaining strong passwords, not sharing user IDs and passwords, and installing anti-virus programs and firewalls. Therefore, it is important to:

- Provide security based training to employees. This would ensure best practices on part of the employees, and reduce potential instances of employee neglect that may result in security incidents.
- Assure that all legal requirements have been met. This is to ensure that requirements pertaining to different security legislations are met.
- Customize security training, education, and awareness plans according to organizational policies. This would ensure that control measures designed to reduce the incidences of accidental security breaches by employees are reduced due to their direct relevance to how the organization operates.
- Document security training, education, and awareness procedures. This would allow an organization to make changes to training, education, and awareness programs in an efficient manner.

Therefore, we posit:

P6. Comprehensive security training, education, and awareness programs will enhance HRIS and e-HR security.

3.7. Risk analysis

The level of HRIS and e-HR security should be commensurate with the level of assumed risk. For example, unlike HRIS, e-HR systems may be suspect to web based attacks. Detailed risk analysis identifies and assesses factors that may jeopardize the successful implementation of a system. It also helps define preventive measures to reduce the probability of these factors from occurring and identifies countermeasures to deal with these constraints when they occur (Peltier, 2005).

It is also advisable to monitor acceptable risk levels on a continual basis (Smith, McKeen, & Staples, 2001). Risks deemed as being acceptable (or unacceptable) may change due to changes within or external to the organization. Metrics-based measures may be applied to identify risks as well. These are benchmarking comparisons based on numerical standards such as successful attacks, dollars spent on protection, number of security personnel, and loss in productivity hours associated with successful attacks. With regard to risk analysis some recommendations (Whitman & Mattord, 2011) are:

- Identify system functions, boundaries, and criticalities. This would reduce the risks to an organization's data and information systems.
- Identify security threats and vulnerabilities. This entails the formal process of examining and documenting the security posture of an organization's information systems.
- Calculating risk factors. This is an analysis of potential dangers faced by a firm that are quantified via risk ratings.
- Assure that all risks with a significant negative impact are addressed.
- Document results of risk analysis.

Therefore, we posit:

P8. Comprehensive risk analysis will enhance HRIS and e-HR security.

3.8. About documentation

It may be noted that each set of recommendations provided in the previous section included documentation. In all of its security related documents NIST focuses on the importance of documenting information technology related changes or updates (Kissel et al., 2008). The reason is that technologies change rapidly, and with multiple users and system developers, it becomes imperative that system consistency is maintained over a period of time. Extensive documentation at each stage also allows for the development of a knowledge database, which could be helpful in the event of system issues that may be faced with in the future.

4. Future research and conclusion

This study explored the under-researched area of HRIS and e-HR security. HRIS and e-HR security related issues were discussed, while guidelines to cope with these security issues were offered through a research model. Considering that the use of HRIS, e-HR, and similar enterprise systems will only continue to increase, it is essential that concerns related to HRIS security be addressed.

In order to fully comprehend HRIS and e-HR security, it is important that future research be focused on organizational level studies investigating different facets of HRIS/e-HR security. Since enterprise systems such as the ones that offer HRIS/e-HR vary in implementations across different companies, a qualitative research method may prove to be a more beneficial choice. Issues such as HRIS adoption, privacy concerns, security, and trust are complex and sensitive in nature, and a qualitative based method will provide the opportunity to provide a rich context to the study. We also contend that this method will also be effective due to the fact that HRIS security and information security in general are naturally intrusive topics. A study can be derailed if participants are initially skeptical about taking part in a study that may highlight information security based problems in their organization (Kotulic & Clark, 2004).

References

Accorsi, R. (2009). Safe-keeping digital evidence with secure logging protocols: State of the art and challenges. *Fifth International Conference on IT Security Incident Management and IT Forensics* (pp. 94–110). Stuttgart, Germany: IEEE.

Alge, B. (2001). Effects of computer surveillance on perceptions of privacy and procedural justice. *Journal of Applied Psychology*, *86*, 797–804.

Anderson, R. J. (2008). *Security engineering: A guide to building dependable distributed systems* (2 ed.). : Wiley Publishing.

Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys (CSUR)*, *25*, 375–414.

Beadles, N., II, Lowery, C., & Johns, K. (2005). The impact of human resource information systems: An exploratory study in the public sector. *Communications of the IIMA*, *5*, 39–46.

Bedell, M., Canniff, M., & Wyrick, C. (2008). Systems considerations in the design of an HRIS. *Human resource information systems: Basics, applications, and future directions* (pp. 45–76).

Beynon-Davies, P., Carne, C., Mackay, H., & Tudhope, D. (1999). Rapid application development (RAD): An empirical review. *European Journal of Information Systems*, *8*, 211–223.

Brehm, N., & Gomez, M. J. (2010). Federated ERP-systems on the basis of Web Services and P2P networks. *International Journal of Information Technology and Management*, *9*, 75–89.

Broderick, R., & Boudreau, J. W. (1992). Human resource management, information technology, and the competitive edge. *The Executive*, *6*, 7–17.

Bussler, L., & Davis, E. (2002). Information systems: The quiet revolution in human resource management. *Journal of Computer Information Systems*, *42*, 17–20.

Candler, I. W. (2001). The future of employee data management. In A. Doran (Ed.), *E-work architect: how HR leads the way using the internet* (pp. 55). Austin: Rector-Duncan.

Cerullo, M. J., & McDuffie, R. S. (1992). Computer contingency plans and the auditors: A survey of businesses affected by Hurricane Hugo. *Computers & Security*, *11*, 620–622.

Clark, J. G., Beebe, N. L., Williams, K., & Shepherd, L. (2009). Security and privacy governance: Criteria for systems design. *Journal of Information Privacy and Security*, *5*, 3–30.

CSA (2008). Computer Security Act of 1987. Available at. http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf Retrieved January 25 2011.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*, 79–98.

DeLone, W., & McLean, E. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, *19*, 9–30.

DeSanctis, G. (1986). Human resource information systems: A current assessment. *MIS Quarterly*, *10*, 15–27.

Dhillon, G. (2007). *Principles of information systems security: Text and cases.* Hoboken, NJ: Wiley.

Eddy, E., Stone, D., & Stone-Romero, E. (1999). The effects of information management policies on reactions to human resource information systems: An integration of privacy and procedural justice perspectives. *Personnel Psychology*, *52*, 335–358.

FCRA (2004). The Fair Credit Reporting Act. Available at. http://www.ftc.gov/os/statutes/031224fcra.pdf Retrieved May 11 2011.

FPA (2007). The Privacy Act of 1974. Available at. http://www.justice.gov/opcl/privacyact1974.htm Retrieved January 25 2011.

Gamma, E., Helm, R., Johnson, R., & Vlissides, J. (1995). *Design patterns: Elements of reusable object-oriented software.* Westford, MA: Addison-Wesley Professional.

Hagen, J., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*, 377–397.

Hamilton, S., & Chervany, N. L. (1981). Evaluating information system effectiveness—Part I: Comparing evaluation approaches. *MIS Quarterly*, *5*, 55–69.

Hitchings, J. (1996). *A practical solution to the complex human issues of information security design.* London, UK: Chapman & Hall, Ltd.

Hoglund, G., & McGraw, G. (2004). *Exploiting software: How to break code.* Boston, MA: Pearson Higher Education.

Holden, G. (2003). *Guide to firewalls and network security: Intrusion detection and VPNs.* Boston, MA: Course Technology Press.

Hughes, J. R., & Beer, R. (2007). A security checklist for ERP implementations. *Educause Quarterly*, *30*, 7–10.

Hussain, Z., Wallace, J., & Cornelius, N. (2007). The use and impact of human resource information systems on human resource management professionals. *Information & Management*, *44*, 74–89.

Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: The enduring problem of human error. *Data base*, *36*, 68–79.

Ioannidis, S., Bellovin, S. M., & Smith, J. M. (2002). Sub-operating systems: A new approach to application security. *Proceedings of the 10th workshop on ACM SIGOPS European workshop* (pp. 108–115). Saint-Emilion, France: ACM.

Johnson, E. (2006). Security awareness: Switch to a better programme. *Network Security*, *2006*, 15–18.

Joshi, J. B. D., Aref, W. G., Ghafoor, A., & Spafford, E. H. (2001). Security models for web-based applications. *Communications of the ACM*, *44*, 38–44.

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review*, *50*(4), 1193–1294.

Kavanagh, M. J., Gueutal, H. G., & Tannenbaum, S. I. (1990). *Human resource systems: Development and application information.* : PWS Publication.

Kavanagh, M., & Thite, M. (2009). *Human resource information systems: Basics, applications, and future directions* (1 ed.). : Sage Publications, Inc.

Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J., & Guilick, J. (2008). Security considerations in the system development life cycle. Available at. http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf Retrieved February 04 2010.

Korhonen, I., Paavilainen, P., & Särelä, A. (2003). *Application of ubiquitous computing technologies for support of independent living of the elderly in real life settings.* Ubicomp.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, *41*, 597–607.

Kovach, K., & Cathcart, C. (1999). Human resource information systems (HRIS): Providing business with rapid data access, information exchange and strategic advantage. *Public Personnel Management*, *28*, 275–282.

Kovach, K., Hughes, A., Fagan, P., & Maggitti, P. (2002). Administrative and strategic advantages of HRIS. *Employment Relations Today*, *29*, 43–48.

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*, 4–13.

Lam, W. (2005). Investigating success factors in enterprise application integration: A case-driven analysis. *European Journal of Information Systems*, *14*, 175–187.

Lengnick-Hall, M., & Moritz, S. (2003). The impact of e-HR on the human resource management function. *Journal of Labor Research*, *24*, 365–379.

Listerman, R. A., & Romesberg, J. (2009). Are we safe yet? *Strategic Finance*, 27–33.

Mahoney, M. S. (2004). Finding a history for software engineering. *IEEE Annals of the History of Computing*, *26*, 8–19.

Maurice, E. (2009). SANS top 25 most dangerous coding errors. Available at. http://blogs.oracle.com/security/entry/sans_top_25_most_dangerous_cod Retrieved June 12 2011.

McGraw, G. (2004). Software security. *IEEE Security & Privacy*, *2*, 80–83.

Panko, R. (2010). *Corporate computer and network security* (2 ed.). Upper Saddle River, NJ: Prentice Hall.

Pauli, J. J., & Xu, D. (2005). Misuse case-based design and analysis of secure software architecture. *International Conference on Information Technology: Coding and Computing*, *Vol. 2*. (pp. 398–403): IEEE.

Peltier, T. R. (2005). *Information security risk analysis.* Boca Raton, FL.: Auerbach Publications.

Peterson, G. (2007). Security architecture blueprint. Available at. http://www.arctecgroup.net/pdf/ArctecSecurityArchitectureBlueprint.pdf Retrieved July 29 2011.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, *29*, 38–47.

Siponen, M., Baskerville, R., & Heikka, J. (2006). A design theory for secure information systems design methods. *Journal of the Association for Information Systems*, *7*, 725–770.

Smith, H. A., McKeen, J. D., & Staples, S. (2001). New developments in practice I: Risk management in information systems: Problems and potential. *Communications of the Association for Information Systems*, *7*, 1–29.

Spinellis, D., Kokolakis, S., & Gritzalis, S. (1999). Security requirements, risks and recommendations for small enterprise and home-office environments. *Information Management & Computer Security*, *7*, 121–128.

Spirig, J. E. (1991). The HRIS investment is cost effective in managing change. *Employment Relations Today*, *18*, 193–202.

Stallings, W., & Brown, L. (2008). *Computer security: Principles and practice.* Upper Saddle River, NJ: Pearson Prentice Hall.

Stine, K., Kissel, R., Barker, W. C., Lee, A., & Fahlsing, J. (2008). Volume II: Appendices to guide for mapping types of information and information systems to security categories. Available at. http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf Retrieved May 25 2011.

Stone, D., & Lukaszewski, K. (2009). An expanded model of the factors affecting the acceptance and effectiveness of electronic human resource management systems. *Human Resource Management Review*, *19*, 134–143.

Stone, D., Lukaszewski, K., & Isenhour, L. (2005). E-recruiting: Online strategies for attracting talent. In H. G. Gueutal, & D. Stone (Eds.), *The brave new world of eHR: Human resources management in the digital age* (pp. 22–53). San Francisco, CA: Jossey-Bass.

Stone, E., & Stone, D. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management*, *8*, 349–411.

Stone, D., & Stone-Romero, E. (1998). A multiple stakeholder model of privacy in organizations. In M. Schminke (Ed.), *Managerial ethics: Moral management of people and processes* (pp. 35–59). Mahwah, NJ: Erlbaum.

Stone, D., Stone-Romero, E., & Lukaszewski, K. (2003). The functional and dysfunctional consequences of human resource information technology for organizations and their employees. In D. Stone (Ed.), *The functional and dysfunctional consequences of human resource information technology for organizations and their employees* (pp. 37–68). Greenwich, CT: JAI Press.

Stone, D. L., Stone-Romero, E. F., & Lukaszewski, K. (2006). Factors affecting the acceptance and effectiveness of electronic human resource systems. *Human Resource Management Review*, *16*, 229–244.

Stone-Romero, E., Stone, D., & Hyatt, D. (2003). Personnel selection procedures and invasion of privacy. *Journal of Social Issues*, *59*, 343–368.

Strohmeier, S. (2007). Research in e-HRM: Review and implications. *Human Resource Management Review*, *17*, 19–37.

Strunk, J. D., Goodson, G. R., Scheinholtz, M. L., Soules, C. A. N., & Ganger, G. R. (2003). Self-securing storage: Protecting data in compromised systems. *Foundations of intrusion tolerant systems (OASIS'03)* (pp. 195).

Townsend, A., & Bennett, J. (2003). Privacy, technology, and conflict: emerging issues and action in workplace privacy. *Journal of Labor Research*, *24*, 195–205.

Varian, H. R. (2004). System reliability and free riding. In L. J. Camp, & S. Lewis (Eds.), *Economics of information security* (pp. 250). Norwell: Kluwer.

Ward, P., & Smith, C. L. (2002). The development of access control policies for information technology systems. *Computers & Security*, *21*, 356–371.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*, 101–105.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, *17*, 4–19.

Wheatman, J. (2010). Ten database activities enterprises need to monitor. Available at. http://www.gartner.com/DisplayDocument?id=1361013 Retrieved December 9 2010.

Whitman, M. E., & Mattod, H. J. (2004). *Management of information security.* Boston, MA USA: Thomson.

Whitman, M. E., & Mattord, H. J. (2006). *Principles of incident response and disaster recovery.* Boston, MA: Course Technology Press.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*, *Vol. 4*, Boston, MA: Course Technology.

Whitman, M. E., Mattord, H. J., Austin, R. D., & Holden, G. (2009). *Guide to firewalls and network security: With intrusion detection and VPNs* (2 ed.). Boston, MA: Course Technology.

Wong, Y., & Thite, M. (2009). Information security and privacy in HRIS. In M. Kavanagh, & T. Mohan (Eds.), *Human resource information systems: Basics, applications, and future directions* (1 ed.): Sage Publications.

Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems*, *24*, 557–596.

Zviran, M., & Haga, W. J. (1999). Password security: An empirical study. *Journal of Management Information Systems*, *15*, 161–185.