Information Security & Privacy in e-HRM

Shankar Subramaniyan, Mohan Thite & S Sampathkumar

Subramaniyan, S., Thite, M. & Sampathkumar, S. (2019) Information security & privacy in e-HRM. In M. Thite (Ed.). *e-HRM: Digital Approaches, Directions & Applications*, Abingdon, UK: Routledge. P. 250-267

Abstract

Fast changing technologies and increased sophistication in cyber-attacks have heightened the information security and privacy risks for all contemporary organizations. Research shows that security breaches are mainly internal and caused by ignorant and disgruntled employees. Since Human Resource manages employees from recruitment to separation and handles most sensitive personal data of employees in the organization, it plays a critical role in protecting information security and privacy. This chapter provides an overview of the basics of information security and privacy concepts and frameworks. It highlights the major roles Human Resource functionaries can play in designing, applying and monitoring appropriate controls throughout the employment cycle i.e. before, during and after employment to protect information security and privacy.

Learning Objectives

- Understand the critical importance of information security and privacy
- Describe the critical steps under the Information Security Management System
- Describe Privacy Principles and related statutory requirements

- Explain the critical role of HR in protecting information security and privacy, before, during and after employment

Introduction

“With a huge increase in the number of internet-connected devices, industry and governments are both waking up to the reality that much of what is already out there is unsecured and readily hackable.” Paula Januszkiewicz, CEO of CQUREAcademy.com

Consider this incident:

“Cybercriminals are posing as job applicants as part of a new campaign to infect victims in corporate human resources departments with GoldenEye ransomware …GoldenEye targets human resources departments in an effort to exploit the fact that HR employees must often open emails and attachments from unknown sources” (Palmer, 2017, p.1).

The incident highlights the vulnerability of HR departments to attacks on sensitive information held by them. Now consider the following incidents as reported by von Ogden (2016):

- At Snapchat, a social networking firm, an employee with criminal intent posed as CEO and sent an email to someone in the company’s payroll department, resulting in the release of protected information about employees.
- An employee of the City of Calgary in Canada accidentally leaked the personal information of employees while sending the information via email in the process of asking for technical assistance.

- An employee at Whitehead Nursing Home in Northern Ireland took home an unencrypted work laptop, which was stolen later in a home burglary and in the process exposed protected data on employees and patients.
- At Revenue and Customs department in Great Britain, two password-protected digital disks containing the details of every child and family in Great Britain subject to benefits payments were mailed by poorly trained junior employees to another government agency but never arrived.

What is common in these incidents? As von Ogden (2016, p. 1) reports,

> "In the past year, *77% of data breaches involved an insider,* according to Verizon. From disgruntled employees committing sabotage to innocent mistakes, humans are one of your organization's greatest information security risks. In fact, a shocking amount of high-profile data breaches in recent years have occurred because of employee behaviors".

Today, the mantra in management is to 'work anywhere, anytime, using any device in a 24/7 work environment'. With rapid changes in technology landscape, including Big Data, Cloud Computing, Social Media, use of personal devices for work purposes, outsourcing/offshoring of services, and daily release of new gadgets with weak security features, coupled with increasing sophistication in cyber-attacks, ensuring information security has become one of the most critical challenges for today's organizations. Organizations implement various information security measures to protect against cyber-attacks that include performing risk assessment, implementing information security framework and technologies to prevent, detect and protect against cyber risks and attacks.

But the most critical need in ensuring cyber security is to understand the nature and severity of threats in the first place. Cybercrime costs the global economy a staggering $450 billion every year and according to The Hiscox Cyber Readiness Report 2017, ‘53 percent of the companies assessed were ill-prepared to deal with an attack’ (Graham, 2017, p.1). Another study by McAfee revealed that that among companies experiencing data breaches, internal actors were responsible for 43% of data loss in 2014, half of which was intentional, and half accidental (von Fischer, 2015). The findings from both studies highlight the fact that organizations need to be vigilant of not only external cyber threats, but also the potential for trouble within their workforce.

When implementing information security measures, Human Resources (HR) function plays a critical role for two reasons. Firstly, HR is at the forefront of workforce planning, implementation and management. Given that a number of cyber security problems emerge due to the actions of an organization's own workforce, HR functionaries, alongside information technology (IT) professionals can play a crucial role in the fight against cybercrime at the workplace (GHRR, 2016). HR can implement effective security controls before, during and after employment to ensure people related security controls are in place.

Secondly, HR departments hold some of the most private, important and sensitive information. Privacy data is most sought after credit card data by cyber criminals in the ‘dark web’, a part of the World Wide Web that requires special software to access and where much of the illegal activities are supposed to take place. An HR database holds sensitive employee information such as bank details, date of birth, social security numbers, home addresses and many more. With skilled cyber criminals constantly looking for these sensitive data, HR becomes the main target for them. It also results in serious breach of privacy laws and regulations. Therefore, it is crucial that HR departments not only understand how to protect their own data, but also comply with various information security and privacy laws.

In this chapter, we explain why this topic merits the utmost attention of HR professionals dealing with technology and describe the concept, principles, and framework of information security and privacy. We also emphasize and explain how HR can play a pivotal role in partnering with IT to design, apply, enforce and monitor various control mechanisms in this regard.

Increasing Importance of Information Security

With fundamental changes in business models, technology trends, increasingly sophisticated cyber-attacks, followed by complex statutory regulations, information security and privacy have become critically important. What is more, as Morgan (2014, p. 2) states, 'the new rule for the future is going to be, "anything that can be connected, will be connected". This raises the frightening possibility of the information economy becoming extremely vulnerable to criminal mischief with individuals, firms, nations and the global economy having to pay a heavy price in the quest for a connected world.

Changing business models: With a view to 'do more with less', organizations are now moving towards outsourcing and collaborative models to improve the supply chain and cost efficiency. They are also increasingly adopting flexi workforce, crowd sourcing and Gig economy models that rely more on independent contractors and casualized workforce rather than permanent employees. These trends result in lack of visibility and control over what work is done, when, where and by whom which make enforcement of information security controls more and more difficult and challenging.

Rapid technology changes: Technology has rapidly evolved from Mainframe (one computer, many users) to Desktop Personal Computer (one computer, one user) and now to ubiquitous computing (one user, many computers). Now users can login from their phone, tablet or laptop and access the required application. More people, applications and smart devices are getting connected to the internet. This refers to the concept of the "Internet of Things" (IoT), a giant network connecting virtually any device at home or work to the internet, resulting in a 'relationship between people-people, people-things, and things-things' (Morgan, 2014, p.1). The IoT is expected to grow from 2 billion objects in 2006 to projected 200 billion by 2020 powered by 26 smart devices per every human on earth.

Some of the risks posed by new technologies, such as mobile, cloud and big data are:

1. Loss of control and visibility for the organization
2. Data Leakage or Loss
3. Increased risk with additional end points
4. Blurred data ownership due to personal and private usage
5. Volumes of data (Big Data) expose organizations to more risks
6. Harder to predict vulnerabilities in new technologies

Rising sophisticated cyber-attacks: Cyberattacks have evolved from worms and viruses to more advanced and organized attacks with the emergence of deception technologies. The rising number of attacks such as organized data intrusion, fraudulent use and theft of the information assets of organizations and government agencies together with theft of user credentials from a number of popular sites by “hacker” groups, in some cases instigated by state sponsored entities, are a major concern. Widespread attacks such as Ransomware exploiting zero day vulnerabilities and Distributed Denial of Service Attacks (DDoS) affect the organizations’ business operations and impact their profitability and revenue growth.

Increasingly complex regulations: Previously, information security regulations used to focus more on data protection like protecting financial data and intellectual property. But with recent concerns on privacy and national security, regulatory bodies are now focusing more on cyber disclosure and national security. The privacy definition, scope, data localization and breach notification requirements vary widely from one country or region to another. These varying laws and regulatory requirements pose challenges for multi-national organizations with a global network.

Information Security Management System (ISMS)

The primary *purpose/goals of information security* are “to protect Confidentiality, Integrity and Availability (CIA) of the information assets of the organization, in which

- Confidentiality refers to ensuring only the right people have access to the information
- Integrity refers to ensuring data is accurate and not modified, and
- Availability refers to ensuring the data is available for the right people at the right time, that is, when needed”.

Information Security Management System (ISMS) is the "management framework to initiate, implement and control information security within the organization". It typically follows the Plan-Do-Check-Act (PDCA) Cycle, that is,

- Plan: Define security policies & procedures
- Do: Implement and manage security controls/process
- Check: Review/audit security management and controls, and
- Act: Implement identified improvements, corrective/preventive actions.

Organizations follow various information security frameworks to protect their information security assets such as ISO/IEC 27000 family, COBIT (Control Objectives for Information and Related Technologies), and NIST (National Institute of Standards and Technology**)**. In this chapter, we have adopted the "*ISO/IEC 27001"* approach as stipulated by the International Organization for Standardization (ISO) as it is considered the best-known standard in providing requirements for an information security management system (ISMS). ISO defines ISMS as "a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process" (https://www.iso.org/isoiec-27001-information-security.html). An overview of ISMS is presented in Figure 15.1 and the steps involved are briefly described below.

Insert Figure 15.1 somewhere here

Security Requirements: ISMS starts with identifying the information security requirements for the organization. Every organization is unique with its own set of information assets, requirements and concerns. Security requirements are collected from the compliance and regulatory requirements applicable to the organization, contractual requirements and business requirements. One aslo needs to identify the stakeholders of the ISMS and the scope of the ISMS.

Security Policy & Governance: The security organization structure is important to drive and implement the ISMS across the organization. Hence defining the security organization and assigning the responsibilities is the foundation for the ISMS.

Asset Profiling: The key success factor of ISMS is through risk assessment and effective risk management. Risk assessment starts with asset identification which involves identifying all the information repositaries that need to be protected for running the business. Information with higher value needs more protection and information with lower value needs less protection. All assets in the company can be classified as:

- People Assets: Employees who are a part of the organisation
- Paper based Information Assets: Contracts, guidelines, company documentation, business results, HR records, purchase documents, invoices etc.
- Electronic Information: Databases, data files, system documentation, user manuals, training material, operational and support procedures, intellectual property, continuity plans, fallback arrangements etc.
- Hardware Assets: Computers, Servers, IT Networking equipments, storage devices etc.
- Software Assets: Application systems, databases, development tools, and utilities.
- Support Services/Equipment: Safes, rooms, furniture, AC plant, DG Sets etc.

Once the assets are identified , they are then classified according to their business criticality such as Public, Internal purpose, Confidential, High Confidential. These information assets need to be classified to indicate the degree of protection. The classification should result into appropriate information labeling to indicate whether it is sensitive or critical and what procedure is appropriate for copying, storing, transmitting or destruction of the information asset. Thus, asset identification and classification give the organization the necessary knowledge about "what to protect".

Risk Assessment: Risk Assessment and Risk Management deal with "how to protect". Risk assessment phase determines the risks associated with each asset for various threats and vulnerabilities. Threats are the external agents which could act to malicious effects. Some of the *types of threats* are Malware, hackers, attackers, BOTS (Internet robots, also known as spiders, crawlers, and web bots**)** etc. Vulnerabilities are the internal weakness in the system, such as unpatched system. When the Threat acts on the Vulnerability, it results in Risk.

All the possible threats need to be identified taking in to account the relevant vulnerability (eg. no virus threat for a paper based information). Different *categories of threats* are

- *Natural Causes*, such as flood, earthquakes and cyclonic storms
- *Man Made*, such as intrusions/hacking, virus attack, theft, operator error and deliberate destruction/sabotage
- *Emergencies*, such as civil strife/war, fire outbreaks, system crashes, disk failures, power outages, power glitches, communication link failure and network component failure

The impact of a threat should be described in terms of loss or degradation of any, or a combination of any of the three security goals: Confidentiality, Integrity and Availability. The impact can be measured by loss of system functionality, degradation of system response time, monetary losses, loss of public confidence, or unauthorized disclosure of data. Once the risk value is determined, risks are classified as High , Medium and Low risks to detemine the urgency and criticality of the actions to be taken to reduce the risks. High risks need immediate action.

Control Selection & Risk Treatment: If it is decided to mitigate the risks, then appropriate controls should be selected to mitigate the impact of the risks. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The various *types of Controls* are

- *Technical Controls:* Desktop secuiry, network security, encryption, identitfication, authentification etc
- Operational Controls: Physical access, Security Awareness Training, Personal security etc
- *Management controls:* Security policy & procedures, securty organizarion, risk management, audit etc.

Controls can also be classified, based on the *purpose*. For example, assume you would like to prvent the risk of unauthorized person accessing the system.

- *Preventive*: Prevents the risk before it occurs like ensuring strong Password policy to access the system.

- *Detective*: Detects the risk after it occurs like System Logs which catpture who accesed the system and when. By using System Log, one can identify if any unauthorized user accesed the system.
- *Corrective*: Corrects the risk after it occurs. For example, review the list of users to ensure only authorized persons have access to the system.
- *Compensating*: If any other types of controls can not be implemented, then it is recommeded to implement compensating controls. For example, if the application does not contain technical capability to configure strong password policy, then compensating controls can be more frequent user access review and log review to increase the oversight.
- *Deterrent:* Provides warnig or deterrent messages for the attacker like Log-on message before accessing the system.

Once the types and purpose of controls are determined the *Risk Treatment* begins. Risk Treatment involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls, considering the risks and the existing controls. Based on the value of the risk, organizations can decide to take the any of the following risk treatment methods:

- *Accept*: Accept the risk if the cost of treating the risk is more than the impact.
- *Avoid*: Avoid the risk by changing the process or technology or assets involved.
- *Mitigate*: Mitigate the risks by implementing the appropriate controls
- *Transfer*: Transfer the risks to other thrid party like insurance providers

Implement/Audit/Improve: After the controls are selected and implemented, they need to be continuously monitored and improved to increase the effctiveness of the controls. Periodic audits assist in finding any gaps and improving the effectiveness of controls. Third party validation by external auditors and Certifications like ISO27001 increase the credibility of the system protections adopted.

Benefits: Thus, Information Security Management System forms the backbone of information security infrastructure. The key benefits of implementing ISMS are

- Increases security awareness within the organization
- Enables identification of critical assets via the Business Risk Assessment
- Provides a framework for continuous improvement
- Boosts confidence internally as well as to external business partners
- Enhances the knowledge and awareness of security-related issues at the management level.

Privacy: Concept, Principles & Regulations

Information privacy is widely regarded as a fundamental human right in all democratic societies. Privacy comprises ethical, moral and legal dimensions. It is defined in many ways. For example, some view privacy as the “fundamental right to be left alone”. Others define privacy as the “right of an individual to be protected against intrusion into his personal life or affairs by direct physical means or by publication information”. According to Kovach, Tansey & Framinan (2000), privacy is “a human value consisting of four elements, namely,

- Solitude: The right to be alone without disturbances

- Anonymity: The right to have no public personal identity
- Intimacy: The right not to be monitored
- Reserve: The right to control one's personal information including the methods of dissemination of that information".

In general, data privacy can be defined as an "individual's expectation that one will use their personal data as intended and protect it from disclosure to unauthorized parties". Every organization has legal responsibility to protect their employees' and business partners' personal data.

Personal data are also called as *Personal Identity Information* (PII). It refers to "any information which can be used to identify, contact, or locate an individual, either directly or indirectly". Some of PII data is considered as the Sensitive Personal Data. Sensitive personal data is a subset of personal data which require special protection because they could cause harm to the individual if they are compromised. Examples of sensitive personal data include personal profile and contact information, bank account number, government identification (social security number or tax file number), information regarding the race, ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, sexual lifestyle or orientation, criminal checks and the medical history of a person, called PII Principal. The harm caused by unauthorized exposure of PII data could be financial, such as identity theft, or physical or psychological harm such as discrimination or criminal activity.

It is worth noting that some of the attributes may not be directly identifying an individual. But when they are combined, they can identify an individual. Whether a natural person is identifiable based on a combination of attributes might also be dependent on the specific domain. For instance, the combination of the attributes “male”, “25” and “manager” can be sufficient to identify a natural person within a particular company, but will often be insufficient to identify that natural person outside of that company. Also it is worth noting that confidentiality requirement of PII might vary from country to country. For example, criminal records are public information in the USA whereas it is confidential information in Europe.

In order to protect the PII, organizations implement *privacy framework*. As part of the framework, first they identify the privacy safeguarding requirements based on legal and regulatory requirements, contracts and business requirements. Some examples of legal requirements include data protection laws, consumer protection laws, breach notification laws, data retention laws, employment laws and relevant international laws affecting cross-border transfer of PII, some of which are described later in the section. Safeguarding requirements can relate to many different aspects of PII processing, e.g., the collection and retention of PII, the transfer of PII to third parties, the contractual relationship among PII controllers and PII processors, the international transfer of PII, etc.

Once the privacy requirements are identified, an organization should

- Develop Privacy principles based on established Standards, such as ISO29100.
- Conduct the Privacy risk assessment to identify the gaps
- Develop and implement specific Privacy controls based on Standards such as ISO27002 and ISO27018. Privacy controls include encryption of PII data, data masking, privacy awareness training, privacy notification process, etc.

Privacy Principles

Privacy principles are safeguards to be followed while collecting, using, storing, transferring or deleting the personal data. These privacy principles should be used to guide the design, development and implementation of privacy controls. Some of the common privacy principles are given below.

- *Consent and choice*: PII principals should be given an opportunity to choose how their PII is handled and to allow them to withdraw consent easily and free of charge. There are two types of consent and choice: "Opt-in" and "opt-out". Opt-in consent occurs when PII principal affirmatively and explicitly indicates his/her desire to have their data processed by the organization. Opt-out consent occurs when PII principal implicitly consents by not indicating their disapproval of requested processing. Opt-in consent is generally required for more intrusive processing like handling sensitive personal information, While opt-out consent is appropriate for less intrusive forms of processing like signing up for marketing emails.

- *Purpose legitimacy and specification*: Organization should have a legitimate reason to collect personal data and use it only for that purpose. The purpose for which personal data is collected should be specified at or before the time of data collection and subsequent use should be limited to the fulfilment of that purpose or compatible purpose.

- *Collection limitation*: There should be limits to the collection of PII data and any collected data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the PII principal.

- *Data minimization*: Collect only the minimum amount of personal data needed for the purpose. Data minimization is closely linked to the principle of “collection limitation” but goes further than that. While “collection limitation” refers to limited data being collected in relation to the specified purpose, “data minimization” strictly minimizes the processing of PII.

- *Use, retention and disclosure limitation*: PII data should not be used, retained or disclosed for the purpose other than those specified, except with the consent of the data subject or by authority of law.

- *Accuracy and quality*: Organizations that collect data should ensure that they are accurate, complete and up to date. This principle is particularly important in cases where the data could be used to grant or deny a significant benefit to the natural person (PII principal) or in which inaccurate data could otherwise result in significant harm to the natural person.

- *Openness, transparency and notice*: An organization should inform individuals what personal data are collected and why before they collect the data. They should make their privacy policies and practices relating to processing of PII easily accessible to PII principals. In order to be transparent, these policies and practices, including general information on the logic underlying the PII processing, can be made available to PII principles, particularly, if the processing involves a decision impacting the PII principal.

- *Individual participation and access*: Organizations should give individuals the ability to review their personal data and correct factual inaccuracies. Organization should apply appropriate controls to ensure that PII principals access strictly their own PII and not that of other PII principals.

- *Accountability*: The responsible unit or person in the organization (called the PII controller) should be accountable for effectively complying with measures adopted to implement the organization's privacy policies and procedures.

- *Security*: Organizations should protect personal data with adequate security and ensure that they address physical security and information security.

The World Information Technology and Services Alliance (WITSA) summarizes the key dimensions of privacy principles as detailed in Table 15.1 (WITSA, 2017).

Insert Table 15.1 somewhere here

Privacy Laws and Regulations

Different countries have various laws to address their unique privacy concerns. Some of them are given below.

- *USA*: While there is no single, comprehensive national law regulating the collection and use of personal data in the USA, a number of federal and state laws exist (Jolly, Loeb & Loeb, 2017), including, Health Insurance Portability and Accountability Act (HIPAA); Genetic Information Nondiscrimination Act (GINA); Fair Credit Reporting Act (FCRA); Gramm-Leach-Bliley Act (GLBA); Telemarketing Sales Rule (TSR); Electronic Communications Privacy Act; USA PATRIOT Act
- *Canada*: The Privacy Act; The Personal Information Protection and Electronic Documents Act (PIPEDA) (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/)

- *European Union (EU)*: General Data Protection Regulation (GDPR) which comes into effect from May, 2018 brings a new set of "digital rights" for EU citizens and provides for a harmonization of the data protection regulations throughout the EU
- *Australia*: Privacy Act, 1988

These Privacy laws typically incorporate the Privacy principles outlined above. For example, Australia's Privacy Act, 1988 specifies 13 Privacy Principles as listed in Table 15.2.

Insert Table 15.2 somewhere here

Since Human Resource Information System (HRIS) contains personal data, above requirements will also be applicable to HRIS applications. Hence HR team along with IT should review the above requirements and ensure their compliance. Meeting some of these requirements such as data subject access rights, right to have data erased, data portability, data anonymization, timely data breach notification and data deletion after the objective is met could be challenging in legacy applications (which refer to outdated computer systems) and might need major changes or upgrades.

Role of HR in Information Security & Privacy

Building awareness is the starting point for a stronger Information Security Culture. Human Resource Team plays a major role in building the security awareness and strong information security culture. Alert and well-trained employees who are aware of what to look for can prevent several major security breaches. Human errors, negligence and greed are responsible for most thefts, frauds or misuse of facilities. Various proactive measures that should be taken such as, background verification, confidentiality agreements, terms and conditions of employment, and information security education and training, are grouped under "Personnel Security" Domain. Human Resource team is involved in these safeguard measures/controls that apply to before, during and after employment as outlined below.

Before Employment

- *Background verification check*: At the time of recruitment, verification checks are performed to identify any potential fraud or malicious user. Verification checks vary based on the type of industry, role and responsibilities. Generally, they include reference check, confirmation of claimed academic and professional qualifications, independent identity checks, medical test, criminal background check etc.

- *Confidentiality / Non-Disclosure Agreement*: Confidentiality Agreement legally binds the employee/contractor from disclosing any company-owned confidential or proprietary information without appropriate approval to unauthorized persons. It is to be noted that confidentiality agreement binds the employees even after they leave the organization.

- *Declaration Form*: Declaration Form signed by all employees signify that all employees have read and understood the information security and privacy policy and will abide by the same.

- *Inclusion of information security in job responsibilities*: Information security is the responsibility of everyone. Hence general responsibility for implementing and maintaining security policy, responsibility for protection of assets and execution of specific security process or activities should be included in the job description and responsibilities.

During Employment

- *Security Awareness training*: Security Awareness training educates employees about the organization's security policy and procedures. Incident reporting process and guidelines on secure use of company resources are also covered in security awareness training so that employees are alert and perform their duty securely.
- *Security incident management and violation history*: The HR department plays the critical role in handling security incidents especially when it involves disgruntled employees. Any violations or incidents by the employees/contractors invites disciplinary action and HR is responsible for handling the disciplinary process and maintain the records for any future verification. e-HRM or HRIS plays a critical role in maintaining the records for compliance purpose.

After Employment

- *Clearance process to revoke user rights/ accounts during employee exit*: In the event of an employee leaving the organization due to resignation, termination or absconding, all associated access of the employee should be terminated and 'no dues clearance' process should be followed to recover any company owned assets.

Apart from these general controls, there are some specific controls required as part of regulatory and compliance requirements. These controls might vary based on the type of industry and compliance.

The security policy should be comprehensive enough to encompass ‘personnel, physical, procedural and technical’ aspects and should be specific to organizational environment and requirements. Verizon (2017, p. 7) advises organizations to “be vigilant; make people first line of defense; only keep data on a ‘need to know’ basis; apply security patches promptly; encrypt sensitive data; use two-factor authentication and don’t forget physical security”. Table 15.3 summarizes the key roles that IT and HR can play in mitigating data breaches and cyber security threats (GHRR, 2016, p. 3; Lewis, 2014).

Insert Table 15.3 somewhere here

Role of HR in Privacy

Generally, HR department handles PII data as part of various HR functions and processes in the organization such as recruitment and selection, performance management, health and wellness program, learning and development, payroll, and termination. While handling PII data, HR should ensure it is strictly handled as per the organization’s privacy policies and procedures. Any violation should be taken seriously and reported. Incidents such as misplacing a document, losing a laptop or mobile media, improperly sharing document or accidentally sending an email to wrong person—can result in privacy risks. Hence protecting the personal information form privacy risks is the responsibility of the organization. Privacy incidents could impact the reputation of the organization, customer trust and possible legal fines.

Generally, invasion of privacy in the workplace from unreasonable conduct by an employer includes

- *Intrusion into seclusion*: This occurs when an employer intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns. For example, conducting video surveillance in a locker room or rest room may constitute an intrusion into seclusion.

- *Public disclosure of privacy facts*: This occurs when an employer gives publicity to a matter concerning the private life of employee. Example would be an employer issuing a press release indicating a specific employee has a serious life threatening medical condition.

- *Portrayal in false light*: This occurs when an employer gives publicity to a matter which places the employee in a false or bad light. It is similar to defamation. While false light requires dissemination to the public at large, defamation may occur when the false statement is published to only a single third party. For example, terminated employees may file claims for defamation and/or false light over their employer release of information surrounding their termination.

Some of the key HR activities and processes where HR should be extremely cautious in adhering to organizational privacy policies and procedures to avoid any privacy incidents are given below.

- *Pre-employment practices*: It is critical that anti-discrimination practices are reviewed and prevented in job posting, pre-employment screening, test and interviewing process. As a best practice, the information obtained and requested through the pre-employment screening process should be limited to those essential for determining if a person is qualified for the job. Any inquiry or question should be justified by some business purpose and questions related to personal information should be avoided.

- *Monitoring and investigating the conduct of an employee*: Employers must be careful to protect the results of drug and alcohol tests and background screening results. They should use extreme discretion when disciplining employees for drug or alcohol related misconduct. Also they should know the applicable legal practices for monitoring telephone calls, email monitoring, video surveillance, intercepting wire or oral communications. An employer should inform employees of these surveillance and monitoring activities in advance and document the need for such surveillance.

- *Post termination activities*: Employers must ensure that any information provided about former employees, for example during reference checks or recommendations, are accurate and factual information to protect against defamation and /or false light claims by terminated employees. Other major concern is to protect the files and records related to former employees. Various data breach laws mandate that organizations are required to protect the personal information and notify the individuals affected by data breach.

The e-HRM System is best placed to protect the personal information and to ensure accuracy and validity of the information. It should have features to easily locate and provide the PII data so that access rights of the PII principles are ensured. The system should be enabled with adequate logging and monitoring to detect any data breaches and violations.

Summary

It is now well established that organizations everywhere and of all types and sizes are vulnerable to data breaches and the security threats are only going to increase and intensify as the digital economy becomes all pervasive. The commonly held perception is that the threats mostly originate from outsiders and that it is basically an IT issue. In this chapter, we have highlighted the critical importance of information security and privacy, described their key principles within the information security management system architecture and outlined the regulatory environment. We have also reinforced the key role that HR can play to secure the digital assets with people as the first line of defense and the measures that it can take before, during and after employment. Safeguarding information security and privacy is not a one off exercise but an ongoing effort aimed at continuous improvement where people treat data as seriously as money and make it a personal commitment.

Case Study: How Silly Mistakes Become Serious Problems

Sally is an HR Manager in a medium size IT company that provides software services. One day she was told that the company was expecting a major project from a key client and that the HR department needed to launch a major recruitment drive to hire 50 IT personnel within 3 months. Sally understood the urgency and importance of the task and immediately convened a meeting of HR personnel to initiate the hiring process, using employee referrals, walk-in interviews and university graduate recruitment.

Few days later, a senior project manager in charge of the new project called Sally to say that he personally knows and worked with a very good candidate with highly relevant experience. Sally said she will call him for an interview. But the project manager said he already interviewed the candidate and insisted that the candidate should be on boarded immediately since this candidate was earmarked for a critical lead role and the client was eager to meet key project members. Sally was initially hesitant to hasten the recruitment process but realizing the urgency of the matter she agreed to issue the appointment letter without back ground verification.

Since it was late evening, Sally decided to work on the offer letter from home. When she went home and logged into her office laptop, it had some technical issue and she could not login. She called her colleague in the office and shared her password and asked her to login to HR portal to generate the offer letter and email it to her personal email ID. Upon receiving the letter, she wanted to print it, sign and scan and send it to the candidate. Unfortunately, the printer at her home was not working.

So she uploaded letter from her personal laptop into the USB drive that she normally used for office work and went to nearby internet kiosk. She took the printout, signed the letter and then scanned and sent it to the candidate. She was happy that she finished her task quickly and supported the business effectively. She came home and forgot to bring the USB drive which had the offer letter and also other personal identity information (PII) about company employees. USB drive was neither encrypted nor password protected.

The next day she realized that she did not have the USB drive. She rushed to the internet kiosk only to find that somebody else had taken it. Sally did not think much about it and thought she will buy another USB. She did not report this to her company. The company found out few days later through an IT security agency that the information in the USB drive was uploaded to the dark web sites.

Case Study Questions

- List the mistakes that Sally made that resulted in data theft.
- What actions do you recommend to the company to prevent such occurrences in the future?

Debate: Is an Internal IT Auditor a Watchdog or a Blood Hound?

Introduction

Research shows that there is a significant confusion between auditors and stakeholders as to the former's role and contributions (Lenz, 2016). IT internal audits are performed to assess the effectiveness of the security measures implemented to protect the organization from cyber threats and to meet various compliance requirements. Auditors use various methods and techniques to make their assessment. These are typically long-drawn processes involving information gathering from a variety of sources. Some of these audit findings have very high visibility and impact in the organization when the reports are sent to external parties such as customers or regulatory bodies. One may argue that auditors are the watchdogs and they help us to improve the overall compliance of the organization by finding the gaps and areas of improvement. One may also argue that auditors are like blood hounds since audit objectives are not clear and they use biased or subjective methods, resulting in unnecessary harassment of employees.

Arguments in Favor of 'IT Auditor is a Watchdog'

- Audit helps to improve the overall effectiveness of the process and safety measures
- Audit boosts customer confidence and provides competitive advantage
- Auditors act as change agents and audit should be used as tool for improvement.

Arguments in Favor of 'IT Auditor is a Blood Hound'

- The value and relevance of internal audit are questioned by many and IT audit runs the risk of becoming a marginalized function (Lenz, 2016).

- Sometimes major audit findings result in disciplinary action and adversely affect the career of the auditee
- Audits can take lot of time and efforts
- Audits can sometimes be biased and subjective
- Sometimes audit documentations are too onerous, cumbersome and affect the productivity and flexibility of the process
- Auditors may not be transparent in the way they gather and interpret evidence

Useful References

- Cohen, F. (2006). Internal IT audit: Friend not foe. [Online] https://www.gartner.com/doc/1404981/internal-it-audit-friend-foe Accessed 12th January, 2018.
- Lenz, R. (2016). Internal Auditors as Change Agents: What a difference a year makes! [Online] http://www.kppsearch.com/news/the-open-auditor-edition-3/ Accessed 12th January, 2018
- Rojas, J. (2016). Auditors: Friends or foes. [Online] https://www.accountingtoday.com/news/auditors-friends-or-foes Accessed 12th January, 2018

Video Learning Resources

- HRIS Security: https://www.youtube.com/watch?v=4bkobskp8q0
- Human resource security requirements in ISO 27001 implementation:

https://www.youtube.com/watch?v=Z0hXiLm8X1c

- Audit of human resources and payroll:

  https://www.youtube.com/watch?v=fqfukGeRRdU

- Information security: Anish Bhimani at TEDxUConn 2013:

  https://www.youtube.com/watch?v=UPmVTPyE5DM

- Human Resources – Domain 5 – Information Security & Privacy Program:

  https://youtu.be/J2jHjA94CQ0

References

GHRR (2016). *The role of HR in mitigating cyber security threats*. GlobalHR Research. [Online] http://www.ghrr.com/the-role-of-hr-in-mitigating-cyber-security-threats/ Accessed 11th January, 2018.

Graham, L. (2017). *Cybercrime costs the global economy $450 billion: CEO*. [Online]. https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html Accessed 11th January, 2018.

Jolly, L., Loeb & Loeb. (2017). Data protection in the United States: overview. [Online]. https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 Accessed 12th January, 2018.

Kovach, K. A., Jordan, J., Tansey, K., & Framinan, E. (2000). The balance between employee privacy and employer interests. *Business and Society Review*, 105(2), 289-298.

Lewis, R. (2014). *What HR can do prevent data breaches and cyber threats*. [Online]. http://www.humanresourcesonline.net/hr-can-help-prevent-data-breaches-cyber-threats/ Accessed 11th January, 2018.

Morgan, J. (2014). *A simple explanation of 'The Internet of Things'*. [Online] https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#7c7255571d09. Accessed on 10th January, 2018.

Palmer, D. (2017). *This ransomware targets HR departments with fake job applications*. [Online] http://www.zdnet.com/article/this-ransomware-targets-hr-departments-with-fake-job-applications/ Accessed 9th January, 2018.

Verizon (2017). 2017 Data Breach Investigations Report. Executive Summary. [Online] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ Accessed 12th January, 2018.

von Fischer, S. (2015). *Data Exfiltration in Five Easy Pieces*. [Online]. http://vonfischer.com/blog/2015/12/07/data-exfiltration-in-five-easy-pieces/ Accessed 9th January, 2018

von Ogden (2016). *8 Examples of internal-caused data breaches*. [Online]. https://www.cimcor.com/blog/8-examples-of-insider-internal-caused-data-breaches

Accessed 9th January, 2018

WITSA (2017). *WITSA's statement of policy on privacy, security and data protection*. [Online] https://witsa.org/wp-content/uploads/2013/10/Privacy-Security-Data-Protection-final-1.pdf Accessed 11th January, 2018.

Table 15.1: Key Dimensions of Privacy Principles

Transparency	To ensure individuals have the right to be informed when their personal data is being collected, stored or processed.
Legitimate Purpose	Personal data can only be processed for specified explicit and legitimate purposes, and not processed further in a way incompatible with those purposes
Proportionality	Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which the data are collected.
Accuracy	The data must be accurate and, where necessary, maintained up to date, with inaccurate data removed or corrected; and destroyed when no longer needed.
Specificity	Data protection also incorporates the practice of collecting and retaining personal data for specific objective and specific period

Source: Adapted from WITSA, 2017

Table 15.2: Privacy Principles Listed in Australia’s Privacy Act, 1988

1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use or disclosure of personal information
7. Direct marketing
8. Cross-border disclosure of personal information
9. Adoption, use or disclosure of government related identifiers
10. Quality of personal information
11. Security of personal information
12. Access to personal information
13. Correction of personal information

Source: https://www.oaic.gov.au/resources/agencies-and-organisations/guides/app-quick-reference-tool.pdf

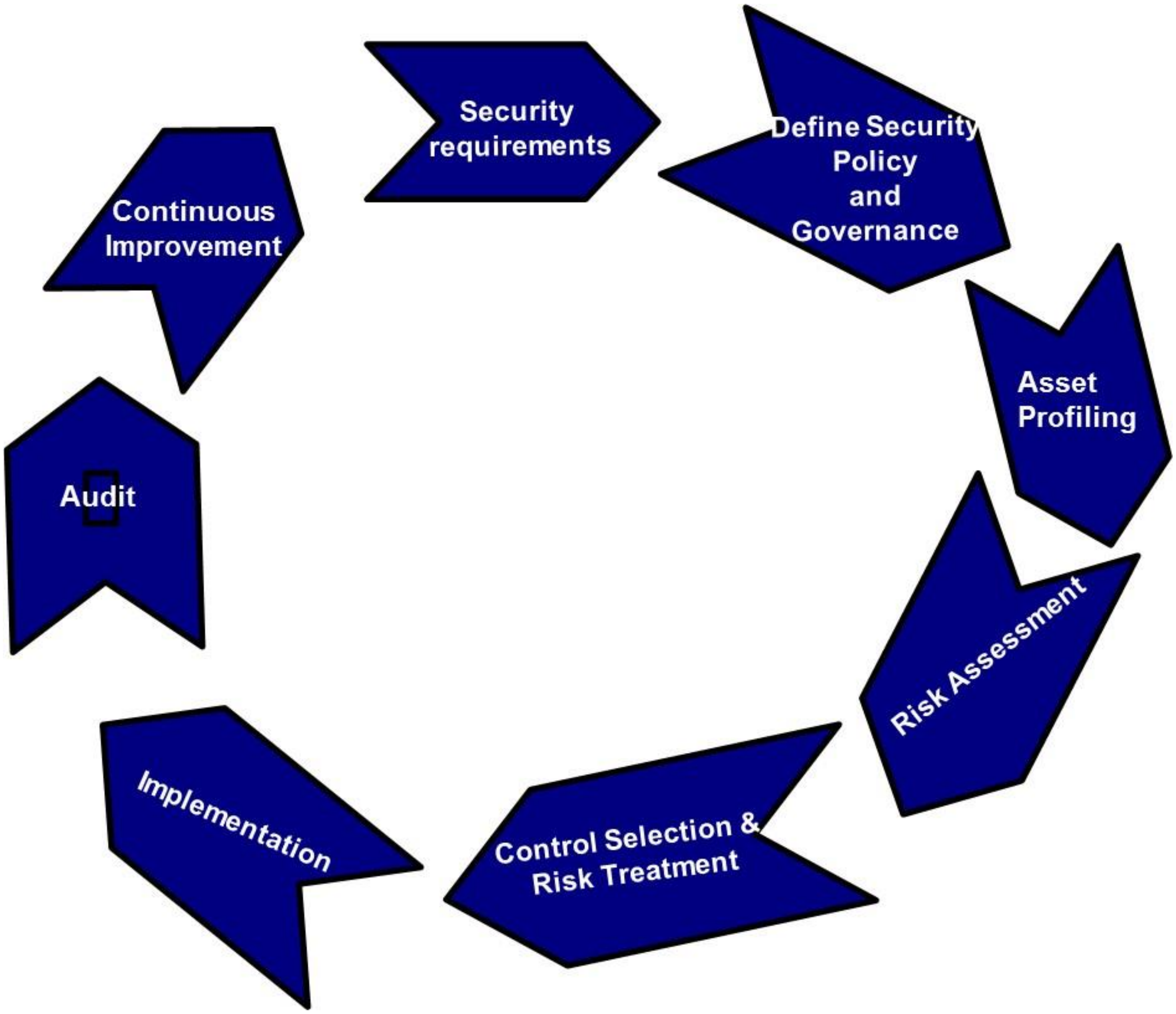
Table 15.3: Role of IT & HR in Mitigating Data Breaches & Cyber Security Threats

Know your Data	The first step in protecting organizational data is in knowing where it is, and who has access to it. Organizations should document and understand what and how data enters, stored, processed/modified, transmitted, used, shared and destroyed.
Info. Security & Privacy Policy & Guidelines	- It is critical for HR and IT to 'develop and disseminate' comprehensive and robust policies and guidelines on info. security and privacy. - They need to be periodically 'updated' in line with changing technologies, threats and regulatory requirements. - It is equally important to review the policies adopted by 'third-party providers' associated with the organization to make sure they are compliant and vigilant as well.
Top Management Support	The top management needs to walk the talk and make sure senior managers lead the way and act as role models to convince employees that the organization is dead serious about info. security and privacy matters
Staff Training	- Training all HR staff and employees on cyber security protocols is is one of the critical roles of HR. Cyber security training should be a central component of any on-boarding process, with new employees schooled in issues pertaining to accessing and using confidential data, alongside basic security training. There should also be a focus on email security, and learning to spot signs of potentially malicious activity. - The training programs should be held on an ongoing basis and made a 'mandatory component' of performance appraisal process.
Regular Audits	Conduct regular information security audits and publish anonymized results of audits. Seeing that policies are being enforced and policed can be a powerful deterrent.
Secure Digital Assets	- Physically secure IT equipment to immovable fixtures, and store sensitive assets — including paper documents — in a separate, secure area. - Apply patches supplied by vendors promptly.
Password Policies	- Ensure employees use strong (difficult to guess) passwords that are

	compulsorily changed periodically. - Where possible, use ‘two-factor authentication’ (e.g. password & one-time security code)
Encrypt Devices	While encryption won’t affect the chances of an asset going missing, it will protect the data it stores.
Back Up	Regular backups can prevent the loss of valuable data, reduce downtime, and help with forensics should you be breached
Review User Accounts	Having identified who has access to sensitive data, implement a process for revoking access when employees leave or change role
Former Employees	It is necessary to close the online accounts of any former employees as soon as possible because research shows that well over half of former employees have stolen confidential company data upon departing.
Disciplinary Actions	HR should stress the disciplinary repercussions, including termination, for employees that do not comply with security guidelines

Source: Adapted from GHRR, 2016; Lewis, 2014

Figure 15.1: Overview on ISMS (Information Security Management System)



Source: Authors