Top Information Security Concerns for HR Leaders & Process Participants

Last reviewed: June 2017

Related Resources:

- **Top Information Security Concerns for Campus Executives & Data Stewards**
- **Top Information Security Concerns for Researchers**

Top Information Security Concerns for HR Leaders & Process Participants – *Protecting Your HR Assets*

Do HR Leaders and HR Process Participants know:

1. What/Where is my data?
2. How sensitive is it?
3. Who's responsible for it?
4. Who has access to it?
5. Do I need to keep it?
6. What if it gets into the wrong hands?

The questions below can/should be asked by any organization; the answers, however, will vary. The examples provided after the questions are intended to stimulate thinking; not all examples will be relevant to all organizations.

1. What/Where is my data?

What are the HR processes used by my organization, and how is the data used?

a. What are the major HR processes (e.g. hiring, termination, payroll, benefits provisioning, pensions, FMLA, Workers Comp, pay reviews, performance appraisals, employee self-service, etc.)
b. Who are the process participants? (e.g. central HR, departmental HR staff, financial department, individual employees, etc.)
c. What data is now (or has ever been) included in each process? (e.g. SSN, bank account number, birth date, other personally identifiable information, demographic information, performance ratings, salary, emergency contact, home address, etc.)
d. For whom is "HR" data collected? (e.g. regular employees, retirees, students, temporary staff, contractors, spouses, dependents, etc.) Approximately how many individuals are represented in my HR systems?
e. Did my institution ever use SSN as employee id? If so, when did the transition to non-SSN id occur? (SSN is a favorite target of identity thieves, and is protected under all state data breach laws. Institutions that have relatively recently made such a transition need to remain vigilant about the data (paper and digital) that pre-dates the conversion).
f. How does the data flow through the process – who collects it? in what form/system? (don't overlook fax machines, copiers, multifunction devices, mobile devices, as well as downstream uses to manage multiple roles and levels of authorization for the institution's identity management system), where is it stored? (paper, central system, distributed Excel files, other business applications, etc.), how is it stored - e.g. is it encrypted? who can see it ? (central staff, departmental staff, etc.), when and how is it purged?
g. Who is responsible for maintaining the security of electronic files (e.g. central IT), and paper files (e.g. department administrators)?
h. What third parties participate in which processes, and how are they integrated? (e.g. bank direct deposit feeds, 401(k) feeds, outsourced HR system, etc.)

RESOURCES

- Asset and Data Management - Information Security Guide chapter

Top of page

2. How sensitive is it?

How sensitive is the HR data?

a. Does my institution have a data privacy and security policy and do I know what it is? Is there a group that oversees the institution's policy?
b. Which data elements have regulatory requirements for handling, storing and/or reporting, if data is potentially compromised? (Most states have data breach laws re: SSN and bank account information; HIPAA/HITECH rules may apply to health plan information or other medical records; FERPA applies to student educational records; other laws may protect individual's information such as medical leave, wage garnishment, etc. There may also be regulatory requirements regarding encrypting data - in motion or at rest)
c. Beyond regulatory requirements, what policies does my institution have regarding sensitivity? E.g., salary information is generally not protected under the law, but may be considered 'business confidential' at many institutions.
d. What are the consequences if sensitive data potentially gets into the wrong hands? Consult with Counsel re: state data breach laws and other regulatory requirements; consult with institute management if there is a breach of 'business confidential' information.
e. Do I know the legal and civil consequences of failing to protect the data or failing to follow the laws and policies regulating the data?
f. Are there personal consequences if data is not protected? (Check whether the employee handbook discusses disciplinary action, and/or whether there is a separate disciplinary schedule for data incidents. If the institution's handbook is sufficiently robust, then there may be no need to have a separate disciplinary policy for data protection infractions – the data handling policy could simply refer to the institution's standard disciplinary policy. Individuals regularly handling sensitive information may be asked to sign confidentiality statements upon accepting assignments.)
g. Do I appropriately mitigate the risk level of data under my responsibility? Do I have a risk mitigation plan? (e.g. eliminate SSN as a 'key' field; redesign processes to minimize the exposure of sensitive information; provide regular training; encrypt laptops; regularly run a PII discovery tool; etc.)
h. What are the responsibilities and risks associated with outsourcing to a third-party data for which I am responsible? Depending on the state and/or type of data, there may be regulatory requirements to consider in addition to good business practices.

RESOURCES

- Data Classification Toolkit
- Risk Management Framework

Top of page

3. Who's responsible for it?

Who's responsible for the security of information (i.e., who collects, handles, stores, or destroys HR information)?

a. Does my institution have a group or groups responsible for information security and/or awareness training. Are there clearly defined roles and responsibilities for securing information during all phases of the data lifecycle (acquiring, using, storing, destroying)?
b. Do those handling/using the data have ready access to information (training, policies, procedures) and tools so that they understand how to protect data? It can be particularly effective to incorporate data sensitivity training in the training for the business process – e.g., "protecting SSN" as part of the HR training for setting up a new hire. Some institutions have professional development teams that can be particularly helpful in getting these 'inserts' implemented.
c. What is my role and responsibility for information and how do I communicate that to employees in my department as well as any institutional user of HR data?
d. How do I ensure the data protection policies of my institution are being followed?
e. Whom may I rely on for assistance outside of my organization and how do I contact them? E.g. Chief Information Officer, General Counsel, Chief Information Security Officer, Compliance Officer, etc.

RESOURCES

- Security Program Development - Information Security Guide chapter

Top of page

4. Who has access to it?

a. Do only those with a business need have access to the data? This requires knowing who needs to see what, and having the tools/procedures to map roles to individuals. For people regularly handling HR data, it may be appropriate to do background checks before hiring, and to ask all personnel (including temps) to sign confidentiality statements before they are granted access.
b. Are they authorized, documented and tracked? If possible, tools should be put in place to monitor key controls, such as logging all attempts to access systems/databases, verifying whether anti-virus software is being updated, and laptops are encrypted.
c. Are authorization records periodically reviewed? At a minimum, there should be annual reviews.
d. Do transition procedures (e.g., new hire, position changes, departure) include steps to update authorization records promptly? Don't overlook temporary employees, IT contractors, etc. It is useful to also have standards for hard drive clean-up and data turnover when someone exits a position. The departure process may also include the return of any assets (physical or digital) that were held by the individual and reminding the individual that confidentiality expectations continue. It may be appropriate to have individuals sign a short affirmation that all assets have been returned, and confidentiality will be maintained.
e. Have information (e.g. training, policies, procedures) and tools been made available to users so that they understand how to protect data? Some institutions will mandate training as part of the approval process to get authorization to access systems/databases. Training may also address the typical security issues, such as crackable passwords, careless management of a laptop or flashdrives, or phishing and other social engineering ploys. Consider providing tools for password management, data destruction and tips when traveling.
f. Do those with access to data know where to find information about how to protect it?

RESOURCES

- Identity and Access Management - Information Security Guide chapter
- Organizational Security Awareness - Information Security Guide chapter

Top of page

5. Do I need to keep it?

a. How long is the institution required to keep each type of record? Does my institution have a retention schedule for HR records? (e.g. many HR records have federal or state requirements, and the retention rules have been known to change over time.)
b. What are the benefits of keeping the data longer than required by law and do the benefits outweigh the costs and risks?
c. Do I know my institution's procedures for secure disposal of paper, electronic files, and equipment (faxes, copiers, computers) used by HR process?

RESOURCES

- Electronic Records Management Toolkit

Top of page

6. What if it gets into the wrong hands?

a. Do I know how to recognize a potential data compromise, data exposure, or data loss? (e.g. lost laptop; unauthorized access to electronic records; paper records disposed of via regular trash, file inadvertently posted on public Internet and indexed by search engines, etc.)
b. Do I know what my institution's procedures are to address data incidents and who to notify? (e.g., data incident response team, which should minimally include IT, Legal, and Public Relations resources; how and when law enforcement is engaged; when are forensics required; who determines what regulations/requirements are relevant - PCI, state laws, HIPAA, FERPA, etc.)

RESOURCES

- Data Incident Notification Toolkit
- Incident Management and Response - Information Security Guide chapter

Top of page

Questions or comments? Contact us.

Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0).