COMPLIANCE IN THE CLOUD FOR HR DATA

Introduction

The landscape regarding protecting sensitive data – such as the data managed by Human Resources organizations – is changing.

The advent of the Software-as-a-Service model for Human Resources Information Systems (HRIS) has meant that the data has moved to "the cloud", a term referring to an outsourced datacenter managed by someone outside your organization.

With that comes a plethora of regulatory and legal considerations, as well as technical jargon in which we must familiarize ourselves. This document shall address key considerations and technologies important to protect your data.

> …What is new with the coming of the cloud is the *discontinuation of services to which people have entrusted a lot of personal or otherwise important data* – and in many cases devoted a lot of time to creating and organizing that data. As businesses ratchet up their use of cloud services, they're going to struggle with similar problems, sometimes on a much greater scale. It's the *price we pay for the convenience of centralized apps and databases*.
>
> – **Nick Carr,** author of *Does IT Matter?*, *The Big Switch* and *The Shallows*

I don't need a hard disk in my computer if I can get to the server faster... Carrying around these non-connected computers is byzantine by comparision

- Steve Jobs

THE CLOUD IS HERE AND IT'S HERE TO STAY

The Reality is Our Data Has Moved

Cloud computing has been a transformation shift in the way enterprises store and manage their data. Business applications that previously were housed in on-premise databases and servers have since moved to the cloud.

Human Resources Information Systems are no exception. We as HR and IT professionals are not faced with the reality that much of the most-sensitive, and most-personal data in our stewardship is in fact stored on someone's else's infrastructure.

We are made to trust these disparate cloud vendor's care of our data, protected by several Service Level Agreements (SLAs) and our own knowledge and understanding of the solutions themselves. Here we will discuss the important topics we need to understand in order to be aware of how data is stored and protected in the cloud.

Who's Now Responsible?

The reality is that the protection of this sensitive personnel data falls between the custody of two enterprise groups; Human Resources and Information Technology.

Each has their own specialty areas of expertise and each has a job to do to achieve the greater goal. Both groups, however, must start by understanding the concepts of data protection and compliance in order to adequately understand solutions to these issues.

Mistakes are expensive.

$5.5 billion

Average cost per security and privacy regulation breach for a company

Report “2011 Cost of Data Breach Study: United States”, Ponemon Institute, March 2012

$52,000 - $87,000

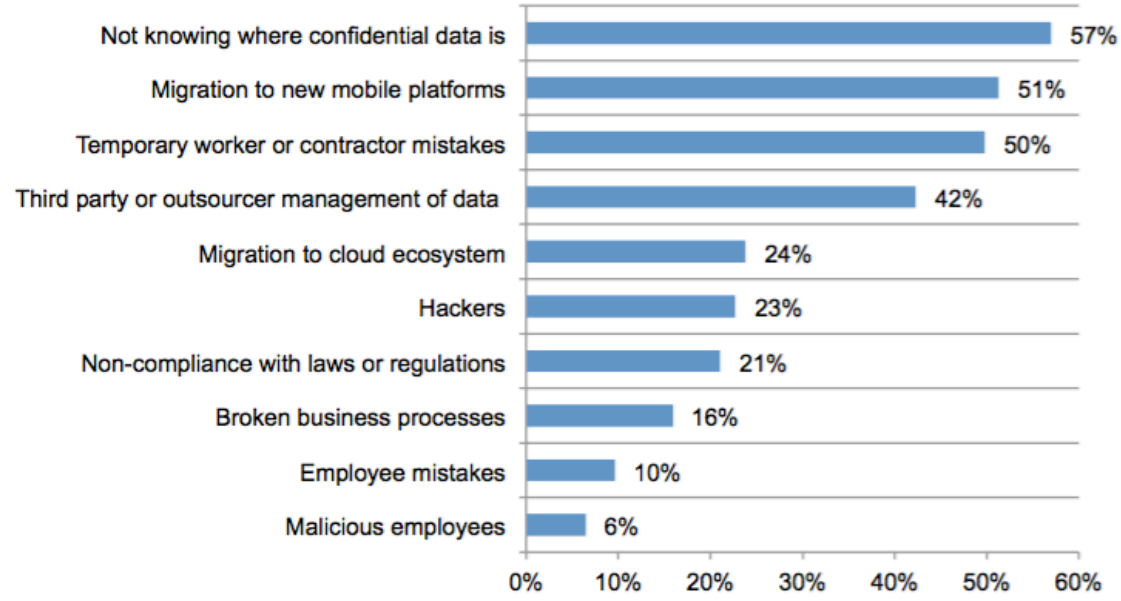
The forecasted average financial loss for a breach of 1,000 records

Report “2015 Data Breach Investigations Report” Published 2015 available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach- investigations-report-2016-ebk_en_xg.pdf

Many employees are unaware where their data resides.

Results from a survey of 1,587 Global IT and IT security practitioners in 16 countries

Figure 1. What keeps you up at night?
Three responses permitted



Report "The State of Data Centric Security", Ponemon Institute, June 2014

What you need to know.

DATA AT PLAY

Various governmental policies have standardized data protection and security, creating a new category of data that must be protected: Personally Identifiable Information (PII). PII is any information that can be used to identify, locate, or contact an individual. This includes:

- Birthdates
- Social Security Numbers
- Driver's License
- I-9 verification data (Passport number, etc.)
- Salary data

Such information is loaded into enterprise systems during the onboarding process of its employees or as it gains new customers. If this information is not stored or protected correctly, there can be significant damage done to the individuals, like identity theft, if the system is ever invaded. Breaches that result in data loss also have significant consequences for the enterprise as well, including heavy fines. However, having stringent data protection policies in place throughout the enterprise can present a strong shield against such attacks. This prevents the sensitive, unnecessary data from ever being stored or retrievable.

COMPLIANCE FACTORS

SOX

Sarbanes-Oxley Act

SOX was passed to provide greater transparency to public company stockholders about financial and operational events in the company. It required enterprise changes to comply with new standards, many of which involved HR to implement and streamline.

HIPPA

Health Insurance Portability and Accountability Act

HIPPA was created to standardize and protect how health care information is handled. HIPPA's Security Rule and Privacy Rule implements guidelines for the handling of protected health information (PHI).

Public Data Breaches

As data increasingly gets stored on computers and clouds, the number of public data breaches have increased due to poor implementation or lack of proper data security policies. These include procedures not just for IT, but also HR.

DATA PROTECTION PROCESS CONCEPTS

CIA TRIAD

The CIA Triad is the security professional's acronym for policy creation.

- ***Confidentiality***: Data is only available to the users it pertains to
- ***Integrity***: Data remains authentic and accurate
- ***Availability***: Data is accessible when needed

ACL

Access Control Lists

ACLs specify permissions to a database or the software that interacts with a database. They define who is able to access objects and what they can do to those objects, such as read, update, delete, or create data.

SLA

Service Level Agreements

SLAs are formalized contracts between a provider and a customer, that specify terms of a service. This could include guarantees from the provider, such as Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) and consequences of violations.

DATA PROTECTION TECHNOLOGY CONCEPTS

MASKING

Allows you to either hide or remove portions of the data, when it is either put into or taken out of the database. There are different ways to mask the data.

You can mask all the data or a specific part of the data.

Masking can remove the data, replace it with something else, or replace it with a token.

GENERATING

Allows database developers and testers to populate the database with random sample data.

This ensure everything is working as expected, and is critical for quality assurance purposes of database security techniques.

SCRAMBLING

Sometimes data must be changed in the database. This often happens when you transfer data between databases.

This gives you data that is realistic to use, but not the same as actual user data.

ACTIONS YOU MUST TAKE

Now that you're aware of the issues, how can you as an HR professional mitigate risks to your organizations?

CHOOSE WISELY

When selecting a cloud platform to store your sensitive data, ensure it meets these criteria:

- Offers user access based on contextual Role-based security
- Offers the ability to define and refine ACLs for maximum protection
- Supports both encryption at rest and in flight
- Provides transparent and acceptable SLAs
- Allows customization and extensibility to maintain compliance as new regulations are introduced

KNOW YOUR SLAs

Service Level Agreements are the process protections in place to protect data:

- **Availability** – Defines what percentage of time you can access a service. This is generally measured in percentages, and should exceed 99%. 99.9% - or "three nines"- uptime per month means that should the service be down more than 43.8 minutes per month, the SLA would be breached.
- **Response Time** – When you contact your cloud provider, how long does it take them to acknowledge your incident? That target is their Response time. Generally, this should be measured in hours and be less than 1 business day.
- **Resolution Time** – If you have a legitimate incident with your cloud provider, what is the target time they provide to solve it? That target is their Resolution time. This may range, but the fewer days the better.
- **Work Hours** – Does your cloud provider offer support 24/7/365? Or do they work 9am-5pm on weekdays? This is the calendar time that the SLA clock is measured against. Make sure it's defined, and includes any holidays or periods with degraded service.
- **Response Time Objective (RTO)** – If the cloud service does go down, how long until service is restored? The time it should take is defined using this metric.
- **Response Point Objective (RPO)** - If your cloud service crashes and needs to be restored, how old is the restore point? This refers to the age of the backup used in the event a recovery is needed. Depending on the velocity of your data, this should be an hour or less.
- **Operating Level Agreements (OLAs) and Underpinning Agreements** – You may see these terms. OLAs are like SLAs, but internal to a company between different business groups. Underpinning Agreements refer to foundational services, such as building electricity and Internet backbone access.

UNDERSTAND YOUR DATA

- **What is the authoritative source of all data?** The same data is copied and appears in numerous places, such as an employee's address. What system serves as the "system of record"?
- **Which data is sensitive?** Take an inventory of which fields of data are sensitive and document that in a data dictionary. You can't protect, what you don't know about.
- **Audit your data:** Do you have a process in place to identify missing or incorrect data in your systems? Do you follow Governance, Risk, and Compliance (GRC) best-practices? Are your audits performed internally, or by a 3rd-party?
- **Corrective Actions and Preventative Actions (CAPA)** Mistakes happen. What do you do then? Do you have defined corrective actions and preventative actions in place?

INVOLVE ALL STAKEHOLDERS

- **IT** will co-own any HRIS along with **HR**. Ensure both teams have a process to communicate and jointly resolve issues.
- **Legal** will be responsible for determining policy on how to respond to new requirements and regulations. Ensure periodic reviews and audits are in place.
- A corporate **training team** should be utilized to explain to the business acceptable data policies and usage.
- Buy-in and support from **senior management** is critical for success.

Infographic.

Data Tools

Enterprise data is subject to many standards that require stringent data protection policies to be in place and followed throughout the enterprise. **Data Tools: Data Masker, Generator, Scrambler**, helps implement the rules for you so you don't have to worry about liabilities.

Data Scrambling

Change production data when migrating between production databases so administrators can run tests without using or altering sensitive data. This way, bugs can be fixed in a secure manner.

Data Masking

Hide or remove portions of data with the Data Masker. When people enter unwanted data into the system, like social security numbers and other types of PII, Data Masker hides some or all of the information so it isn't ever entered into the system.

Data Generation

Automatically populate the sub-production database with realistic sample data. This helps testers and administrators ensure that everything in the database is working as expected.

Conclusion

Stringent data protection policies must be put in place throughout the enterprise to present a strong shield against attacks. Data masking, scrambling and generating are important and effective methods to protect sensitive data.

Protect your data.

Evaluate possible cloud vendors before storing data with them, make sure SLAs are in place, utilize all resources within your enterprise to their full potential, and make sure you understand how your data works.


STAVE
For more resources on cloud data protection and other topics, visit:
learn.staveapps.com
You Tube