HUMAN RESOURCES' ROLE IN DATA SECURITY

HOW PROPERLY ASSESSING HCM CLOUD VENDORS AND DRIVING EMPLOYEE AWARENESS CAN HELP HR PROTECT DATA FROM COSTLY BREACHES

InfinityHR

One System. Infinite Possibilities.

Table of Contents

Human Resources’ Role in Data Security

Data breaches are an unfortunate reality of our digital lives. It seems that every month **headlines of massive breaches blare** across our news feeds: from 53-million Home Depot user accounts compromised in September 2014 to 1-billion Yahoo user accounts in December 2016. These large numbers belie the threat faced by smaller businesses, as they may not have the infrastructure to properly secure data or bounce back from a costly cyberattack. Therefore, it is vital for Human Resources to become actively involved in data security through choosing the right cloud vendors to partner with as well as driving employee awareness around data security.

Data Security is an HR Responsibility

Technology has helped us work better, faster, and smarter, but it has also led to an unprecedented vulnerability at all levels of data. These threats are further compounded by changes in the workplace, as more employees work from home, rely on their own mobile devices, and increasingly use cloud-based systems. With the click of a mouse by an unaware employee, companies stand to lose control over customer, employee, and business data.

As a result, the number of U.S. data breaches hit an all-time high of 1,093 in 2016, according to **Identity Theft Resource Center (ITRC) and CyberScout**. Hacking/skimming/phishing attacks were the leading cause of data-breach incidents (55.5 percent). The second most common type of breaches (9.2 percent) involved accidental email/Internet exposure of information. Employee error was the third most common breach at 8.7 percent.

Some HR teams may wonder why data security is their concern rather than the sole purview of the IT department. The fact is that HR departments oversee a vast array of sensitive employee data, and it is their job to protect it. This data can include personally identifiable information, such as social security numbers, addresses, and open enrollment and benefits data. HR also holds the keys to information about compensation and payroll, as well as information about potential hires and employees leaving the company. A breach of this data could degrade employee morale and cause irreparable harm to a company.

What to Expect from a Cloud-Based Vendor

Employees and customers want on-demand access to their data on any device, which has exponentially increased threats to data security. Companies cannot keep up with this technological demand alone and have turned more to Human Capital Management Systems (HCM) in the cloud. It is, therefore, vital for HR professionals to know what cloud service they are using and how it can secure and protect important employee information.

The good news is that **cloud architectures have been built from the ground up** with a laser-focus on security. Many cloud systems have been built to deal with daily probes from the Internet and have agile designs that can react faster to threats than most traditional enterprise systems. Despite these advances, it is still imperative that HR teams vigorously assess cloud vendors and what they offer. The best cloud providers will include a number of extra features to protect data. This could include two-factor authentication that may send a user a code through a text message. Furthermore, good cloud vendors should be on the cutting edge of security practices, which should also include 24/7 support and state-of-the art security at their data centers. Attributes such as these can actually enhance a company’s data security when compared to a legacy, on-site enterprise system that may currently be in use.

Oracle points to a number of other expectations HR departments should have for a HCM cloud vendor. First, the vendor should be on solid financial ground to ensure longevity. In addition, a good cloud vendor will not mix your sensitive data with other customers’ data; your data should be isolated with security at multiple layers. Cloud vendors should also provide unified access controls that can help HR manage access and authorizations to certain areas of data. As a steward of employee data, HR teams must ensure that their cloud-based HCM is providing these basic measures and ask questions to make sure they know employee data will be safe.

HR Best Practices for Data Security

Despite the broad security strategies deployed by cloud-based HCM vendors, it is still the end-user—the employee—who truly holds the keys to security. Without their involvement, the best technical plan could still fail. Luckily, one of HR’s core functions is to manage people, and this skill can set the stage for helping to educate and train employees to be vigilant partners in data security. **This focus** can range from developing policies and procedures to educating the workforce and providing awareness training.

In terms of policy, HR can **limit access to information** based on roles and responsibilities, and also require authorization to make any changes. It is also important that HR departments have a disaster recovery plan in the event a breach does occur. This will help reduce the amount of time a company’s computer system is down and quickly re-secure data. In regard to awareness, employees need continuous education about security protocols, phishing scams, and password safety to further secure data. This effort should also start with new hires to ensure they are bought into this data-security mindset from day one. It is also important to break down inter-departmental walls to enhance continuous training. Marketing, IT, and HR may need to work closely to craft personalized communication strategies to understand where gaps in understanding may exist.

For HR, the awareness strategy may start with a **risk assessment** to understand root causes and how trainings should be different for various employees, especially in regards to their technological behavior. Information about employee behavior can aid in creating awareness campaigns. For example, Millennials are arguably the most plugged-in generation, and they may intuitively be seen as strong supporters of data security. However, they may have worse security habits of all generations. **A Softchoice survey** found that nearly 30 percent of 20-somethings left their passwords in plain sight; only 10.8 percent of Baby Boomers did the same. They are also more likely to store passwords on shared drives and email work documents on personal accounts, despite being the most informed about the risks. In the end, all workers will likely choose personal efficiency over security and find ways around restrictive security controls.

Now is the Time to Start Securing HR Data

Cyberattacks can happen at alarming speeds, and data breaches can cause severe damage to companies. According to the **2016 Cost of Data Breach Study** from IBM and the Ponemon Institute, the 383 companies participating in the study had an average cost of $4 million per breach and the average per capita cost of a data breach was $221 in the United States. The monetary costs of data breaches may be staggering, but businesses also risk the loss of customers, reputation, and goodwill in the marketplace. These are difficult to get back. Given the high stakes involved with corporate data security and the speed at which hackers can attack, HR must be proactive and ensure data security through understanding what services cloud-based HCM can provide, how vendors protect important employee information, and how to drive employee awareness. This approach can help HR departments provide employees the flexibility they desire in today's interconnected workplace while also protecting their data from outside threats.

Infinity Software Solutions
9362 E Raintree Drive
Scottsdale, AZ 85260

Website: www.infinity-ss.com
Phone: 1-866-TRY-HRMS (1-866-879-4767)
Email: sales@infinity-ss.com