THE IMPORTANCE OF SAFE AND SECURE HCM SYSTEMS

PDS®
HCM
BUILT
FOR YOU

The Importance of Safe and Secure HCM Systems

Safe and secure HCM platforms are essential to organizational success. Research from Gartner identifies a 29% increase in the market for secure access service and that the primary concern of companies between now and 2027 will be the ability to provide secure work from any location, in person or remote.[1] Gartner also found that HCM software market grew 11.7% in 2022 and grew far faster in North America than any other region with 61% of that growth.[2] HR professionals need to leverage a safe and secure HCM platform and consider cyber security, employee data protection, and the need for accurate data to benefit for the future.

Introduction

In today's dynamic business landscape, safe and secure Human Capital Management (HCM) systems stand as the linchpin of organizational success. As we navigate an era of unprecedented digital transformation, the importance of safeguarding sensitive employee information cannot be overstated. Cybersecurity threats loom larger than ever, making it imperative for organizations to fortify their HCM platforms against potential breaches. Beyond compliance with data protection regulations, the assurance of a secure HCM system nurtures a culture of trust among employees. It signifies a commitment to their privacy, assuring them that their personal information is shielded from the ever-evolving threats in the digital realm. Moreover, a safe HCM system is not just a defensive measure but a proactive investment in operational resilience. It ensures the seamless functioning of HR processes, from payroll management to talent acquisition, fostering an environment where organizations can thrive, innovate, and adapt to the challenges of the future with confidence. A safe and secure HCM system is the bedrock upon which an organization can build its path to sustained success and employee well-being.

Cyber Security

With all the modern technological advancements in recent years, cybersecurity is shifting more frequently to accommodate, and businesses are using it to help drive better business outcomes. According to the State of Cybersecurity Resilience 2023 Report, 58% are applying strong cybersecurity operational practices and experiencing positive digital transformations as a result.[3] More than half the organizations revealed that they recognize the importance of security when making any sort of digital change. To increase the chances of a successful change, these three cybersecurity actions were taken:

- Before going live with any new digital solution cybersecurity controls must be required.
- Apply cybersecurity in each part of the implementation milestones.
- Make cybersecurity someone's role and responsibility throughout any digital transformation.

30% of respondents are showing that prioritizing cybersecurity is making a difference. These organizations are being called cyber transformers. They can align their cybersecurity programs to their business objectives. This makes them 18% more likely to have improved customer satisfaction and trust, as well as greater employee productivity.[4]

Security

According to the State of Security Report 2023, the IT leaders' biggest challenge to operational security is the increasing sophistication of threats and workload demands trapping their teams in "react mode".[5] 86% of organizations have relied on service providers to help close security skills gaps. This makes it particularly important to work with companies you trust so you can ensure the system you are using will not be a source of extra work and weakened security.

Cloud Vs. On-Premise HCM

With modern technology cloud adoption is becoming increasingly popular. HCM technology is especially important for any organization and there are various IT and security requirements that each option brings to the table.

On-Premise means the HCM system is located within an organization's physical office and hosted on-site. This means the software is installed on physical hardware owned by the organization. This gives the IT department control over all the security, data management, and configuration.

Cloud HCM means the software and servers are run over the internet and not stored locally on any physical equipment in the organization. This can be more cost effective, require less maintenance, but also poses more potential security risks.

Key Differences between On-Premise and Cloud for Software Purchases:

Condition	***On-Premise***	***Cloud***
Cost	Higher upfront investment for implementation	Minor upfront investment
Deployment	In-house resources required	Limited in-house requirements, third party
Security	Complete organizational control over security and data	Security provided by vendor
Flexibility & Scalability	Less flexible for scaling but more customizable	Limited customization options but easier for organizational growth and needs

With all the differences and benefits to both cloud and on- premise software systems, it is important to understand what your organization needs, and which one would provide the most benefits. Typically, companies with less IT support and smaller HR & payroll teams would lean towards cloud software as fewer in-house resources are required. Larger organizations with bigger IT and HR departments may choose to utilize on-premise systems as they have the capabilities to support it better and may prefer to keep their data on their own servers. Cloud adoption is on the rise, seeing a 45% year on year growth and is being used to boost business performance, drive strategic outcomes, and enable breakthrough innovation.[6]

PDS Perspective

PDS Vista Disaster Recovery Services

PDS offers our on-premise customers the same piece of mind that we provide our Cloud customers by offering PDS Vista Protect, a service to help protect their on-premise HCM investment in case a disaster occurs. Send your encrypted Vista database, at a frequency of your choice for safekeeping.

- If disaster strikes, PDS will enable your Vista system and environment so you can use and continue your HCM and payroll functions.
- PDS will restore and replicate everything subject to the last available backup.
- Periodic DR testing and verification will happen throughout our partnership to satisfy compliance needs.

Employee Data Protection

A key component in every HCM system is ensuring employee data is protected and abides by the country specific privacy laws that the organization operates in. It is crucial to protect employees and reduce the company's liability. In the end of 2022 alone, there were at least 15 million records exposed throughout the world due to data breaches, a 37% increase from the same period in 2020.[7]

In the ever-expanding digital landscape, the incorporation of multi-factor authentication (MFA) capabilities within HCM software emerges as a pivotal defense mechanism for organizations safeguarding their biggest asset—employee data. MFA provides an additional layer of protection beyond traditional password systems, requiring users to authenticate their identity through multiple verification steps. This might involve a combination of something known (like a password), something possessed (such as a mobile device), or something inherent (like a fingerprint). By necessitating multiple forms of verification, MFA significantly reduces the risk of unauthorized access, mitigating the common threat of password breaches.

What Data Needs Protecting?

Employee data protection refers to identifiable personal information on current and past employees and it covers the following:

Name, Address, Phone Number, Date of Birth, Social Security Number, Sex, Gender, Race, Banking Information, medical information, and any other identifying information.

Laws & Protections

There are a mix of federal and state regulations to keep in mind when collecting and storing employee records.

- ***The Health Insurance Portability and Accountability Act (HIPAA)*** - This law requires employers to ask employees for permission before seeking any of their health information from health care providers or benefits plans. HR professionals in the healthcare industry potentially have added layers of responsibility, ensuring HIPAA training is happening to remain compliant, as well as training for complaints regarding misuse of protected health information.[8]
- ***The Americans with Disabilities Act (ADA) -*** Employers may only ask disability-related questions or require medical exams only after a job offer has been made or when accommodating a worker's special needs. This information must be stored separately and includes limiting access to supervisors and any third parties.
- ***Fair Credit Reporting Act (FCRA) -*** Any use of credit reports or background checks in the hiring process must comply with the FCRA. Permission must be obtained from the employee before any check is conducted and all information obtained must be destroyed after it is no longer needed.
- ***State Protections for Social Security Numbers*** – Various states have passed laws on the protection of employee's social security numbers which means some limit the collection of it, others require limiting access to the numbers collected.
- ***Vendor Contract Mandates*** – Several states require organizations that share personal information with third party services providers obtain written assurances that all information collected will be safe.
- ***Breach Notification Laws*** – All 50 states, including certain cities, require a business to provide notice when there has been a breach of any personal information owned by the business.

- ***California Consumer Privacy Act (CCPA)*** - The CCPA grants consumers many rights concerning their confidential information, including:
  - What information is being collected and how it is being used
  - Correcting and deleting collected information
  - Opting out of data collection
  - Protection from discrimination for exercising these rights
  - Most for-profit organizations in California fall under the CCPA. If you are using a third-party service provider for your HCM system you will need a Data Processing Agreement (DPA).[9]

It is Important to Take a Few Steps to Ensure the Security of your Employee Data:

1. Know the Laws and Regulations

Knowing all the different laws and mandates that your organization operates in is key to understanding how you need to protect any collected employee information.

2. Privacy Policies

Create policies that cover all the data you are collecting to ensure everything is protected such as limiting employees access to data, data encryption, and secure physical devices for information storage.

3. Training

Make sure all employees are trained in what they can and cannot share about their organization. The new methods in cybercrime are constantly changing and any employee can become the target. It is important that they know to report suspicious emails, phone calls, and that there are safeguards in place.

- ***Actionable Employee Data***

  Your HCM system collects employee information everyday but is it collecting the right things? The need for accurate employee data is especially important for organizations today as it helps ensure accurate analytics to help drive better business outcomes. Here are a few ways to better manage it:

  - Consider your Data Sources & Standards – Before any information goes into your HCM system, make sure it is coming from the right sources. Check for relevancy, consistency, and make sure your sources are unbiased. As for data standards, ensure you are collecting information with the right data types and naming conventions to avoid confusion and inconsistency.

- Cleansing and Validation – Data cleansing involves checking and validating the data you collect every day and making sure you are getting complete and consistent data. This is where data adding, modification or deletion needs to happen. Next up is validating and ensuring you have the right data using various testing and quality check methods to be thorough.[10]

▶ *The Benefits of Accurate Employee Data*

Informed Decision-Making: Accurate data is the foundation for making informed decisions. HCM systems rely on precise information for tasks such as workforce planning, performance evaluations, and talent management. Inaccuracies can lead to flawed decision-making with potential negative consequences for the organization.

Strategic Planning: Organizations use HCM data to formulate strategic plans and policies. The accuracy of this data ensures that these plans are based on reliable insights, contributing to the long-term success and growth of the organization.

Enhanced Operational Efficiency: Accurate data streamlines HR processes. From payroll management to employee onboarding, having reliable data reduces errors, minimizes operational inefficiencies, and allows HR professionals to focus on strategic initiatives rather than fixing data discrepancies.

Conclusion

The landscape of Human Capital Management (HCM) is undergoing significant transformations, necessitating a vigilant approach to security, data protection, and information accuracy. The statistics from Gartner highlight the exponential growth in the HCM software market, with North America leading the charge. The State of Cybersecurity Resilience 2023 Report underlines the positive impact of robust cybersecurity practices, with organizations recognizing the importance of security in the digital realm.

The critical choice between cloud and on-premise HCM solutions requires a nuanced understanding of their respective advantages and challenges. While cloud solutions offer cost-effectiveness and scalability, on-premise solutions provide organizational control over security and data. The increasing sophistication of cyber threats, as identified in the State of Security Report 2023, emphasizes the need for strategic partnerships with trusted service providers.

Employee data protection, governed by a complex web of federal and state regulations, is a paramount consideration. Understanding laws such as HIPAA, ADA, FCRA, and CCPA is essential for organizations to avoid liabilities and protect sensitive employee information.

About PDS

PDS is a leading developer of HCM solutions that offer complete all-in-one HR and Payroll management through leveraged technologies and world-class client support services in the US, Canada, and the Caribbean. PDS' Vista encompasses recruiting, onboarding, HR, full benefits management, cross-border payroll capabilities, analytics, and more - fully designed with you in mind. PDS works to keep their community informed on all HCM-related issues that may affect the workplace. Contact their team of experts today and let them revolutionize the way you work.

Endnotes

1 Gartner Research. (2023). Forecast Analysis: Secure Access Service Edge, Worldwide. Forecast Analysis: Secure Access Service Edge, Worldwide (gartner.com)

2 Gartner Research (2023). Market Share Analysis: Human Capital Management Software, Worldwide, 2022. Market Share Analysis: Human Capital Management Software, Worldwide, 2022 (gartner.com)

3 State of Cybersecurity Report 2023 | Accenture pg.15

4 State of Cybersecurity Report 2023 | Accenture pg.13

5 The State of Security 2023 (splunk.com) pg.3

6 us-future-of-cloud-survey-report.pdf (deloitte.com) pg.3

7 Data records breached worldwide 2023 | Statista pg.3

8 Importance of Protecting Employee Information as Privacy and Cybersecurity Laws Proliferate - Jackson Lewis

9 California Consumer Privacy Act (CCPA)

10 How to Ensure HCM Data Accuracy for HR Consulting (linkedin.com)