# Cyber security challenges in human resource technology: protecting employee data in the digital age

**Prerna Srivastava[1]* and Kirti[1]**

[1] Assistant Professor, Department of Management, Integrated Academy of Management and Technology, Ghaziabad, Uttar Pradesh, India

*Corresponding Author: Prerna Srivastava

Received 11 Sep 2025; Accepted 1 Oct 2025; Published 4 Nov 2025

DOI: https://doi.org/10.64171/JSRD.4.S1.114-121

**Abstract**

In the age of digital revolution, Human Resource Technology (HRTech) has emerged as a key facilitator for organizations to automate hiring, on boarding, payroll, employee management, performance management, and workforce analytics. Yet, the growing adoption of digital platforms, cloud computing, and data-based decision- making in (HRM) brings along substantial cyber security threats. These are due to the private and sensitive nature of worker information, such as personally identifiable information (PII), financial data, health information, background reports, and performance histories, which make HR systems potential targets for cyber attackers, This review critically examines the integration of Artificial Intelligence (AI) into Human Resource (HR) systems and its implications for cyber security. As organizations accelerate their digital transformation journeys, HR systems are increasingly responsible for storing and managing large volumes of sensitive employee data, necessitating robust cyber security frameworks. The study focuses on identifying key cyber security risks, evaluating AI-based security solutions, and assessing their effectiveness in protecting employee information such as salaries, performance evaluations, and personal identifiers.

With the spread of remote work and mobile access to HR systems, endpoint security is now more difficult to control. Moreover, applications of artificial intelligence (AI) and machine learning (ML) in hiring and employee monitoring raise ethical issues and new attack surfaces, including algorithm manipulation and data poisoning.

Sources were chosen for relevance to AI use in HR systems, their contributions to cyber security, and empirical information regarding threats and countermeasures. The review points out the convergence of HR management and information security, listing primary challenges and best practices for protecting data in modern organizational environments.

Findings reveal that while AI significantly enhances anomaly detection and automates security responses, it simultaneously introduces new risks, including AI-driven attacks and algorithmic biases. Notable solutions include AI-enabled encryption, behavioral threat detection, and AI-powered security training simulations. The dual-edged nature of AI underscores the need for adaptive security frameworks that evolve alongside emerging technologies. For HR professionals, embracing AI-based security tools offers a proactive approach to data protection, but it also demands a re-evaluation of traditional cyber security strategies. The paper further recommends that policymakers consider stringent, AI-focused regulations to address the unique threats posed by intelligent systems. Ultimately, the study advocates for a forward-looking, aggressive cyber security strategy to ensure the resilience and trustworthiness of HR technologies.

The abstract also highlights the need to implement a strong cybersecurity practice within HRTech environments. This involves practices such as end-to-end encryption, multi-factor authentication, periodic vulnerability scans, access controls, employee training and awareness programs, and incident response planning. Strategic coordination between HR and IT functions is required to instill security culture and build HR systems resilient to adapting cyber threats.

In summary, while HR Tech provides operational efficiencies and enhanced decision-making, it also introduces significant cybersecurity threats that need to be addressed immediately and in the long run. Organizations need to consider cyber security as an essential aspect of HR technology adoption and governance to safeguard their employees' data, ensure trust, and preserve business continuity in a digital-first ecosystem.

**Keywords:** Data Privacy, Cyber security, HR Technology, Data Protection, AI in HR

## 1. Introduction

The digital evolution has significantly reshaped human resource management by introducing automated software and cloud-based systems capable of managing a wide range of administrative tasks, including payroll processing, benefits administration, recruitment, and performance appraisals. Collectively known as Human Resource Technology (HR Tech), these platforms have become ubiquitous across organizations of all sizes due to their user- friendliness, scalability, and cost-effectiveness.

Despite their advantages, HR Tech systems introduce a new layer of cyber security vulnerabilities, particularly in relation to the protection of personally identifiable information (PII). Employee records often contain sensitive data such as Social Security numbers, bank account details, medical records, and employment history. As a result, HR databases are frequently

targeted by cybercriminals seeking to exploit or monetize this information.

The increasing reliance on digital HR infrastructure raises serious concerns about data integrity, confidentiality, and compliance with global data protection regulations. Ensuring the security of HR systems is not only a matter of technical necessity but also a legal and ethical obligation.

This research paper examines the most critical cyber security threats facing HR Tech platforms, explores the regulatory landscape, and presents a set of best practices and technical countermeasures to mitigate risk. The goal is to provide human resource professionals, IT security leaders, and organizational stakeholders with the insights needed to protect employee data in an increasingly digital and interconnected environment.

**Purpose of the study**

The aim of this research is to perform a thorough examination of the current cyber security environment, focusing especially on the discovery of threats and the formulation of effective defense mechanism in the digital age. Through an analysis of recent trends, up –and-coming technologies, and tried-and-true-best practices, this research hopes to improve our current understanding of the issues of contemporary cyber security and offer viable solutions for mitigating risk and cyber threat protection.

## 2. Literature review

**Critical cyber risks in digital HR environments**

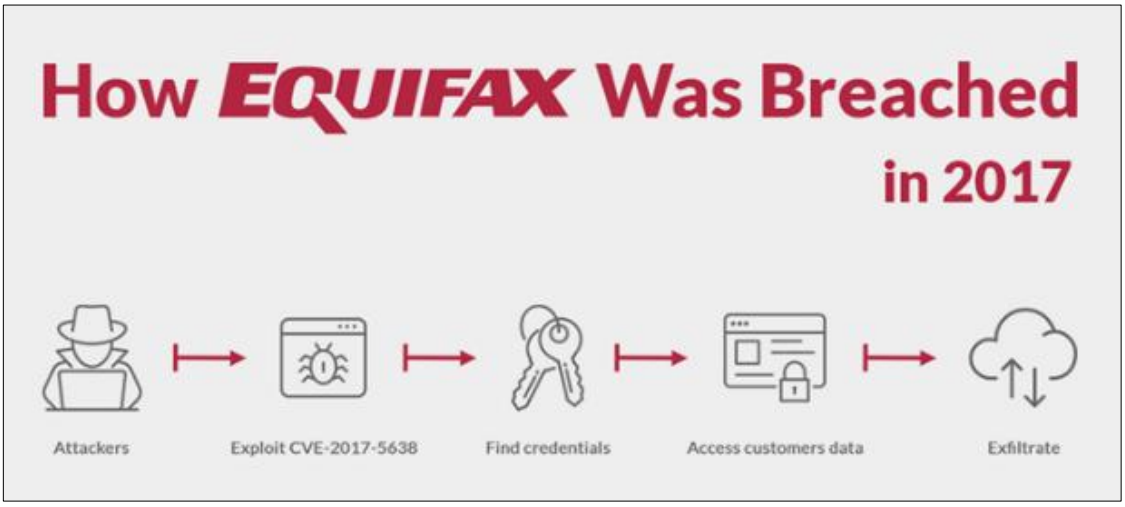
### 2.1 User-targeted threat vectors

Human resources personnel are frequent targets of phishing campaigns designed to manipulate them into disclosing confidential information or inadvertently granting unauthorized access to organizational systems. Cybercriminals often employ tactics such as impersonation emails, counterfeit job applications, and fraudulent W-2 requests. These methods exploit the trust inherent in HR communications and capitalize on the high-level access HR staff typically hold to sensitive employee data.

### 2.2 Breach of confidential HR records

One of the most critical threats facing Human Resource Technology (HR Tech) systems is the unauthorized access to sensitive employee data. Such incidents often result from sophisticated cyber attacks that exploit system vulnerabilities or user behavior. High-profile cases, such as the 2017 Equifax data breach, underscore the potentially severe consequences of such compromises—including identity theft, regulatory penalties, legal liability, and long- term reputational harm. These breaches demonstrate the urgency of implementing robust data protection measures within HR systems, particularly given the volume and sensitivity of personally identifiable information (PII) they contain.

One of the most critical threats facing Human Resource Technology (HR Tech) systems is the unauthorized access to sensitive employee data. Such incidents often result from sophisticated cyber attacks that exploit system vulnerabilities or user behavior. High-profile cases, such as the 2017 Equifax data breach, underscore the potentially severe consequences of such compromises—including identity theft, regulatory penalties, legal liability, and long- term reputational harm. These breaches demonstrate the urgency of implementing robust data protection measures within HR systems, particularly given the volume and sensitivity of personally identifiable information (PII) they contain.

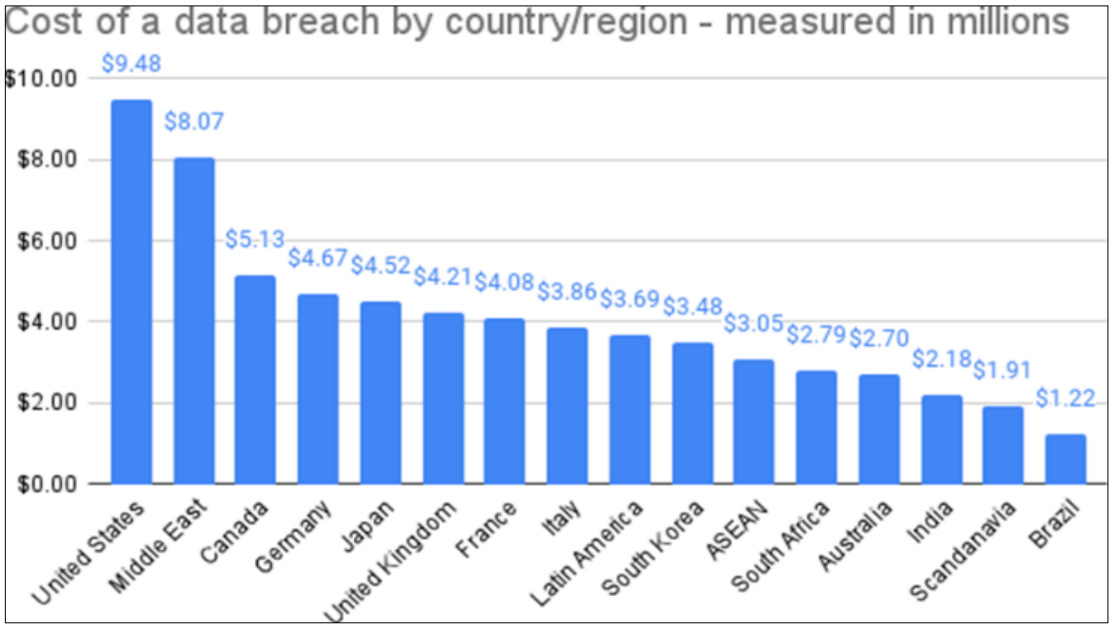



***Source:*** https://blog.0x7d0.dev/history/how-equifax-was-breached-in-2017/

**Fig 1**

### 2.3 Organizational insider vulnerabilities

Employees, contractors, and third-party vendors with authorized access to organizational systems can pose significant security risks, either through intentional misconduct or inadvertent actions. These internal actors may exploit their access privileges, leading to data leakage, policy violations, or system compromise. According to IBM's 2024 *Cost of a Data Breach Report*, insider-originated incidents account for approximately 22% of all data breaches in enterprise environments. Human Resource systems are particularly susceptible, given the elevated level of access they require and the volume of sensitive personal data they manage.




***Source:*** www.breachsense.com

**Fig 2**

### 2.4 Risks associated with external service providers

A significant portion of human resource operations is either outsourced or closely integrated with third-party service providers, including payroll processors, benefits administrators, and background screening firms. While these partnerships enhance efficiency and specialization, they also expand the organization's cyber security attack surface. A breach occurring at any point within the supply chain can lead to the compromise of sensitive employee data. The 2020 Solar Winds incident serves as a notable example, where attackers exploited a vulnerability in a third-party vendor to infiltrate multiple organizations, demonstrating the far-reaching implications of supply chain security failures.

### 2.5 Access control weaknesses

The absence or inadequate implementation of role-based access control (RBAC), multifactor authentication (MFA), and periodic account audits can lead to excessive privilege assignments, thereby significantly increasing the risk of unauthorized data exposure within HR systems.

## 3. Corporate compliance and regulatory obligations

Organizations must navigate a complex regulatory environment for employee data protection. Key regulations include:

- California Consumer Privacy Act (CCPA). This act grants employees the right to know what personal information is collected and how it is used.


***Source:*** https://databrackets.com/event/how-to-comply-with-california-consumer- privacy-act-draft/

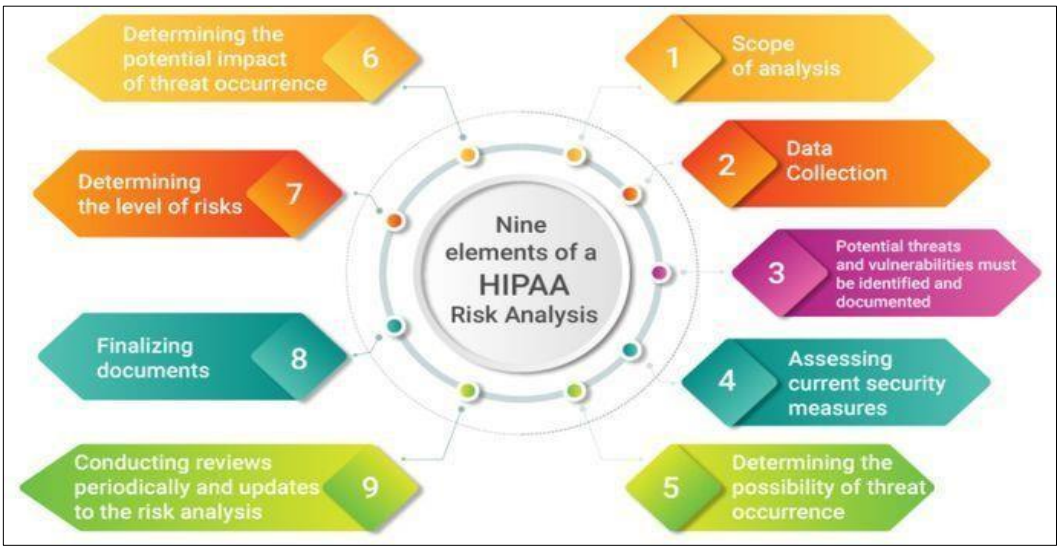
**Fig 3**

- General Data Protection Regulation (GDPR). This law enforces strict data handling, consent, and breach notification requirements for organizations that operate within or process data from the European Union.


***Source:*** https://gttb.com/compliance-regulatory-requirements/eu-general-data-protection- regulation-gdpr/

**Fig 4**

- ISO/IEC 27001 and SOC 2. These provide frameworks for information security management and auditing. Non-compliance can lead to significant financial penalties and damage to reputation.
- Health Insurance Portability and Accountability Act (HIPAA). This law regulates the handling of health-related employee data.




**Source:** https://www.pinterest.com/pin/9-elements-of-a-hipaa-risk-analysis-- 841539880370207746/

**Fig 5**

## 4. Cybersecurity innovations in human resource management

Human Resource Management (HRM) has become a data-heavy function. It handles large amounts of sensitive information, such as personal identification details, financial records, health data, and performance metrics. As companies speed up their digital transformation, securing HR systems has become a crucial issue. Cybersecurity innovations are vital for reducing risks, ensuring compliance with regulations, and maintaining employee trust.

- Artificial Intelligence (AI) for Threat Detection Modern HR systems are using Artificial Intelligence (AI) and Machine Learning (ML) more often to spot patterns that suggest security threats. These technologies can: - Detect unusual user behavior (e.g., odd login times or locations) – Send real-time alerts for unauthorized access attempts – Improve fraud prevention during hiring and payroll processing AI-driven cyber security tools speed up response times and improve accuracy in handling threats.
- Blockchain for Secure Recordkeeping Although still new, blockchain technology shows great potential in HR cyber security. It can: - Create tamper-proof employee records and credentials – Confirm the authenticity of education and employment histories – Secure HR transactions like contract signing and benefit distribution Blockchain's decentralized nature improves transparency and cuts the risk of data manipulation or insider attacks.
- Role-Based Access Control (RBAC) and Identity Management To stop unauthorized access to employee data, organizations use Role-Based Access Control (RBAC) systems. These systems ensure that users only see the information necessary for their jobs. When combined with Identity and Access Management (IAM) platforms, these tools allow for: - Centralized control over user permissions – Automatic removal of access when employees leave the organization – Integration with Multi-Factor Authentication (MFA) to strengthen login security
- Automated Compliance and Audit Tools Laws like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) require organizations to manage HR data responsibly. Cyber security tools now help automate compliance by: - Tracking data access and changes – Generating audit trails – Managing consent and data retention policies This cuts down on administrative tasks and helps HR departments comply with changing legal standards.
- Cloud-Based Security Solutions As HR functions move more to the cloud, organizations are adopting new cloud security solutions to protect data storage and transmission. These solutions include: - End-to-end encryption (e.g., AES-256, TLS 1.3) – Intrusion detection systems (IDS) – Cloud access security brokers (CASBs) that monitor data transfers between users and cloud platforms Cloud-native security tools provide scalability and real-time protection suited for modern HR processes.
- Security Awareness and Employee Training Platforms Cyber security innovation includes more than just technology; it also involves better employee training platforms. Interactive e-learning modules, phishing simulations, and gamified training sessions are commonly used to educate HR professionals and employees about security best practices. These tools help create a culture of cyber security awareness within the organization.

## 5. Expansion and operational capabilities

HRTech has also developed significantly with the emergence of Software as a Service (SaaS) products, mobile accessibility, artificial intelligence, and data analytics. These systems like Workday, Oracle HCM Cloud, and BambooHR now encompass various functions such as recruitment, onboarding, processing payroll, benefits administration, and monitoring performance.

### Digital risk landscape

The HR digitization has widened the attack surface for hackers. Centralization of data, cloud storage, third-party integrations, and remote access points raise the chances of security breaches. Moreover, the volume and sensitivity of HR data increase the stakes for the organizations.

### Research methodology

**Primary data:** "A timed questionnaire will be completed through Google Forms or email to collect preliminary data. Furthermore, semi-structured interviews will be done with chosen HR leaders and cyber security experts to gain more in-depth ethical insights."

**Secondary Data:** A thorough review of scholarly journals, case studies, industry reports, and organizational policies dealing with HR data management and cybersecurity shall be conducted.

### 1. Case study

Capital One Data Breach (2019).

### Background

Capital One, one of the largest banks in the U.S., experienced a data breach which revealed information of more than 100 million customers as a result of a misconfigured firewall in their AWS (Amazon Web Services) cloud environment.

### What happened

Data stolen were names, addresses, credit scores, and social security numbers

The incident was discovered and highlighted by an outside researcher who observed the data on GitHub.

### Primary challenges

Misconfigured cloud infrastructure.

Poor cloud security governance.

Potential insider threat from cloud service staff.

Late detection of abnormal activity in cloud environment.

**Lessons learned**

Configuring cloud environments properly and auditing them on a frequent basis is critical. Use the principle of least privilege for access controls.

Audit and log all cloud activity.

Perform routine penetration testing and vulnerability scans.

*Source:* capitalonedatapaper.pdf

**2. Case study**

The Equifax Data Breach (2017)

Topic: Cybersecurity Failure in Data Protection Industry: Credit Reporting / Finance

**Background**

Equifax is a major United States consumer credit reporting agency that experienced a record-breaking data breach in 2017 where 147 million people's sensitive personal information, including names, Social Security numbers, birth dates, addresses, and driver's license numbers in some instances, was compromised

**How the breach happened**

**Vulnerability:** Apache Struts web application framework employed by Equifax contained a known vulnerability (CVE-2017-5638).

**Patch failure:** Although the vulnerability was made public in March 2017, Equifax did not implement the required security patch within a reasonable amount of time.

**Exploitation:** Attackers took advantage of this weakness in May 2017, gaining unauthorized access to systems at Equifax.

Lack of Detection: The attackers went undetected for more than two months before the breach was detected late in July 2017.

Major Cybersecurity Failures

**Area description**

Patch Management Failure to patch and update known vulnerabilities Detection and Response Delayed detection of the breach provided attackers with extended access Data Encryption Sensitive data not encrypted properly Internal Security Policy Weak internal controls and lack of accountability Public Response Poor response to the incident and delayed public reporting of the breach

**Consequences**

- **Reputational harm:** Massive loss of consumer trust and brand reputation.
- **Financial sanction:** Equifax settled with the FTC, CFPB, and states for $700 million. Leadership Consequences: The CEO, CIO, and CSO all left.
- **Regulatory attention:** Increased regulatory emphasis on data protection throughout the financial industry.

**Lessons learned**

- **Prompt Patch Management:** Organisations need to have automated patch identification and deployment systems.
- **Monitoring in Real Time:** Monitoring networks in real time will identify anomalies and prevent breaches early.
- **Encrypt Sensitive Data:** Even if information is accessed, encryption lowers the threat of misusing it.
- **Incident Response Planning:** A tried and true cybersecurity incident response plan is crucial.
- **Security Culture:** Cybersecurity isn't solely an IT problem—it needs to be an organizational priority.

**Conclusion**

The Equifax breach is a textbook example of how lack of fundamental cybersecurity hygiene can cause ruinous outcomes. It also shows the value of regulatory compliance, active risk management, and inter-departmental cybersecurity cooperation.

***Source:*** https://www.researchgate.net/profile/Jason-Thomas-21/publication/337916068_A_Case_Study_Analysis_of_the_Equifax_Data_Breach

**Comprehensive approaches to safeguarding HR data**

Ensuring the confidentiality, integrity, and availability of HR data is critical in modern organizations. As custodians of sensitive employee information, HR departments must adopt comprehensive data protection strategies. The following best practices reflect current standards in cyber security and data governance, tailored specifically for HR functions.


**Source:** https://pipeline.zoominfo.com/operations/data-governance

**Fig 6**

- **Data encryption and minimization**

Data encryption is essential to protect both stored and transmitted HR information. It is recommended to utilize Advanced Encryption Standard (AES-256) for data at rest and Transport Layer Security (TLS 1.3) for data in transit. These protocols provide robust protection against interception and unauthorized access. Furthermore, organizations should adhere to data minimization principles by avoiding the retention of unnecessary or outdated personal data, thus limiting potential exposure in the event of a breach.

- **Continuous monitoring and security auditing**

Proactive monitoring and auditing mechanisms are critical for early threat detection. Regular penetration testing and vulnerability assessments help identify system weaknesses before they can be exploited. The maintenance of detailed audit logs enables organizations to track access and modification activities, facilitating the investigation of suspicious or anomalous behavior.

- **Access management and role-based controls**

Effective access management is foundational to HR data security. Organizations should implement Role-Based Access Control (RBAC) to ensure that individuals can only access information necessary for their defined responsibilities. This principle of least privilege minimizes the risk of unauthorized data exposure. Additionally, enforcing Multi-Factor Authentication (MFA) and mandating regular password updates significantly reduces the likelihood of credential-based attacks.

- **Vendor and third-party risk management**

HR functions often rely on third-party vendors for payroll processing, recruitment platforms, or cloud-based HR systems. To mitigate associated risks, organizations should ensure that vendors comply with recognized cyber security frameworks (e.g., ISO/IEC 27001, SOC 2). Rigorous due diligence must be conducted to evaluate vendors' data protection practices, and all contracts should include binding cyber security and data handling clauses.

- **Incident response and legal compliance**

An effective incident response plan is essential for managing data breaches and minimizing impact. This plan should be periodically tested and include HR-specific scenarios, such as unauthorized access to employee records. Furthermore, organizations must remain compliant with applicable data protection regulations (e.g., GDPR, CCPA) by adhering to mandatory breach notification timelines and maintaining proper documentation.

- **Security awareness and training**

Human error remains a significant vulnerability in information security. Therefore, it is imperative to provide comprehensive cyber security awareness training for HR personnel. Training should include instruction on identifying phishing attempts, social engineering tactics, and secure handling of confidential data. These initiatives should be incorporated into both initial employee onboarding and ongoing professional development programs.

## Conclusion

In the digital era, data serves as both a critical asset and a potential liability. The protection of employee information within Human Resource (HR) technology systems has emerged as a strategic priority for organizations. With increasing reliance on cloud platforms, artificial intelligence tools, and third-party software for essential HR functions—such as recruitment, payroll, and performance management—the risk of cyber threats has grown substantially. These include data breaches, phishing schemes, identity theft, and insider threats, all of which pose significant risks to employee privacy and organizational integrity.

This research underscores the multifaceted cyber security challenges HR professionals face and the pressing need for a proactive, multi-layered defense strategy. Key measures include implementing robust access control mechanisms, encrypting sensitive data, conducting regular security assessments, and fostering a culture of cyber security awareness across all organizational levels. Moreover, as regulatory frameworks such as GDPR, HIPAA, and CCPA continue to evolve, compliance has become not just a technical necessity but a legal and ethical imperative.

Ultimately, safeguarding employee data is a shared responsibility—not limited to the IT department, but extending to HR, leadership, and every employee. As digital transformation reshapes the HR landscape, organizations that prioritize resilient, adaptive, and privacy- centric cyber security practices will be best positioned to uphold trust, ensure compliance, and achieve sustainable operational success.

## References

1. California Consumer Privacy Act. Cal Civ Code § 1798.100 et seq., 2018.
2. European Parliament and Council of the European Union. General Data Protection Regulation (GDPR) [Regulation (EU) 2016/679], 2016.
3. IBM Security. Cost of a data breach report [Internet], 2024 [cited 2025]. Available from: https://www.ibm.com/security/data-breach
4. Workday Inc. Security whitepaper: Protecting HR data in the cloud, 2023.
5. National Institute of Standards and Technology (NIST). Zero trust architecture. NIST Special Publication 800-207. Gaithersburg (MD): NIST, 2020.
6. 0x7d0 Blog. How Equifax was breached in 2017 [Internet]. Available from: https://blog.0x7d0.dev/history/how-equifax-was-breached-in-2017/
7. Breachsense. Data breach and cyber security resources [Internet]. Available from: www.breachsense.com
8. ZoomInfo Pipeline. Data governance and operations insights [Internet]. Available from: https://pipeline.zoominfo.com/operations/data-governance
9. Data Brackets. How to comply with California Consumer Privacy Act (Draft) [Internet]. Available from: https://databrackets.com/event/how-to-comply-with-california-consumer-privacy-act-draft/
10. Global Trade & Technology Blog (GTTB). EU General Data Protection Regulation (GDPR): Compliance and regulatory requirements [Internet]. Available from:

https://gttb.com/compliance-regulatory-requirements/eu-general-data-protection-regulation-gdpr/
11. Pinterest. 9 elements of a HIPAA risk analysis [Internet]. Available from: https://www.pinterest.com/pin/9-elements-of-a-hipaa-risk-analysis--841539880370207746/
12. Capital One. Capital One data paper [document].
13. Thomas J. A case study analysis of the Equifax data breach [Internet]. ResearchGate. Available from: https://www.researchgate.net/profile/Jason-Thomas-21/publication/337916068_A_Case_Study_Analysis_of_the_Equifax_Data_Breach.