Shumaker

MAY 8, 2026 | PUBLICATION

Client Alert: Human Resources at the Intersection of Data and Digital Risk - What Every Executive Needs to Know

The landscape of human resources data management has fundamentally shifted. Data no longer lives in a locked filing cabinet, IT no longer handles cybersecurity alone, and artificial intelligence is no longer science fiction. HR departments today sit at the center of a decentralized cloud ecosystem, serving as active defenders of what should be considered the corporate crown jewels: employee data. With the rise in litigation related to a data breach, a proactive approach and partnership with counsel can help minimize risk to employers and their business.

INDUSTRY SECTOR

Technology

SERVICE LINE

Labor & Employment

RELATED PROFESSIONALS

C. Jade Davis
Tricia W. Magee

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

The Stakes: Why Employee Data Is a Critical Corporate Asset

Your organization's HR systems house Social Security numbers, bank and direct deposit information, health and benefits data, performance reviews, disciplinary records, and background checks. This information is not merely an administrative record—it is a high-value target. Threat actors exploit this data through payroll fraud (stealing direct deposits), identity theft (exploiting SSNs and background data), ransomware leverage (extorting the company using sensitive identity files), and insider theft (data hoarding or theft by departing employees). To illustrate the magnitude of this risk: a single phishing email requesting executive direct deposit changes can result in six-figure payroll theft.

Top Risk Areas for Executive Review

A. Business Email Compromise and Social Engineering

One of the most prevalent attack vectors targeting HR teams is business email compromise (BEC). In a typical scenario, a fraudster impersonates the CEO via email and sends an urgent request to HR to change a direct deposit account. Technology alone does not stop BEC—human process does. Organizations that implement out-of-band verification procedures, such as calling the executive directly before processing changes, neutralize these attacks. Executives should ensure that verification protocols are embedded into every payroll and benefits change workflow.

B. The Expanding HR Technology Perimeter

Modern HR operations rely on a sprawling ecosystem of payroll systems, applicant tracking systems, HRIS platforms such as Workday and ADP, collaboration applications like Teams and Slack, benefits platforms, performance management tools, shadow HR tools, and AI-enabled HR tools. Excessive permissions and integrations across these platforms create compounding vulnerabilities. If a vendor processes employee data, they become part of your security perimeter. Executives should demand clear answers from every HR technology vendor about how employee data is stored, processed, and protected.

C. Credential Theft, Ransomware, and Insider Threats

These three categories represent the core of the HR threat matrix. Ransomware attackers target HR files specifically because they contain sensitive identity data; the defense requires restricting access to sensitive files on a strict need-to-know basis. Insider threats arise most acutely when departing employees download candidate databases or other sensitive records; the defense requires seamless coordination with IT for rapid offboarding and access revocation. Credential theft exploits weak passwords to gain unauthorized access to HR systems; the defense requires mandating multi-factor authentication (MFA) across all HR and payroll systems.

D. Artificial Intelligence: Opportunities and Hidden Risks

AI is transforming HR through resume screening, candidate ranking, employee FAQ chatbots, performance analytics, and workforce productivity tools. However, executives must be aware of significant hidden risks that accompany these tools. AI systems may introduce bias and discrimination that disadvantages protected groups. They may lack transparency, producing inexplicable decisions. They create data leakage risks when employees paste sensitive data into public AI tools. They introduce vendor AI risk when software providers use AI behind the scenes without the organization's knowledge.

Executives should ensure their organizations adopt the following safe AI operations principles: never allow AI to make final employment decisions autonomously; ban the use of unvetted, consumer-grade AI platforms for HR work; strictly prohibit entering personally identifiable information or sensitive employee data into AI prompts; and proactively ask software vendors whether employee data trains their AI models.

E. Privacy Compliance: The Data Minimization Imperative

With evolving privacy laws across jurisdictions, executives should ensure their HR teams follow a privacy funnel approach. First, practice data minimization—collect only what you truly need, and question whether you really need SSNs during the initial application stage. Second, enforce access controls so that only individuals whose immediate job requires the data have visibility into it. Third, implement retention and deletion policies—do not keep resumes, background checks, or old employee records indefinitely.

Equally important, employees must clearly understand exactly what data is being collected about them, how

that data is being actively used by the organization, and whether AI tools are involved in processing their data or evaluating their performance. Privacy is not just compliance; it is the foundation of workplace trust.

Incident Response: The Critical First Hour

When a data incident occurs involving HR data, the response timeline is measured in minutes, not days. At discovery (T=0), the organization must alert IT and Security immediately—stop, assess, and not panic. Within ten minutes, executive leadership and legal must be notified and messaging aligned. Within thirty minutes, evidence must be preserved—organizations must not delete files, wipe devices, or try to clean up the mess. Within one hour, full coordination across functions must be underway.

HR's operational lane during a crisis involves four key functions: identifying exactly which employees or candidates are affected by the breach; classifying the specific type of data involved (e.g., names versus SSNs); communicating with impacted employees in coordination with IT and legal; and supporting and managing the emotional and logistical impact on the workforce. Employers who proactively prepare a rapid response plan can help contain and address issues promptly, which can limit exposure and loss.

A Five-Point Executive Checklist

We recommend that every executive ensure the following five actions are completed without delay:

1. Map HR data by conducting an audit to know exactly where employee data lives across all systems and shadow tools.
2. Enable MFA by mandating multi-factor authentication on everything, prioritizing payroll and HRIS platforms.
3. Limit access by conducting a permission purge to ensure only those who critically need HR data currently have access to it.
4. Establish AI rules by drafting and distributing a clear policy clarifying exactly how HR staff may and may not use AI tools.
5. Vet HR vendors by initiating a vendor review to understand exactly how third parties protect your data and whether they utilize AI.

With AI, evolving privacy laws, and increasing cyber threats, cybersecurity is no longer just an IT issue. Small operational changes in HR—access control, verification, and responsible AI use—are the organization's strongest defense. We encourage every executive reading this advisory to treat HR data security as a board-level priority and to engage qualified counsel to assess your organization's current posture.

We welcome the opportunity to discuss how these risks apply to your specific organization. Please do not hesitate to reach out.

We welcome the opportunity to discuss how these risks apply to your specific organization. Please do not hesitate to reach out to Jade Davis or Tricia Magee.

Shumaker