2026 OHIO SHRM CONFERENCE

SECURE HR: ESSENTIAL CYBER AND DATA PROTECTION PRACTICES FOR TODAY'S WORKPLACE

Matthew E. Ritzman, Ph.D., J.D.
Labor & Employment Attorney
Honigman LLP

SHRM26

1

SPEAKER BIOGRAPHY
Matthew E. Ritzman, Ph.D., J.D

- Labor and Employment Attorney at Honigman LLP, advising organizational leaders on navigating complex workplace issues.
- Five Years as a trial attorney at the NLRB
- Decade of college-level teaching experience and five years as an NLRB attorney, he holds a Ph.D. in Educational Technology.
- Regular presenter on HR—labor, employment law, and performance improvement—keep me in mind for your groups

SHRM26

2

STAY CONNECTED

- Presentations are interactive—we can all learn from each other
- I lead with this because I know people will be in a hurry to get to their next session. Please stay in touch and continue sharing your experiences!
- Find contact information at the end of this presentation. I share updates and future presentation announcements on LinkedIn.
- linkedin.com/in/matthewritzman

SHRM26

3

How does this relate to HR?

CYBERSECURITY IS A PEOPLE ISSUE…

- Data breaches are often human issues — having HR ready to help is a massive advantage for any organization seeking to contain risk
- Cybersecurity is no longer just an IT issue — it's a people issue. HR shapes security culture from onboarding through ongoing training and policy development
- Today we explore strategies to promote a security-first mindset, ensure compliance, and support continuous learning

SHRM SHRM26 SHRM

4

…AND HR IS A HIGH-VALUE TARGET

- HR holds highly sensitive data: SSNs, direct deposit info, health elections, I-9s, background checks, and disciplinary records.
- HR platforms connect to payroll, benefits, performance tools, and third-party recruiters — broadening the attack surface.
- HR routinely interacts with external parties: applicants, staffing agencies, insurers, and vendors — opening phishing channels.
- HR professionals are perceived as authoritative and trusted, making them prime targets for social engineering and impersonation.

SHRM26

5

…AND HR IS IMPORTANT TO KEEPING EMPLOYEE DATA SAFE

- Managing Data Access: Ensure employees are categorized correctly, granting access only to data necessary for their roles.
- Policy Development & Compliance: Partner with legal and IT to develop and enforce practical cybersecurity policies.
- Fostering a Cybersecurity Culture: Embed cybersecurity training into onboarding and ongoing education so employees can spot threats.

SHRM26

6

TOP THREATS TO HR: DEEPFAKE TECHNOLOGY

7

WHAT IS A DEEPFAKE SCAM?

- A deepfake scam uses artificial intelligence to create highly realistic fake audio, video, or images that impersonate trusted individuals—such as executives, coworkers, family members, or business partners.
- These sophisticated impersonations are designed to manipulate victims into transferring money, sharing sensitive information, or bypassing established security procedures.
- This is not a future threat. Deepfake technology has already been used to steal millions of dollars from organizations, facilitate business email compromise schemes, and even enable individuals to secure employment using entirely fabricated identities.

8

What does this look like? The Fake Executive

The first, a scammer posing as an executive asking an employee to authorize transactions and fake applicants interviewing and being hired to work, and being paid, using deepfake technology

The case that should be on every HR professional's radar: In early 2024, a finance employee at a multinational company in Hong Kong participated in a video call with what appeared to be the CFO and several other senior executives. They instructed him to execute wire transfers totaling $25 million USD. Every person on that call was a deepfake. He transferred the money.

For HR specifically, deepfakes are used in two ways: financial fraud — fake executives ordering payments — and in hiring, where fake candidates impersonate real people or fabricate identities entirely.

9



10

RISE IN DEEPFAKE JOB APPLICANTS

- Deepfake applicants use AI to impersonate others or fabricate skills via AI-generated video, synthetic audio, or fake resumes.
- Advancements in AI: Ongoing advances have drastically reduced the cost and time to create convincing deepfakes.
- Remote & Hybrid Interviews: Reduced in-person contact makes fraud easier to go unnoticed.
- High Demand in Tech Roles: Cybersecurity and digital marketing roles are prime targets due to system access.
- Globalization of Hiring: Cross-border hiring expands opportunities for fraudulent applicants to exploit gaps.

SHRM26

11

DEEPFAKE BEST PRACTICES FOR HR

- Educate: Train HR teams to recognize suspicious media, red flags in interviews, and common impersonation tactics.
- Verify: Use secure platforms with facial recognition and screen sharing to confirm identity during hiring. Interview in-person.
- Collaborate: Work with Legal, IT, and Security on protocols for identifying and responding to deepfakes.
- Protect: Include image/voice consent clauses in contracts; update policies on digital content use.

SHRM26

12

TOP THREATS TO HR: PHISHING AND BUSINESS EMAIL COMPROMISE

13

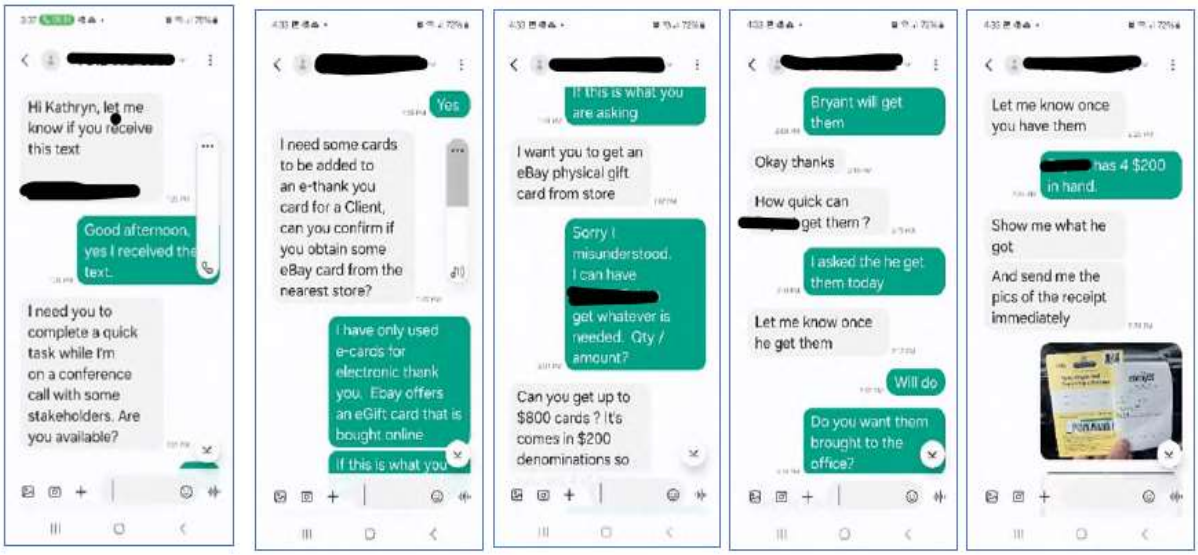
PHISHING AND BUSINESS EMAIL COMPROMISE

Cybercriminals impersonate executives, vendors, or HR personnel to manipulate staff into disclosing sensitive data or taking unauthorized actions — such as changing direct deposit bank account information.

These scams are highly targeted, often convincing, and increasingly common. The CEO gift card scam and spoofed payroll emails are among the most frequently reported.

14

The Gift Card Scam



15

The Phishing Email

From: [redacted] – My name
<mediabest62@gmail.com> – Not my email
Date: [redacted]
Subject: Direct Deposit Change
To: [redacted] – My boss' work email

Hi [redacted] – My boss' name

I just switched my bank and would like to update my direct deposit details, would the change be effective for the next pay date?

Regards,
[redacted] – My name
Senior Software Engineer – My job title
[redacted] – My company

SHRM26

16

BEST PRACTICES FOR HR

- Educate: Train not to respond to unrecognized emails or phone numbers. If there is any suspicion—verify the person's identity.
- Clear Reporting Procedures: Establish a simple process for reporting suspicious emails and messages.
- Phishing emails: Run periodic mock phishing campaigns to test employee awareness.
- ANY request to change financial information requires a callback to a verified number on file, not the number in the email. No exceptions. Even if it looks exactly right. Even if it comes from the "CEO."
- Audit and address your policies and incorporate this information into your training

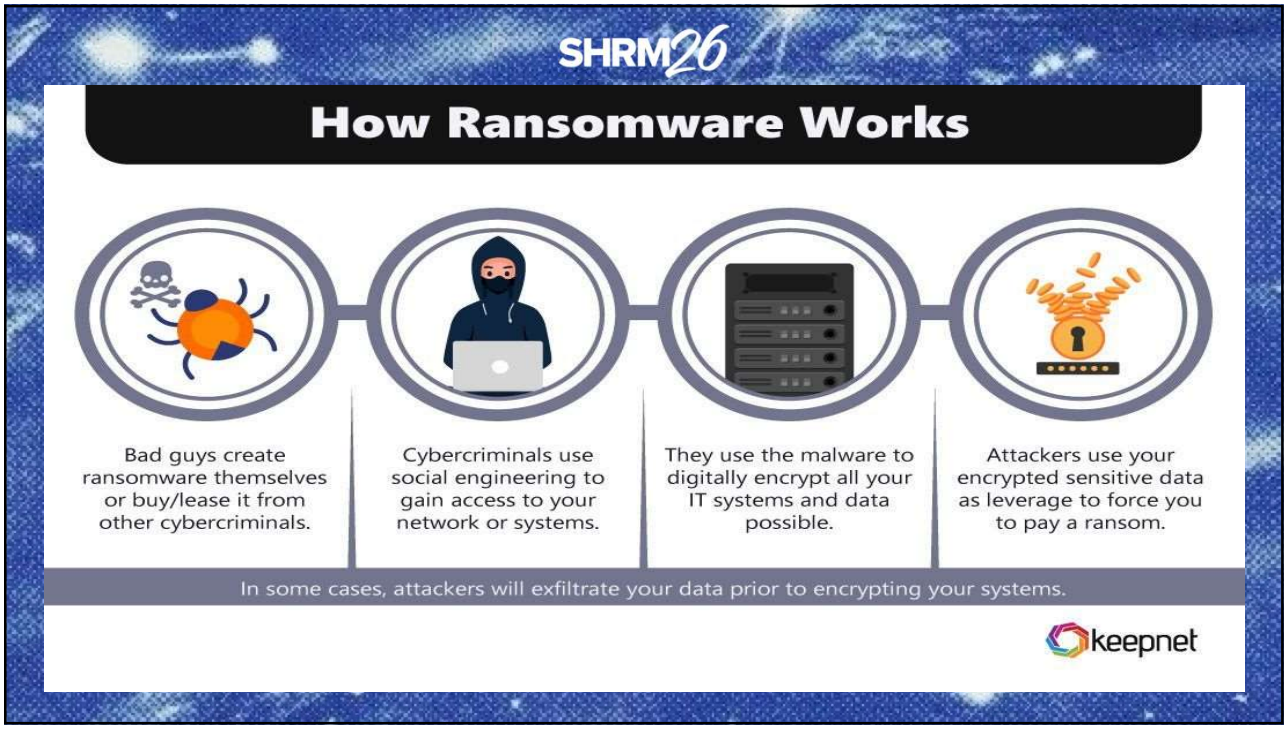
SHRM26

17

SHRM26

TOP THREATS TO HR: RANSOMWARE

18



19

RANSOMWARE: WHAT HR NEEDS TO KNOW

- What it is: Ransomware is a malicious type of software (malware) that blocks access to a user's files, devices, or networks and demands a financial payment—usually in cryptocurrency—to restore access—while HR, payroll, and benefits are completely inaccessible.
- HR departments are prime targets for ransomware attackers because they manage highly sensitive employee data (e.g., payroll, PII) and are trusted sources of internal communication
- Double extortion: Attackers now steal data BEFORE encrypting it, then threaten to publish employee personal data publicly — triggering breach notification laws even if IT restores from backup.

SHRM26

20

RANSOMWARE: WHAT HR NEEDS TO KNOW

- The People Aspect - Most ransomware enters through phishing emails and social engineering tactics. HR receives more external email from unknown senders than almost any other department. Additionally, it deals with the outflow of employee actions

SHRM26

21

RANSOMWARE: WHAT HR NEEDS TO KNOW

- Prevention – discussed training, handbook and policy updates
- Advocate for regular, tested, offline backups of HR data.
- Use phishing email simulations to ensure employees are aware of and can recognize phishing emails in the midst of their everyday activities.
- Make security everyone's responsibility
- Have clear reporting structure for concerns and near misses
- Technology interventions: VPN, dual factor authentication, etc.

SHRM26

22

TOP THREATS TO HR: AI MISUSE IN EMPLOYEE CONFLICTS

23

AI MISUSE: FAKE RECORDINGS AND FABRICATED EVIDENCE

-Voice cloning and other deepfake tools make it possible to create convincing fake content that can be highly damaging.

-Even a single disgruntled employee can create significant reputational and legal risks.

-Employees can now easily create fake call logs and/or fabricated recording evidence to present in support of defenses against allegations of misconduct

Example – Baltimore Principal

24

COMPLICATING WORKPLACE INVESTIGATIONS

- Scrutinize all electronic evidence to ensure authenticity (this won't be an issue in every case)
- Employees can now easily fabricate call logs, recordings, or documents to support false defenses.
- Verify authenticity of digital content — emails, recordings, and written documents. Establish audit trail and chain of custody
- Cross-check evidence with multiple independent sources– esp. Employer owned devices
- Involve IT, legal, and HR when suspicious content is identified.
- Maintain clear documentation of all investigative steps taken
- Address this in your policies—ie misconduct to fabricate evidence

SHRM26

25

SHRM26

TOP THREATS TO HR: Welcomed Outsiders Vendors

26

VENDOR BREACHES

HR works with payroll processors, benefits administrators, background check vendors, recruiting platforms, LMS providers, and wellness apps — all handling sensitive employee information, all potential entry points for attackers.

Even well-known platforms have been breached. Some vendors subcontract to additional providers, creating chains of access HR may not fully oversee. Proper due diligence is critical: verify cybersecurity practices, require data protection clauses and breach notification terms, and regularly review vendor access controls.

27

TOP THREATS TO HR: INSIDERS

28

MALICIOUS AND NEGLIGENT INSIDER BEHAVIOR

Insiders — employees, contractors, consultants — may deliberately misuse access: downloading personnel files, copying evaluations, or leaking internal communications.

- Intentional or Negligent
- Even without malicious intent, negligence is just as dangerous: storing confidential HR documents on personal devices, emailing sensitive data to the wrong recipients, or pasting employee information into public AI chat tools — exposing organizational data beyond company control.

SHRM26

29

CREDENTIAL THEFT AND ACCESS MISMANAGEMENT

- Weak or Reused Passwords: Employees reusing passwords across systems are easy targets for credential stuffing.
- Lack of Multifactor Authentication (MFA): A stolen password alone can give attackers full system access.
- Credential Phishing: Hackers use fake HR or IT emails to harvest login credentials.
- Poor Access Revocation: Delayed removal of access after role changes or departures increases risk.
- Shared Accounts: Generic logins obscure accountability and complicate security investigations.

SHRM26

30

Insider Threats
How to Win the Lottery?



31

HR'S STRATEGIC ROLE IN CYBERSECURITY

HR sits at the intersection of people, policy, and technology — making it uniquely positioned to drive cybersecurity culture across the entire organization.

SHRM26

32

WHAT CAN YOU DO? POLICY ACTION STEPS

- Review and update handbooks and policies regularly — at least once per year.
- Ensure required notices are current and reflect any regulatory changes.
- Conduct a year-end audit: identify what is working, resolve pending disputes, set compliance goals.
- Begin the update process early — it typically takes several months to implement changes.

SHRM26

33

HR'S STRATEGIC ROLE: ACCESS AND TRAINING

- Define and enforce access control policies: employees should only access systems needed for their role.
- Regularly audit and adjust access rights during role changes or terminations.
- Embed cybersecurity in onboarding: make security expectations clear from day one.
- Provide periodic, role-specific training tailored to each team's risk exposure.

SHRM26

34

From Day 1 to Offboarding

- **PRE-DAY ONE:** Acceptable Use Policy signed before first login. Security expectations in the offer letter. Identity verification required for sensitive-access roles.
- **DAY ONE:** HR-led security orientation framed as shared responsibility, not IT compliance. MFA enrollment before credentials issued. Reporting channel for suspicious activity introduced.
- **DAYS 30-90**: First phishing simulation run — diagnostic baseline, not punitive. Role-specific training tracked by HR. Manager confirms completion at onboarding checkpoint.
- **ANNUAL:** Mandatory refresher tied to performance cycle. Updated for new threats. Completion rates reported to leadership — not just IT. This creates organizational accountability.
- **OFFBOARDING:** Access revocation same day as departure. Device return confirmed before final paycheck. Exit interview for sensitive-role employees includes a security debrief.
- **KEY PRINCIPLE:** Security awareness is woven into every transition point HR already manages. You already own these moments — add the security dimension.

SHRM26

35

HR'S STRATEGIC ROLE: INCIDENT RESPONSE AND CULTURE

- Collaborate with IT and Legal on incident response — know HR's role before a breach happens.
- Coordinate messaging and follow-up actions with cross-functional teams.
- Shape behavior by embedding cybersecurity in organizational values and performance metrics.
- Recognize and reward security-conscious behaviors; promote top-down accountability.

SHRM26

36

KEY CYBERSECURITY POLICIES FOR HR

- Acceptable Use & Internet Safety: Define appropriate use of company devices, email, internet, and file sharing.
- Remote Work & Device Security: Require VPN use, password protection, auto-lock screens, and encrypted connections.
- Offboarding with Access Termination: Define how quickly logins are disabled and devices retrieved for departing staff.
- Third-Party Vetting: Mandate written vendor agreements covering data security obligations and breach notification.
- Social Media & Personal Devices: Educate employees on risks of accessing sensitive systems from unmanaged devices.

SHRM26

37

TRAINING AND EMPLOYEE AWARENESS

- Role-Specific Training: Customize content to employees' access levels — HR, finance, and IT need more advanced training.
- Phishing Simulations: Run realistic email simulations; enable one-click reporting for suspected phishing.
- Executive-Level Cyber Education: Train senior leaders on BEC scenarios and their high-risk access responsibilities.
- Ongoing Awareness Campaigns: Use newsletters, tips, posters, and short videos to keep security top of mind.
- Contractors and New Hires: Extend training to temporary staff and integrate it into onboarding.

SHRM26

38

COLLABORATING WITH IT AND COMPLIANCE

- Conduct Shared Risk Assessments: Identify and prioritize risks specific to HR data and workflows.
- Define HR's Role in Data Classification: Work together to assign appropriate protection protocols to sensitive data.
- Include HR in System Audits: Ensure HR participates in access control, data handling, and vendor management audits.
- Align Policies with Legal and IT Standards: Ensure HR policies align with NIST frameworks and data privacy laws.
- Establish Incident Response Protocols: Document HR's role in breach notifications and credential revocation.

SHRM26

39

REGULATORY AND LEGAL CONSIDERATIONS

HR must understand the legal landscape governing data privacy and security. Multiple laws create overlapping obligations for how employee data is collected, stored, and protected.



40

KEY REGULATORY FRAMEWORKS

- HIPAA: Protects health-related information — applies when HR manages benefits or wellness programs.
- FCRA: Regulates background checks — requires strict consent, disclosure, and dispute resolution procedures.
- SOX and PCI DSS: Impact HR when involved with financial reporting or payroll processing of card data.
- State Data Breach Notification Laws: Most states require timely notification to employees if personal data is compromised.
- GDPR / State Privacy Laws (CCPA, etc.): Govern collection, storage, and transfer of employee personal data.

SHRM26

41

SHRM26

TECHNOLOGY AND VENDOR RISK MANAGEMENT

42

VENDOR RISK MANAGEMENT BEST PRACTICES

- Require Vendor Security Certifications: Ensure vendors meet SOC 2, ISO 27001, or NIST 800-171 standards.
- Include Security Terms in Contracts: Specify data protection requirements, audit rights, and breach notification timeframes.
- Conduct Initial and Ongoing Risk Assessments: Evaluate vendors before engagement and review annually.
- Use a Centralized Vendor Management System: Maintain a complete inventory of third-party vendors and their data access.
- Disable Access Promptly When Contracts End: Treat vendor offboarding with the same rigor as employee separation.

SHRM26

43

WHAT TO DO IN A DATA BREACH

Breaches are stressful — but organizations that have a clear plan respond faster, limit damage, and meet legal notification obligations.



44

DATA BREACH RESPONSE: HR'S ROLE

- Have a plan for how to respond and follow it.
- Notify IT and Legal without delay; do not attempt to investigate alone.
- Begin employee communications only after legal guidance on what to say and when.
- Document everything: timestamps, actions taken, communications sent.
- Debrief after resolution: conduct a post-incident review and update policies to prevent recurrence.

SHRM26

45

SHRM26

CREATING A SECURITY FIRST CULTURE

46

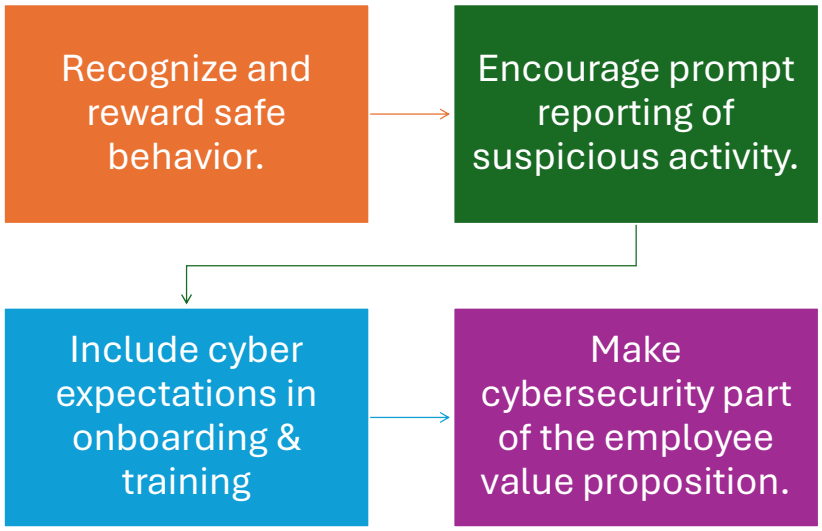
BUILDING A SECURITY-FIRST CULTURE

- Recognize and reward security-conscious behaviors — make security part of performance culture.
- Encourage prompt reporting of suspicious activity without fear of blame.
- Include cybersecurity expectations in onboarding and the employee value proposition.
- Make cybersecurity visible at the leadership level — top-down commitment drives behavior.

SHRM26

47

BUILDING A SECURITY-FIRST CULTURE



SHRM26

48

AI IMPLEMENTATION IN HR

AI adoption in HR is surging: 72% of HR professionals used AI in 2025, up from 58% in 2024. HR leaders report a 63% productivity boost. But rapid adoption creates new cybersecurity risks that demand attention.

49

AI IN HR: KEY CONSIDERATIONS

- AI use is exploding — development and deployment are happening faster than policy can keep up.
- The potential is seemingly limitless, but legal, ethical, and data risks are real.
- Employees are using AI tools regardless of whether the organization has a formal policy.
- Responsible AI adoption requires intentional governance, not just enthusiasm.

50

DEVELOPING AN AI USE POLICY

- Ensure your organization has a formal AI Use Policy — even if you have not deployed a proprietary AI tool.
- Consider how your AI policy interacts with existing organizational policies, contracts, and agreements.
- Employees using free public AI tools may inadvertently expose sensitive data — a policy is essential.
- Involve legal counsel in drafting and compliance — there are many laws and regulations to navigate.

SHRM26

51

THE IMPORTANCE OF CONTINUOUS TRAINING

The threat landscape changes constantly. One-time training is not enough. Organizations that invest in ongoing, role-specific cybersecurity education:

Build a workforce that can recognize and respond to evolving threats. Reduce risk of misuse and biased AI-driven decisions. Promote ethical and legally compliant technology adoption. Build employee trust and a stronger organizational security posture.

SHRM26

52

SUMMARY AND KEY TAKEAWAYS

HR plays a direct and strategic role in cybersecurity.

Cyber threats are people problems before they are technology problems.

Policies, training, and culture are HR's strongest tools.

Cross-functional collaboration with IT, Legal, and Compliance builds resilience.

Stay current: update handbooks, train continuously, and audit regularly.

When in doubt, involve legal counsel early.

53

10 THINGS – Checklist

- 1. Verify offboarding: how quickly are credentials revoked after departure? If not same-day, fix the process.
- 2. Check your employee handbook for 'deepfake,' 'synthetic media,' 'AI-generated content.'
- 3. Establish a callback policy for any request to change direct deposit or banking info. Write it. Distribute it. Enforce it.
- 4. Confirm all HR systems require multi-factor authentication (MFA). If any don't, escalate to IT today.
- 5. Ask your top 3 HR vendors: who else has access to our employee data? Get the answer in writing.
- 6. Confirm your organization has a written AI Use Policy. If not, raise it with leadership and legal this week.
- 7. Schedule a phishing simulation if one hasn't run in the last 6 months.
- 8. Find your incident response plan. Confirm HR is named in it. If not, ask to be included.
- 9. Review your handbook update schedule. If it isn't annual, make it annual.
- 10. Create a regular touchpoint with IT Security. HR and IT must be aligned BEFORE a breach — not during

54

CONTACT INFORMATION

Matthew E. Ritzman, Ph.D., J.D. | Labor & Employment Attorney | Honigman LLP

mritzman@honigman.com | (419) 699-4787 | (313) 465-7742

linkedin.com/in/matthewritzman

55

DISCLAIMER

This presentation is for informational purposes only and does not constitute legal advice, nor does it create an attorney-client relationship. You should not act or refrain from acting based on any content included herein without seeking appropriate legal or professional advice based on the facts and circumstances of your specific situation. While efforts are made to ensure accuracy, laws and regulations may change; the presenter assumes no responsibility for errors or omissions.

56