



Labor and Employment Law Seminar

**2026
LAS VEGAS**

**SAFETY, CYBER, PRIVACY, AND REGULATED
WORKPLACES:**

**THE EMPLOYEE DATA BREACH
PLAYBOOK: PAYROLL, BENEFITS,
HR FILES, AND THE
FIRST 72 HOURS**



Presented by

**KILE
MARKS**



**SAFETY, CYBER, PRIVACY, AND
REGULATED WORKPLACES:
THE EMPLOYEE DATA
BREACH PLAYBOOK:
PAYROLL, BENEFITS, HR
FILES, AND THE
FIRST 72 HOURS**

Agenda

- What's in your HR files
- The first 72 hours**
- Who must be told
- Cyber insurance
- Vendor breaches
- Ransomware and communications
- Your action plan

PART 1: WHAT'S IN YOUR HR FILES

HR Files Hold Everything An Identity Thief Needs

- Payroll, tax, SSNs and direct deposit details.
- Benefits, medical notes, background checks and I-9s.
- Especially exposed: medical and dental offices, restaurants, nonprofits, schools, and startups that outsource HR. One personnel folder, or one HR portal login, can hold identity, financial and sensitive personal details together, so a single lapse can expose many facts at once.



Nevada Law Covers HR Data

Identity and money

- Name plus unencrypted SSN, driver's license or identification number, or financial account information with the credentials needed for access.
- Example: a payroll export listing employee names beside unencrypted SSNs or bank account numbers is the typical case to check first.

Health identifiers

- Name plus a medical or health insurance ID number.

Account access

- Username or email plus a password or security answer that permits access to an online account.
- Example: an HR login saved in a shared spreadsheet alongside employee records.

NRS 603A.040 · Review the actual fields, not just the file name

PART 2:
THE FIRST 72
HOURS

RESPONSE SEQUENCE

The First 72 Hours: Contain, Then Scope

01

Hours 0 to 24

- Isolate systems; preserve evidence.
- Name an incident lead.
- Check the cyber policy; engage counsel.

Worked example: on a Friday at 9 p.m., the restaurant payroll laptop shows ransomware locking the payroll folder. Hours 0 to 24: disconnect it without wiping it, keep the drive, and alert the incident lead and insurer. Hours 24 to 72: list which employees' SSNs and bank details were in that folder and which states they live in.

An operating plan, not a Nevada statutory 72-hour deadline

02

Hours 24 to 72

- Identify employees, data fields and states.
- Check encryption and vendor involvement.
- Ask about a law-enforcement delay.



**PART 3:
WHO MUST
BE TOLD**

Nevada Requires Notice Without Unreasonable Delay

ACQUIRED.

OR REASONABLY BELIEVED ACQUIRED.

- For covered, unencrypted personal information, that is the notice trigger.
- Allow time to scope the breach and restore systems. Law enforcement may require a delay when notice would impede an investigation.
- Record the reason for any delay, with dates, so you can show it was reasonable. Example: if forensic work runs over a weekend, log when it started, what it found, and when notice went out.

NRS 603A.220 requires consumer notice · The Nevada AG enforces

NOTIFICATION AUDIENCE

Who Else Must Hear From You

Affected employees

- Include former and remote staff. Check each person's state of residence; laws and deadlines vary by state.

Nationwide credit bureaus

- Notify them when more than 1,000 people are notified under Nevada's requirement.

Nevada Attorney General

- Optional notice at OperatorAGNotices@ag.nv.gov.

Your response partners

- Carriers, vendors and benefit plans may have separate notice requirements. Example: a benefits administrator may need its own notice covering enrolled staff.
- NRS 603A.220 · Nevada AG breach-notice guidance

PART 4: CYBER INSURANCE



A SEPARATE CLOCK

Cyber Insurance Has Its Own Clock

- Check policy notice conditions first.
- Use panel counsel and approved forensic vendors.
- Get carrier consent before spending or settling.

Example: a laptop with payroll files goes missing on a Friday evening. Call the carrier through the policy's required channel before hiring a vendor, and log every call.

Mistakes that can cost coverage

Late notice. Unapproved vendors. Admitting liability in employee letters. Describe what happened and what you are doing, without admitting fault in writing.

Read your policy; requirements vary

Labor and Employment Law Seminar

2026 LAS VEGAS

Insurers' Minimum 12 Controls



Multifactor authentication (MFA) for remote access and admin/privileged controls



Endpoint Detection and Response (EDR), MDR or XDR



Secured, encrypted, and tested backups



Privileged Access Management (PAM)



Email filtering and web security



Patch management and vulnerability management



Cyber incident response planning and testing



Cybersecurity awareness training and phishing testing



Hardening techniques, including Remote Desktop Protocol (RDP) mitigation



Logging and monitoring/network protections



End-of-life systems replaced or protected



Vendor/digital supply chain risk management

PART 5: VENDOR BREACHES

OUTSOURCING DOES NOT END RESPONSIBILITY

A Vendor Breach Is Still Your Problem

Your Employees.
Their System.

Payroll processors, PEOs, benefits administrators and cloud HR systems hold your employee data.

The vendor must tell the owner

A vendor that only maintains covered data must notify its owner immediately following discovery of a qualifying breach. For example, a payroll processor that finds employee records were accessed should tell you at once, not after its own investigation ends.

Security belongs in the contract

Contracts must require reasonable security for covered personal information. Ask for specific safeguards: encryption of stored data, access controls, and written incident procedures.

Labor and Employment Law Seminar

2026 LAS VEGAS

Fix Vendor Contracts Before A Breach



Set the notice clock

Require a deadline in hours, not “promptly.” Example: “within 24 hours of discovery.”



Allocate response costs

Decide who pays for notice and credit monitoring. Name the payer in writing, including mailing and call-center costs.



Align financial protection

Review indemnity and insurance limits together. Check that caps cover realistic notice and recovery costs.



Keep oversight and an exit

Secure audit rights and data return. Also set how and when employee data is returned or deleted at contract end.

Negotiate while you still have leverage

Vendor Management Best Practices

- Maintain a vendor inventory and data-flow map
- Review contracts, DPAs, and data-use terms
- Ask vendors what data they collect, receive, store, share, or use for their own purposes
- Confirm whether features can be configured, disabled, or limited
- Require prompt support when a demand letter arrives



Vendor Management Best Practices

- AI
 - New “AI Features”
 - Training Data
- Policy
 - Due diligence
 - Negotiation
- Comprehensive review of all contracts
 - Too many? Prioritize!
 - Centralized repository
- Similar protections
 - Security
 - Privacy



**PART 6:
RANSOMWARE &
COMMUNICATIONS**

Ransomware And Communications

Payday does not move

Keep a manual payroll plan. Test restores. Write down who approves manual checks, where timesheets are stored, and how staff are paid if systems stay down.

Do not promise what you cannot confirm

- “No data was taken” or “you are fully protected.”
- A restoration date.
- Free services not yet arranged.

Your first message

What happened? What is affected? What to do now? When the next update will come? Keep it short, plain, and factual, and say when staff will hear again.



**PART 7:
YOUR
ACTION PLAN**



PREPARE BEFORE THE CALL

Your Action Plan, And Where We Help

- 01** Map systems holding employee data.

- 02** Read your cyber policy notice terms.

- 03** Renegotiate vendor breach clauses.

- 04** Write a payroll-continuity plan.

- 05** Run a tabletop with HR.

We help with privacy and cyber, employment, vendor contracting and incident response.

Nevada is the anchor · Other states differ · Not legal advice

Labor and Employment Law Seminar

2026 LAS VEGAS



**KILE
MARKS**



Questions?



Labor and Employment Law Seminar

2026 LAS VEGAS



Thank you.