HR AS THE BUSINESS'S FIRST LINE OF LEGAL PROTECTION: HOW HR PROTECTS THE COMPANY'S BUSINESS INTERESTS EVERY DAY

By Jordan B. Segal, Esq.

I. INTRODUCTION: HOW LAWYERS SEE YOUR WORK LATER

A. Lawyers don't see intentions — they see documents.

B. Lawyers don't hear conversations — they read emails and notes.

C. Lawyers don't fix facts — they work with the record HR created.

D. Good HR systems shrink disputes; bad ones expand them.

E. Everything that follows is about controlling that record.

II. ACT 1: ESSENTIAL BUSINESS PROTECTIONS

A. Focus on protecting revenue, customers, data, and deal readiness.

1. These are the risk surfaces where value is lost or preserved.

B. Anti-discrimination and harassment: protecting reputation and talent.

1. Inconsistent treatment becomes the company's story.

2. Retaliation risk often eclipses the original complaint.

3. Clean intake and investigation paths protect credibility.

4. Michigan reality: comparators and consistency drive outcomes.

5. Business impact: brand, recruiting, and leadership bandwidth.

6. Case Study: the two-employee problem.

a. Two similar violations, two different outcomes.

b. A later complaint reframes the issue as inconsistency.

c. The rule wasn't the problem — the variance was.

d. Lesson: explainable, repeatable outcomes protect the business.

C. Acceptable use of AI: speed with guardrails.

1. AI increases speed and scale — but also amplifies mistakes.
2. Risk areas: hiring, reviews, discipline drafts, investigations.
3. No confidential or regulated data in unapproved tools.
4. AI assists; humans decide; outputs are drafts.
5. Business impact: decision quality, record quality, and trust.
6. Case Study: the magical AI performance review.
    a. AI-generated praise conflicts with later termination.
    b. The record looks clean — but is wrong.
    c. The dispute becomes about the company's own document.
    d. Lesson: guardrails and human review protect narrative control.

D. Confidential information and trade secrets: protecting the crown jewels.

1. Most valuable assets walk out the door every night.
2. Courts look at behavior, not labels, to decide what is "secret."
3. Access limits, training, and exits create the protection story.
4. Business impact: customer relationships, know-how, and leverage.

E. Leave, wage and hour: protecting operations and financing.

1. Overlapping rules create decision risk under pressure.
2. Manager-level mistakes drive most exposure.
3. Class and collective actions affect financing and M&A.
4. Michigan overlay: ESTA plus federal regimes.
5. Business impact: cost, distraction, and deal friction.

III. ACT 2: OPERATIONALIZING PROTECTION

A. Policies don't protect businesses — systems do.

1. Process creates consistency; consistency creates defensibility.

2. This is where HR turns intent into outcomes.

B. Discipline systems: turning risk into predictability.

1. Progression and documentation control the story over time.

2. Surprise terminations create disruption and exposure.

3. Standard paths protect managers and the company.

4. Business impact: morale stability and leadership focus.

5. Anecdote: the surprise termination.

a. Years of complaints, zero documentation.

b. First time the employee hears it is the termination meeting.

c. The question becomes "why now?" not "what happened?"

d. Lesson: predictable systems protect credibility.

e. Documentation: narrative control.

C. Disputes are stories told with paper and email.

1. Facts beat conclusions; boring beats clever.

2. Assume every note is future evidence.

3. Business impact: smaller, faster, cheaper disputes.

4. Anecdote: the email that wouldn't die.

a. A venting email becomes the headline exhibit.

b. Tone, not substance, drives the narrative.

c. Lesson: write like a neutral third party is watching.

D. Confidentiality controls and access management.

1. Role-based access limits the blast radius.

2. Clean onboarding and offboarding prevent lingering risk.

3. HR and IT together own the human side of security.

4. Business impact: containment instead of crisis.

E. BYOD: convenience versus containment.

1. Personal devices increase speed — and risk.

2. Without clear rules, data and relationships leave with the device.

3. Security requirements and exit steps matter.

4. Business impact: customer and data leakage.

5. Anecdote: the pocket sales database.

    a. Contacts sync to a personal phone.

    b. Clients get calls from the new employer.

    c. The fight is about controls, not loyalty.

    d. Lesson: exits and access control protect value.

F. Restrictive covenants: protecting relationships and revenue.

1. Tools to protect legitimate business interests.

2. Most value is deterrence and leverage, not litigation.

3. Work only when tied to roles and handled consistently.

4. Business impact: goodwill, pipelines, and deal value.

G. Investigations and litigation holds: defensibility under stress.

1. Who leads, who decides, who communicates.

2. When to involve outside counsel.

3. Preserve documents early; control the process.

4. Business impact: credibility and outcome control.

H. Social media and off-duty conduct: reputation risk.

1. Screenshots travel faster than explanations.

2. Clear boundaries on work-related use and branding.

3. Consistent enforcement avoids viewpoint or favoritism claims.

4. Business impact: brand and customer trust.

I. Leave law interplay: a simple decision path.

1. Is there a medical issue? Think ADA/FMLA/ESTA/workers' comp.

2. Is the employee requesting time or an accommodation?

3. Centralize decisions; don't let managers freelance.

4. Business impact: fewer missteps at high-risk moments.

IV. ACT 3: WHAT TO DO MONDAY MORNING

A. Turn principles into repeatable tools.

1. Reduce variance, increase speed, protect value.

B. Tool: policy and process audit (business lens).

1. Where do we lose time, money, or momentum?

2. Where do managers improvise the most?

3. Where are records weakest?

4. Which exits were messiest?

5. Prioritize by business impact, not by statute count.

C. Tool: manager documentation template.

1. Date and context.
2. Objective facts.
3. Business impact.
4. Employee response.
5. Next step and expectation.

D. Tool: incident response playbook.

1. Who decides, who investigates, who communicates.
2. Preserve evidence and control messaging.
3. Escalate early, not emotionally.
4. Goal: contain the blast radius and keep operating.

E. Tool: exit checklist.

1. Return property and shut off access.
2. Reconfirm confidentiality and covenants.
3. Document the reason cleanly.
4. Business goal: protect data, customers, and momentum.

F. When to call your lawyer.

1. Before terminating someone who complained or requested leave.
2. Upon receiving a charge, subpoena, or agency inquiry.
3. When planning a reduction in force.
4. When a data breach or leak is suspected.
5. When a key employee is exiting to a competitor.