Seyfarth

Digital Exfiltration & Departing Employees: Protecting Trade Secrets in a Modern Risk Environment

June 18, 2026

Legal Disclaimer

This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal or expert opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

Speakers

Jay Carle
Partner
Chicago

Marcus Mintz
Partner
Chicago / Los Angeles – Century City

Joe Greenfield
President & Chief Forensic Examiner
Maryman

Agenda

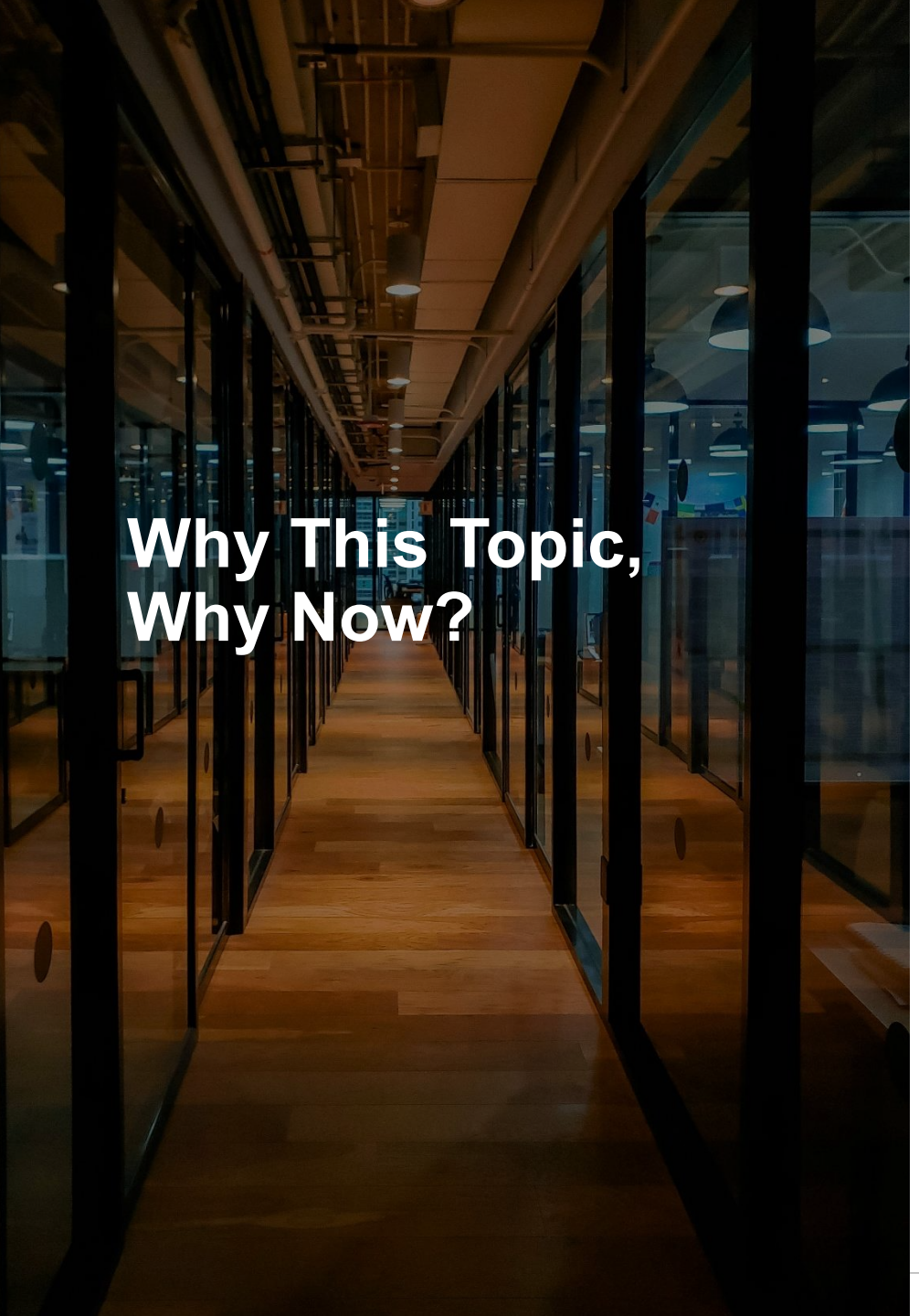
1 | Why This Matters Now

2 | How Data Walks Out the Door

3 | Prevention Strategies

4 | Responding to Departures

5 | Practical Takeaways & Action Plan



The Business & Legal Stakes Are High

- Majority of trade secret misappropriation involves **departing employees.**
  - Exfiltration vectors have multiplied
  - Narrow window to detect and respond
  - **Loss of Competitive Advantage**
  - **Litigation Cost & Disruption**
  - **Reputational & Regulatory Risk**

Understanding the Threat Landscape

How Data Walks Out the Door

Common Exfil Techniques

- USB Devices (thumb drives, hard drives, SSDs)
- Personal computers masquerading as company computers
- BYOD (bring your own device)
  - Backups of personal devices that store company data…
- Cloud Storage (iCloud, Google Drive, Dropbox, etc.)
- Email (Business, Personal)
- Remote Desktop/Control Software (TeamViewer, GoToMyPC, etc.)
- Printed documents
- Photos/Videos using mobile devices/tablets
- AI Platforms

How Data Walks Out the Door

Behavioral Red Flags

- Unusual after-hours access or downloads
- Sudden interest in files outside job scope
  - Requests for access permissions
- Declining performance / disengagement
- Communications with competitors
- Resignation timed to project milestones

High-Risk Data Categories

Know what you have before you can protect it.

CROWN JEWELS

STRATEGIC

RELATIONAL

Customer lists · Sales pipeline · CRM data

OPERATIONAL

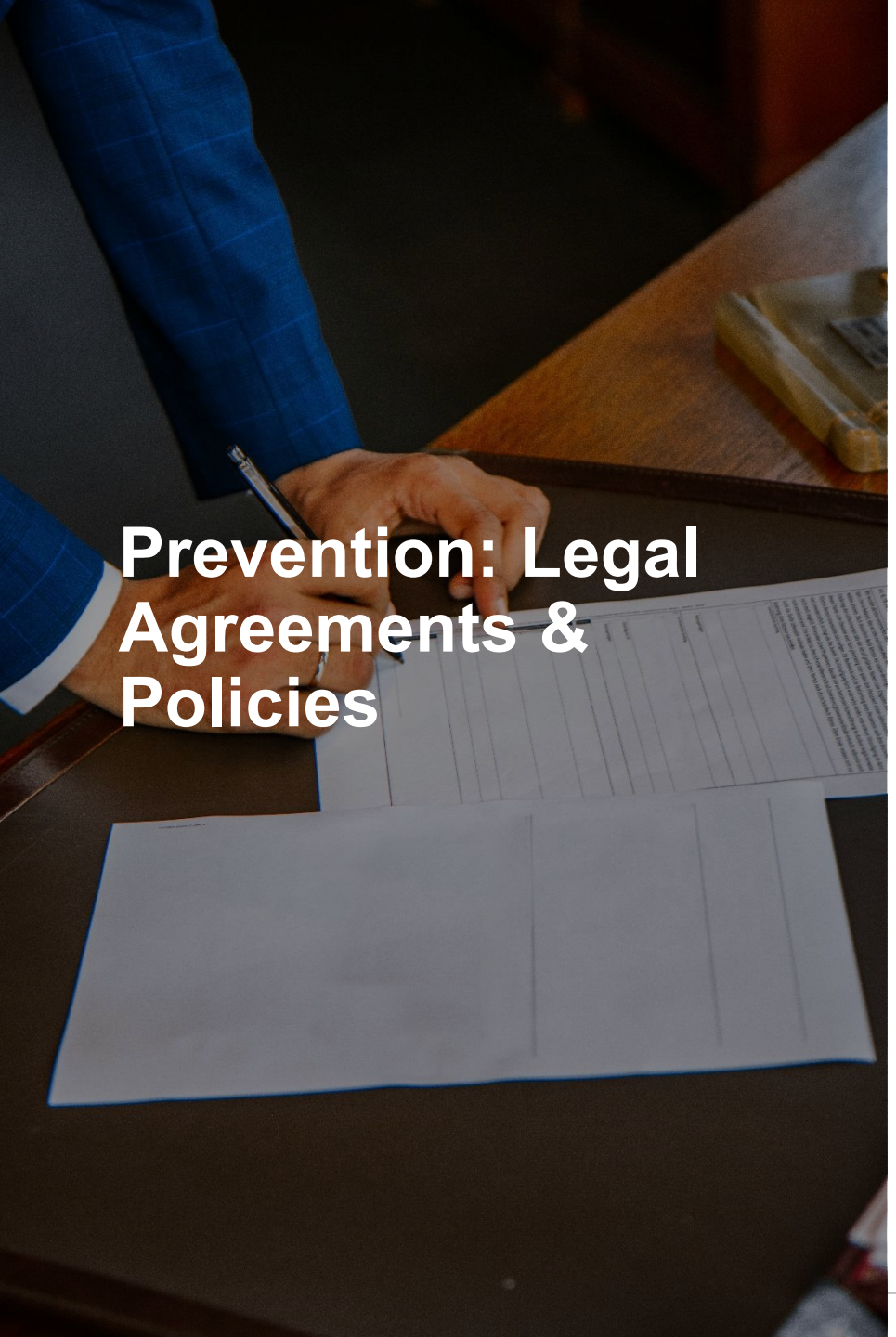
Vendor terms . SOPs · Training materials · Internal processes

The Litigation Lens

Most-litigated categories:

- Source code
- Customer & pricing data
- Product roadmaps

Prevention: Legal Agreements & Policies



Prevention: Legal Agreements & Policies

Employment Agreements

- **NDAs / Confidentiality**
  - Define "Confidential Information" with precision and flexibility
  - Duration, return obligations, and post-employment hooks
  - Assignment of invention
- **Non-Competes**
  - State-by-state enforceability
  - FTC rulemaking developments & status
  - Choice of law and venue strategy
  - Alternatives
- **Non-Solicits (customer & employee)**
  - Customer non-solicits vs. no-hire provisions
  - Employee non-solicits — current enforceability trends
  - Tailoring scope: who, what, how long
  - Pairing with confidentiality for layered protection
- **Return-of-Property & Cooperation**

Prevention: Legal Agreements & Policies

Acceptable Use & Technology Policies

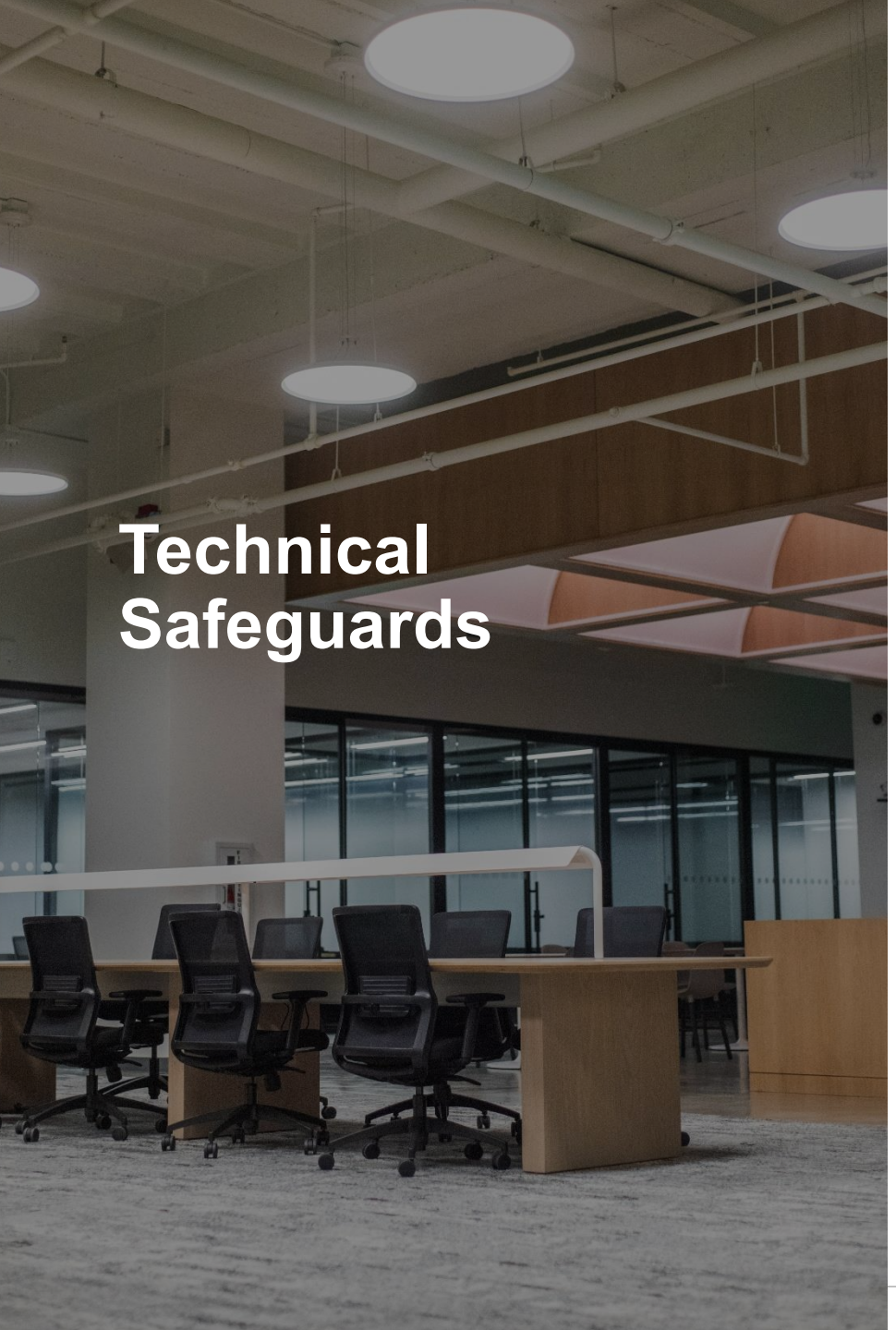
- **BYOD: employer access, remote wipe, segregation**
- **Cloud storage, personal email / Accounts**
- **AI tool use**
- **Social media & LinkedIn**
- **Monitoring & consent disclosures** — and actually monitoring

Prevention: Legal Agreements & Policies

Exit & Offboarding Protocols

- Exit interview — remind of continuing obligations.
- Written certification of return/deletion.
- Re-sign confidentiality acknowledgments.
- Trigger departing employee forensics process where warranted.


Preventive Security
& Technical
Controls



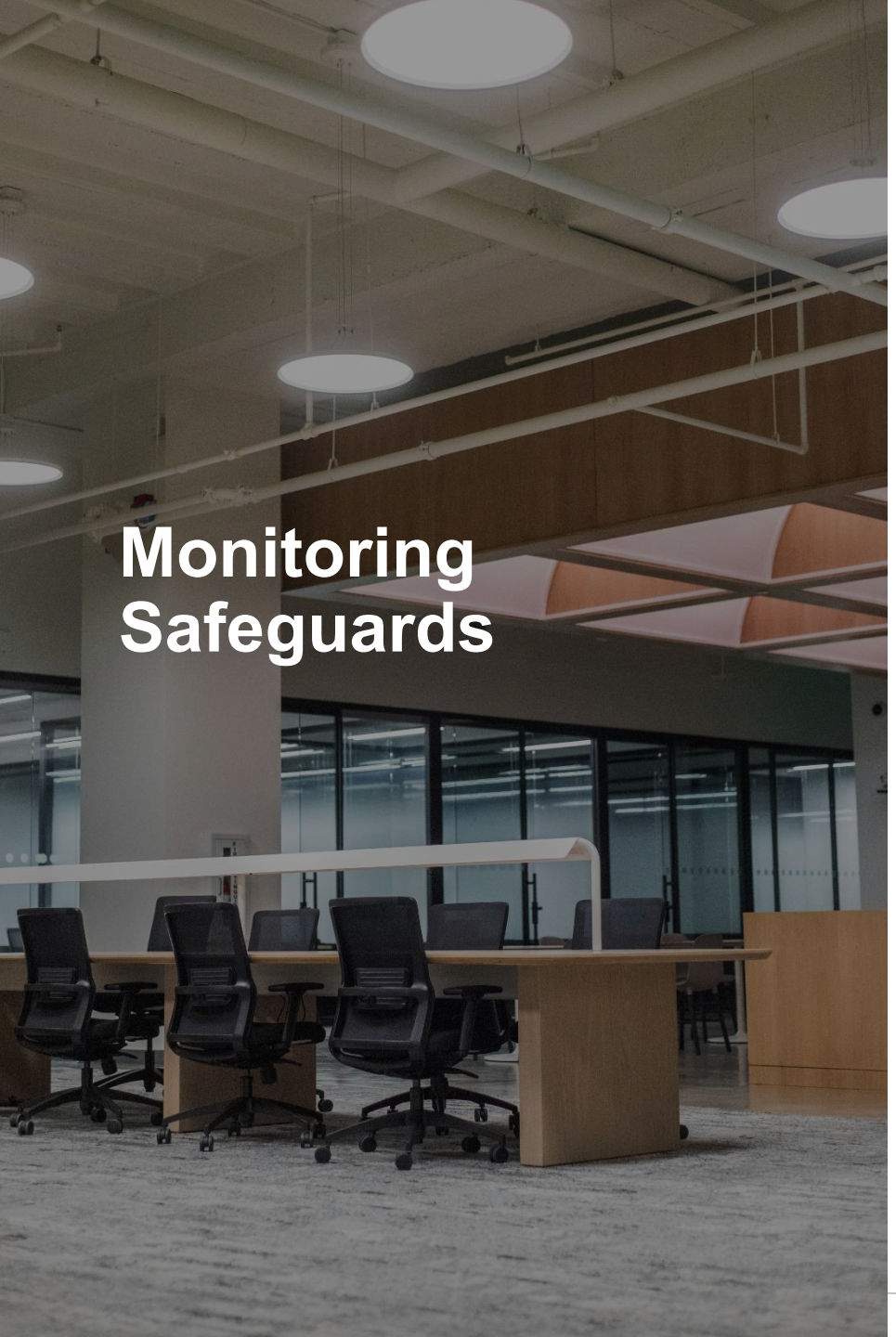
The Technical Control Stack

- **Identity & Access**
  - Least privilege principles
  - Just in Time (JIT) access
  - Multi-Factor Authentication (MFA)

- **Endpoint**
  - Endpoint Detection & Response (EDR)
  - Data Loss Prevention (DLP)

- **Cloud**
  - Cloud Access Security Brokers (CASB)
    - sharing controls,
    - shadow IT discovery

- **Data** classification, tagging, encryption



Employee Monitoring: Legal Guardrails

- Clear, conspicuous notice
- Written consent
- State-law variations (CA, NY, IL, CT, etc.)
- Cross-border considerations

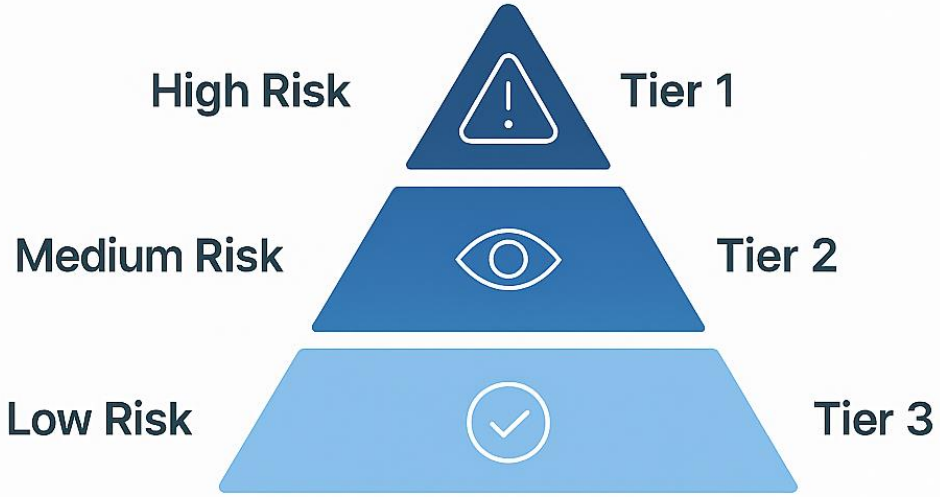

When an Employee
Departs

Triggering an Investigation

Employee Departure Playbook

Risk-Tiered Approach

Not every departure warrants a deep dive



- Proactive forensic review vs. reactive investigation
- Coordinated playbook: HR + IT + Legal + Management

Criteria for Risk-Tiering Rubric Role • Access • Destination • Behavior

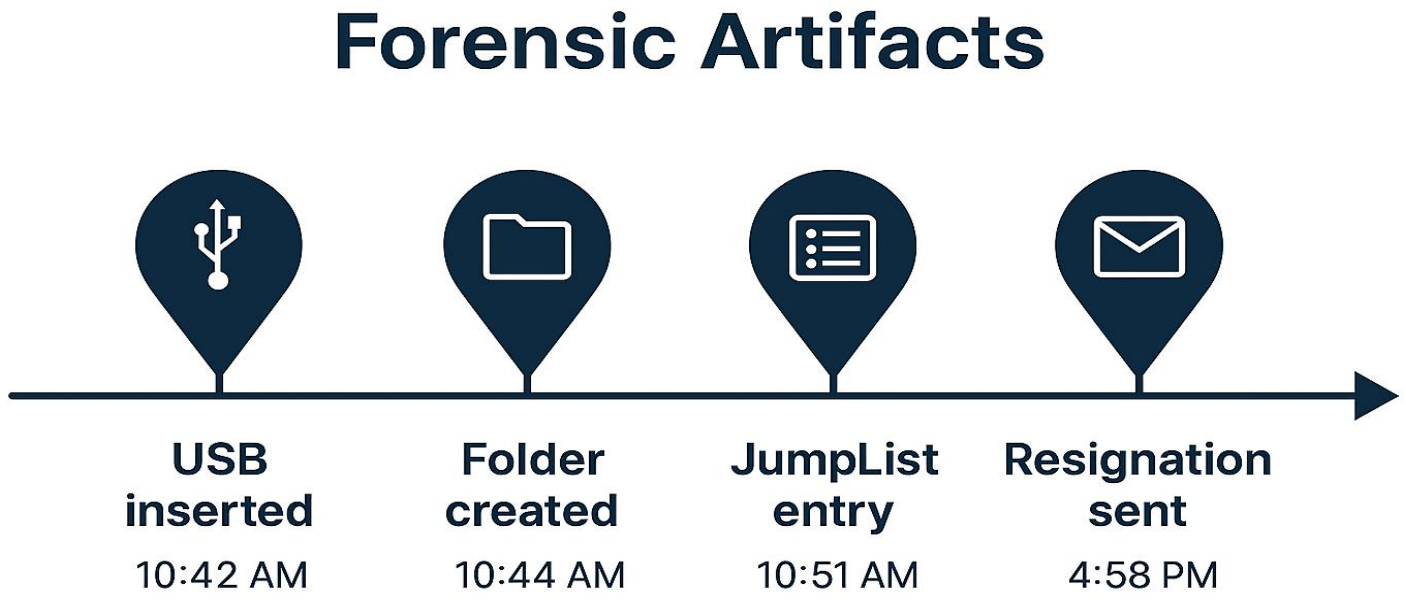
Forensic Preservation & Evidence Collection

- Primary sources:
  - laptop image,
  - email,
  - cloud logs,
  - mobile devices,
  - badge data

- Often overlooked:
  - USB history,
  - browser artifacts,
  - printer logs,
  - chat exports,
  - mobile device pictures, videos, and audio recordings,
  - **AI tool history**

Forensic Investigation

Building the Narrative from Artifacts



- Stitching activity into a coherent timeline
- Corroboration across data sources

What To Do When It Happens

What To Do When It Happens:

Rapid Legal Response

Pre-Litigation: Preservation & Demand

- Litigation hold
- Cease-and-desist strategy and timing
- Demand return, deletion, and certification
- **Emergency & Injunctive Relief**
  - TROs and preliminary injunctions — standards & evidence
  - Expedited discovery & forensic protocols

What To Do When It Happens:

Considerations for the New Employer

New Employer Liability

- Vicarious liability & inducement claims
- Knowledge-based theories (willful blindness)
- Onboarding protocols that protect the company
- Ethical walls, screening, and agreed protocols


Practical
Takeaways

Takeaways

- Prevention is layered
  - legal + policy + technical
- Speed wins
  - the first 72 hours matter most
- Documentation is your best evidence
  - before, during, and after

Action Items

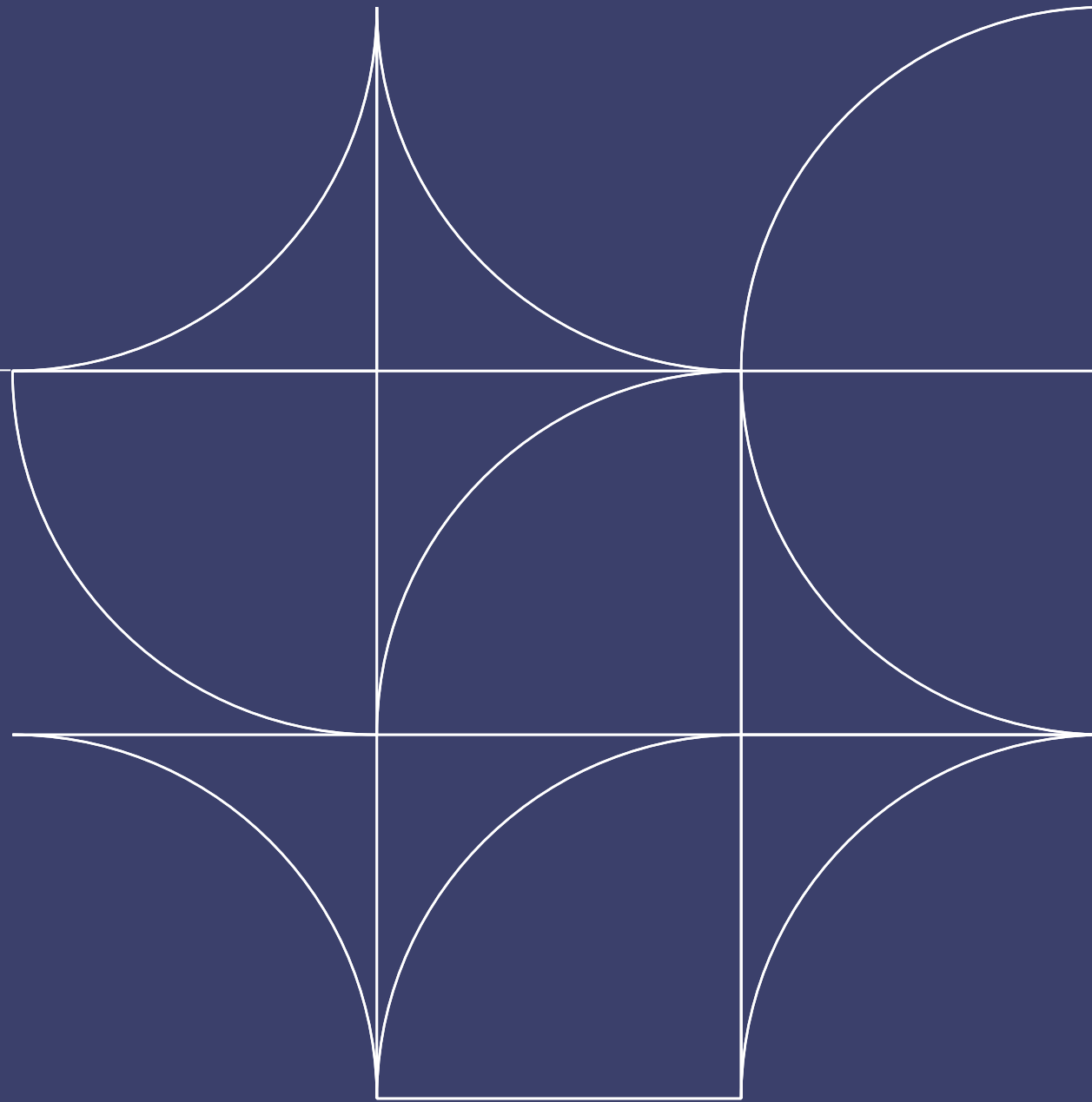
- **Legal & Compliance**
  - Audit & update NDAs, non-competes, IP assignments
  - Document an exit/offboarding protocol with legal and IT checkpoints
  - Map your crown jewels
- **HR & Management**
  - Train managers on behavioral red flags
  - Standardize exit interviews with confidentiality reminders
  - Cross-functional coordination on high-risk departures
- **IT & Security**
  - Inventory & classify sensitive data
  - Tune DLP, logging, and egress visibility
  - Pre-build a forensic preservation playbook
  - Tabletop the departure scenario before you need it

thank you

Jay Carle
Email: jcarle@seyfarth.com

Marcus Mintz
Email: mmintz@seyfarth.com

Joe Greenfield
Email: jgreenfield@maryman.com



VERIFICATION FORM

Please scan the QR code to complete the digital attendance verification form to receive CLE credit for this program.

QR code directs you to our electronic form which can also be found in the calendar invite that was sent to you for this program.

You will need:

1. **Title:** Digital Exfiltration & Departing Employees: Protecting Trade Secrets in a Modern Risk Environment
2. **Date Viewed:** June 18, 2026
3. **Attendance Verification Code:** SS3851

State-specific CLE credit information can be found in the form.