Crisis Control:
Managing Trade Secret Misappropriation and Data Breaches

2025 Trade Secrets Webinar Series

September 25, 2025

Seyfarth Shaw LLP

Legal Disclaimer

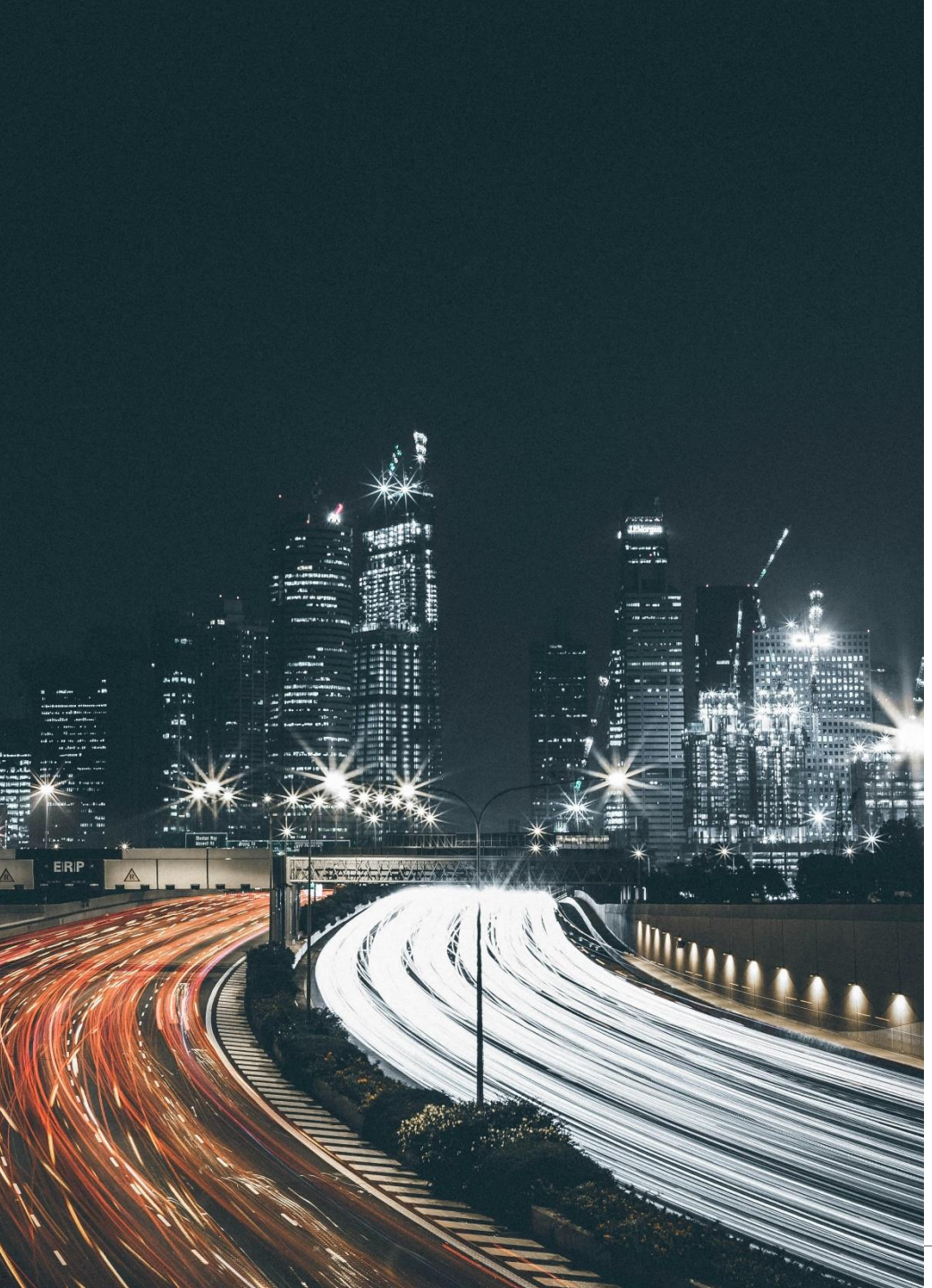
This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you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

Speakers

Dawn Mertineit
Partner
Boston

Jay Carle
Partner
Chicago

Kevin Mahoney
Partner
Chicago



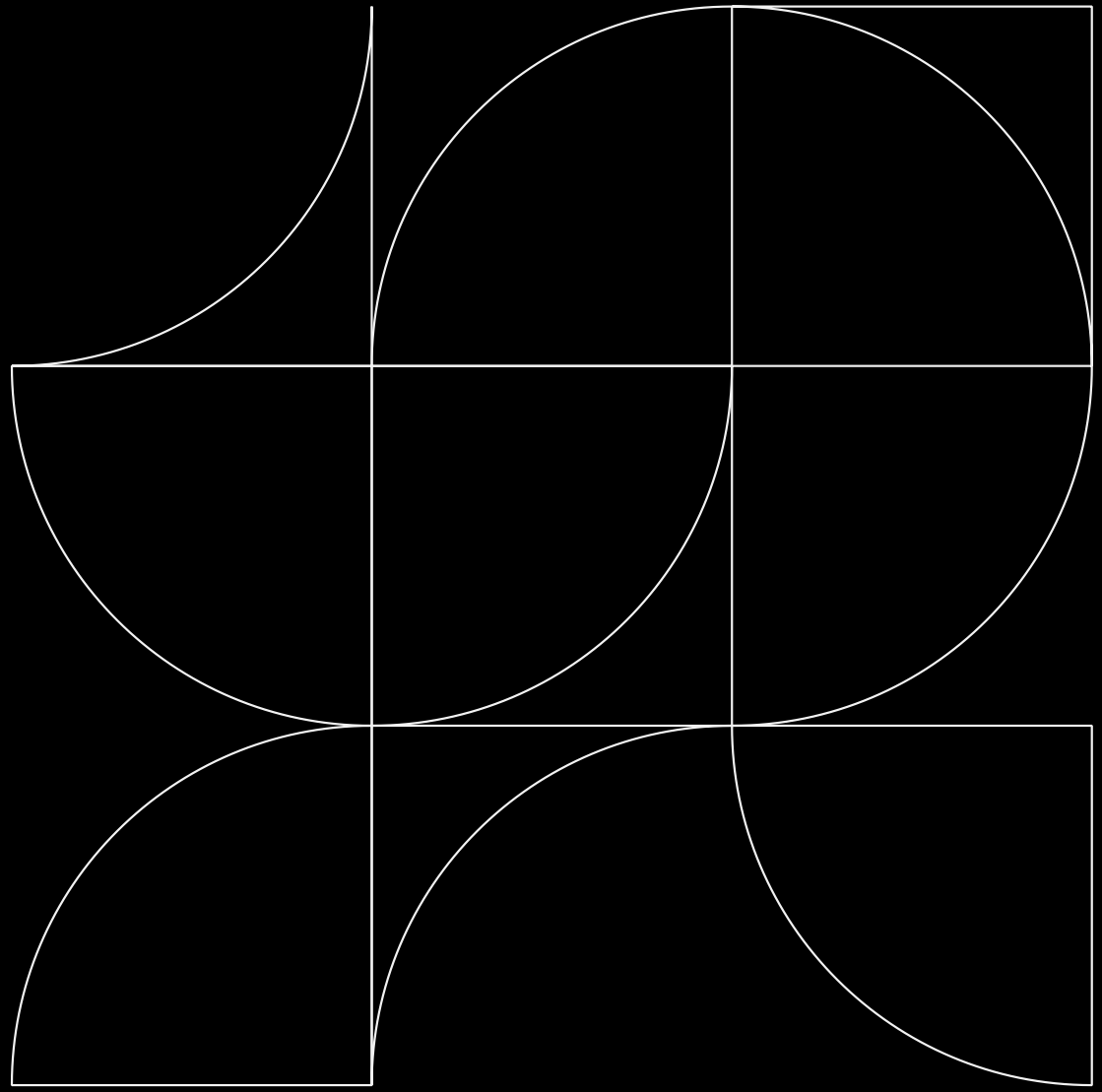
Agenda

1. **The Risk Landscape: Why This Matters**
   - The value and vulnerability of trade secrets
   - Financial impacts
   - Emerging threats

2. **Legal Framework: What the Law Requires**
   - Case law trends & lessons learned
   - Courts' expectations around secrecy and reasonable protection

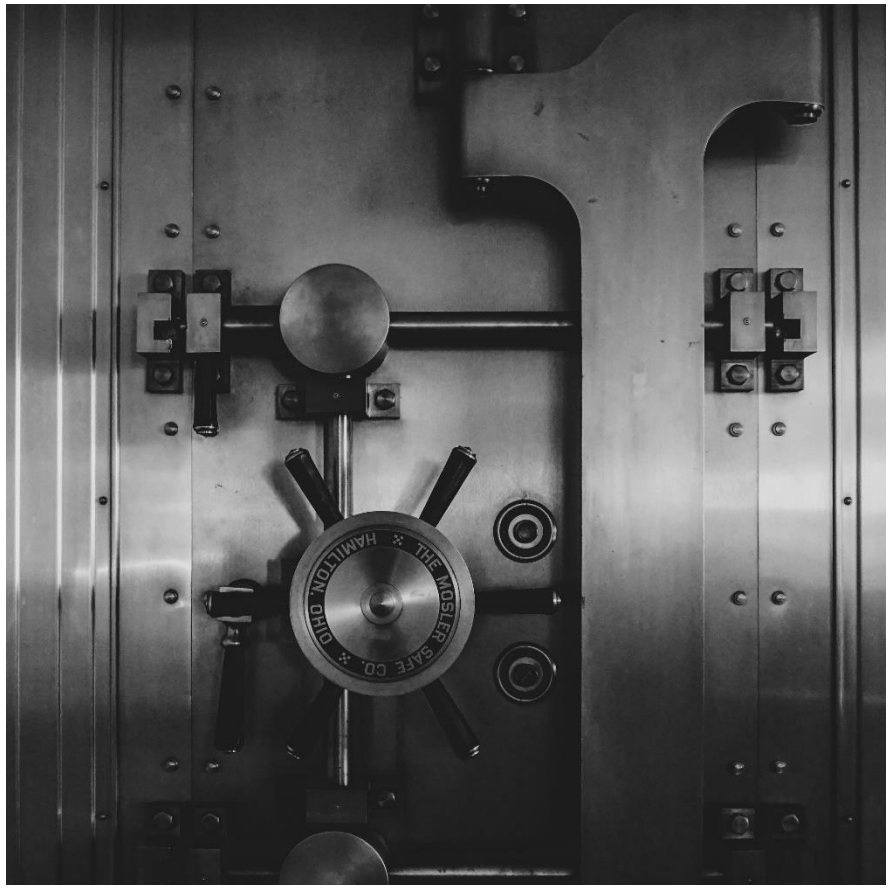
3. **Crisis Control: What Clients Can Do to Manage Risk**
   - Reactive strategies
   - Proactive strategies
   - Governance fundamentals
   - Integrated approach: legal, IT, compliance, and cybersecurity collaboration

The Risk Landscape: Why This Matters



Trade Secrets Are Critical to Businesses

- Trade secrets are often a business's most critical assets
  - Trade secrets are often what drives a business's revenue, whether via unique products or services provided to customers
    - Source code
    - Processes
    - Customer information
    - Strategies
    - Financial information
  - Patent protections are time-limited; trade secrets can remain protected for as long as a business takes reasonable measures to keep them secret



Trade Secret Misappropriation is Expensive

- Trade secret misappropriation costs American businesses ***$300 billion*** annually
  - Lost brand dominance
  - Decreased profits
  - Legal spend (average for trade secrets cases $3-5M)
  - Reputational damage
  - Decreased market valuation

- The impact of poor data security and information governance leading to a data breach can be significant
  - Reputational damage
  - Lost business, Breach Response, and class action litigation risk
  - Top 10 settlements in 2024: Totaled $593.2 million

Trade Secrets Must Be *Secret*

Public disclosure of a trade secret destroys the information's status as a trade secret.

Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984)

“It is axiomatic that without secrecy, no trade secret can exist.”

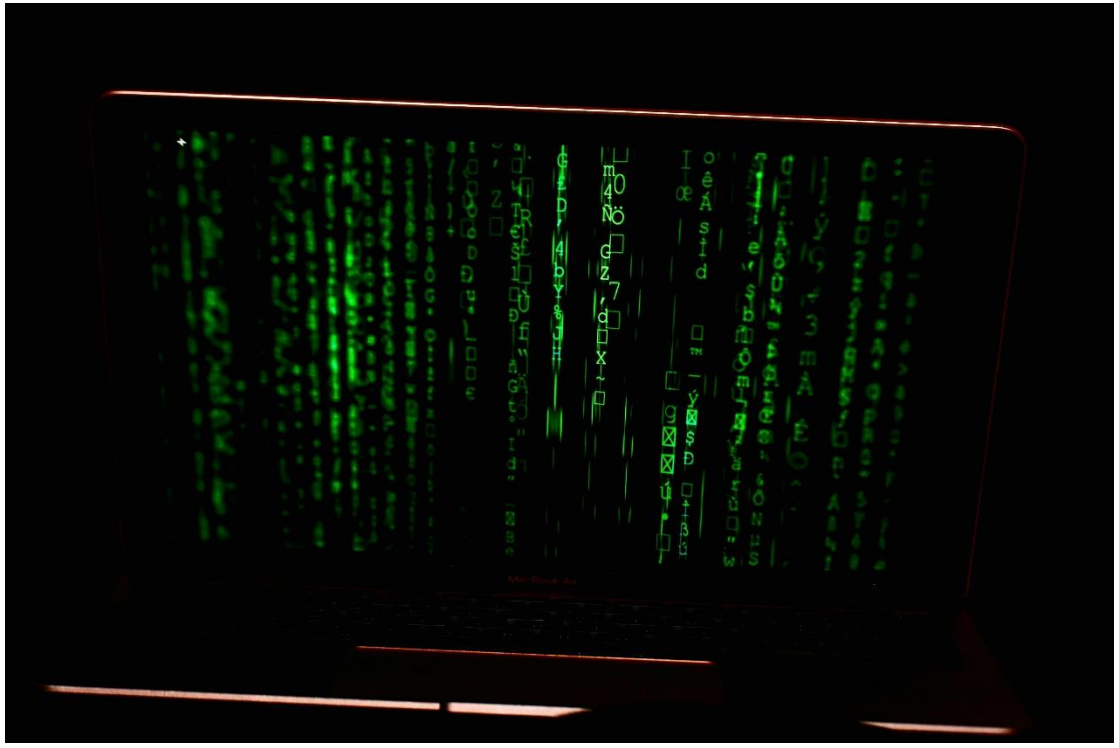
BDT Products, Inc. v. Lexmark, International, Inc., 274 F. Supp. 2d 880, 891 (E.D. Ky. 2003)

Publication – Intentional or Otherwise – Has Downstream Effects

- Publishing information (whether on a company website, in news articles, at earnings calls, or otherwise) will render the information no longer subject to protection
- Failure to adequately prevent trade secret misappropriation will have the same result
  - In other words, it's not just a business's proactive publication of confidential information that will result in a loss of legal protection
  - Failure to implement reasonable measures aimed at protecting confidential information/trade secrets will also be considered (more on this later)
- 90% of misappropriation is accomplished by employees and business partners

The Misappropriation Landscape is Changing

- Methods of misappropriation change over time – many ways for bad actors to steal data
  - Forwarding information to private email accounts
  - USB drives
  - Unauthorized uploads
  - Use of private devices for work (esp. while remote)
  - Good old-fashioned printing and screenshots
- It's not just malicious actors
  - Insecure systems
  - Lax remote policies
  - Lack of employee training
  - Use of generative AI



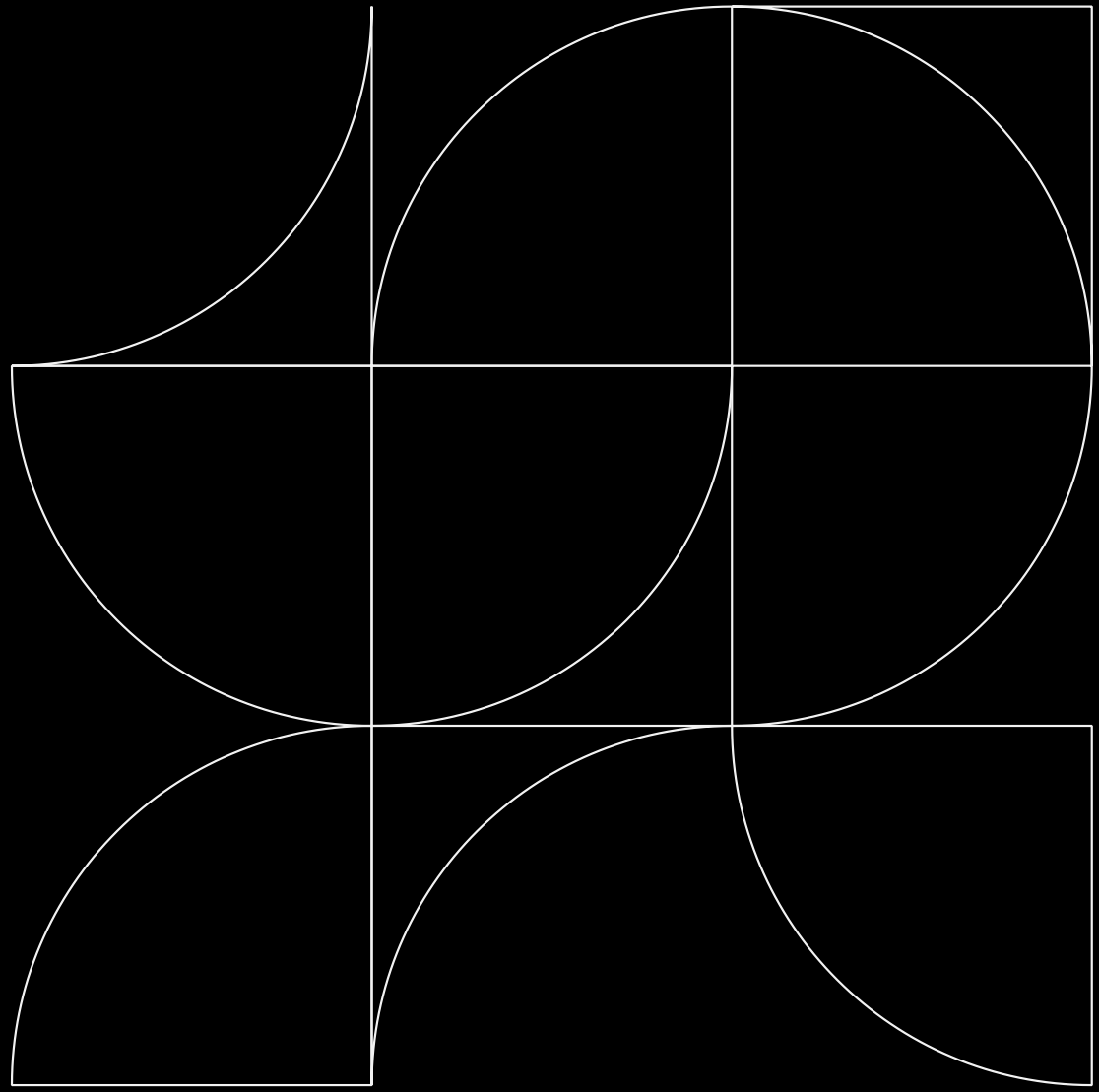
Insulet v. EOFlow – a Cautionary Tale

- This case resulted in the largest DTSA jury verdict to date – **$452M**
  - $170M in compensatory damages
  - $282M in exemplary damages

- Not so fast, though….
  - Both parties have appealed
  - One likely issue on appeal is Insulet's suspicions and whether it moved quickly enough to protect its IP
  - The Federal Circuit overturned the trial court's preliminary injunction, in what may be foreshadowing

What the Law Requires

Emerging Case Law Trends



Emerging Case Law: Speed in Responding to Misappropriation is Critical

1

Elite Semiconductor, Inc., v. Anchor Semiconductor

(N.D. Cal. Jan. 13, 2025)

- Statute of limitations begins running upon discovery of any evidence of misappropriation, even if ultimately unable to prove claim.

2

Pliteq, Inc. v. Mostafa, 775 F. Supp. 3d 1231, 1259 (S.D. Fla. Mar. 31 2025)

Delay of approximately 2 months after learning of data breach was not fatal to request for injunctive relief, although Court noted it was a close call and credited Plaintiff for trying to arrange informal return in the interim.

f

3

iTalent v. Kotha (N.D. Cal. Sept. 19, 2025)

"The Court notes that the gap in time between itD's filing of the initial complaint and submitting the TRO application is explained by the need to conduct a thorough investigation before asking the Court for relief."

Emerging Case Law: Early Detection Efforts are Key

1

PhysioTherapy Assoc. v. ATI Holdings (N.D. Ala.)

- Password protections for electronic accounts alone may not be enough.
- Courts increasingly looking to other levels of protection to see if sufficient steps were taken.

2

Yellowfin Yachts, Inc. v. Barker Boatworks LLC (11th Cir.)

- Failure to follow through on practices during employment.
- Failure to follow up on evidence of exfiltration after employment.

3

BCOWW Holdings, LLC v. Collins, (W.D. Tex.)

- Applying trade secret protections internally v. externally.
- Once information is out in the public, it's no longer a trade secret.

Real World Case Studies: Unsuccessful

PhysioTherapy Assoc. v. ATI Holdings **(N.D. Ala.)**

- Employee with access to critical information about customer information presented it in a memorandum to plaintiff's competitor seeking to expand into market.
- Focus of decision was on the fact that Plaintiff failed to take reasonable steps to secure information.
  - Passwords on their own are not enough. "**…**the use of password-protected servers shows reasonable secrecy *only* when paired with other substantial efforts... This court finds that Physiotherapy's password-protection system reflects little more than a 'normal business practice.'"
  - No information marked confidential.
  - Lack of confidentiality agreements for some employees with access is a problem, but existence of agreements likely not sufficient.
  - No evidence that employees were instructed to keep information a secret.

Real World Case Studies: Unsuccessful

Yellowfin Yachts, Inc. v. Barker Boatworks LLC **(11th Cir.)**

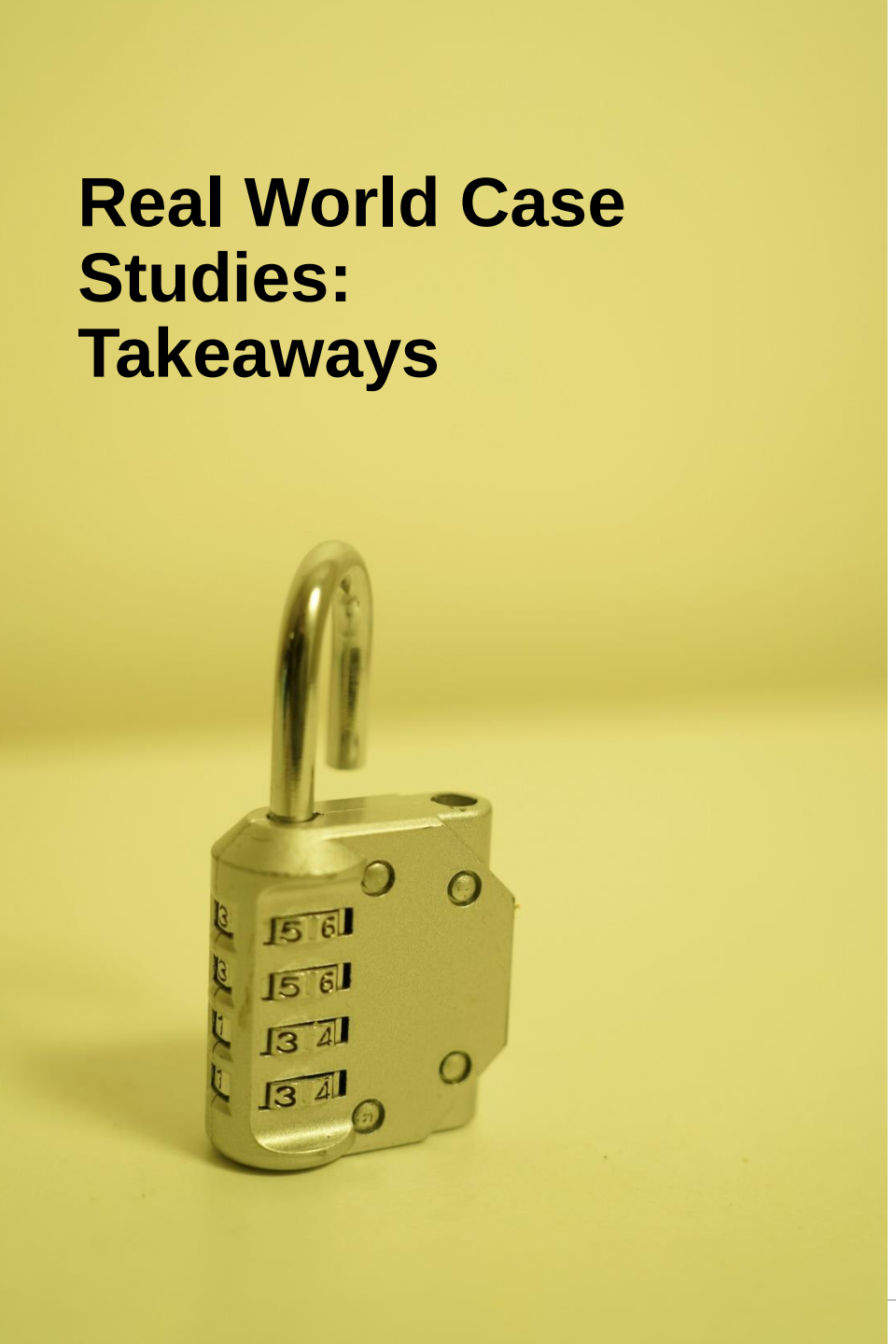
- Executive left to found his own competing company. On his last day, downloaded “hundreds of files” with detailed customer information and design specifications.
- Court found that plaintiff had failed to take reasonable steps to protect trade secret information:
  - Executive had refused to sign confidentiality agreement during onboarding but was given access anyway.
  - Company policies prohibited external sharing of information, but in practice had “encouraged Barker to store [the] information on a personal laptop and phone.”
  - Despite knowing that company information was sent, company never asked Defendant to delete the information after he left.

Real World Case Studies: Unsuccessful

BCOWW Holdings, LLC v. Collins, (W.D. Tex.)

- Plaintiff alleged former partner left with critical information about vendor and client relationships.
- While internal confidentiality measures were suspect, key factor in court ruling was that allegedly trade secret information was shared with third party vendors without any confidentiality obligations.
  - "[Plaintiff] BCOWW did not require [vendors] to sign confidentiality or exclusivity agreements and routinely transmitted files to these vendors via unsecured email."
  - **"**BCOWW did not mark any of these documents as confidential or restrict its vendors' storage or use of the information."
  - "Nor is there any evidence that BCOWW even *verbally* imparted (or even internally discussed) the need for these vendors to maintain the secrecy of its information."

Real World Case Studies: Takeaways



- Just requiring a password for electronic users is “table stakes.” Courts are increasingly looking to what other steps are in place.
- Inconsistent application of policies and rules creates problems. What does the handbook say versus what does everyone actually do?
- For “need to know” information access, what does the plaintiff claim versus what is actually in practice.
- Consider implementation of software or specialized teams for early detection of insider threats of misappropriation, and ensure checks and balances in place.
- For countering external threats, thoughtful and regular trainings for employees pay dividends.

Emerging Vulnerabilities Associated with Trade Secret Theft in Cases

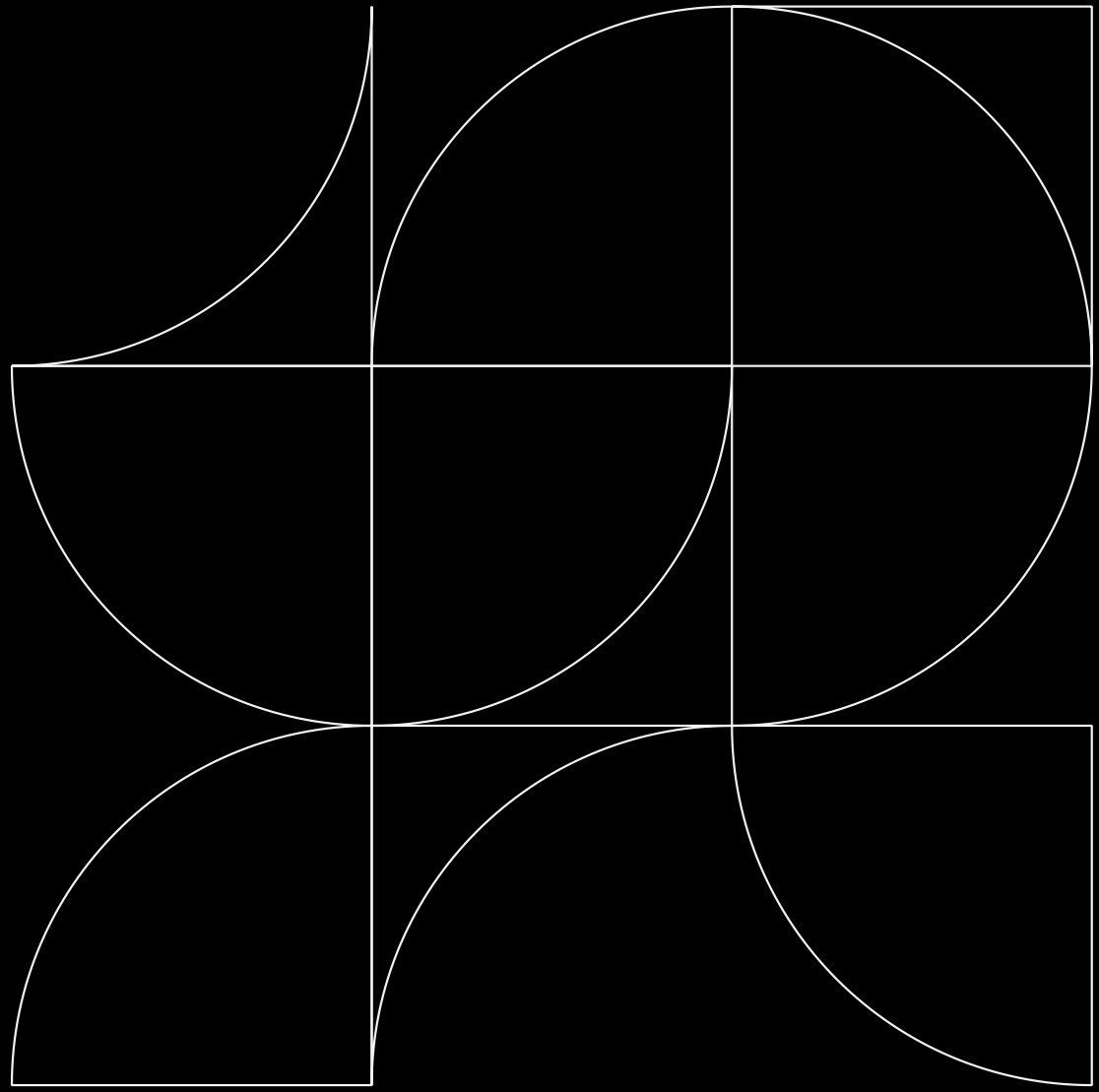
- Ease of use and wide availability of cloud-based transfer and storage for insider threats of misappropriation.
- Effect of remote work environment has made it harder to discern actual threats form “business as usual.”
- External threats including phishing continue to become more sophisticated, including use of generative AI in scams.
- External threats from overseas mean limited legal options when it comes to emergency situations.

Emerging Case Law Trends: the “California Model” of Early Particularity

- Courts outside of California increasingly requiring an upfront identification of particular trade secrets, rather than after discovery.
- *Integrity Sols., Ltd v. MCS Consulting, Inc.*, D. Colo. Apr. 25, 2025) (explaining that a plaintiff “ ‘will normally be required first to identify with reasonable particularity the matter which it claims constitutes a trade secret, before it will be allowed ... to compel discovery of its adversary's trade secrets.’ ”)
- *Terran Biosciences, Inc. v. Compass Pathfinder Ltd.*, (D. Md. June 3, 2025) (particularity requirement is fact dependent on each case).
- If someone asked you tomorrow what your 3 most important trade secrets are, could you explain what those are in plain English?

Crisis Control Practical Solutions

Effective strategies to safeguard confidential information.



From Chaos to Control

Effective Protection Requires Both Reactive and Proactive Strategies

Misappropriation risk is dynamic — threats can emerge from insiders, outsiders, or systemic vulnerabilities.

Reactive strategies help contain damage, preserve evidence, and enforce rights after an incident occurs.

Proactive strategies reduce the likelihood of incidents and improve readiness to respond.

Integrated protection combines legal, technical, and operational tools to manage risk across the data lifecycle.
Information governance is foundational — access controls, retention policies, and monitoring are key.

DATA Law approach aligns cybersecurity, information governance, compliance, eDiscovery, and privacy into a unified framework.

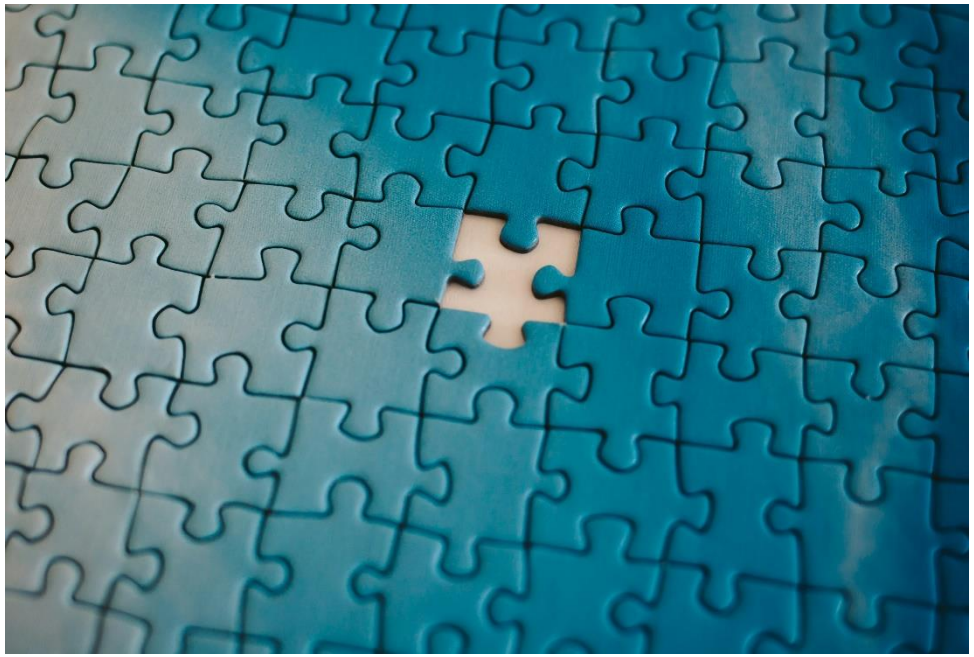
Where Are You on the Maturity Assessment?

QUESTION	PURPOSE
Is your incident response plan tested and cross-functional?	Determine readiness and coordination across departments (Legal, IT, HR)
Do you have clear access controls for sensitive data?	Assess data protection and role-based access maturity
Are retention and deletion policies consistently enforced?	Evaluate governance and compliance with legal obligations
Do you actively monitor for insider threats or unusual activity?	Gauge proactive detection capabilities
Are legal, IT, and compliance teams aligned on data governance?	Identify integration and strategic alignment across functions

Coordinated Incident Response

- Cross-Department Collaboration

  Incident response requires seamless alignment among Legal, IT, HR, and leadership to ensure effective crisis management.



- Clear Roles and Escalation

Establishing defined roles and escalation paths helps organizations respond swiftly and cohesively during incidents.

- Legal / Outside Counsel
- Forensics / Vendors
- IT / Security
- HR / Communications

Preserving Digital Evidence

- **Legal Holds Implementation**
  - Phones, tablets, computers, chats, email, access logs, monitoring logs, vpn, etc.
- **Forensics**
  - Internal solutions
  - External partnerships (remote solutions, speed, competence)
  - Chain of custody
- **Best Practices Checklist**
  - Using a checklist guides teams through proper preservation steps reducing risks of preservation gaps.

Move Quickly to Litigation

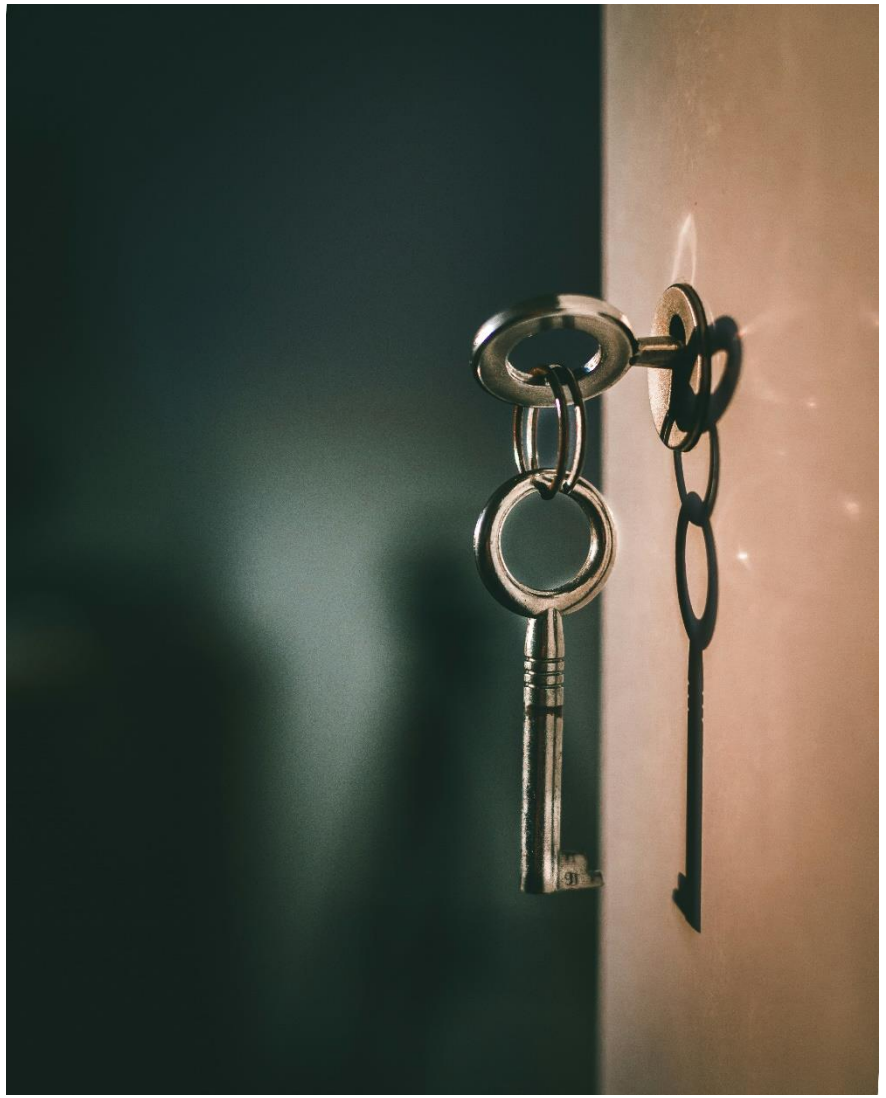
- **Importance of Speed**
  - Quick action preserves leverage, securing critical access to key individuals and sensitive information.
- **Effectiveness of Injunctive Relief**
  - Injunctive relief works best when the perpetrator is still accessible, preventing further data breaches.

Active Monitoring Tools

- **Proactive Threat Detection**
  - Monitoring tools detect unusual file access, transfers, and deletions to prevent security breaches early.
- **Real-Time Alerts and Dashboards**
  - Dashboards provide up-to-the-minute data enabling quick identification of suspicious activities.
- **Integration into Operations**
  - Integrating monitoring tools into daily workflows enhances response capabilities and breach prevention.

Offboarding Protocols

- **Access Revocation**
  - Revoking employee access promptly protects sensitive systems from unauthorized entry post-departure.
- **Device Retrieval**
  - Retrieving company devices ensures physical control over data and prevents information leaks.
- **Forensic Activity Review**
  - Conducting forensic reviews of recent employee activity detects suspicious behavior before departure.
- **Use of Checklists**
  - Structured checklists / IT SOPs to ensure all offboarding steps are completed comprehensively and consistently.



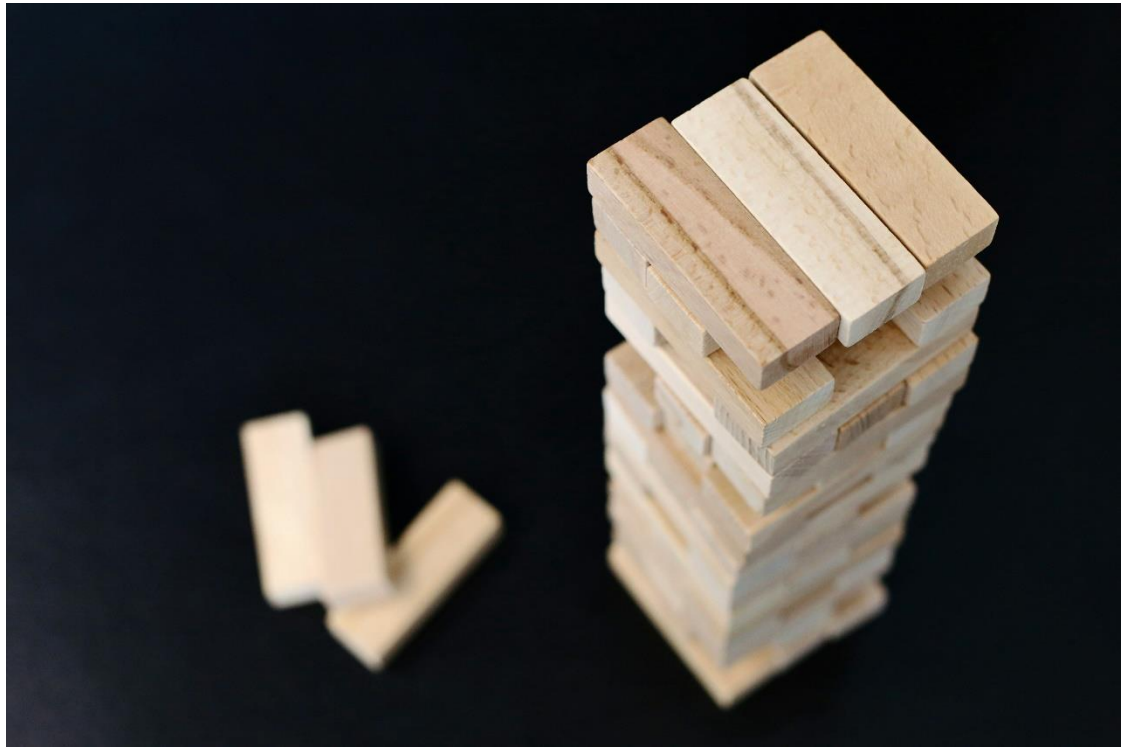
Employee Training & Culture

- **Building Awareness Culture**
  - Employee training fosters a culture of awareness crucial for preventing data breaches and protecting trade secrets.
  - Onboarding and annual training for key personnel.
  - Promote a culture of accountability.

- **Clarifying Confidential Information**
  - Training clarifies what is confidential and shares examples of acceptable and unacceptable behaviors.
  - Use real-world examples to illustrate what can and cannot be shared.

- **Embed Security into Daily Habits**
  - Teach secure practices like locking screens, avoiding public Wi-Fi for sensitive work, and reporting suspicious activity.
  - Make confidentiality part of routine workflows, not just compliance checkboxes.

Good Information Governance = Good Defense

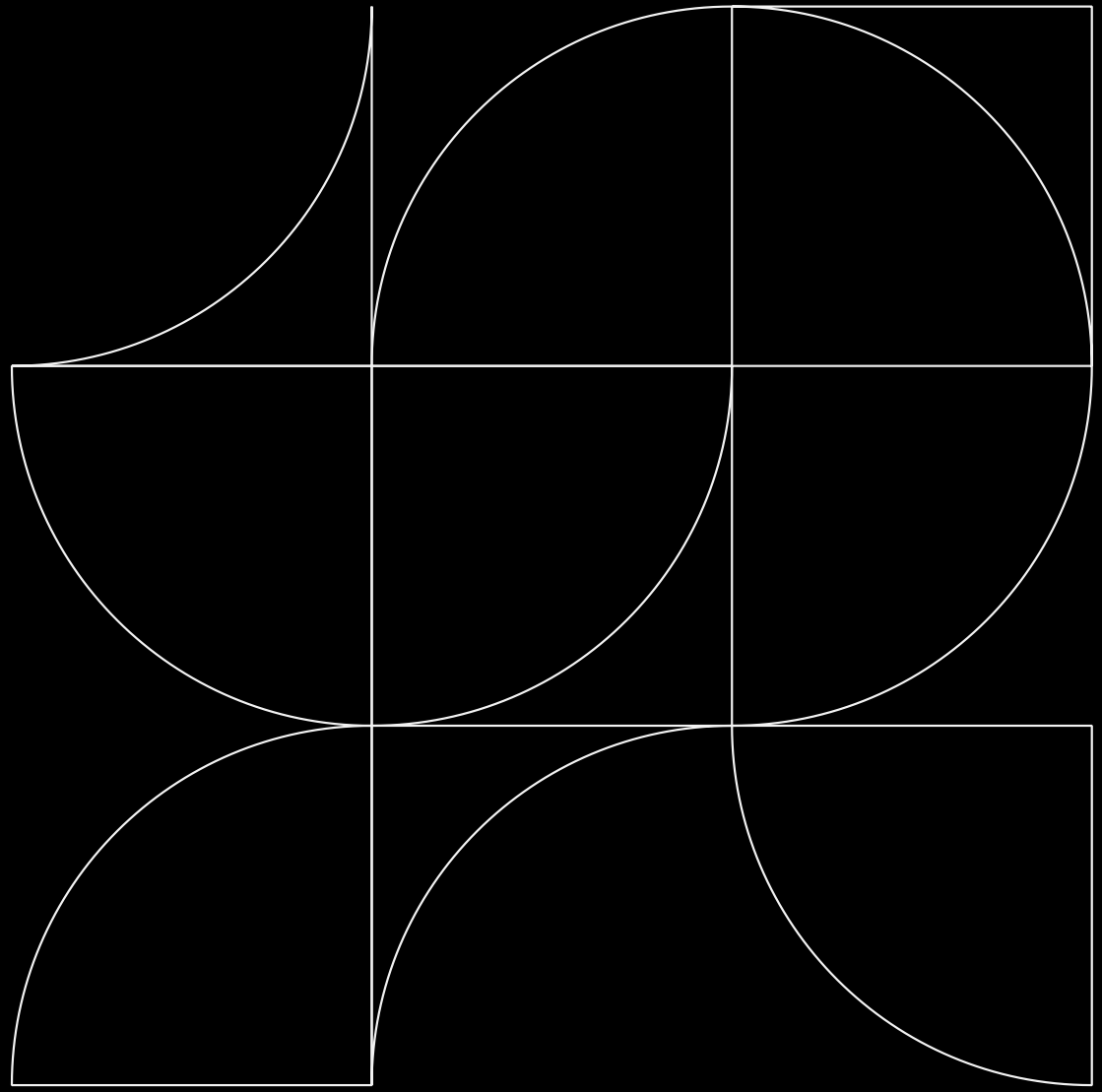


- **Information Governance Fundamentals**
  - Access controls, retention policies, and deletion protocols build a strong foundation for protecting sensitive information.
  - Having what you don’t need = RISK.
- **Risk Reduction and Compliance**
  - Effective governance lowers breach exposure while ensuring regulatory compliance and operational efficiency.
- **Integrated Security Strategy**
  - Governance works with security and legal strategies in a layered defense to manage risks effectively.

Aligning Governance with Legal Strategy - Key Takeaways

- **Crisis Response Coordination**
  - Fast and coordinated action during crises ensures effective response and recovery outcomes.
  - Know what to do / who to call.
- **Proactive Risk Management**
  - Monitoring, governance, and training help reduce risks and enhance preparedness effectively.
- **Effective Information Governance**
  - **Multidisciplinary Integration: Legal, Cyber, eDiscovery, IT, Compliance**

Questions?



SCAN ME

CLE ATTENDANCE 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:** Crisis Control: Managing Trade Secret Misappropriation and Data Breaches
2. **Date Viewed:** 09/25/25
3. **Attendance Verification Code:** SS0996

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

thank you

For more information, please contact us

Dawn Mertineit
email: DMertineit@seyfarth.com

Jay Carle
email: JCarle@seyfarth.com

Kevin Mahoney
email: KMahoney@seyfarth.com