MAYER | BROWN

THE NEW CONSUMER PROTECTION PLAYBOOK:
HOW IN-HOUSE COUNSEL CAN NAVIGATE PRIVACY AND CYBER RISKS IN A RAPIDLY CHANGING TECH ENVIRONMENT

March 27, 2026

TODAY'S SPEAKERS

PARTNER

SPENCER GLENDE

SALT LAKE CITY +1 801 907 2740
SGLENDE@MAYERBROWN.COM

PARTNER

AMBER THOMSON

WASHINGTON DC +1 202 263 3456
ATHOMSON@MAYERBROWN.COM

AGENDA

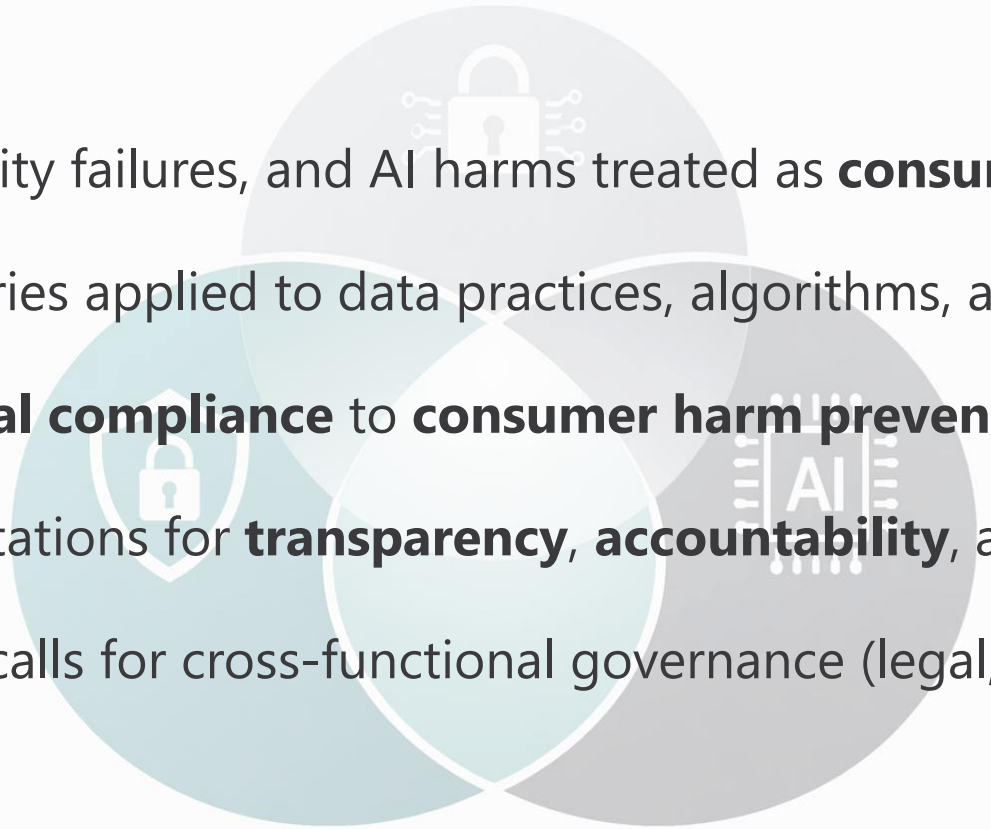
1. Regulatory and Enforcement Trends
2. Key Risk Factors for Companies
3. Practical Strategies for In-House Counsel
4. What In-House Counsel Should Prioritize
5. Q&A

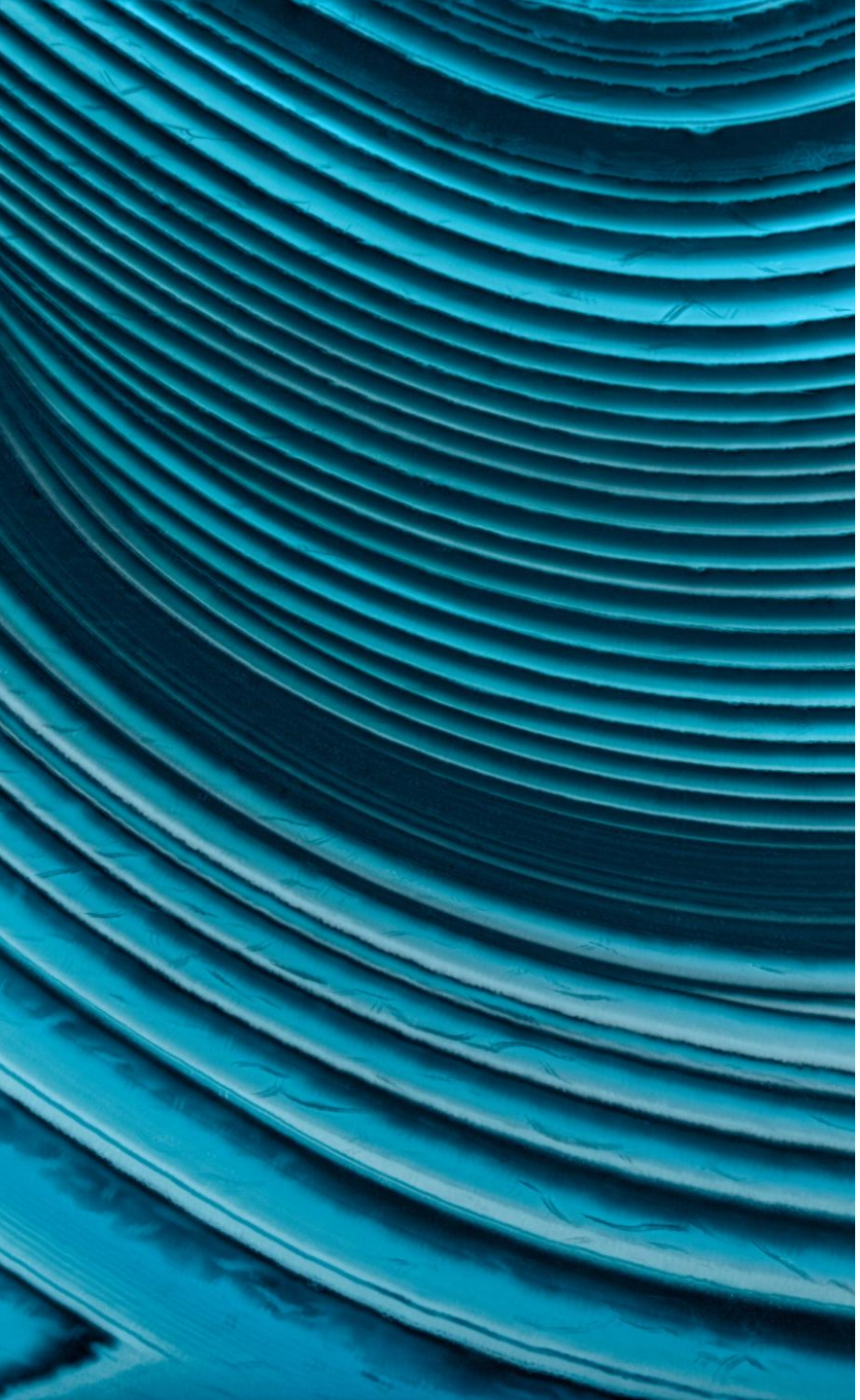
01

REGULATORY AND ENFORCEMENT TRENDS

A NEW CONSUMER PROTECTION PARADIGM: PRIVACY, CYBER & AI CONVERGE

- **Regulators now view privacy, cybersecurity, and AI as a single consumer-risk ecosystem:**
  - Data misuse, security failures, and AI harms treated as **consumer protection** issues
  - "**Unfairness**" theories applied to data practices, algorithms, and security controls
  - Shift from **technical compliance** to **consumer harm prevention**
  - Heightened expectations for **transparency**, **accountability**, and **explainability**
  - This convergence calls for cross-functional governance (legal, IT, product, security, compliance)



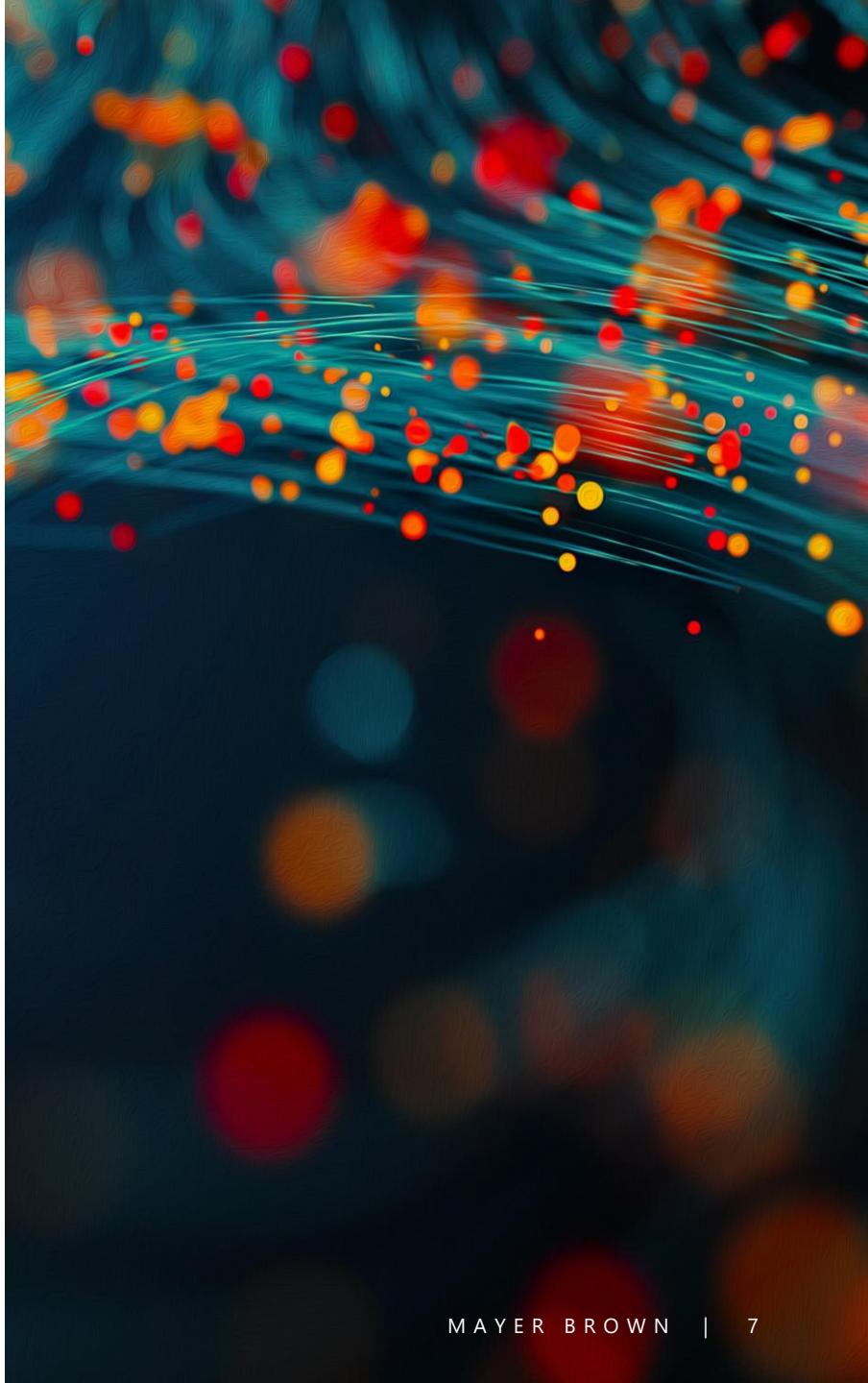


EMERGING THEORIES OF LIABILITY IN ENFORCEMENT

- **Regulators are stretching existing laws to reach new technologies:**
  - "Dark patterns" = deceptive UX
  - Algorithmic bias = unfair discrimination
  - AI-washing = deceptive marketing claims
  - Inadequate vendor oversight = unfair practice
  - Failure to secure training data = unreasonable security
  - Opaque automated decision-making = lack of transparency

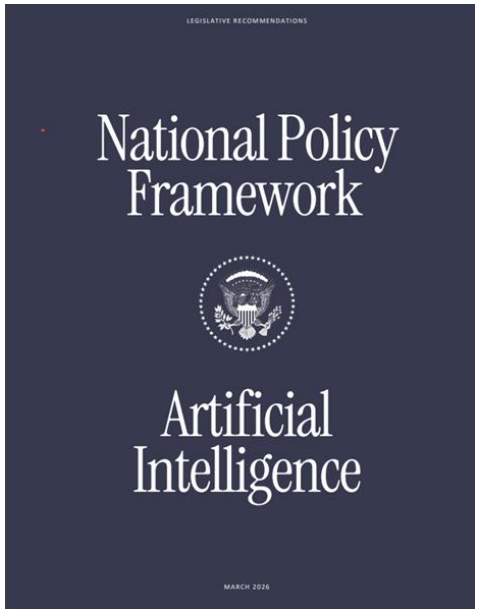
EMERGING AI LAWS AND GUIDANCE

- **Comprehensive AI Laws**
  - EU AI Act, Colorado, South Korea, Vietnam
- **Narrower AI Laws in the US**
  - Utah, California, Illinois, Texas, New York, NYC
  - Common focuses: transparency, consent, bias
- **New interactions with existing laws**
  - Privacy regs (e.g., CCPA), employment laws (EEOC), unfair/deceptive trade practices (FTC), credit decision rules (CFPB)



EMERGING AI LAWS AND GUIDANCE (CONT.)

- **Non-binding guidance is shaping legislation and enforcement expectations**
  - **White House:** March 20, 2026, A National Policy Framework for Artificial Intelligence
    - Generally pro-AI recommendations for federal legislation
    - Proposes preempting stricter state AI laws (but not "traditional police powers")
  - **FTC:** transparency, substantiation, fairness, accountability
  - **NIST AI RMF:** risk identification, measurement, mitigation
  - **State AG guidance:** notice, consent, opt-out for automated decisions
  - **Global regulators:** documentation, human oversight, impact assessments



ENFORCEMENT TRENDS

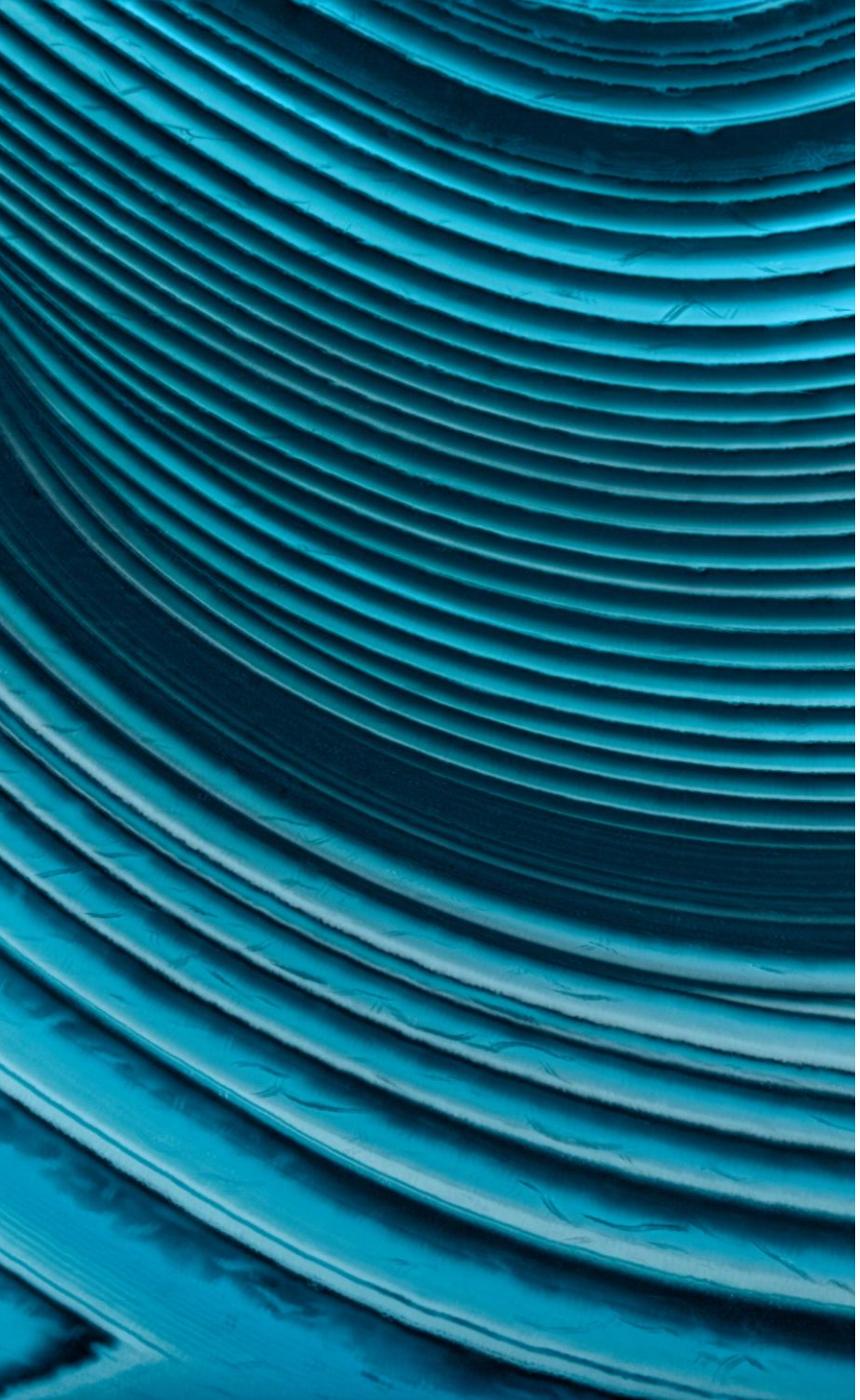
- **Cybersecurity/privacy enforcement activity is up overall**
  - Most enforcement follows cyber incidents (**cyber risk = enforcement risk**)
- **Increased enforcement activity at the state level**
  - **State AGs staffing up** and ramping up enforcement
  - Formation of **multi-state privacy enforcement consortium**
  - More **50-state cyber enforcement actions**
  - State AG investigations into **location data, consumer-rights handling**, **cookie banners**
  - **NYDFS** very active in banking space: **$63 million** in Part 500-related penalties in 2024-25

ENFORCEMENT TRENDS (CONT.)

- **Mixed signs** at the federal level but **no broad pullback**
  - **SEC** has continued to emphasize **cyber enforcement**
  - **FTC** shift toward **traditional enforcement** (i.e., fraud, misrepresentation)
    - Continued scrutiny of children's privacy, biometric data, and commercial surveillance
  - **DOJ** has continued to pursue cybersecurity **False Claims Act cases** and implementation of new **Data Export Rule**
  - **Banking regulators** have continued to scrutinize cyber practices, including more horizontal exams and "**enforcement by examination**"
- **Sensitive data remains a top enforcement priority**

COMMON TRIGGERS FOR ENFORCEMENT

- **Regulatory priorities (often sector-specific), such as:**
  - Government data; children's safety; health info; lending; third-party cybersecurity risks
  - Data management and retention
  - Access controls (MFA in particular "a focus" of NYDFS cyber enforcement)
- **Red flags**
  - Incident timeline delays (discovery, containment, mitigation, notification)
  - Impact on consumers and economy
  - Control failures & program maturity
  - Patterns & frequent flyers



LITIGATION TRENDS PARALLEL TO ENFORCEMENT

- **Private litigation is rising alongside regulatory risk:**
  - Data-breach class actions (even without clear harm)
  - Pixel/SDK tracking lawsuits / CIPA and ECPA lawsuits
  - Biometric privacy litigation
  - AI-related claims (copyright, discrimination, consumer deception)
  - Securities litigation tied to cyber disclosures, breaches
  - Plaintiffs' firms using regulatory findings as litigation roadmaps

02

KEY RISK FACTORS FOR COMPANIES

HIGH-RISK POPULATIONS AND DATA TYPES

Risks—regulatory, litigation, reputational, etc.—increase when dealing with:

High-Risk Populations

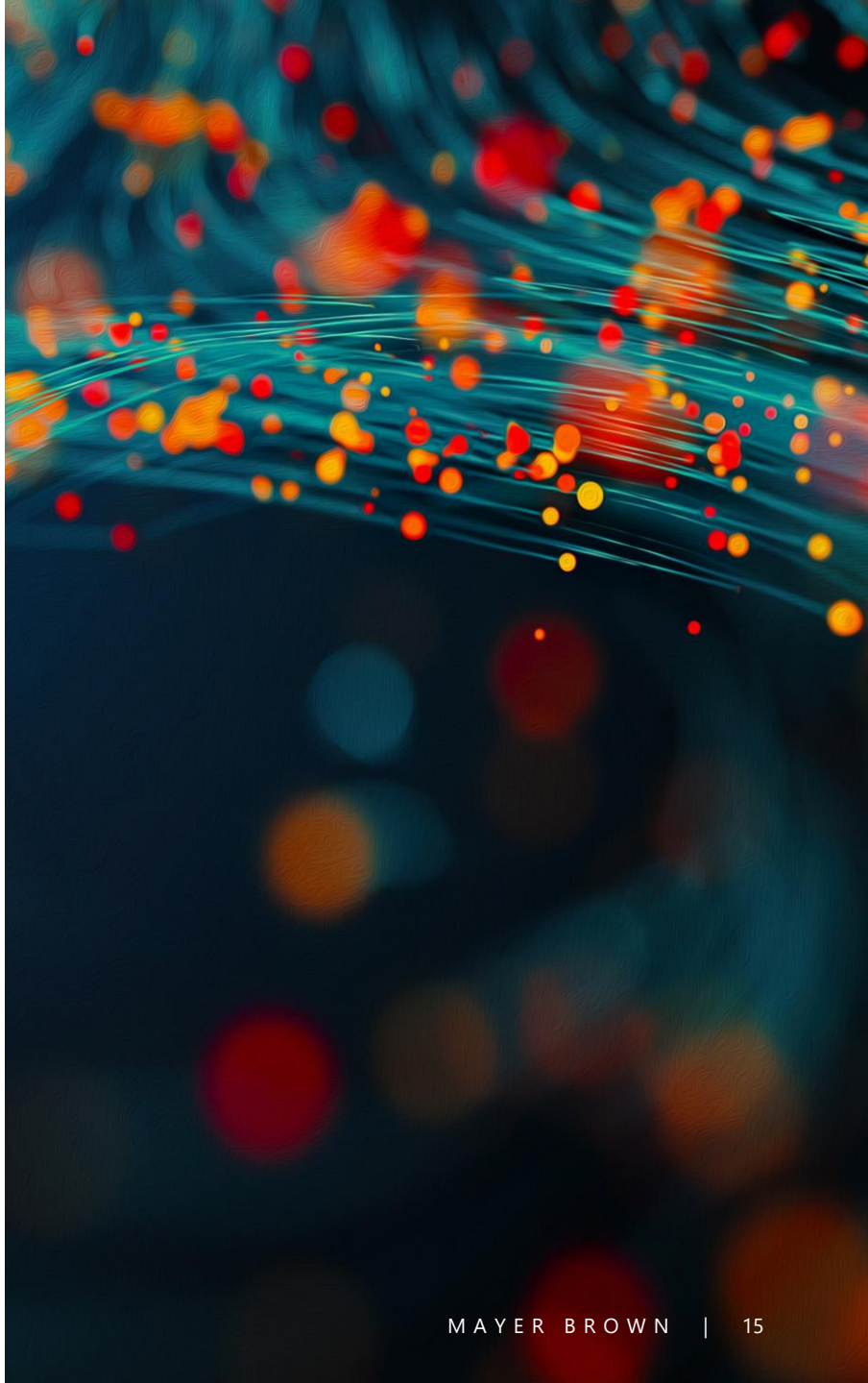
- Minors and teens
- Vulnerable consumers
- Employees and job applicants
- Patients and health-related users
- Financially at-risk consumers

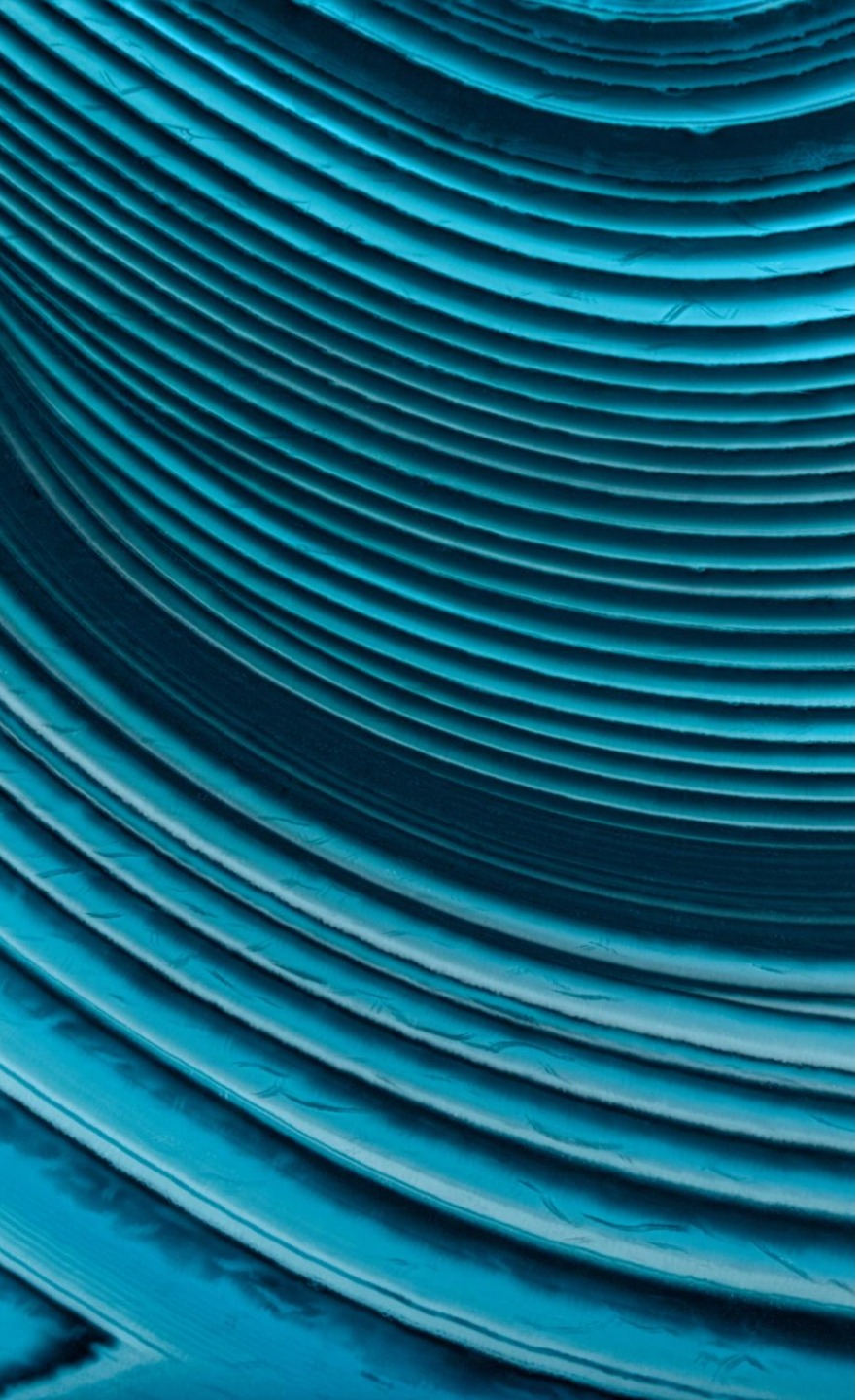
Sensitive or High-Risk Data Types

- Biometric identifiers
- Precise geolocation
- Health and wellness data
- Financial data
- Children's data
- Data for automated decision-making

PRODUCT & ENGINEERING RISK FACTORS

- Lack of privacy-by-design or security-by-design
- Unclear data flows
- Use of unvetted datasets or third-party code
- AI features deployed without transparency or governance



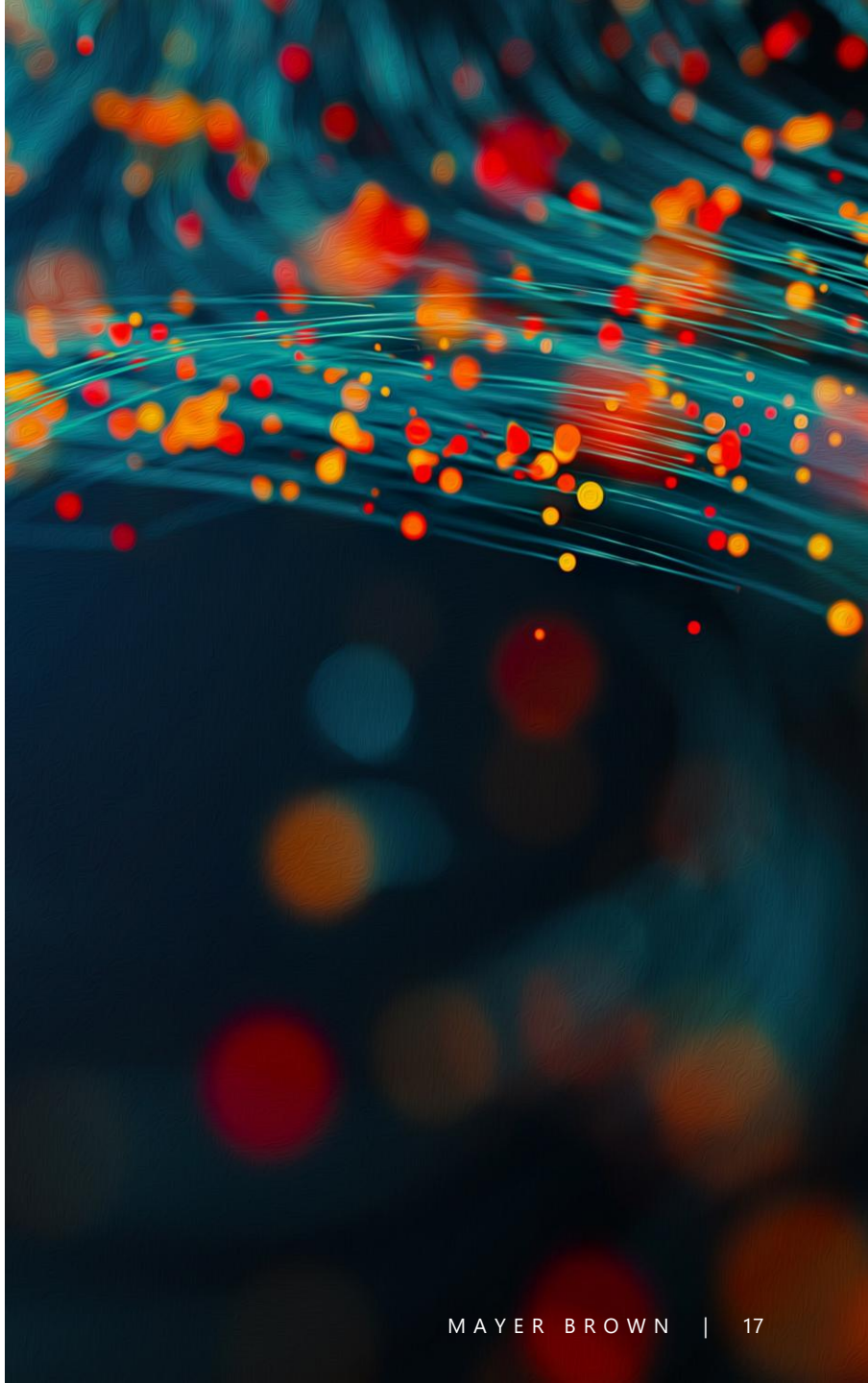


CYBERSECURITY & OPERATIONAL RISK FACTORS

- Vulnerability management gaps
- Weak access controls
- Inadequate logging, monitoring, and detection
- Overreliance on vendors for critical security functions
- Increasing sophistication of social engineering and fraud
- Employee and insider threats (e.g., BYOD, departing employees)
- Cross-border data flows

CORPORATE GOVERNANCE & TRANSACTIONAL RISK FACTORS

- Inadequate board oversight of cyber and AI risk
- Inaccurate or incomplete disclosures (SEC, investors, customers)
- M&A due diligence failures (data, AI models, IP, security posture)
- Contractual obligations around data, security, and AI use
- Misalignment between legal, product, and security leadership



PRIVACY RISK FACTORS IN THIRD-PARTY RELATIONSHIPS

Data handling & processing risks

- Data use for unspecified purposes or purposes in violation of the agreement and/or privacy laws
- Mishandling of data subject requests
- Overcollection or unauthorized use of borrower data
- Inconsistent security practices
- Insufficient contractual controls
- Limited visibility into vendor operations
- Incident response gaps

Emerging technology risks

- AI systems used in credit decisions or consumer-facing applications (may result in unlawfully discriminatory outcomes)
- Biometric data collection and storage risks

03

PRACTICAL STRATEGIES FOR IN-HOUSE COUNSEL

OPERATIONALIZING COMPLIANCE

How to turn policies into practice:

- **Embed legal early** in product and engineering workflows
- **Create lightweight review processes** (intake forms, checklists, risk tiers)
- **Automate where possible** (data mapping, retention, access controls)
- **Train teams regularly** on privacy, cyber, and AI expectations
- **Use playbooks** for incidents, model deployment, and vendor onboarding
- **Measure compliance** with KPIs (e.g., review turnaround time, incident response readiness)

PRIVACY-FOCUSED VENDOR ONBOARDING

Pre-Contract Due Diligence

- Example: Confirm vendor's data-handling practices align with relevant data protection law requirements

Risk-Based Vendor Training

- Example: Require periodic refresher training for high-risk vendors (e.g., those handling sensitive data or confidential information)

Core Privacy Contract Terms (Including AI-Specific Considerations)

- Example: Mandatory incident-notification timelines and cooperation obligations
- Example: Prohibit using consumer or employee data to train AI models

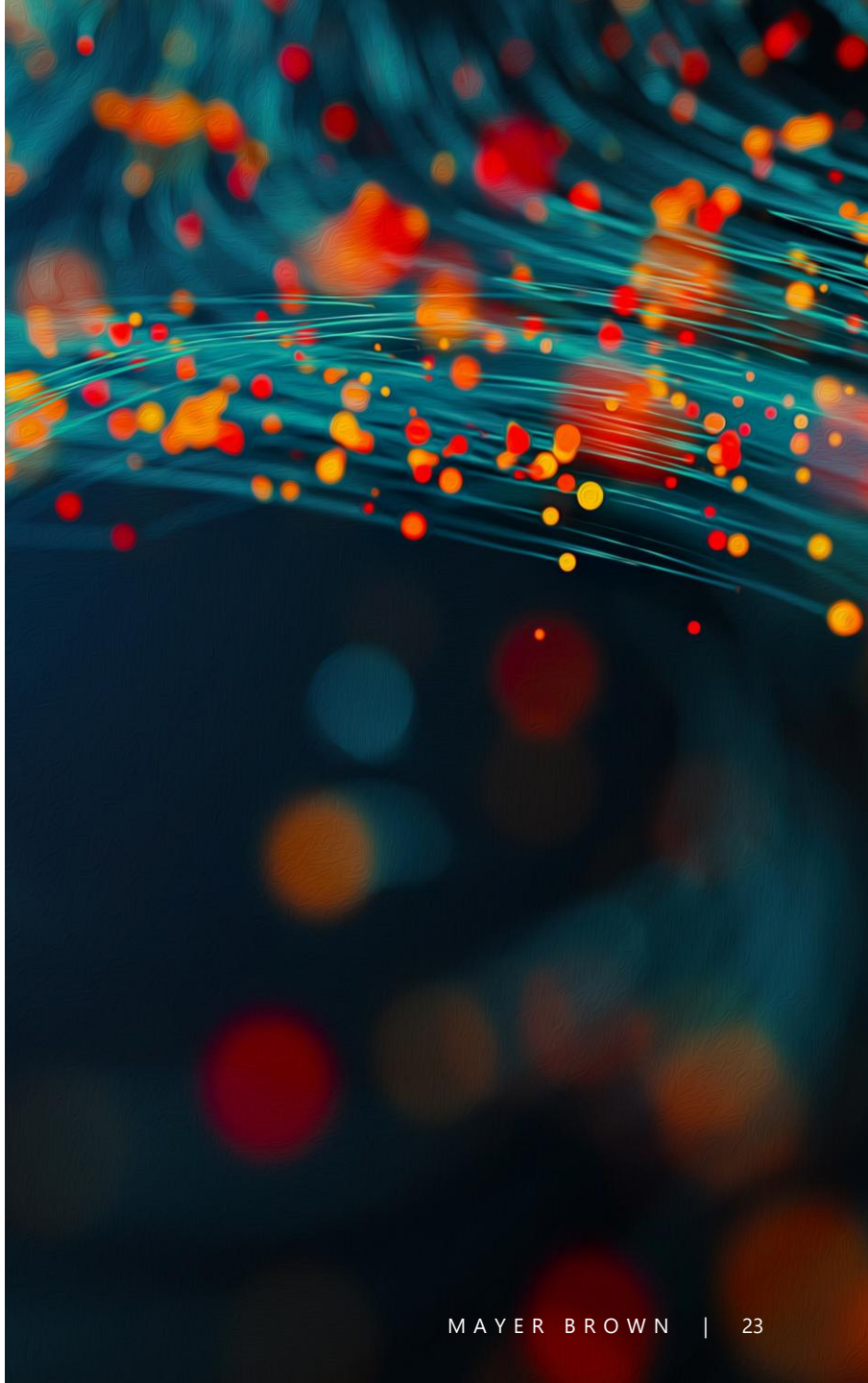
CORPORATE CONSIDERATIONS

- **Public Company Disclosures:** Must evaluate whether cyber incidents (or other privacy, cyber, AI, or consumer-protection risks) are material. If so, report on 8-K/10-K.
- **Internal Controls:** SOX-aligned internal controls should capture privacy and cyber risk as part of enterprise risk management.
- **Board Oversight & Governance:** Board's duties increasingly involve overseeing data-related risks; counsel should advocate for regular, substantive reporting to board on these matters.
- **Accuracy of Market Communications:** Statements about security posture, privacy practices, AI safeguards, or consumer-protection commitments must be accurate and supported by internal documentation.
- **M&A and Investments:** Privacy, cyber, and AI-related risks are core due-diligence items.

CYBER PREPAREDNESS

A simple 3-step pattern can be a framework for improving cybersecurity posture and preparedness and mitigating corresponding legal risk.

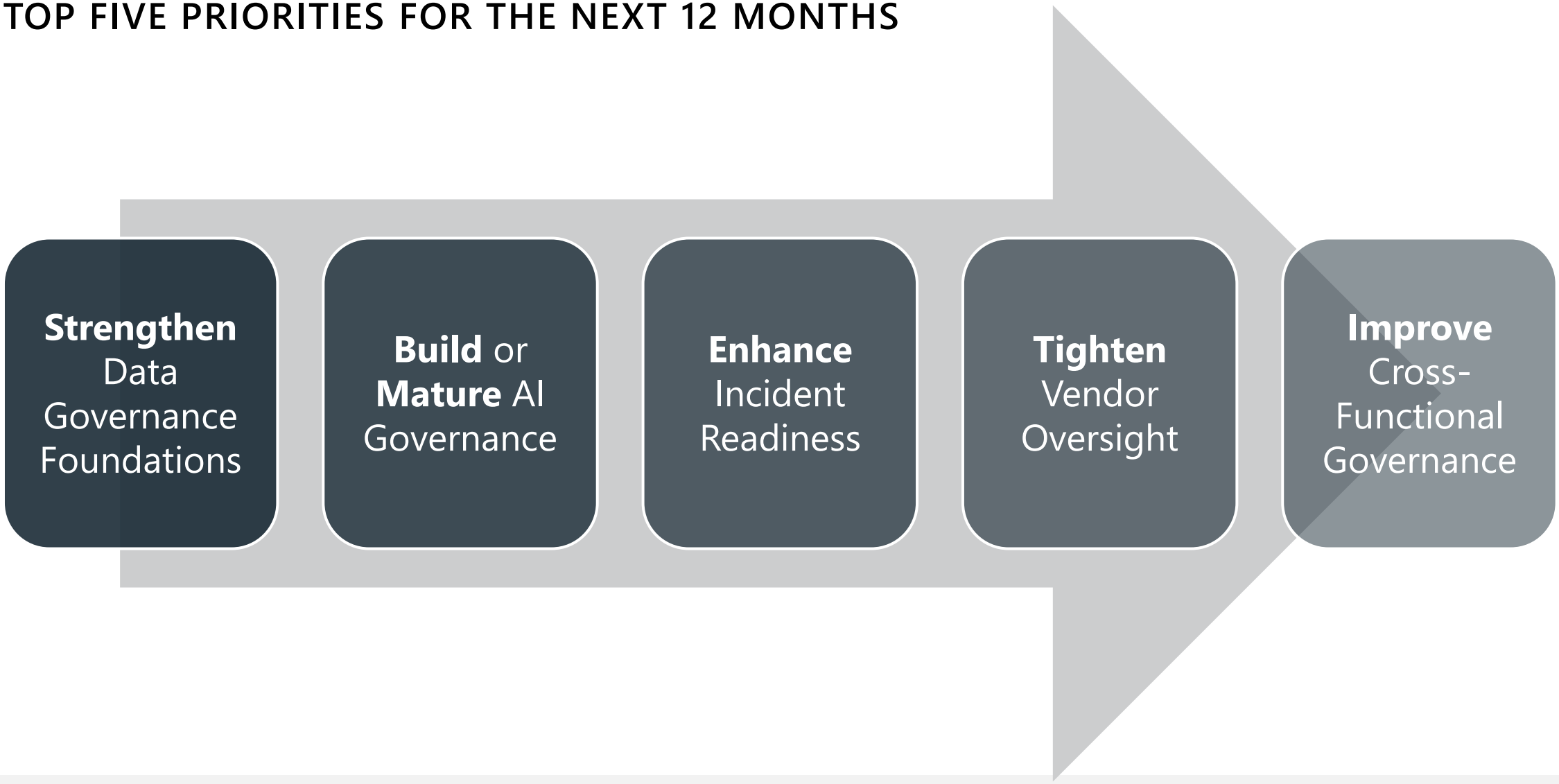
1. **Assess:** Identify and evaluate significant legal risks posed by the organization's current cybersecurity posture.
2. **Govern:** Develop appropriate plans and policies as well as internal coordination, escalation, and oversight bodies.
3. **Ensure:** Tailor incident response plans to the organization’s needs—and practice in regular tabletop exercises.



04

WHAT IN-HOUSE COUNSEL SHOULD PRIORITIZE

TOP FIVE PRIORITIES FOR THE NEXT 12 MONTHS



6 "QUICK WINS" FOR LEAN LEGAL TEAMS

Standardize Review Templates

- Create simple intake forms for product, AI, and vendor reviews
- Use checklists to streamline repeatable decisions

Refresh Consumer Disclosures

- Ensure privacy notices, in-product disclosures, and AI claims are accurate
- Remove outdated or overly broad statements

Implement a "No Suprises" Rule for Product Teams

- Require early legal review for new data uses, AI features, or tracking tech
- Embed legal in sprint planning or product kickoff meetings

6 "QUICK WINS" FOR LEAN LEGAL TEAMS (CONT.)

Prioritize High-Risk Vendors

- Conduct quick assessments of vendors handling sensitive data
- Update contracts with modern privacy, security, and AI clauses

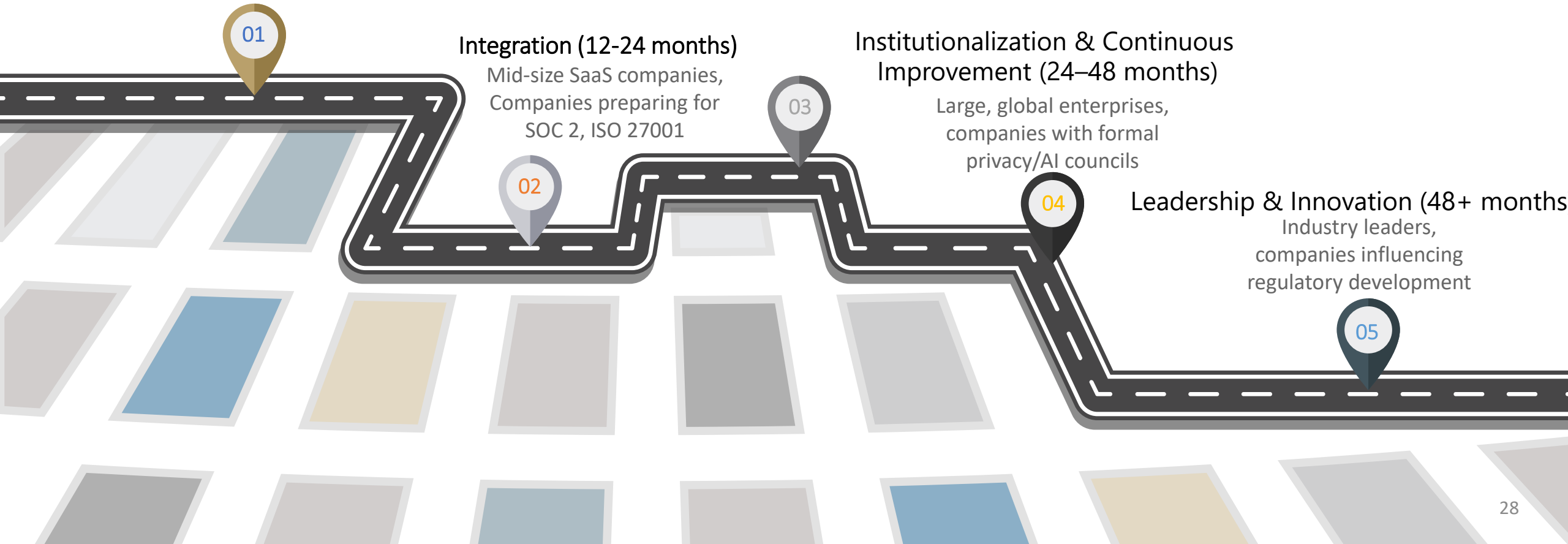
Run a Mini TTX

- 60-minute scenario focused on data misuse, AI error, or cyber incident
- Identify gaps in escalation, communication, and reporting

Create a Centralized Resource Hub

- One place for policies, playbooks, templates, and FAQs
- Reduces ad-hoc requests and improves consistency

LONG-TERM MATURITY ROADMAP



Foundations (0-12 months)

Early-stage startups, Fast growing tech companies, Organizations entering a regulated market

Integration (12-24 months)

Mid-size SaaS companies, Companies preparing for SOC 2, ISO 27001

Optimization

Established tech companies, Cloud service providers, Digital health and fintech companies

Institutionalization & Continuous Improvement (24–48 months)

Large, global enterprises, companies with formal privacy/AI councils

Leadership & Innovation (48+ months

Industry leaders, companies influencing regulatory development

Q&A

SPENCER GLENDE
+1 801 907 2740
SGLENDE@MAYERBROWN.COM

AMBER THOMSON
+1 202 263 3456
ATHOMSON@MAYERBROWN.COM

DISCLAIMER

These materials are provided by Mayer Brown and reflect information as of the date of presentation.

The contents are intended to provide a general guide to the subject matter only and should not be treated as a substitute for specific advice concerning individual situations.

MAYER | BROWN