



exterro<sup>®</sup>

# Data Risk & Resilience: Navigating the Nexus Between Privacy, Cyber & AI

# Welcome & Introductions



**Rebecca Perry, CIPP/US/G**

Director,  
Strategic Partnerships

Exterro



**Jonathan Yellin**

Executive Vice President &  
General Counsel

Charles River Associates



**Peter Stockburger**

Office Managing Partner,  
San Diego

Dentons

# Agenda

1. Key Findings from the 2024 ACC CLO Report
2. Balancing Risks, Regulations & Innovation
3. Challenges & Opportunities in AI & Data Risk Management
4. Future-Proof Strategy – Unleashing the Power of AI



The background features a dark purple-to-blue gradient. At the top and bottom, there are white-outlined geometric shapes: two downward-pointing triangles at the top and two upward-pointing triangles at the bottom, arranged in a symmetrical pattern. A solid orange vertical bar is located on the far left edge of the slide.

What are Chief Legal Officers  
most concerned about?



2024

**ACC CHIEF  
LEGAL  
OFFICERS  
SURVEY**

**ACC** Association of  
Corporate Counsel

**exterro**

*Created in collaboration with* **exterro**<sup>®</sup>

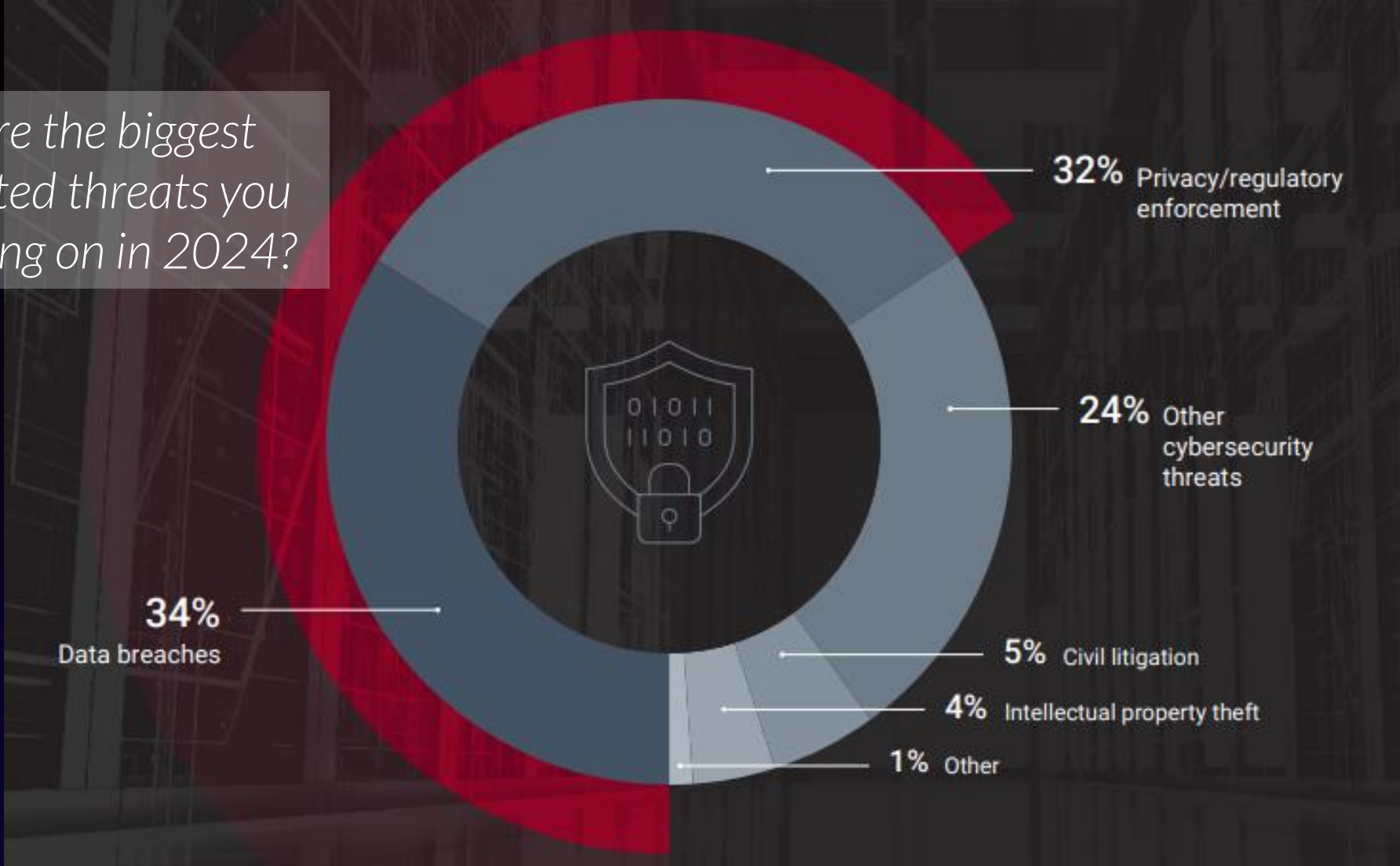
669 Chief Legal Officers/General Counsel


Across 20 Industries

31 Countries

# CLO's Biggest Concerns Revolve Around Data

*What are the biggest data-related threats you are focusing on in 2024?*





# Balancing Risks, Regulations & Innovation

# Notable Privacy, Cyber and AI Laws & Regulations

- **Privacy.** 18 states now have comprehensive data privacy laws that impose requirements around data minimization, data impact assessments, responding to data subject requests, and data classification.
- **Old School Cybersecurity.** Most of the 50 states have affirmative data security requirements around name + something highly sensitive, including the duty to maintain “reasonable” security around that data. Data governance and insight is critical to compliance and risk prevention.
- **New School Cybersecurity.** Many of the new omnibus state privacy laws impose affirmative security requirements around a broader set of data (triggering broader data classification requirements). Emerging states like NY and others are pushing forward affirmative data security requirements as well, requiring data minimization and classification as a policy.
- **AI Laws & Opportunities.** States like Utah and Colorado have new AI laws in effect that require careful data governance. Good data governance also drives opportunity. Think brakes on a racecar.





# Utah Artificial Intelligence Policy Act



- **Effective Date.** May 1, 2024
- **Application.** Applies to the use of generative AI.
- **General Requirements.** For general organizations, must disclose to a consumer if generative AI is being used if asked.
- **Regulated Professional Requirements.** Regulated professionals (i.e., health care) must disclose verbally or in writing prior to using generative AI.
- **Enforcement.** No private right of action. Enforced by Utah Division of Consumer Protection and Attorney General. \$2,500 - \$5,000 per violation.
- **Defense.** No defense to blame AI for consumer protection violations. Businesses are accountable for the outputs of their AI systems.



# Colorado Artificial Intelligence Act



- **Effective Date**. February 1, 2026
- **Passed**: May 17, 2024
- **Scope**. Imposes governance, risk assessments, disclosure, and documentation requirements on developers and deployers of AI. Impacts “high-risk” AI systems, which can relate to the delivery of health care.
- **Governor Statement**. Hopes the law to receive some clarity before 2026 effective date so scope may change.
- **Enforcement**. No private right of action, can only be enforced by the CO AG.



# The EU AI Act



Takes a “**risk based**” approach, classifying AI systems according to separate tiers:

1. prohibited
2. **high-risk**
3. limited risk
4. minimal risk  
(e.g., spam filters and AI within video games)



“**High risk**” systems will be subject to **strict requirements** on:

- risk management system
- transparency and data governance
- human oversight
- conformity assessment (CE marking)



**Foundation models** (e.g. LLMs) will be a regulated category

→ **Fines** up to €30 million or, up to 6% of total global revenue for worst offenses

→ Unlikely to apply until **2025**, at the earliest





# Privacy & AI Governance Structure





# Balancing Data Minimization & AI Model Requirements



## Data Minimization

Limit collection

- Directly relevant and necessary
- Specified purpose

Retain data only as long as necessary

## AI Models

Expansive need for data

- Web scraping
- Repurposing existing data
- Licensing data from third parties



# Challenges & Opportunities in AI & Data Risk Management

# Questions

Do you know where all your data is stored?

Do you know how long to keep data and when to dispose of it?

Do you know what regulations govern your data?

Can you easily and quickly respond to requests for data (DSAR, e-discovery, investigation, breach notification, etc.)?

Do you know what 3rd Parties access or have your data?



# Questions

Do you know where all your data is stored?

Do you know how long to keep data and when to dispose of it?

Do you know what regulations govern your data?

What business processes are using AI?

Is personal or sensitive data being used to train AI models?

Can you easily and quickly respond to requests for data (DSAR, e-discovery, investigation, breach notification, etc.)?

Do we have consent to use personal data?

Do you know what 3rd Parties access or have your data?

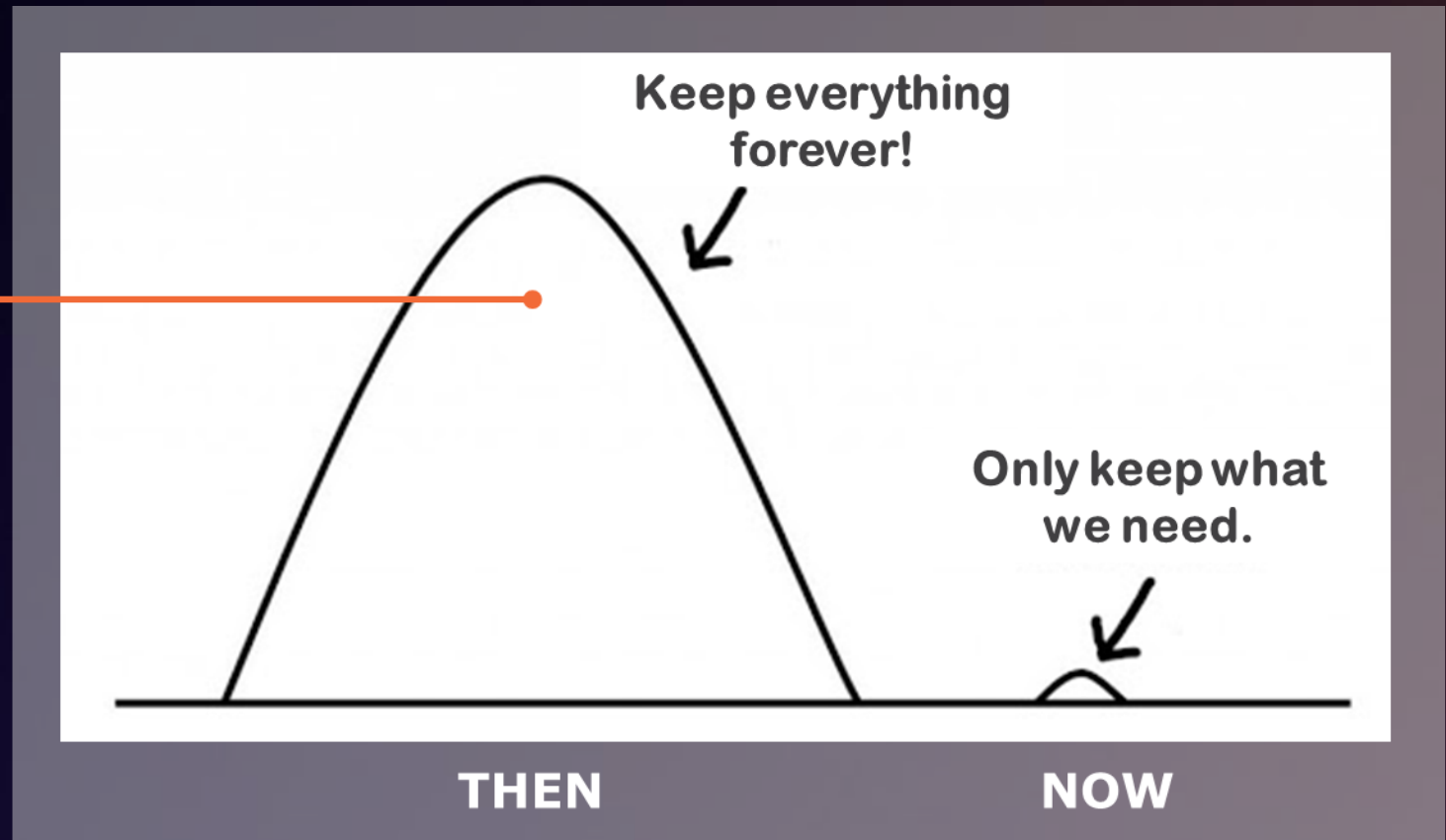




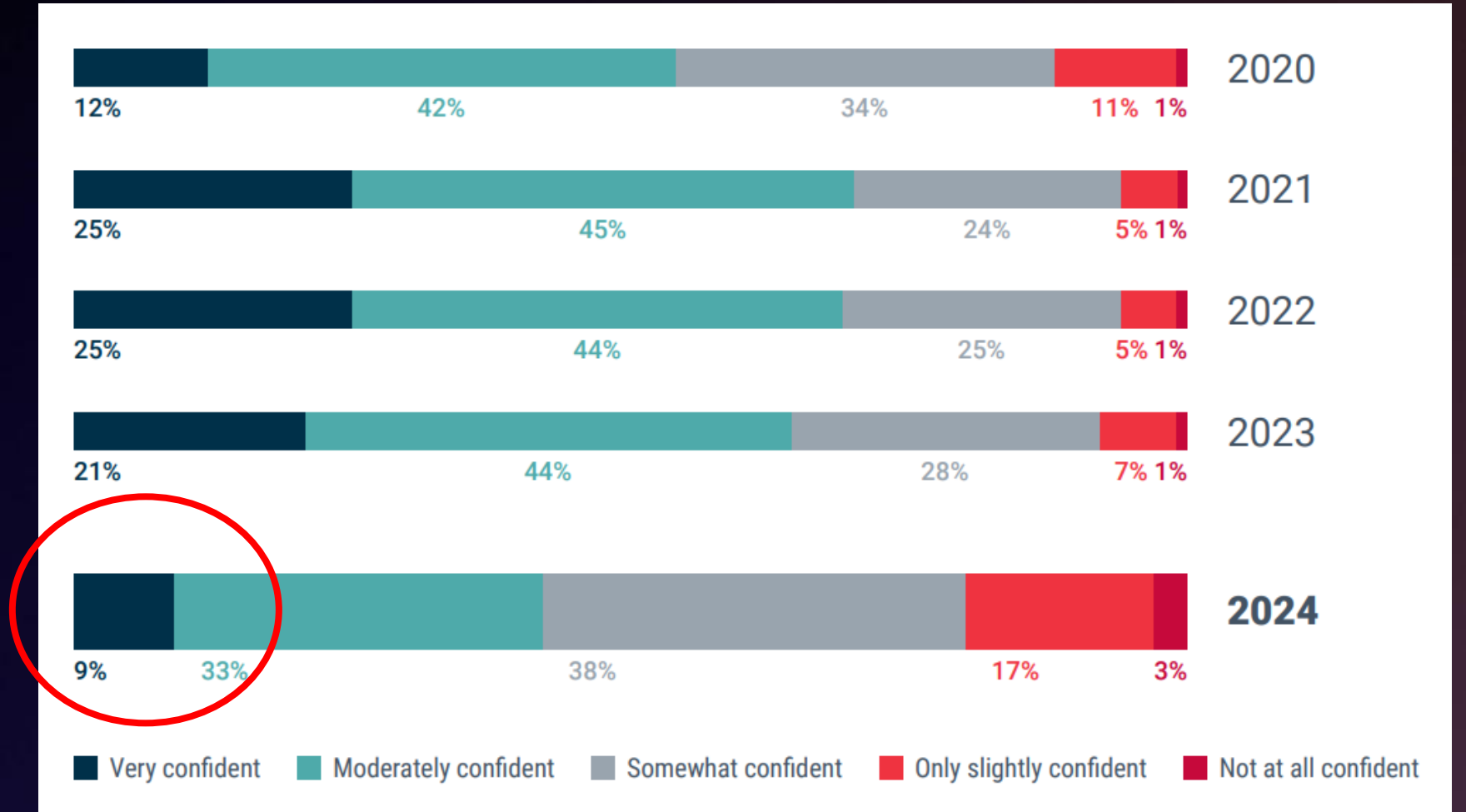
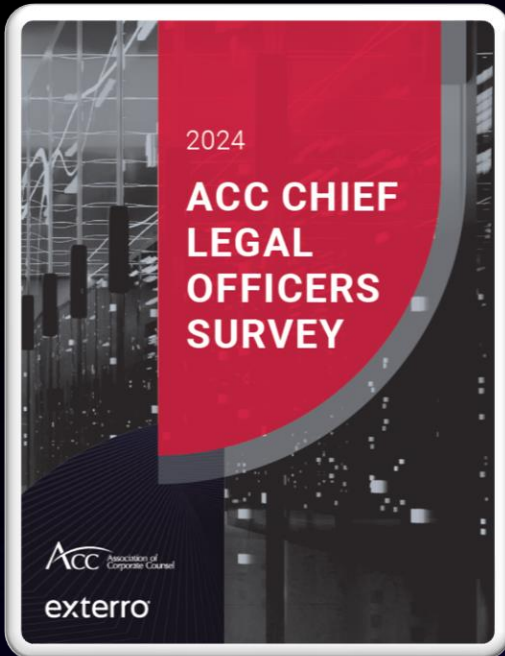
# Over-Retaining Data is a Liability!

## KEY RISKS:

- Data Breach
- Ransomware Attack
- Enforcement Action
- Litigation
- Class Action
- Consumer Requests



# Fewer CLOs are Confident in their Ability to Mitigate Emerging Data Risks



# Opportunity & Competitive Advantage





# A Future-Proof Data Risk Management Strategy



# Are You Ready for Boom?



Litigation



Breach or Cyber Attack



Enforcement Action



Investigation



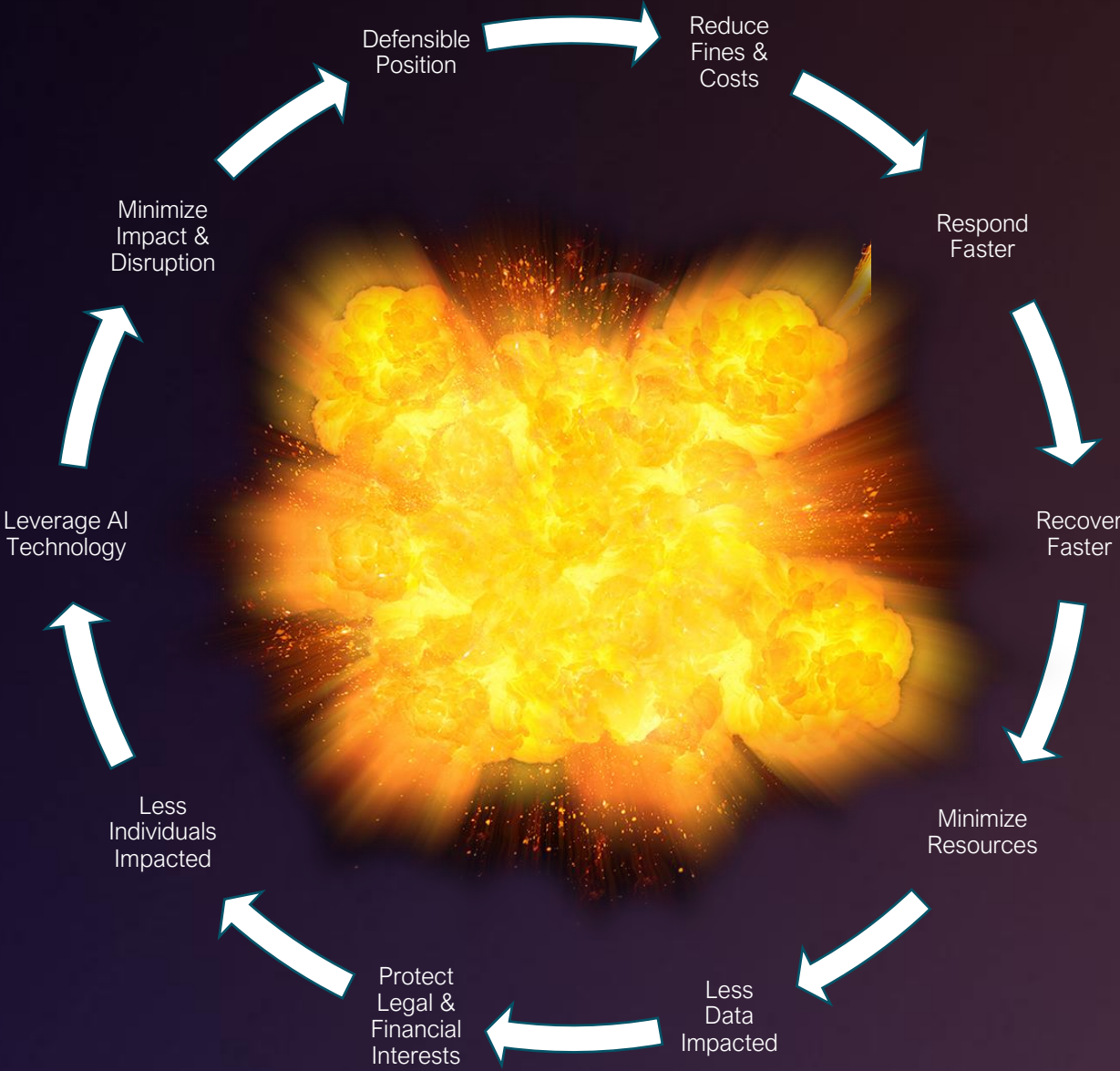
**AI TECHNOLOGY**



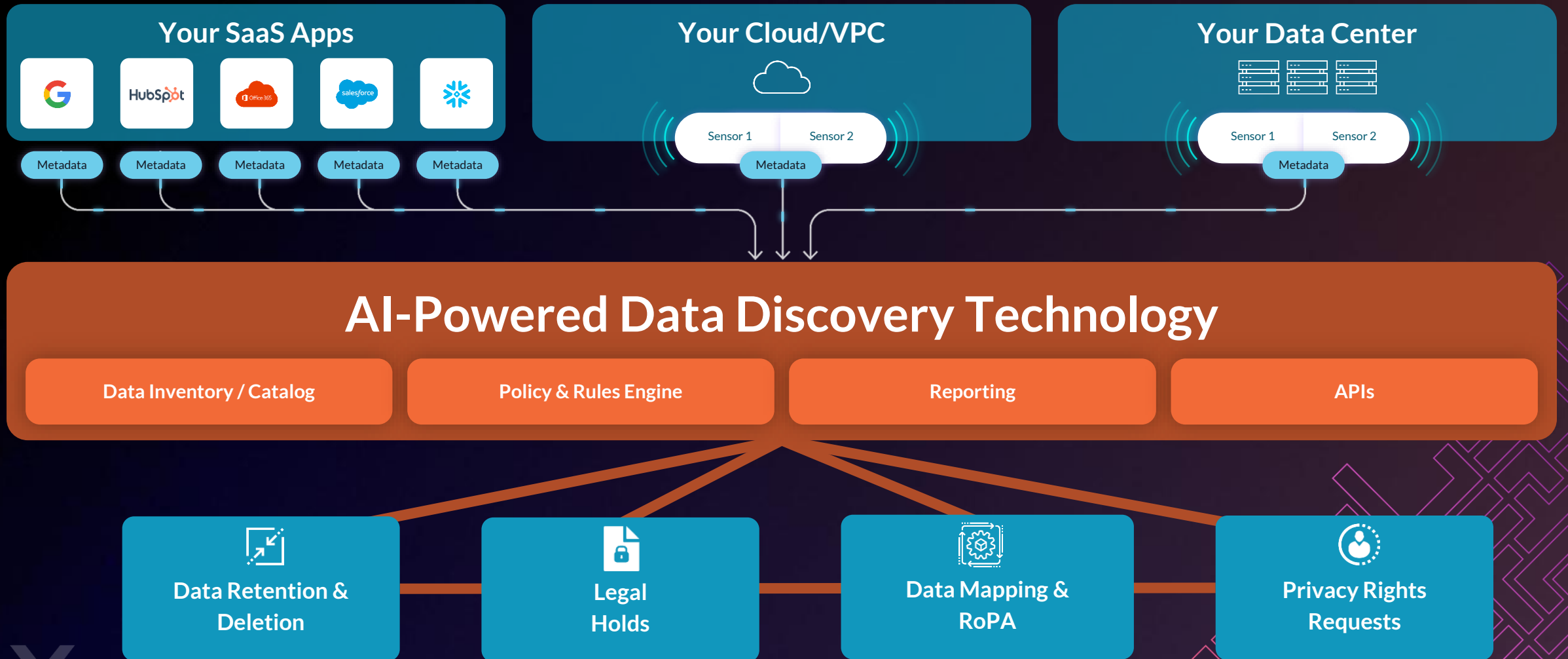
# Impact of a Strong Data Risk Management Strategy



- ✓ Assess PII Processing
- ✓ Assess AI Processing
- ✓ Privacy Rights Processes
- ✓ Notice & Consent
- ✓ Records & Data Retention Rules
- ✓ Legal Hold Processes
- ✓ Data Classification
- ✓ Data Remediation & Disposition
- ✓ Assess Third Party Risks



# Unleashing The Power of Data Discovery



# Thank You!



**Rebecca Perry, CIPP/US/G**  
Director,  
Strategic Partnerships

Exterro



**Jonathan Yellin**  
Executive Vice President &  
General Counsel

Charles River Associates



**Peter Stockburger**  
Office Managing Partner,  
San Diego

Dentons





# A Complete Orchestrated Solution



**DATA RISK  
MANAGEMENT**



**E-DISCOVERY**



**DATA  
PRIVACY**



**DIGITAL  
FORENSICS**



**CYBERSECURITY  
COMPLIANCE**

