

What Data Risks Are Hiding In Your Deals?

exterro[®]

ACC Association of
Corporate Counsel
— SAN FRANCISCO BAY AREA —

exterro[®]



IT, Privacy, & eCommerce Network



Panelist Introductions



Rebecca Perry
CIPP/US/G

Director GTM Strategy
& Operations Privacy &
Data Governance

Exterro



Paola Zeni

Chief Privacy
Officer, Strategic
Advisor

RingCentral



Sushila Chanana
Partner

Farella Braun +
Martel

Agenda

1. Key Findings from 2024 ACC CLO Report
2. Data Risk Considerations
3. Data Risks in Technology Deals
4. Data Risks in M&A
5. Data Risk Management Strategy

2024

**ACC CHIEF
LEGAL
OFFICERS
SURVEY**

ACC Association of
Corporate Counsel

exterro

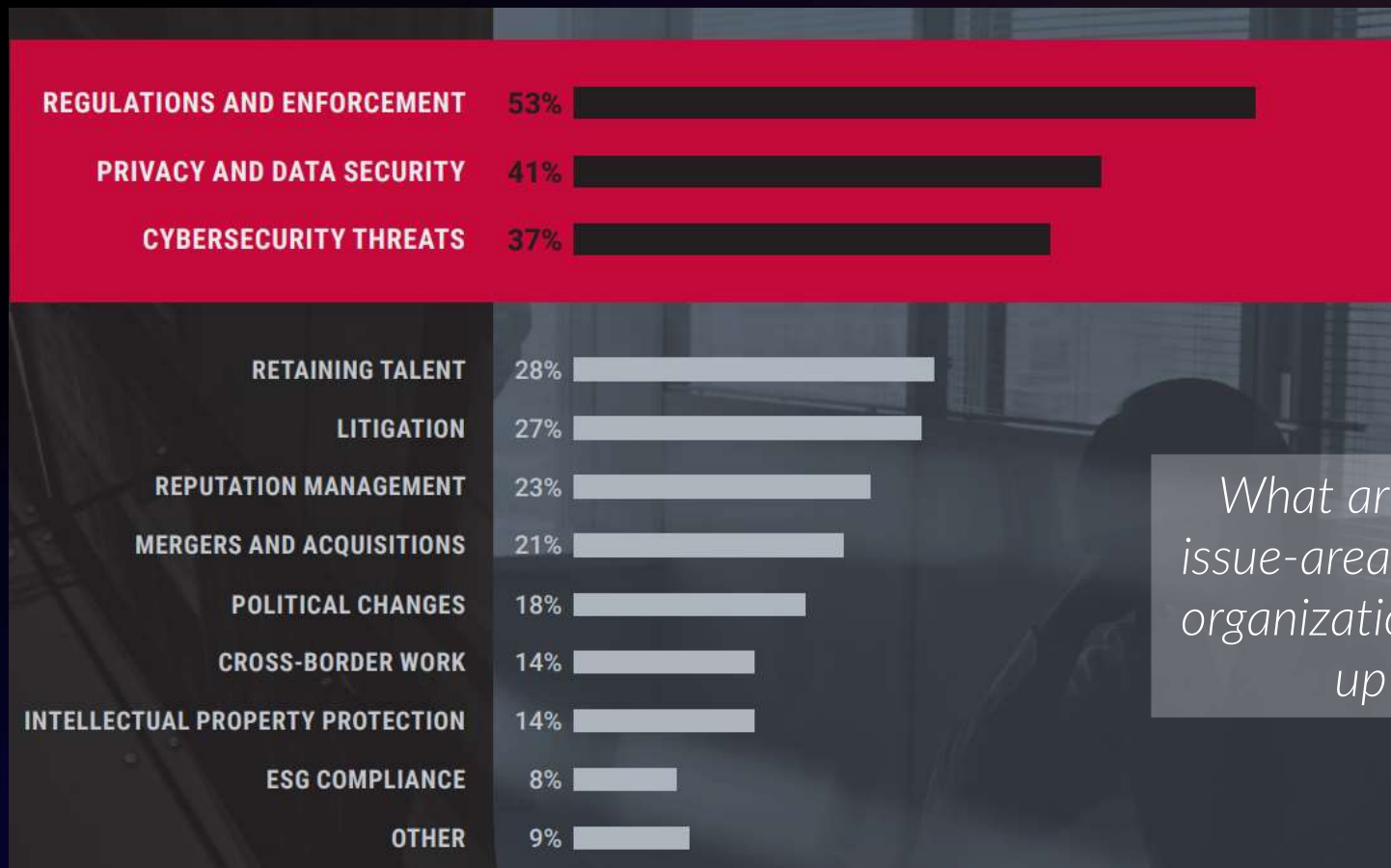
Created in collaboration with **exterro**

669 Chief Legal Officers/General Counsel

Across 20 Industries

31 Countries

Most Important Issues to CHIEF LEGAL OFFICERS Revolve Around Data Risks

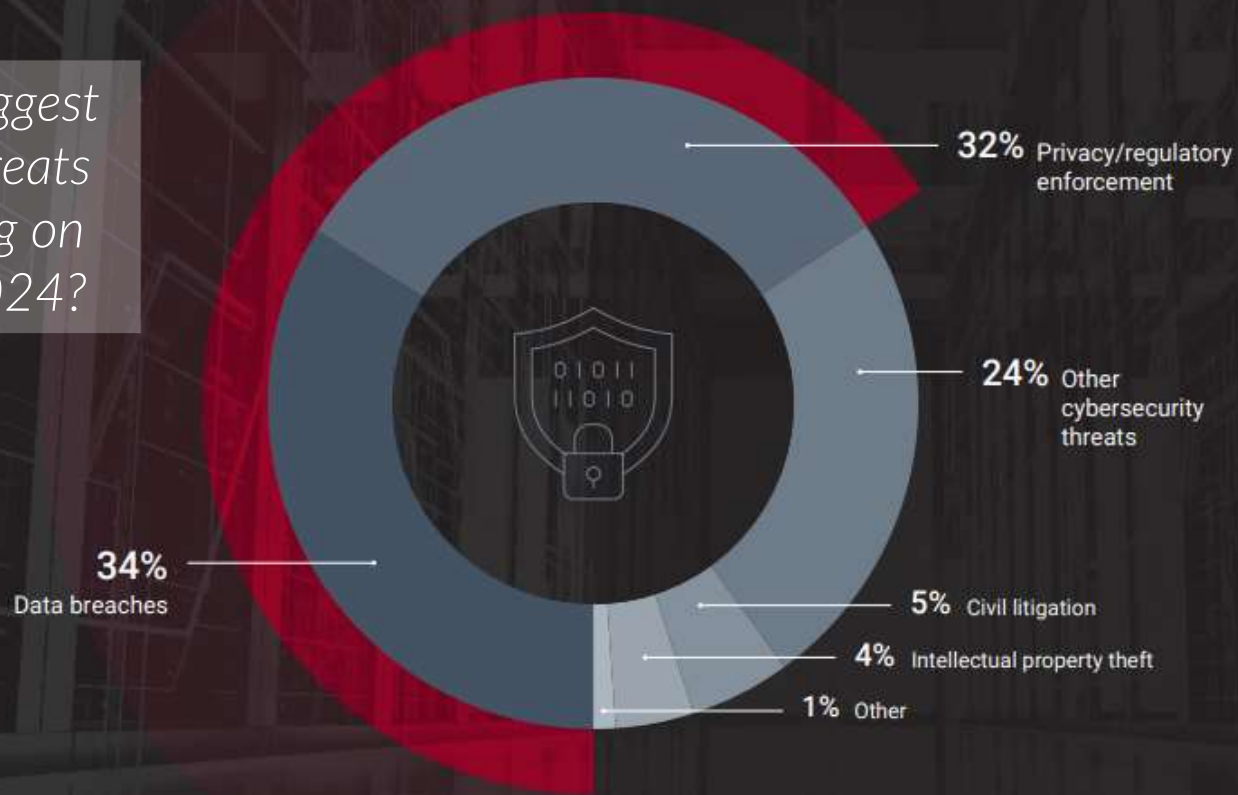


What are the top three issue-areas impacting your organization that keep you up at night?

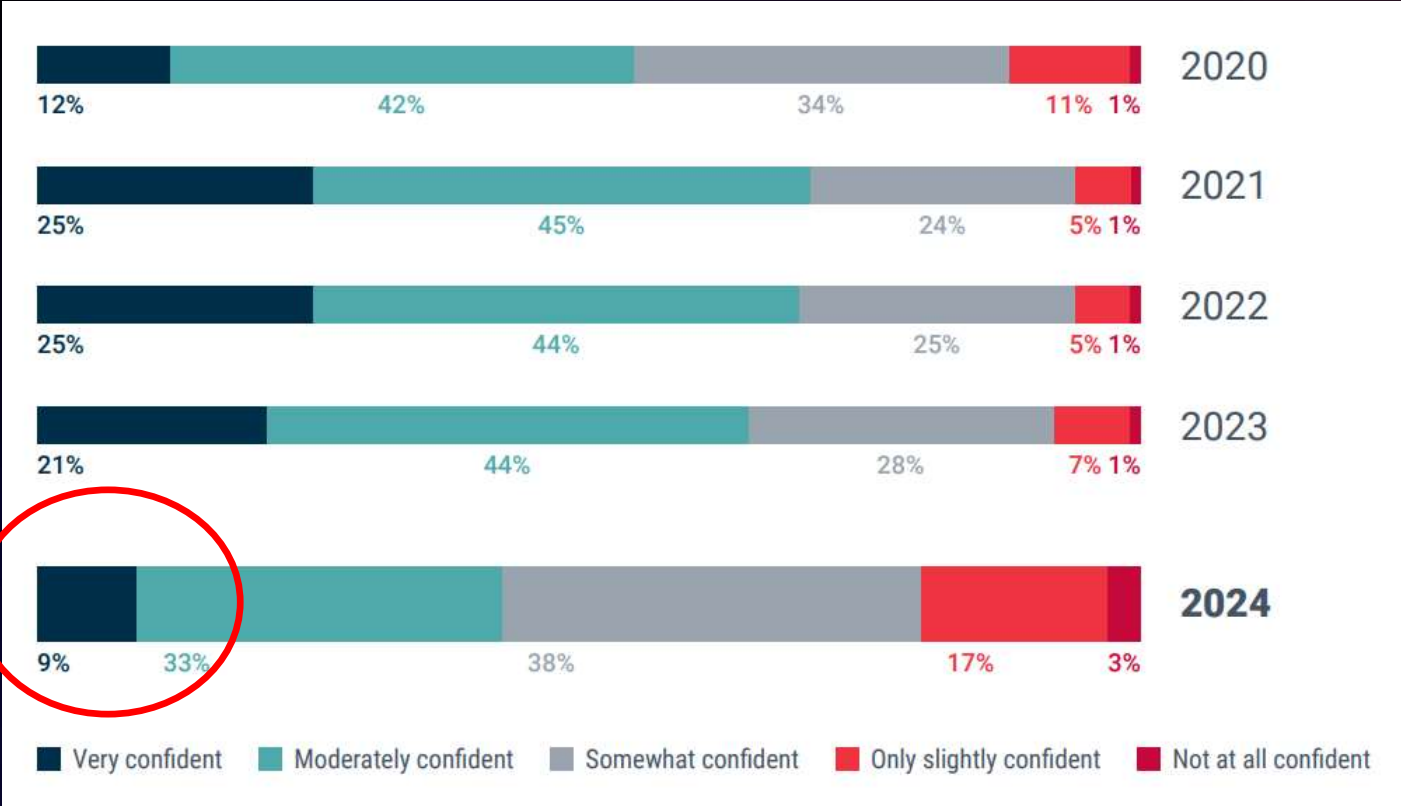


CLOs Focused on Mitigating Breaches & Privacy Enforcement Actions

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



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





Data Risk Considerations

What's Hot

GENERATIVE AI

- ✓ Data Usage for LLM Training
- ✓ Confidentiality
- ✓ Intellectual Property Protection

CYBERSECURITY

- ✓ Expanding Regulations
- ✓ Contractual Requirements
- ✓ Third-Party Risks

DATA GOVERNANCE

- ✓ Retention
- ✓ Data Inventory & Data Location
- ✓ Data Minimization
- ✓ Disposition after Termination

Questions to Avoid Blind Spots

Who is responsible?

- ✓ Storing Data
- ✓ Securing Data (Audits Allowed?)
- ✓ Deleting Data (Deletion Certification)

What about AI?

- ✓ Can Vendor input your data to Generative AI Platform?
- ✓ Do you want to do that with another Company's Data?
- ✓ What is the Process for doing so?
- ✓ Is Prior Consent Required? (recommended)





Data Risks In Technology Deals

Data Risks In Technology Deals

- Conducting third party due diligence
- Understanding the data flow
- Complying with notices and existing agreements when sharing data
- Understanding AI risks
- Assigning responsibility for data minimization
- Data breach notification requirements

Streamline & Document Vendor & AI Risk Assessments

- Leverage Assessment Templates
- Easily Collaborate with Stakeholders
- Surface Hidden Risks
- Document Remediation Steps

The screenshot displays the Exterro Cloud Security Assessment tool interface. The top navigation bar includes the Exterro logo, a grid icon, a home icon, and a help icon. The main header shows the assessment title "Cloud Security Assessment Dup V1", target "Generic", category type "General Assessments", and a "Draft" status. Action buttons for "Exit", "Setup Score Range", "Save", and "Publish" are visible.

The interface is divided into two main sections: "Sections" on the left and "Configuration" on the right. The "Sections" list includes:

1. Configuration
2. Security Controls
3. Authorized Access
4. External Data Sharing
5. Service Provider Oversig...
6. Cloud Activity Monitoring

The "Configuration" section contains a list of assessment questions. Question 11 is highlighted:

11 Is the cloud configured in a way that allows you to control who has access to the data at all times? Add Hint Multiple Choice

Options for Question 11:

- Yes, we are confident we control access Tag: No Risk
- Yes, we control access along with the cloud service provider Tag: Medium Risk
- Don't Know Tag: High Risk

Below the options is a "Please explain" text area and an "+ Add New Option" button.

Question 12 is also visible:

12 Do you have complete visibility and control over your cloud infrastructure? * Display Rule Multiple Choice

Options for Question 12:

- Yes, we control access permissions and security measures Tag: Low Risk
- Don't know, we rely on security controls provided by the cloud service provider Tag: High Risk

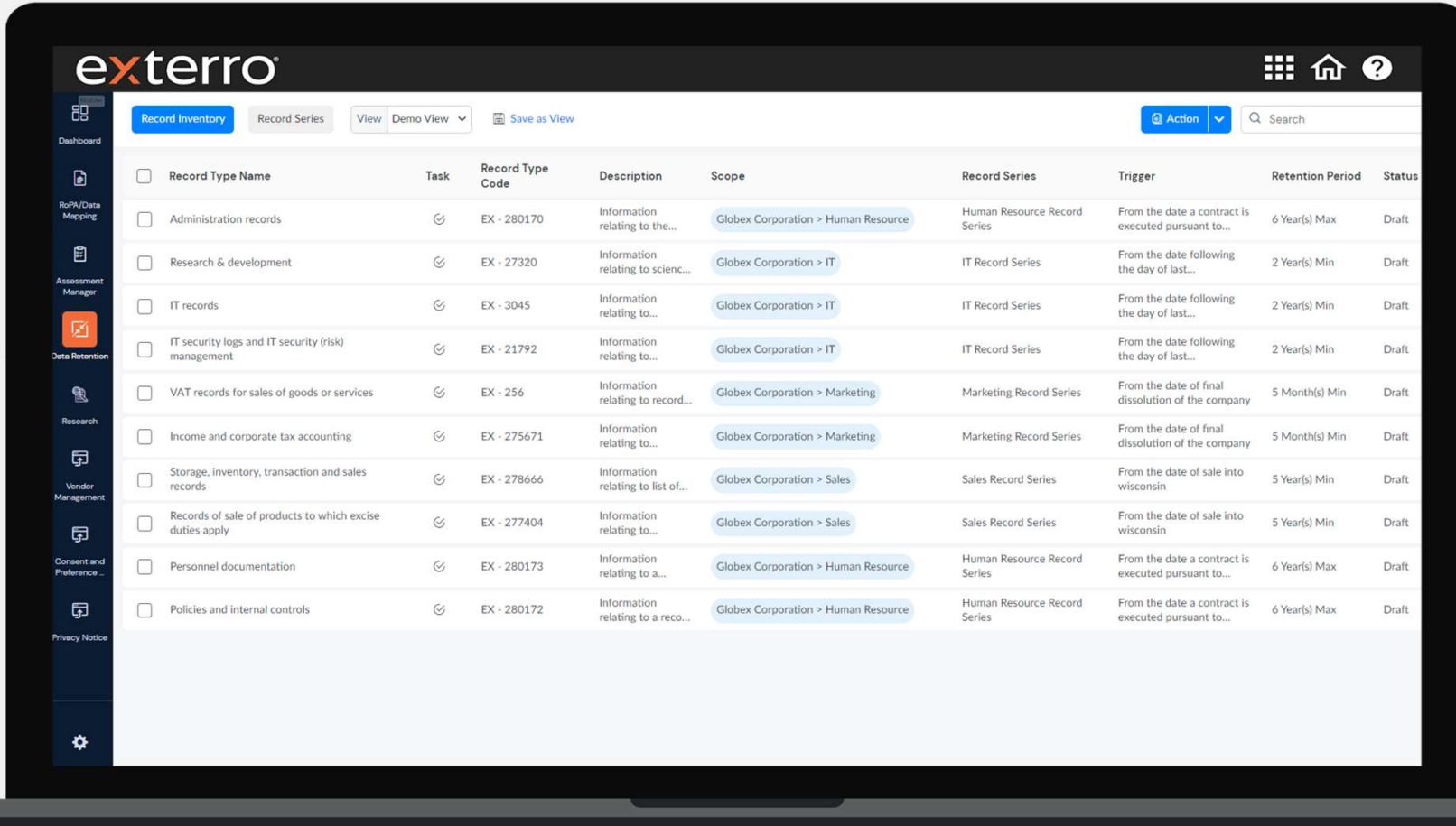
Below the options is a "Please explain" text area.

Question 13 is partially visible:

13 Are you using a multi-cloud approach? * Display Rule Multiple Choice

Develop Retention Rules & Apply Applications & Vendors

- Establish Retention & Deletion Policies
- Action Policies Across Data Sources & Applications
- Ensure Vendors & Third Parties are Compliant



The screenshot displays the Exterro Data Retention interface. The top navigation bar includes the Exterro logo, a home icon, and a help icon. Below the navigation bar, there are tabs for 'Record Inventory', 'Record Series', and 'View Demo View', along with a 'Save as View' button and an 'Action' dropdown menu. A search bar is located on the right side of the interface.

<input type="checkbox"/>	Record Type Name	Task	Record Type Code	Description	Scope	Record Series	Trigger	Retention Period	Status
<input type="checkbox"/>	Administration records	✔	EX - 280170	Information relating to the...	Globex Corporation > Human Resource	Human Resource Record Series	From the date a contract is executed pursuant to...	6 Year(s) Max	Draft
<input type="checkbox"/>	Research & development	✔	EX - 27320	Information relating to scienc...	Globex Corporation > IT	IT Record Series	From the date following the day of last...	2 Year(s) Min	Draft
<input type="checkbox"/>	IT records	✔	EX - 3045	Information relating to...	Globex Corporation > IT	IT Record Series	From the date following the day of last...	2 Year(s) Min	Draft
<input type="checkbox"/>	IT security logs and IT security (risk) management	✔	EX - 21792	Information relating to...	Globex Corporation > IT	IT Record Series	From the date following the day of last...	2 Year(s) Min	Draft
<input type="checkbox"/>	VAT records for sales of goods or services	✔	EX - 256	Information relating to record...	Globex Corporation > Marketing	Marketing Record Series	From the date of final dissolution of the company	5 Month(s) Min	Draft
<input type="checkbox"/>	Income and corporate tax accounting	✔	EX - 275671	Information relating to...	Globex Corporation > Marketing	Marketing Record Series	From the date of final dissolution of the company	5 Month(s) Min	Draft
<input type="checkbox"/>	Storage, inventory, transaction and sales records	✔	EX - 278666	Information relating to list of...	Globex Corporation > Sales	Sales Record Series	From the date of sale into wisconsin	5 Year(s) Min	Draft
<input type="checkbox"/>	Records of sale of products to which excise duties apply	✔	EX - 277404	Information relating to...	Globex Corporation > Sales	Sales Record Series	From the date of sale into wisconsin	5 Year(s) Min	Draft
<input type="checkbox"/>	Personnel documentation	✔	EX - 280173	Information relating to a...	Globex Corporation > Human Resource	Human Resource Record Series	From the date a contract is executed pursuant to...	6 Year(s) Max	Draft
<input type="checkbox"/>	Policies and internal controls	✔	EX - 280172	Information relating to a reco...	Globex Corporation > Human Resource	Human Resource Record Series	From the date a contract is executed pursuant to...	6 Year(s) Max	Draft



Data Risks in M&A Deals

Data Risks in M&A Deals

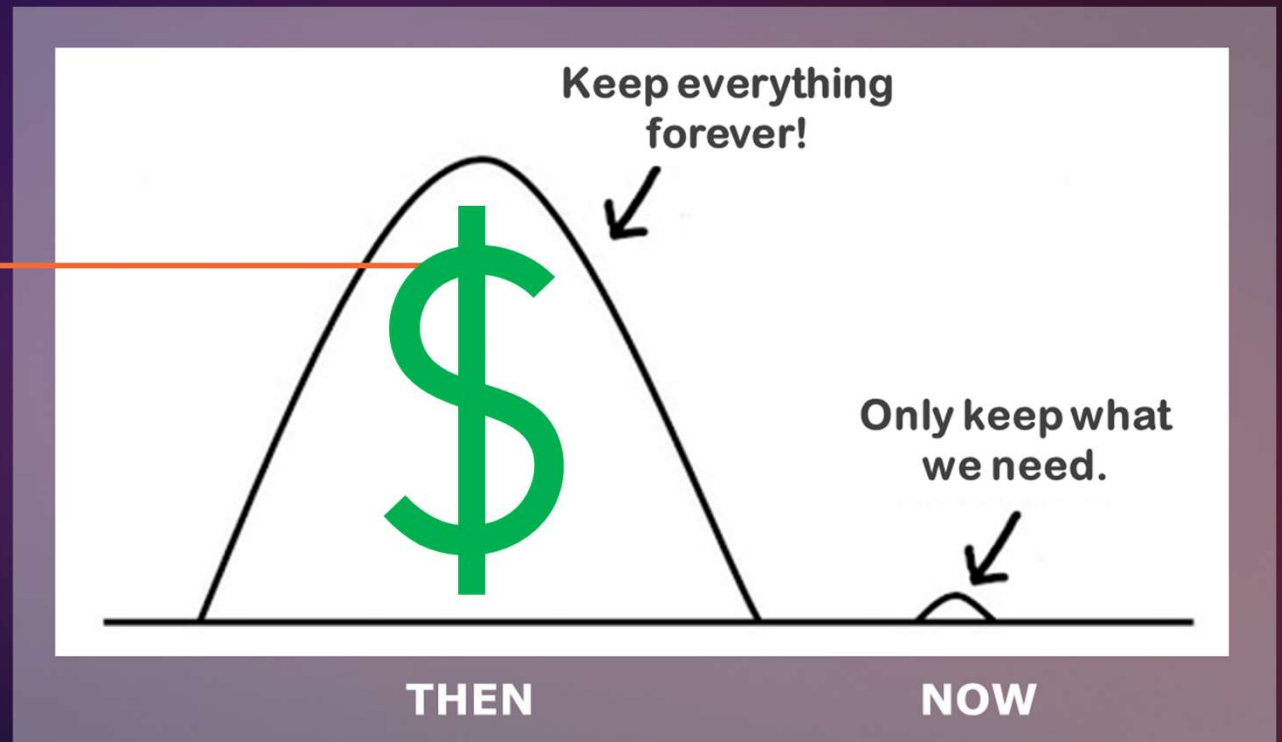
- Understanding the universe and types of data involved in M&A deal
- Reviewing existing contracts after acquisitions and assessing whether to retain or cancel these contracts based on data needs
- Outside counsel needs for navigating various regulations, including GDPR, CCPA and other national and global patchwork of laws and regulations



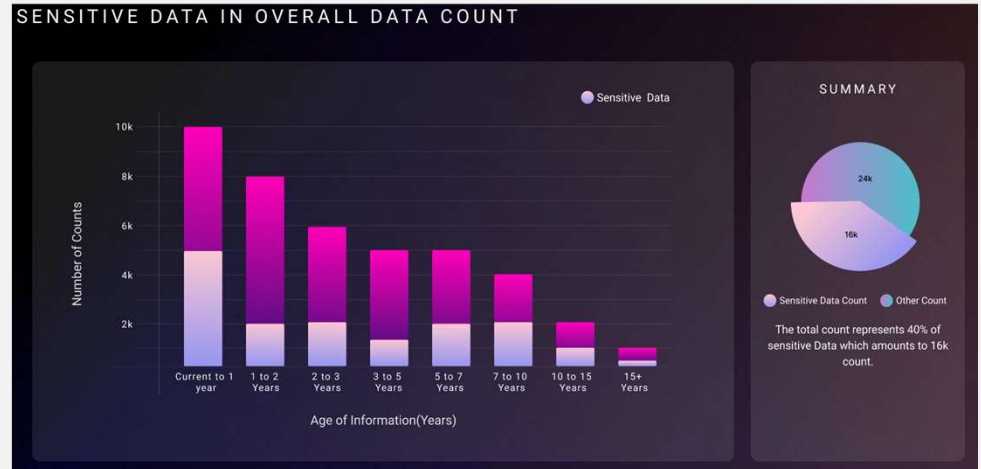
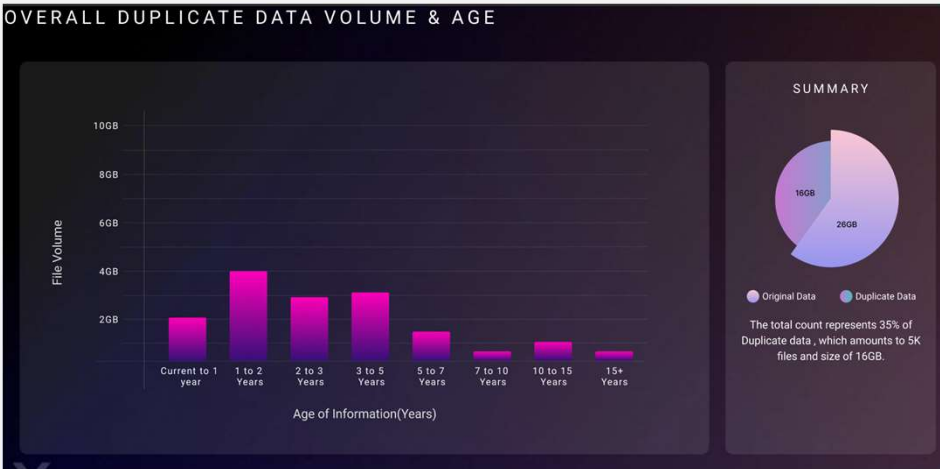
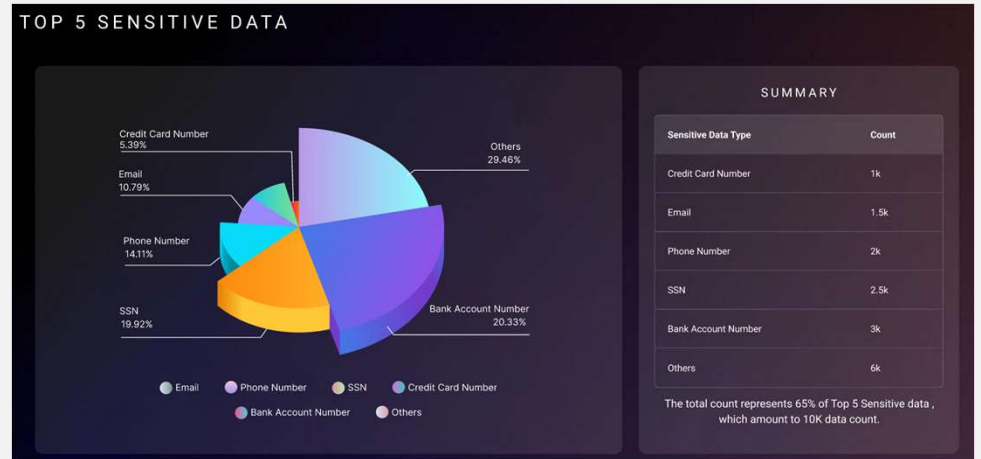
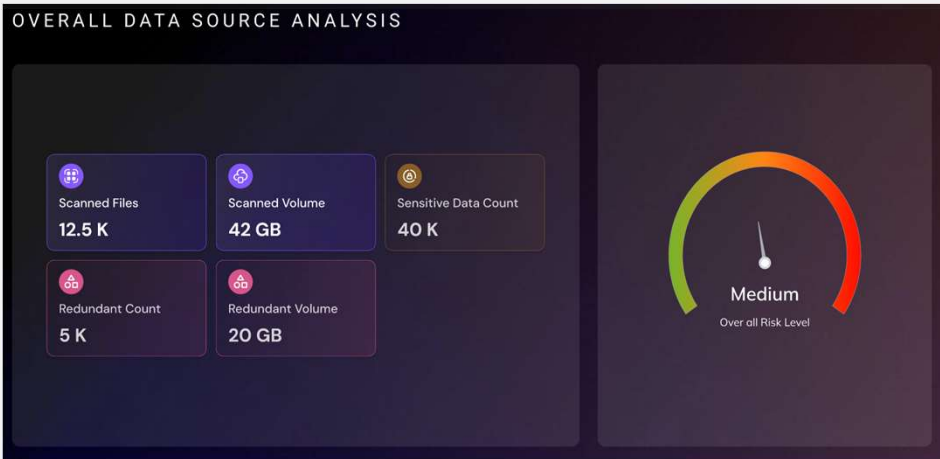
More Data = More Costs, More Risks, More Liability!

KEY RISKS:

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



Conduct Data Risk Assessment of Target Company





Data Risk Management Strategy

Develop Strong Cross Functional Teams

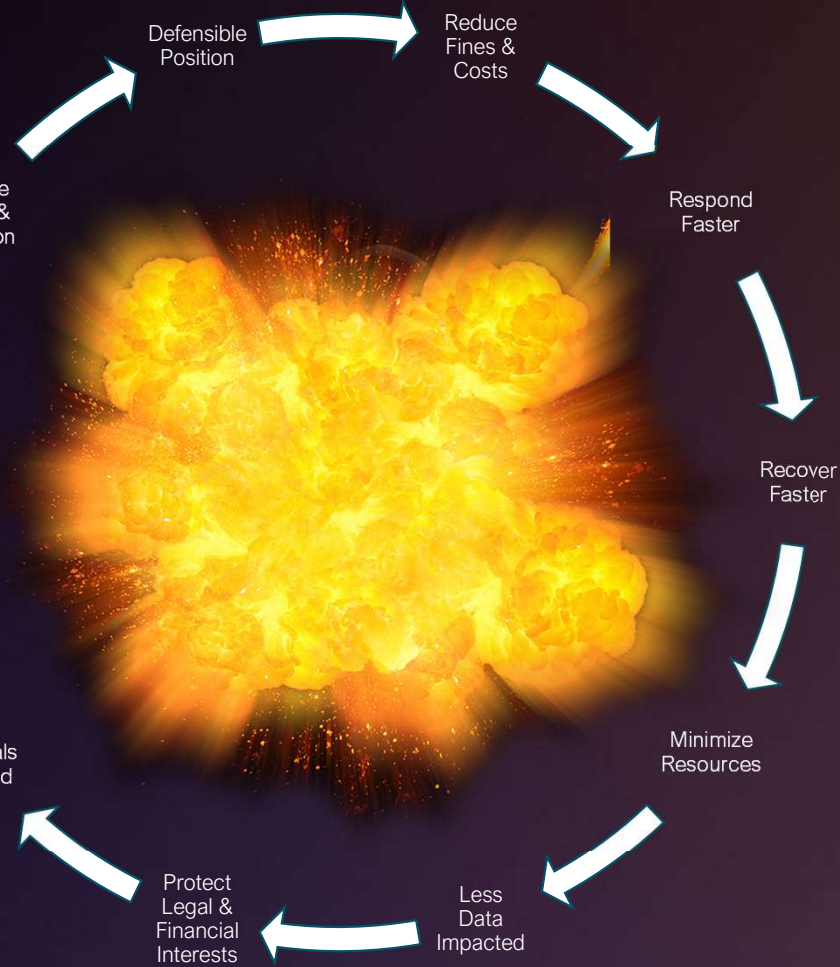


Establish Data Risk Management Processes

- ✓ 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

Data Discovery & Mapping

Leverage AI Technology



A Complete Orchestrated Solution



**DATA RISK
MANAGEMENT**



E-DISCOVERY



PRIVACY & DATA
GOVERNANCE



DIGITAL
FORENSICS



CYBERSECURITY
COMPLIANCE



Thank You!



Rebecca Perry
CIPP/US/G

Director GTM Strategy
& Operations Privacy &
Data Governance

Exterro

rebecca.perry@exterro.com



Paola Zeni

Chief Privacy
Officer, Strategic
Advisor

RingCentral

Rebecca.perry@exterro.com



Sushila Chanana
Partner

Farella Braun +
Martel

Rebecca.perry@exterro.com



Additional Resources

Emerging US AI Regulations

State Consumer Privacy Laws – Profiling / ADM

- Risk Assessments & Remediation
- Notice
- Opt-out
- Appeal

NYC Ordinance re: HR

CA, UT & FCC disclosure requirements

- Also, platform requirements

CO AI Act

- High-risk AI Systems
 - Substantial factor is a consequential decision
- Deployers
 - Risk management policy and program
 - Impact assessments
- Developers
 - Duty of care
 - Assist deployers to assess

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 & 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

Cybersecurity Updates

New York DFS Cybersecurity: 23 NYCRR Part 500

1. More obligations for the largest companies
2. Expanded notification requirements
3. Additional cybersecurity governance provisions
4. New requirements for incident response
5. Obligations for business continuity plans
6. Additional access controls & technical controls including
DATA RETENTION
7. Expanded risk assessment requirements
8. New enforcement provisions



SEC Final Rules on Cybersecurity Disclosures

Report “material” cybersecurity incidents within four business days of when an incident is determined to be material

Describe nature and scope of incident, timing and material impacts (i.e., financial condition and results of operations)

If required information is not determined or is not available at the time of the initial, disclose that fact and provide via an amendment

