exterro®

Protect Your Organization from Increasing Data Risks

An Exterro Data Risk Management Checklist

As the volume, variety, and velocity of data collected, created, and stored continues to skyrocket, it can yield the organizations that hold it ever greater returns.

But it also holds considerable risks. Cybersecurity threats can exfiltrate data or hold it for ransom. Privacy regulators can levy eight-, nine-, and ten-figure fines for data obtained or retained inappropriately. Legal risks stemming from these and other threats, like HR or employment issues, can compound the costs.

Concerns that resided strictly with legal or IT teams now demand executive attention from general counsel, CLOs, CPOs, CISOs, CDOs, and CEOs. This checklist helps executives and other organizational leaders understand what risks they are facing and how well they are prepared for them.

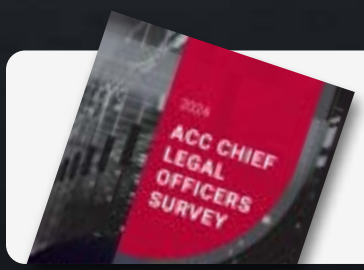
DO YOU UNDERSTAND THE DATA YOU HOLD?

- **Do you have an accurate, up-to-date asset inventory?**
- **Does your asset inventory include data on…**
  - Network attached storage
  - Off-network storage
  - Endpoints (e.g., employee laptops, etc.)
  - Cloud data sources
- **Does your inventory identify and classify data of these types…**
  - Non-public information
  - Personally identifiable information
  - Protected health information
  - Other sensitive personal information
  - Sensitive business information
  - Information under legal hold obligations
- **Do you have an active, operational data retention and deletion program in place?**

Learn all about the fundamentals of data asset inventories in the *Comprehensive Guide to Data Inventory*.

DO YOU HAVE PROCESSES AND TECHNOLOGY IN PLACE TO SAFEGUARD YOUR DATA?

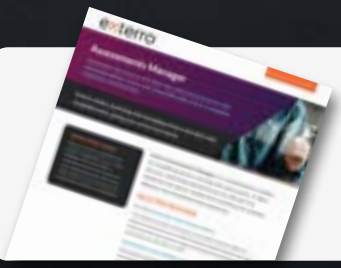
- **Are you prepared for cybersecurity risks?**
  - Have you assessed internal and external threats to your data?
  - Do you have clear policies and procedures for data security?
  - Is your team trained on cybersecurity best practices?
  - Do you have multiple layers of infrastructure security *(i.e., server, application, and device levels)*?
  - Do you have the technical ability to investigate and remediate remote endpoints?
- **Do you have processes and the technical ability to comply with privacy requirements?**
  - Do you obtain and preserve consent that is specific, informed, freely given, unambiguous, and granular?
  - Can you comply with data subject rights, including the rights to access, correct, erase, restrict processing, portability, and opt out of AI processing?
  - Can you report to regulators on demand on privacy risk assessments and records of processing activities?
  - Do you have controls in place that limit access to sensitive or personal data?
- **In response to anticipation or notification of a lawsuit, can you…**
  - Implement legal holds?
  - Preserve data in place to reduce the risk of spoliation?
  - Gain insight into data prior to collection?
  - Collect, review, redact, and produce ESI in compliance with discovery requests?



Find out what data risks CLOs and general counsel are most concerned with in the *2024 ACC Chief Legal Officers Survey*.

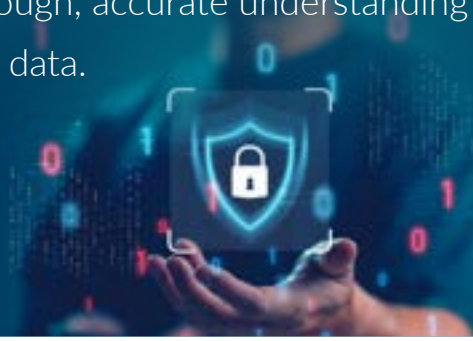
DO YOU UNDERSTAND YOUR DATA RISK LANDSCAPE?

- **Do you understand which privacy regulations apply...**
  - Based on your industry *(e.g., HIPAA, GLBA, etc.)*?
  - Based on jurisdictions your business operates in *(e.g., CPRA, GDPR, etc.)*?
  - To international data transfers between affiliates *(e.g., EU-US DPF)*?
- **Do you routinely conduct and update cybersecurity risk assessments...**
  - That evaluate and categorize internal and external threats?
  - That assess the adequacy of security controls related to these threats?
  - That assess the integrity and security of information systems?
  - That determine appropriate courses of action for risk remediation *(e.g., remediation, mitigation, or acceptance of risk)*?
  - That recommend changes and updates to address new risks?
- **Do you routinely conduct and update legal risk assessments...**
  - That review historic case data?
  - That review your current legal matter portfolio?
  - That account for potential internal risks *(e.g., employment lawsuits, discrimination suits, etc.)*
  - That account for industry regulations or litigation trends?



Learn how you can streamline your privacy and data risk assessment process with ***Exterro Assessments Manager***.

While a thorough assessment of risk includes understanding regulatory, legal, and cybersecurity requirements, it is impossible to adequately protect against litigation, privacy regulatory, and cybersecurity risks without a thorough, accurate understanding of your data.



Exterro Data Discovery can grant you unparalleled visibility into your data with automated inventory and classification of structured, unstructured, and semi-structured data, enhancing control and facilitating compliance over its entire lifecycle.

Schedule a demo today

exterro®