More Data, More Problems: 10 Reasons for Investment in Information Governance

Published

June 05, 2023

Key Contacts

Jake Frazier
Senior Managing Director, Head of Information Governance, Privacy & Security

Grainne Bryan
Senior Managing Director

Brian Boetig
Senior Managing Director

David S. Turner
Senior Managing Director, Co-Leader of Data & Analytics

Topics

OPERATIONAL

Information governance is becoming more expensive, and more critical. As the volume of business data continues to grow exponentially, the cost of managing that data is trending precipitously upward. In FTI Technology's recent Digital Insights & Risk Management survey of global business leaders, including general counsel, chief information security officers and chief privacy officers, more than 70% of respondents with information governance responsibilities stated that the cost of maintaining strong information governance has grown much more or somewhat more expensive over the last year.

At the same time, organizations are facing regulatory pressure to both preserve pertinent business communications (particularly for litigation and compliance under U.S. Department of Justice ("DOJ") guidelines) and maintain stringent data minimization (as per consumer protection and data privacy requirements under authorities including the U.S. Federal Trade Commission ("FTC") and the European Commission).

For example, in September 2022, Deputy Attorney General Lisa Monaco announced revisions to the DOJ's corporate criminal enforcement policies, which place a strong emphasis on corporate data as a key factor in maintaining, demonstrating and investigating compliance.[1] The revisions were released in an agency memo, throughout which corporate data practices and governance were key themes, particularly regarding their importance in ensuring the preservation of data pertinent to business communications and activity.[2]

Another example was the joint action by the U.S. Securities and Exchange Commission and Commodity Futures Trading Commission in late 2022, when the agencies issued more than $1.1 billion in fines to financial services institutions for improper information management and retention relating to employee use of private messaging applications for business communications.[3]

Separately, GDPR and other privacy regulations specify that organizations are only permitted to retain personal data to the extent and duration reasonably necessary per regulatory, legal and business requirements. Data protection authorities in Europe have issued multimillion dollar fines for failure to meet data minimization requirements.

It may seem that expectations to simultaneously preserve and minimize data are in direct conflict. Certainly, the way the corporate data footprint has and is continuing to expand, with an accumulation of massive repositories of information — including legacy records co-mingled with personal data and new sources — has made information governance and data minimization more challenging for organizations.

Yet, defensible data deletion policies and procedures can enable organizations to preserve what is necessary, while also reducing risk by remediating everything that is not needed. Such policies, and the steps to execute them, must address all data repositories, including retired legacy systems and backup tapes, as well as modern data sources such as collaboration tools and cloud-based apps, in which sensitive data, personal information and records may be intertwined with communications and other files not governed by preservation policies.

For legal teams working to develop a business case for new or enhanced information governance and security investments, here are 10 proof points for why with more data come more problems:

- **There is a very real data explosion.** A recent IDG survey found that on average data volumes are growing by 63% per month, and one in 10 data professionals reported that volumes are growing 100% or more per month.
- **Too much data is retained.** Numerous sources estimate that at least one-third of enterprise data is classified as redundant, obsolete or trivial ("ROT") data.
- **Excess data is risky.** Organizations doing business in Europe have faced fines of more than $14 million for data minimization failures. In January 2023, the FTC finalized a widely publicized action against an e-commerce company for data protection and data minimization failures, which included penalties against the company's CEO as well as requirements for the company to make significant changes to its information governance and security procedures. These examples are only the tip of the iceberg as to the consequences organizations may face for poor information governance.
- **Security is a growing concern.** According to Verizon's 2022 *Data Breach and Investigation Report*, 73% of data compromises resulted from external attacks. Threat actors are aware of the value data holds and, in turn, launch cyber attacks to obtain targeted information. In addition to ensuring protections are in place to mitigate cyber risk and minimize damaging impacts, organizations should consider what data they possess that is no longer of relevance and can be properly discarded. Data that has been disposed of cannot be stolen.
- **Data breaches are expensive.** IBM and Ponemon Institute's most recent annual *Cost of a Data Breach* report concluded that the average cost of a data breach in the U.S. is $9.44 million (compared to the global average of $4.35 million). This figure represents a seven-year high in the history of the report. The report has estimated the global cost per breached record at $164, up by 12% from the estimated cost in 2020.
- **Records and information programs are overmatched.** In the 2022 AIIM *State of the Intelligent Information Management Industry* report, 74% of respondents graded their organization's alignment between information management strategy and business strategy at average or worse. More than half said that alignment is not improving, and only 11% said they have the full commitment and support of executive leadership within their organization.
- **There are a variety of impediments to disposing records.** It is not just data volume that is growing — new tools and platforms, particularly for remote collaboration, are giving rise to a host of non-traditional data types and formats. In the IDG study mentioned previously, the mean number of data sources per organization was reported at 400, while more than 20% reported handling data from 1,000 or more sources. In FTI Technology's Digital Insights & Risk Management survey, 85% of respondents said the rise in data types is driving increased cost or risk, and the large majority said the increased use of collaboration tools and cloud-based applications has created significant or moderate information governance challenges.
- **Legal holds are often imperfect.** Studies have reported that over-preservation is common in legal holds, with roughly half of organizations found to over-preserve and retain more information than necessary due to flaws in how legal holds are written or applied. These mistakes can expose an organization to unnecessary additional scrutiny or liability in legal matters and can be significantly improved through the implementation of strong information governance processes.
- **Litigation and e-discovery are expensive.** Corporate litigation costs organizations millions of dollars per case, and document review makes up a large portion of those costs (more than 70%, according to RAND estimates). Moreover, in the 2023 *General Counsel Report* from FTI Technology and Relativity, 63% of chief legal officers said their legal department is experiencing increased demand relating to disputes. Simply put, these matters cost less when there is less data to collect and review.
- **Electronic discovery risk continues to evolve.** In the *General Counsel Report*, 40% of respondents rated the ongoing increase in disputes and investigations as one of their top five risks for the coming year. Similarly, e-discovery risks relating to emerging data sources such as collaboration platforms and cloud file-sharing tools rose by more than 10 percentage points from the previous year's report. One respondent said, "It is a huge discovery mess and has prompted us to look for more legal hold and Slack-related discovery tools." Improper handling of data and improper preservation is against the letter and spirit of e-discovery law and has repeatedly resulted in penalties and adverse inferences within the courts and in regulatory investigations.

Data remediation cannot be ignored amid today's data reality. By investing in robust information governance and security programs, legal teams can support their organizations in securing data, improving data privacy, strengthening compliance, improving e-discovery, reducing costs and enabling faster and deeper insight into valuable information.

Footnotes:

1: "Deputy Attorney General Lisa O. Monaco Delivers Remarks on Corporate Criminal Enforcement," The United States Department of Justice (September 15, 2022), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-corporate-criminal-enforcement.

2: Lisa Monaco, "Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group," The United States Department of Justice (September 15, 2022), https://www.justice.gov/opa/speech/file/1535301/download.

3: "SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures," The United States Securities and Exchange Commission (September 27, 2022), https://www.sec.gov/news/press-release/2022-174.