Chorology.ai
KNOW YOUR DATA

Thought Leadership Series:

Crossing The Compliance Chasm

Sept 01, 2024

Crossing the Compliance Chasm

The Impact of Data Compliance on Business and Profitability

Synopsis:

The gap between regulatory compliance mandates and practical implementation and enforcement is widening. Many would characterize the gap as a "Compliance Chasm". As digital technology penetrates every aspect of modern life, enterprise data volume and data sprawl are growing exponentially. To protect consumers, compliance and governance bodies are increasing data regulations without consideration for the economic and operational impact on business enterprises. Despite rising investments in privacy, security and compliance, today's whack-a-mole enterprise strategy of reacting to new compliance mandates is not keeping up. To "Cross the Compliance Chasm" and take back control to stop expanding enterprise risks, new thinking is required to reduce the cost, complexity and impact of implementing current mandates, while future proofing the enterprise for new regulatory environments.

Expanding Enterprise Risks: Large Compliance Fines

The frequency and size of regulatory fines are rising for enterprises that do not properly protect consumers' data. In January 2023, Meta was fined $225M and $193M for Facebook and Instagram for GDPR violations respectively by the Irish Data Protection Commission. Other GDPR violations include $99 million (€90M) in fines to Google by France's CNIL and $877 million (then €746 million) to Amazon in 2021 by Luxembourg officials. By May 2023, Ireland's Data Protection Commission concluded an enquiry into Meta Ireland and fined the social media giant an additional $1.3 billion (€1.2B) for additional violations.

Expanding Enterprise Risks from Exponentially Rising Enterprise Data

By 2025 the volume of data/information created, captured, copied, and consumed worldwide is forecasted to reach 181 Zettabytes.[1] (That is 181 followed by 21 zeros.) Nearly 80% of companies estimate that 50%-90% of their data is unstructured.[2] Think text, video, audio, web server logs, or social media activities. Data professionals see data volumes growing by an average of 63% *every month* in their companies - and nearly six in 10 organizations say they can't keep up.[3] As enterprise data expands, data breaches are

[1] IDC; Seagate, Statista 2024
[2] ITC, IDC, Gartner and ESOMAR's Global Market Research 2022
[3] Dataversity, 8/14/2023

increasing with a corresponding rise in compliance fines. More data means more data risk and therefore business risk.

Expanding Enterprise Risks from "Business as Usual" Growth

Over the past decades, billions of dollars have been invested in business intelligence and analytics to turn customer engagement and transactional data into behavioral profiles. Enterprises have also been actively buying and selling customers' individual data to enhance the breadth and depth of these profiles. Better data results in better customer understanding, when used in real-time, increases engagement and monetization.

Over the last few decades, these customer data-driven practices have become synonymous with "business as usual". Compliant or not, the truth remains that customer data and its use is of high value to businesses. Profitability has become highly dependent on deep customer understanding, powered by petabytes of sensitive and anonymous consumer data in use before, during and after purchase. "Business as usual" is expanding the Compliance Chasm and associated business risks, with almost no end in sight.

Expanding Enterprise Risks from Hidden Perils

Beyond the risks from rising data volumes, data sprawl, and "business as usual", enterprises also face rising risk from unintended effects of third parties. Large corporate data incidents make for primetime news headlines and revenue. As news spreads about data breaches, consumer fear spikes. Fearful consumers then submit DSRs (enterprise data service requests) to remove their personal data and reduce their exposure. The increased DSR volume is expensive to process in today's highly manual data compliance and enterprise IT workflows.

Another source of hidden enterprise risk comes from profit-driven attorneys with technical skills and international reach, who can detect compliance violations in cross-border enterprises. Large class action lawsuits with big attorney fees are becoming commonplace and the payoff in settlement fees can be substantial for attorneys who are skilled at weaponizing compliance mandates against public or private companies.

Compliance Bodies Need More Than a Clue

Today's global, national, and regional data compliance mandates were created with the best of intentions – to protect consumers' privacy and keep their data secure. But this "protection" has come at a very steep cost and burden to digital enterprises Most security

and privacy compliance policies have been formulated without enough consideration for the impact on business enterprises.

More importantly, these compliance policies were created long before adequate and scalable technologies emerged to enforce these policies. The technical and operating challenges for digital enterprises and organizations go much deeper than most government compliance bodies appreciate. Today's security, privacy, and data compliance technology solutions are simply not keeping up with protecting enterprises and therefore, their customers' data either.

How Are Businesses Likely to Respond to Future Compliance Mandates?

Given the risks and costs of responding to today's compliance mandates, enterprises are likely to start pushing back (strongly) on emerging regulations. The costs from compliance implementation, enforcement, servicing DSRs, and paying regulators' compliance fines will continue to rise as will lost revenue from re-designing or entirely dismantling data-driven consumer services to meet current mandates. Businesses with problematic compliance infrastructure have few choices until new thinking is applied to platforms and tools to intelligently automate compliance and enforcement.

Compliance Solution Choices Can Sacrifice Profitability

Data compliance and enforcement within enterprises is a very intrusive, time-consuming, and costly process. Many enterprises have invested in narrow tools and technology platforms optimized for a single mandate, such as GDPR in the EU, which does not adequately solve for compliance regulations of another mandate such as CCPA in California. Selection of the wrong compliance tools and technology platforms can have devastating intermediate and long-term impact to income and balance sheets after unplanned intra-year investments are required to meet increasingly complex requirements.

How Can Businesses Comply Without Sacrificing Profitability?

There are two lines of thinking that make up the best approach for selecting the right compliance tools and technology to meet the mandate(s). First, enterprises must stay informed of the evolving nature of compliance regulations and the major data technology trends driving business value. They must find and select compliance tools with core technology that is aligned with these enterprise data trends. Second, enterprises must adopt technology, tools and practices that provide compliance assurance without compromising

business objectives. They must seek out solutions that can ensure compliance and enforcement without scaling costs, as data volumes, sprawl and regulatory mandates expand.

Is Technology Available for Decreasing Compliance Complexity and Cost?

Compliance platforms that have evolved over the past thirty years mostly driven by whack-a-mole responses to new mandates, come with two major deficiencies.

First, discovery and classification functions within many of today's platforms are still limited to known data objects such as a customer's SSN or an address. In designing their platforms for specific compliance mandates, developers unwittingly constrained their platform capabilities to simple data types within structured data repositories. Many legacy platforms are incapable of complex data object discovery and classification, and cannot accurately discover data objects in unstructured data repositories

A second major deficiency of today's data compliance platforms is sufficiently automated compliance enforcement. Most of these platforms employ manual processes with marginal automation. They are EXTREMELY LIMITED in their ability to effectuate the data object transforms required to avoid sacrificing business utility. In short, the core capabilities of these platforms are designed for single data compliance mandates , but not for flexibility in data types, cloud or on-prem repositories, scalability, or cost-efficiency across mandates. For example, a digital health enterprise that requires data compliance across PII, GDPR and HIPPA mandates.

In short, legacy data compliance platforms are not "abstracted" to efficiently work across compliance mandates or data types stored in structured AND unstructured data repositories, on-prem and in-the-cloud.

Modern Compliance Technology Solutions – Best in Breed

A new class of data compliance operators have emerged to manage enterprise data privacy, compliance, and security. These best-in-breed data compliance platforms leverage Deep AI to intelligently automate data discovery, classification, mapping, enforcement and processes across mandates, data types and repositories. Data object abstraction combined with automated data mapping and enforcement let compliance teams track and manage risk, *across* compliance mandates for an enterprise with little human intervention.

Crossing the Compliance Chasm

Modern compliance platforms with intelligently automated components, functions, and workflows enable a new class of efficient, highly scalable data compliance operations. With these modern plaforms, compliance teams can efficiently track, quantify, and mitigate enterprise risks associated with data compliance in the digital age.

By having the ability to efficiently assess, manage and control data risk across compliance mandates, enterprises can increase their confidence in their data security, privacy, and compliance operations as their businesses evolve. Enterprises who employ modern, intelligently automated compliance platforms are “Crossing the Compliance Chasm” by increasing their efficiency and capability in responding to today’s dynamic compliance landscape, while future proofing their compliance organizations for tomorrow’s regulatory environments.

Contact Us

For copies of Crossing the Compliance Chasm, please email marketing@chorology.ai.
For further information please contact: info@chorology.ai

Chorology, Inc.
2001 Gateway Place, Suite 710, West Tower,
San Jose, CA. 95110 | Main: (408) 713-3303