Bloomberg Law®

bsi.

Building Information Resilience Into Today's Enterprise

Practical Guidance for Compliance, Risk, and IS Professionals

Building Information Resilience Into Today's Enterprise

Practical Guidance for Compliance, Risk, and IS Professionals

Businesses are benefitting from more technologies than ever before. Third-party platforms can easily authenticate users. Remote clouds can house and transfer data in seconds. Business intelligence tools can gather and disseminate large amounts of information—now with greater reasoning capability through advances in artificial intelligence and machine learning.

In short, a whole technology ecosystem and the wide sweep of data it touches is allowing enterprises across industries to learn more detail about their customers and strategize new market approaches. Experts predict that within the next decade, data holdings will even be reflected on company balance sheets.

This new reality presents both challenges and opportunities, making data both a company's greatest asset and greatest liability.

The need for a global view of information is emerging.

Today's business collects, stores, and accesses data, across platforms and jurisdictions, in ways more far-reaching than it may realize. In the decade that business intelligence technology has skyrocketed—along with advances such as cloud technology, the internet of things, and 5G—technology also has escalated, as have high-profile breaches that disrupt operations and rattle consumer trust.

As concerns about traceability and accountability grow, more public companies are adopting rigorous and often complex frameworks to try to maximize stakeholder confidence. Yet repeated breaches are leaving consumers skeptical that industry self-regulation alone will keep their data safe. To date, more than 100 countries have enacted data privacy laws, which are increasing in complexity as data flows across borders.[1] And a growing number of states, such as California, Vermont, and Colorado, have moved to enact their own data protection requirements in the wake of the May 2018 implementation of the European Union's General Data Protection Regulation.

The need for a global view of information is emerging. In the late 1800s, the art world saw a new painting technique in which small dots, applied in patterns, created an entire visual display only discernable when the viewer stepped back. Similarly, enterprises today can only glean their full information picture by looking beyond single data points, housed in siloed departments. Enterprises must scan vast data held across their organization and with global partners to effectively create, store, track, transfer, and, where mandated, destroy data.

This "information resilience" is essential for companies to comply with increasingly nuanced regulations from state, national, and global jurisdictions.

THE IMPORTANCE OF INFORMATION RESILIENCE

Information resilience is paramount to a company's long-term buoyancy and survival. While leaders understand the need for organizational resilience, this larger strategy requires a broad view of the data that fuels company operations.

"Any organization that deals with data on a day-to-day basis must reassess its information resilience," said John DiMaria, global product champion for information security and business continuity at BSI Group. This means developing a clear overview of the entire information life cycle—how data is created, processed, stored, disseminated, and ultimately, destroyed.

New realities hasten this need. Data is moving at lightning speed, while new regulations worldwide raise the bar on privacy and data governance requirements. In this environment, companies are responsible for data from cradle to grave.

The first step toward information resilience is a thorough assessment. "Companies must identify and understand their risks and the potential impacts to their organization," DiMaria said. These efforts pay off in multiple ways.

"Keeping a line of sight ultimately decreases complexity," he said, "and when you decrease complexity, you increase security."

SOURCE: BSI

[1] David Banisar, "National Comprehensive Data Protection/Privacy Laws and Bills 2018," Social Science Research Network, Sept. 4, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416

Revisiting information governance underpins this growing urgency.

"Today, more and more companies are part of distributed ecosystems, in which the primary fuel for prosperity is information that can be shared," said Jeffrey Ritter, an attorney and external lecturer at the University of Oxford on information governance issues. "That requires common formats, standardized security, and automated validation, none of which can be achieved by insisting on homegrown data governance methods and practices."

New approaches demand new vigilance.

"The critical shift in the status quo requires companies to develop and apply governance to their data assets from the moment of origin—when the data becomes real," Ritter said. "Ultimately, governing information effectively will require organizations to embrace and adapt the successful models used in their operations to manage their physical assets, financial assets, and intellectual property—collaborative, inclusive of all departments, structured, and engaged with the full C-suite and governing board."

Led from the top, a standardized, enterprise-wide approach to information governance can foster collective ownership, experts say, with an emphasis on action over mere compliance.

"There's a big difference between auditable and actionable," said Howard Mannella, a risk management expert and former principal resiliency strategist for a global technology travel company. "Leading practice is to move beyond 'auditable' to 'actionable.' That means less focus on documents and more on plans that are crisp, ergonomic, and usable, that everyone in the enterprise knows where they are and how to use, and have practiced until they are intuitive."

"Organizations that do not rethink their approaches," Ritter said, "will rapidly fall behind their competitors who do so."

Rethinking Information Governance

Information has always been essential to business operations. Lacking troves of data that could be mined for competitive advantage, however, businesses historically preserved information to satisfy public laws and legal proceedings.[2] A relatively simple approach to information governance ensued. Large organizations typically generated extensive, document-level retention schedules with myriad rows tracking single record types and respective locations.[3] This approach is falling behind.

"Simply focusing on retention periods, or understanding where data is stored, is no longer enough," said Wendy Butler Curtis, chief innovation officer and chair of e-discovery and information governance at the international law firm Orrick. "Organizations are constantly creating new records and repositories, especially with the expansion of on-demand technology. Keeping such schedules up to date is cost-prohibitive, and executing on them is also incredibly burdensome, if not impossible."

Regulatory frameworks governing data add to this burden. And data now drives every major industry.

Critical Infrastructure

The Department of Homeland Security identifies 16 sectors whose disruption would adversely impact public life. Among the threats these sectors face, data and security breaches could halt digital and physical operations.

- Chemical
- Commercial
- Communications
- Manufacturing
- Dams
- Defense
- Emergency
- Energy
- Financial services
- Food and agriculture
- Government
- Health care
- Information technology
- Nuclear reactors, material
- Transportation
- Water systems

[2] Bloomberg interview with Jeffrey Ritter, external lecturer, University of Oxford, Oct. 8, 2018

[3] Bloomberg interview with Wendy Butler Curtis, Logan Herlinger, Jeffrey McKenna, Orrick, e-discovery experts, Orrick, Herrington & Sutcliffe, Oct. 8, 2018

Accordingly, businesses face growing regulation. The 1996 Health Insurance Portability and Accountability Act has evolved from an initial focus on streamlining personal health records to setting standards for the protection of personal health information.[4] Data privacy regulations, impacting other industries, have since grown to encompass far more than health records.

The recent General Data Protection Regulation impacts businesses that collect the broadly defined "personal" data on individuals across the European Union. The law applies to anyone working or residing in the EU even if they are not a citizen. In what has been described as the most complex regulation the EU has ever produced, the law states data ownership ultimately resides with the individual.

Businesses risk reputation damage by delaying disclosure.

In practical terms, this means individuals can request businesses disclose specific data used to make decisions such as granting loans—a daunting request, given the complexities involved in retracing steps where "black box" artificial intelligence tools were involved—and account for all data should the individual exercise the "right to be forgotten." Stateside, the California Consumer Privacy Act mandates how companies can gather, store, and use personal data. Most significant, the law may force companies to adopt similar protections nationwide, rather than maintain two separate standards.[5]

These regulations are accompanied by narrow windows for reporting and substantial fines for noncompliance. The GDPR requires companies file a report within 72 hours of a data breach that delineates categories of information exposed and all parties impacted.[6] Beginning in January 2020, California residents can request that businesses identify personal information they have on them, how they collected it, the purposes of gathering it, and any third parties with whom it's shared. Businesses must comply within 45 days of the request.[7]

Where state law provides less explicit deadlines for disclosure, businesses risk reputation damage by delaying response.

Last year, one of the largest health-care groups in Pennsylvania saw the personal data of 300,000 patients hacked, following the merger of two health groups—highlighting the increased security risks that accompany merger and acquisition activity.[8] While state statute required consumer notification "without unreasonable delay," the company disclosed the breach more than two months after first discovering the attack, a timeframe some media reports questioned.[9]

Beyond adhering to mandatory compliance, companies can preempt potential liability and stay competitive by voluntarily adopting frameworks and standards.

"ISOs and frameworks eliminate the guesswork out of organizational risk-mapping and drive standardization in a way that costs are effectively reduced. In this context, they would afford a company defensibility in proceedings that their data security measures were 'state of the art,'" said Jennifer Prisco, vice president and chief legal counsel at Red Lion Controls, a Pennsylvania-based company that manufactures computer network equipment for industrial systems.

"Of course, this will also force companies who have not made sufficient investment in their infrastructure to do so," Prisco said, highlighting the importance of C-suite engagement in any subsequent decision. Executive leaders increasingly are guiding their companies toward standardization. One study finds roughly 30 percent of U.S. companies voluntarily comply with the non-regulatory entity National Institute of Standards and Technology Cybersecurity Framework. That share is expected to reach 50 percent by 2020.[10]

---

4 Rebecca Fayed, "Happy Birthday, HIPAA: How the Law Evolved, and What's in Store," Advisory Board, Aug. 23, 2013, https://www.advisory.com/daily-briefing/2013/08/23/happy-birthday-hipaa-how-law-has-evolved-over-time

5 Tony Romm, "California Legislators Just Adopted Tough New Privacy Rules Targeting Facebook, Google, and Other Tech Giants," *The Washington Post,* June 28, 2018, https://www.washingtonpost.com/technology/2018/06/28/california-lawmakers-just-adopted-tough-new-privacy-rules-targeting-facebook-google-other-tech-giants/

6 Lily Hay Newman, "No One Can Get Cybersecurity Just Right—Especially Lawmakers," *Wired,* Oct. 13, 2018, https://www.wired.com/story/cybersecurity-disclosure-gdpr-facebook-google/

7 Maria Korolov, "California Consumer Privacy Act: What You Need to Know to be Compliant," CSO, July 30, 2018, https://www.csoonline.com/article/3292578/privacy/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html

8 Marc D. Leone, "Here's How to Avoid Cyber Attacks When Considering a Merger," *Philadelphia Business Journal,* July 10, 2018, https://www.bizjournals.com/philadelphia/news/2018/07/10/heres-how-to-avoid-cyber-attacks-when-considering.html

9 Harold Brubaker, "Data Breach at Philly-area Ob/Gyn Practice Among This Year's Largest Nationally," *The Philadelphia Inquirer,* Aug. 12, 2017, http://www2.philly.com/philly/business/pharma/data-breach-at-philly-area-obgyn-practice-among-this-years-largest-nationally-20170812.html

10 "Cybersecurity 'Rosetta Stone' Celebrates Two Years of Success," National Institute of Standards and Technology, Feb. 18, 2016, https://www.nist.gov/news-events/news/2016/02/cybersecurity-rosetta-stone-celebrates-two-years-success

Highlights of a Robust Framework

Released in February 2014, the NIST Cybersecurity Framework delineates best practices for private-sector companies to detect, respond to, and prevent cyber attacks. A 2017 executive order calls for federal agencies to provide an action plan for similar adoption of the NIST framework, which complements roadmaps for information resilience proffered by security standards such as ISO 27001, which delineates information security standards. The framework outlines seven steps to solidify standards, guidelines, and best practices:

- Prioritize and scope
- Orient
- Create a current profile
- Conduct a risk assessment
- Create a target profile
- Determine, analyze, and prioritize gaps
- Implement action plan

Source: National Institute of Standards and Technology, U.S. Department of Commerce

Building on this framework, NIST and the National Telecommunications and Information Administration are developing new consumer privacy guidelines, with standardized protocols for federal agencies and private companies to adopt. This framework follows high-profile cyber breaches—beyond Facebook and Equifax, and the November 2013 breach of Target, one of the nation's largest department store retailers — through a third-party HVAC systems vendor. Experts stress this continued danger.

"Without standardization," Ritter said, "organizations will be handicapped by slower evaluations of data from third parties, longer decision processes, and ultimately lower velocity in competition."

Benefits Can Reach the Bottom Line

While strong data governance maximizes compliance, the role of standardization in supporting customer trust and productivity cannot be underestimated, experts say.

"Easy access to important information allows a business to operate more efficiently. Data about business processes informs opportunities for process improvement, automation, and outsourcing," said Curtis of Orrick. "Data about client habits and trends can inspire new business offerings."

Standardization can help improve customer trust and company productivity.

This insight holds true across industries. Health-care providers are seeing the financial benefit of value-based care models, and of the role data sharing and standardization play in fostering this care.[11] A global consumer credit reporting company has implemented standardized frameworks and tools, accelerating developer productivity from one major release every 12 months to 10 to 15 per month.[12] Medical device manufacturers are emphasizing standardization in clinical trials to foster innovation.[13]

Within any industry that's driven by data, similar discussions are occurring with information resilience in mind.

Yet challenges to implementation remain. "So often, companies overlook that governance requires both new rules and the assets to apply and enforce those rules," Ritter said. "Making the investments to create and enforce those rules will yield real benefits that assure their information always has value."

Those investments begin with leadership and a culture shift.

[11] Jessica Kent, "74 Percent of Execs Say Interoperability is Critical for Value-Based Care," Health IT Analytics, Feb. 21, 2018, https://healthitanalytics.com/news/74-of-execs-say-interoperability-is-critical-for-value-based-care

[12] Jessica Davis, "Experian CIO: IT Standardization Drives Agile," *InformationWeek,* Oct. 11, 2018, https://www.informationweek.com/strategic-cio/experian-cio-it-standardization-drives-agile/d/d-id/1333008

[13] "Efficiency, Transparency and Standardization: The Roadmap for Improved Data Collection in Medical Device Clinical Trials," Mass Device, Sept. 24, 2018, https://www.massdevice.com/efficiency-transparency-and-standardization-the-roadmap-for-improved-data-collection-in-medical-device-clinical-trials/

"Leaders need to take the time to talk to the data custodian or cybersecurity expert on the ground," Mannella said. They must also stress an organization's most important asset. "It's not the factories, or the products—it's data, and leaders should talk about it."

Translating this value into action requires right-sizing job descriptions, so that information and compliance are a natural part of processes.

Above all, implementation begins with a singular focus. "Data governance strategy should be driven by ROI," Curtis said.

"When implementing a record management schedule, focus disposition on data sets with the greatest risk and reward—whether because they are governed by privacy laws, data volumes are impacting performance of technology, or because better data hygiene is needed to use artificial intelligence to solve a business problem or offer a new line of services."

This focus future-proofs operations in the face of regulations and frameworks that will only grow in number and scope.

About Bloomberg Law

Bloomberg Law is a fully integrated legal research solution that delivers comprehensive primary and secondary source material, trusted expert analysis, practical guidance, leading news, and advanced analytics. Leveraging the latest developments in artificial intelligence and machine learning, Bloomberg Law enables legal professionals to provide world-class counsel and actionable legal intelligence to their clients and organizations.

For more information, visit www.bna.com/bloomberglaw

Bloomberg Law®

bsi.

For more than 100 years, BSI (British Standards Institution) has equipped businesses with the necessary solutions to turn standards of best practice into habits of excellence.

Today, BSI partners with 49% of the Fortune 500, 75% of the FTSE 100 and 77% of the Nikkei 225 Index, with clients ranging from large multinational organizations that are global household names, to small corner businesses serving the local community. From assessment, certification and training to software solutions, consulting services and supply chain intelligence, BSI provides the full solution to facilitate business improvement and help clients drive performance, manage risk and grow sustainably.

For more information, visit bsigroup.com or call 1.800.862.4977

Bloomberg Law®