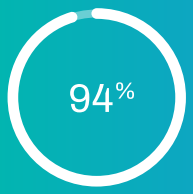
KNOW YOUR DATA: FROM DISCOVERY TO INSIGHT

IDC Info Brief: Managing Risk in Digital Transformation

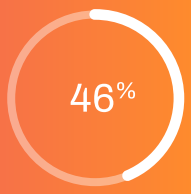


In 2019, 94% of organizations **named digital transformation (DX) a business priority,** according to *IDC's Worldwide DX Executive Sentiment Survey, 2019*. Data insights and analytics capabilities lie at the core of transformation and are defining drivers for business innovation.

IDC: The importance of **data and analytics for innovation** is expected to grow by 75% going forward.

With digital transformation comes data risk—risk posed by compliance requirements, data storage and retention, data poisoning, breaches, and more. Digital transformation demands full visibility into, understanding of, and control over collected data.

Data-driven risk management is the #1 key value businesses seek from their security teams, with 45% of leaders prioritizing it over improved operational efficiency—a distant second at 22%.



TRANSFORM DATA RISK INTO BUSINESS VALUE

Security and privacy done right are business enablers that lead to data insights and reveal business value without amplifying risk. Data discovery, classification, and visibility can generate the right insights for the right outcomes. BigID helps organizations manage data risk and optimize DX.

How BigID Helps Reveal Business Value

BigID's data intelligence platform automates data privacy knowledge, enhances data trust, enriches data governance, and enables business value creation while managing risk.

PUT DATA INTO CONTEXT

Not all data is created equal when it comes to sensitivity. Especially personal data. Applying the right data protection, access, and management policies requires understanding how and why data is related to an individual across data sources—and that is not possible without correlation and data intelligence.

BigID applies multiple classification techniques and advanced machine learning to accurately identify, classify, and tag personal and sensitive data based on correlation for privacy, security, and governance.

IDC: Secure DX demands full visibility and control over collected data to ensure its protection and compliance—and generate value.

TRADE COMPLEXITY FOR INSIGHT

You can't manage what you don't know you have. Data discovery across diverse data types and data sources creates the foundation to manage, enforce, and audit strategic privacy and security policies necessary for successful DX.

BigID's discovery in-depth approach gives 360° visibility into sensitive data and deep data insights across all data types and all data sources—on-prem and in the cloud.

IDC: For sufficient and flexible management of data-driven privacy and security risks, an efficient mechanism to move from data discovery to actionable insight is needed.

DEMOCRATIZE DATA INSIGHT

Data intelligence provides a common frame of reference and shared vision across an organization, fostering collaboration among privacy, security, and data officers.

BigID connects business and policy terms from business glossaries to data elements, objects, and physical assets at scale to build a unified inventory that serves as a single source of truth for your organization's data. This ensures that descriptions, physical data assets, and metadata stay accurate and up to date in a unified inventory.

IDC: It is imperative to balance competing demands at enterprise scale. Data insight fosters collaboration between privacy, security, and DX.

Source: IDC, Know Your Data: From Discovery to Insight, 2020

Know Your Data:

From Discovery to Insight

An IDC InfoBrief, Sponsored by BigID | **January 2020**

By Konstantin Rychkov, Research Manager, Software, Western Europe, and Dominic Trott, Research Director, European Security & Privacy

IDC | ANALYZE THE FUTURE

US45613019TM

In This InfoBrief

Data in this InfoBrief was derived from several sources of primary and secondary research:

- Global DX Survey, 2017
- IDC, Becoming a Data-Driven Organization Survey, 2018
- IDC's Global DX Leaders Survey, 2018
- IDC's European IT Security Survey, 2019
- IDC's Worldwide DX Executive Sentiment Survey, 2019
- IDC's Worldwide Semiannual Software Tracker
- IDC's Worldwide Security Spending Guide

Digital Transformation Pressure

2018 2019

89% 94%

of organizations have transformation as a business priority

AND

65%

of CEOs are under considerable pressure to deliver successful transformation as the central pillar of business success

Secure transformation demands full visibility and control over collected data to ensure its protection, achieve privacy compliance, and generate value.

Data Is at the Core of Transformation

Data and analytics are critical components for DX, and their importance for innovation **will grow by 75% going forward,** according to IDC's *Becoming a Data-Driven Organization Survey, 2018.*

Currently, 4 out of 10 organizations understand the high or extreme importance of data analytics and its fundamental role in the success of today's enterprise.

Data underpins DX across the organization, and it is a cornerstone for transforming IT and data operations together with operationalizing compliance.

However, data retention also represents exposure to risk given the threat of regulatory and policy non-compliance and the dawning realization that each piece of data represents an expansion of the attack surface.

Given the strategic enterprise importance that data and data analysis represents, including within a broader DX context, data risk thus becomes a business risk for digitally transforming enterprises.

To manage this risk, there are two key steps:

- You can't manage what you don't know you have. Successful DX depends on data discovery and understanding.
- All data is not born equal from a sensitivity perspective – especially personal data. To offer contextually-appropriate data protection, access, and management requires data classification in context, an important element for a successful DX strategy.

Privacy-aware data governance that spans data discovery, classification, and the full data life cycle is critical to help DX strategies succeed. Not only does it allow for appropriate protection of data, it also ensures the control and utility of enterprise data.

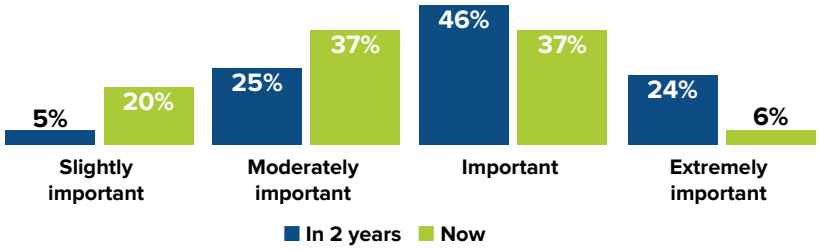
Data-driven Transformation Comes with Escalating Risks

Data risks in DX include:

- **Data privacy.** Compliance requirements such as the EU's GDPR and California's CCPA can have negative implications for business intelligence data utilization.
- **Data storage and retention.** Exponential growth of the data pull is paralleled with increasing risk of holding data.
- **Data hygiene for analytics.** Data poisoning can cause a major business malfunction.
- **Data protection and controls.** Data breaches now can entail civil prosecution and penalization.
- **Data discovery.** The utility of data depends on its quality and the ability to obtain the right information at the right time.

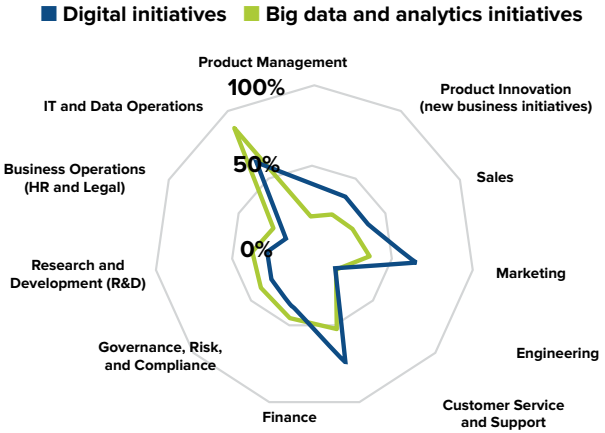
In two years, data and analytics capabilities will define transformation for **70% of organizations.** As new initiatives spread and expand across departments, so do risks associated with data.

Data becomes the cornerstone for business change



Q: How important are your organization's big data and analytics capabilities in driving business/ digital transformation and innovation?

Data initiatives follow and underpin digital change across organizational structures



Q: In which of the following departments are your big data and analytics initiatives being implemented? Digital initiatives?

Source: IDC, Becoming a Data-Driven Organization Survey, 2018, n=750

Data-driven Privacy and Security Risks

For sufficient and flexible management of data-driven privacy and security risks, an efficient mechanism to move from data discovery to actionable insight is needed. Core objectives here are to balance business imperatives to utilize data, data privacy compliance and ethical considerations, and security requirements for protection and controls.

Emerging regulations around privacy and expanding scope of data breach risk are **major drivers for technology spend.** For example, the GDPR prompted significant growth in spend through 2019, when the regulation became enforceable.

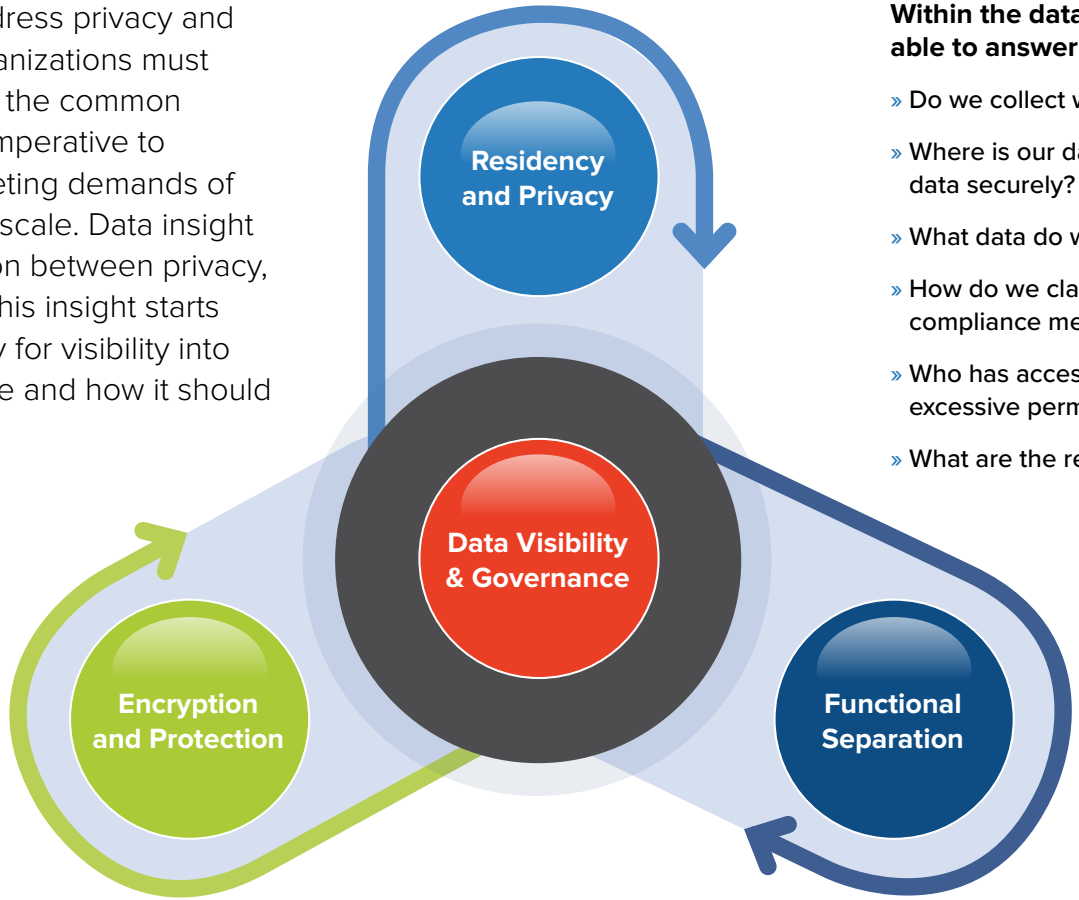
Technologies such as data loss prevention (DLP), identity and access management (IAM), encryption, anonymization, and pseudonymization that directly support regulatory compliance have seen strong growth in demand. The CCPA is likely to reinforce this trend, as will emerging state, federal, and agency regulations. The tension between regulatory initiatives for data protection and organizations' aspirations to maximize intelligence value is increasing. Striking a balance between compliance and business initiatives will be essential going forward.

As much as data is a benefit, it is subject to and a reason for several enterprise risks that should be taken into consideration and mitigated strategically. As the volumes of data generated, analyzed, and stored by enterprises continue to grow, so does the complexity of its management, storage, and compliance. The same applies for the risk that it represents.

Without appropriate controls, duplicated and redundant data further expands the attack surface and increases the risk of a data breach. This concern is especially critical as non-compliance under contemporary privacy regulations entails potential financial loss for the prosecuted company.

Know Your Data – Align Priorities

To elevate and address privacy and security in DX, organizations must use data insight as the common denominator. It is imperative to balance the competing demands of each at enterprise scale. Data insight fosters collaboration between privacy, security, and DX. This insight starts with data discovery for visibility into which data we have and how it should be treated.



Within the data life cycle, organizations must be able to answer the following questions:

- Do we collect what we have a permission for?
- Where is our data, and how do we store sensitive data securely?
- What data do we have, and why do we have it?
- How do we classify and process the data? Are compliance mechanisms functional?
- Who has access to the data? Are there users with excessive permissions?
- What are the retention and deletion mechanisms?

Data Discovery – Reveal the Value of Data

A data-driven strategy has several potential constraints when it comes to the security and privacy implications.
Examples include:

- Data residency
- Functional separation (pseudonymization)
- Encryption
- Compliance with GDPR consent and CCPA “do not sell” requests

For this reason, data intelligence via discovery and classification can be of tremendous value, allowing deeper visibility and insight for active decision-making and data management, helping it to break free from the potential constraints. The data intelligence that is derived should become the backbone of data operations and governance in order to secure the enterprise value of data.

Data visibility, understanding, and insight is the key. For maximum data utility, enterprises must understand what they have and where it is to ensure compliant and efficient use. Data insight should become the common denominator for governance.

The Concept of Data Intelligence

Data intelligence is the interaction and analysis of diverse configurations of data in a way that is meaningful for transforming the data into forms that will provide insight for a company's decision-making in an automated and streamlined fashion. The stages of shaping data intelligence are:

Enhance data trust
Integrate bottoms-up data discovery with metadata classification

Automate privacy compliance
Operationalize data access, deletion rights & automate report validation

Enrich data governance with context
Consolidated metadata store and tagging automation to integrate business, privacy context

Bridge business & technical teams
Review findings and collaborate on mapping discovery to business terms and categories

Manage privacy risk
Enforce consent & purpose of use parameters for data processing, ensure data lake hygiene

Orchestrate data validation
Confirm what users expect in the data, and validate data catalog classification

Enrich data lineage
Extend data lineage flows with per data source PI inventorying and ongoing scans for scoring input

Cross-functional data insights
Propagate metadata tags/ labels for security, IT and access governance policy input and enforcement

Source: BigID

Security and Privacy Are Business Enablers, not "Necessary Evils"

When it comes to DX, security and privacy are not inhibitors of change but rather enablers of it

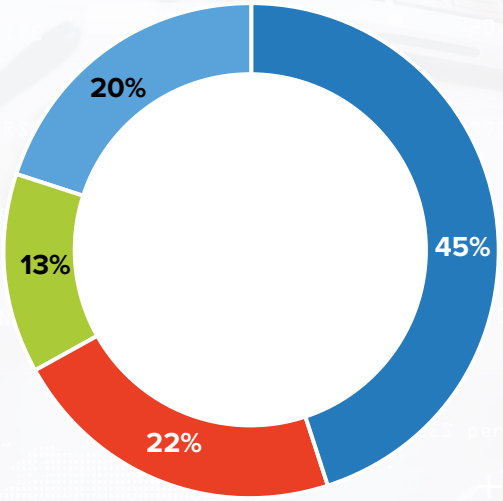
To position security as a field that supports business outcomes, it is critical that security and privacy are embedded within DX initiatives by design.

Security can demonstrate value by positioning itself as the fulcrum of an enterprise risk-based approach to DX, facilitating its deployment and operation while applying policy on a risk-appetite basis.

IDC's European Security Strategies Survey, 2019 shows that risk management is the number 1 key value-add characteristic that business lines seek from their security teams. This value, in the context of supporting data-driven transformation, is grounded in the extraction of intelligence from data. In turn, the benefits here can only be maximized when data discovery, classification, and visibility are embedded within processes and technology environments by design.

Data-driven Risk Management Applies Data Insights to Enhance Security and Business Value

For business leaders, the value of risk management optimization is higher than that of cost and operational efficiencies combined



Q: What is the primary area in which your organization expects IT security to deliver value?

- **Optimized risk management**
- **Improved operational efficiency**
- **Enhanced brand value/perception**
- **Reduced operating costs**

Although there are issues with data-driven risk management:

Balancing security and privacy priorities with business and productivity needs limits the ability to improve IT security capabilities for 43% of organizations. It is the number 2 issue for security leaders after the lack of qualified personnel.

More importantly, there are benefits:

With a comprehensive data governance model and related mechanisms to ensure visibility and context enrichment, organizations can:

- Ensure compliance by design
- Achieve greater business impact with data intelligence
- Align security and business strategy

IDC ANALYZE THE FUTURE

Source: IDC's European Security Strategies Survey, 2019

US45613019TM

Data-Centric DX Security & Privacy Road Map

	Chief Data Officer (CDO)	Chief Privacy Officer (CPO)	Chief Information Security Officer (CISO)
Role	**Subject and Sponsor of Change** Oversees the collection, management, and storage of data. Acts as the center of gravity for data-centric transformation from both technology and governance perspective.	**Supervisor of Change** Responsible for how personally identifiable information is collected, stored, shared, and transmitted; also ensures regulatory compliance. Providing guardrails for data-driven transformation is CPO's main objective.	**Guarantor of Change** Wears many cybersecurity hats from technical operations to communications and compliance. Ensures information confidentiality, integrity, and availability along and across transformation processes and initiatives.
Requirement	Emphasis on deriving insights to inform business strategy and value. Requires high level of data hygiene to ensure data intelligence strategy. Data governance strategy/framework should underpin business strategy and engage security and privacy in a collaborative manner.	Contemporary business floats on the data lake that feeds decision-making with strategic insight. That data is subject to complex sets of domestic and foreign regulations. Data privacy policy should drive compliant action based on information clustering, visibility, and labeling.	DX challenges security both technologically and operationally. To drive transformation in security's value proposition means focusing on enabling strategic business needs by making security the source of digital trust to enable the business's risk appetite.
Best Practices	Evangelize data strategy that improves information governance and security, building an alliance with CPO/CISO and IT. Form Tiger teams with privacy, security, and IT to pursue initiatives and deliver change faster.	Encourage and continuously update the privacy-related awareness program across lines of business in partnership with CDO. Shape achievable policies and SLAs with internal/external digital ecosystem participants.	Discover the location and identify the risk associated with enterprise data. Monitor and control data transfer and access. Determine "correct" user and system behavior, prevent malicious actions, and communicate with the business.
KPIs for CIO Consideration	• Improvement of data privacy and security awareness among team employees and power users across functions • Cutting the number and impact of security incidents inflicted by internal data platform and power users • Products released, rebuilt with data security and privacy by design • Data cataloging and categorization with security and privacy tags for risk measurement	• Net Promoter Score change associated with privacy-related digital trust initiatives rollout • Data feeds collected under consent that power analytics and strategic insight • Time-to-compliance with new regulations release and updates to existing ones (proactive compliance) • Reported privacy violations and overall number of data incidents in conjunction with total cost of compliance remediation per incident	• Estimated value of data assets at risk • Partner and ecosystem participants' security risk score improvement over time • Reducing mean time-to-resolution of the information security incident • Decrease in the number of systems with known vulnerabilities

IDC Analyst Profiles

Konstantin Rychkov
Research Manager, Software, Western Europe

Konstantin Rychkov is Research Manager for security software in the European software and infrastructure team. His primary area of focus, interest, and passion is security software, in which he has accumulated expertise through years of standardized and custom research, constant market monitoring, and frequent communication with software companies. He plays a leading role in the biggest security consulting projects done by IDC globally. He also supports the European Software and Services Group in the broader quantitative software research and semi-annual data reconciliation and plays a key part in ongoing data collection and modeling, content development, analysis, and quality assurance.

Dominic Trott
Research Director, European Security & Privacy

Dominic Trott is the research director for IDC's European Security & Privacy domain. As well as managing this team of analysts, Trott runs IDC's European CISO outreach program, chairing IDC's European CISO Advisory Board and the European 'CISO Hub' panel. Trott focuses on the top challenges for European security practitioners, including: the evolving role of the CISO, security that supports business outcomes; driving efficiency in security through integration/automation/orchestration, and the future of trust. As lead analyst for security and privacy in Europe, Trott leads many of his team's custom consulting projects. These include custom data cuts & forecasts, strategy workshops, whitepapers, peer assessment tools and more besides. He is also the analyst lead for IDC's European security roadshow and CISO Summit, ensuring these events provide actionable insights for delegates.

IDC Corporate USA
5 Speen Street
Framingham, MA
01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

IDC Custom Solutions

US45613019TM