Harvard Business Review
ANALYTIC SERVICES

Research Report

A BLUEPRINT FOR DATA GOVERNANCE IN THE AGE OF BUSINESS TRANSFORMATION

Sponsored by

Microsoft

SPONSOR PERSPECTIVE

Today's digital transformation has caused an influx of data—90% of the world's data has been created in the past two years.[1] Employees are empowered to create, store, and share information across devices and services, resulting in a complex digital environment that is difficult to manage. This complexity increases the likelihood of data leaks and breaches, from both inside and outside the organization. In fact, 53% of organizations have experienced an insider attack in the past year.[2]

KIRK KOENIGSBAUER

CORPORATE VICE PRESIDENT

MICROSOFT 365 & SECURITY

Organizations need to effectively respond to these changes to protect their most valuable resource—their data. We discovered in the study that follows that 61% of organizations still struggle to effectively develop strong data security, privacy, and risk capabilities.[3] There is an opportunity for organizations to embrace data governance and adopt solutions to keep their employee, customer, and company data protected.

As organizations continue to search for ways to identify, govern, and manage their data, there are several essential questions each organization will need to answer to better align compliance initiatives and data requirements with their overall business strategy. How can we enable a workplace that effectively navigates compliance challenges, whether mandated by external regulations or by internal policies? Which organizational changes should we adopt to better manage data security, risk, and compliance? Where do we start our journey to improve data governance and ultimately reduce risk of data leaks?

To explore some of these questions, we partnered with Harvard Business Review Analytic Services to understand how this proliferation of corporate data may require global companies to alter their data security, privacy, risk, and compliance policies. We surveyed close to 500 global business leaders across industries, including financial services, tech, health care, and manufacturing. This study examines the impact that digital transformation has on organizations, how leading organizations are making data governance a strategic priority, which technologies are being adopted at scale to automate data governance, which roles are responsible for overseeing corporate data policies, and the investments that organizations are making to better manage their risk.

1 IBM

2 Crowd Research Partners

3 "A Blueprint for Data Governance in the Age of Business Transformation," Harvard Business Review Analytic Services, 2020"

A BLUEPRINT FOR DATA GOVERNANCE IN THE AGE OF BUSINESS TRANSFORMATION

Digital innovation is reshaping travel and leisure, financial services and health care, manufacturing and communications, and now it's transforming chocolate—or at least how the coveted candy gets into consumers' hands. The Hershey Co. started making chocolate in the U.S. more than 125 years ago and now sells sweets around the world. For most of that time, it relied on grocery stores to distribute its products. As online grocery sales rise, Hershey executives are considering ways to augment that go-to-market strategy by engaging directly with consumers.

"As the business strategy evolves, we'll need as much insight as possible for new product ideas and the best ways to engage with consumers. That is driving us to collect more data to gain those insights," says Stephen Hendrie, Hershey's senior director and chief information security officer (CISO), who's responsible for information security, privacy, and compliance across the company's global operations. "We have to be very proactive about safeguarding data and maintaining the trust that consumers have in our organization."

Hendrie isn't alone. Executives across industries and geographical regions are seeing a direct link between the effective use of data and improved business results. More than three-quarters (77%) of 460 global executives recently surveyed by Harvard Business Review Analytic Services believe that a successful data strategy is essential for business success. That realization is leading many observers to call data the new oil, and for good reason. Data-monetization models are helping five of the world's six most valuable companies achieve a collective market value of more than $4 trillion.[1]

But devising successful data strategies isn't easy. The survey found that many large organizations are struggling to implement modern data-governance policies, the essential guardrails for protecting and managing sensitive information. Eighty-two percent of the respondents report that securing and governing data is becoming more difficult because of new risks and data-management complexities brought on by business transformation. In addition, nearly six in 10 enterprises (59%) say their data-governance approach doesn't span the entire organization, which leaves sensitive information in some departments and divisions vulnerable to data breaches, lost business, and regulatory fines that harm reputations and bottom lines.

KEY TAKEAWAYS

92%
OF BUSINESS LEADERS SURVEYED SAY NEW TYPES OF RISK ARE BEING CREATED BY SHIFTING BUSINESS MODELS ASSOCIATED WITH BUSINESS TRANSFORMATION.

77%
SAY AN EFFECTIVE SECURITY, RISK, AND COMPLIANCE STRATEGY IS ESSENTIAL FOR BUSINESS SUCCESS.

53%
OF ORGANIZATIONS, HOWEVER, HAVEN'T DEVELOPED A STRONG, BUSINESS-WIDE DATA GOVERNANCE APPROACH.

FIGURE 1

FIVE PILLARS OF EFFECTIVE DATA GOVERNANCE

Strong information management requires multifaceted strategies.

SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, OCTOBER 2019

EFFECTIVE DATA GOVERNANCE PROTECTS COMPANIES FROM NEGATIVE HEADLINES ABOUT DATA BREACHES AND MISMANAGEMENT.

Not all organizations are struggling. The survey identified a select group of companies with comprehensive data policies that are helping them outperform peers and gain competitive advantages in their markets. Their message for others is clear: data governance is no longer a concern only for IT experts. Now data governance should also be top of mind for the C-suite, line of business managers, and everyone else who contributes to a business's success. By modeling the lessons of leaders, other organizations can develop a blueprint for data governance to capitalize on their rich data reserves.

The State of Modern Data Governance

If data is the new oil, then data governance is the pipeline that safely brings critical information to the people who need it. The term encompasses all rules and digital plumbing required for managing data security, privacy, risk, and regulatory compliance. FIGURE 1

There is little internal debate about the importance of strong data governance. In addition to the three-quarters of executives noted above who directly link data strategies to business success, 61% of the survey participants say trustworthiness associated with securing and managing data is or will soon become a competitive differentiator in their industries.

Trust is important because customers are more likely to share data and buy from companies with a reputation for securing and governing data, according to 63% of the executives surveyed. In turn, executives say reliable reserves of data are extremely important for many core business goals. FIGURE 2 Topping the list of data-governance business goals for nearly four in 10 (39%) survey respondents is enhanced decision-making capabilities. When companies have large reserves of accurate information, they're better able to mine insights for improving sales and marketing campaigns and spotting new trends in the marketplace.

"One of the main premises of digital transformation is building more personalized experiences for customers," says Joseph Ciuffo, a survey participant and product marketing director for artificial intelligence at Genesys, a software company based in Daly City, Calif. "If you don't successfully protect data, you'll lose trust and the opportunity to build better customer relationships going forward."

Corporate reputation comes in a close second (at 38%) on the list. Effective data governance protects companies from negative headlines about data breaches and mismanagement. One executive from a management consulting firm who participated in the survey saw this in action. He received a 3 a.m. call from a client at a large

corporation that detected a breach in an IT system. Together, the consultant and the client determined that a hacker was attempting to disrupt the company by sending a fictitious email about one of its divisions being sold. "We worked quickly to stop the message from going out before the financial markets opened," says Bechara Chaya, vice president at the Paris office of the consulting firm Capgemini. "Breaches can have very dangerous and long-term consequences for a company's reputation and financial health."

Protecting intellectual property and reducing costs associated with breaches and regulatory fines round out the top four business goals associated with strong data governance.

Unfortunately, business goals don't always translate into successful outcomes, as shown in Figure 2. Executives reported double-digit gaps between aspirations and results when asked to rate their success in achieving each of the business goals related to data governance.

Why is data governance so difficult? Rapidly increasing volumes of data present the biggest challenges, according to 53% of executives. FIGURE 3 "Digital transformation is fundamentally changing the nature of work," says Jay Cavalcanto, vice president of the technology, design, and engineering group at Exelon, a large energy generation and delivery company based in Chicago. "For the longest time, business content was created inside an organization's network using devices fully controlled by IT. Today, business documents and data are being created with cloud applications on a range of laptops, smartphones, and tablets."

"As data sources and the proliferation of information increase, it is increasingly important that the business systems used to create that information have capabilities built into them to address compliance, e-discovery, and records retention," adds Charisma Starr, Exelon's manager of legal technology and eDiscovery operations. "It's imperative that we apply all the legal and regulatory controls necessary to protect data."

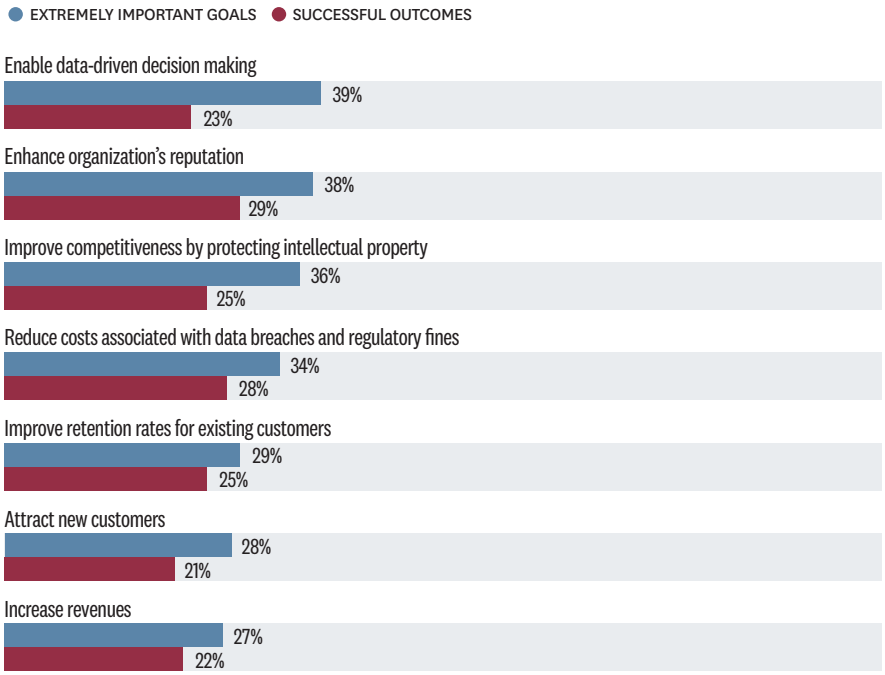
Another roadblock is the so-called democratization of data, where corporate information flows more freely across departmental boundaries and among widespread groups of business users. More than 40% of the survey respondents say new security challenges arise when organizations share more data across departments and divisions. Add to that ongoing struggles to meet complex and frequently changing regulatory requirements. Global companies must not only comply with their home country's laws but also meet the requirements in all the markets where they do business.

FIGURE 2

BUSINESS SUCCESS HINGES ON GOOD DATA GOVERNANCE

Security and compliance aren't just IT's concerns.

Rate the importance of the following business goals when making investments related to data security, privacy, risk, and compliance.



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, OCTOBER 2019

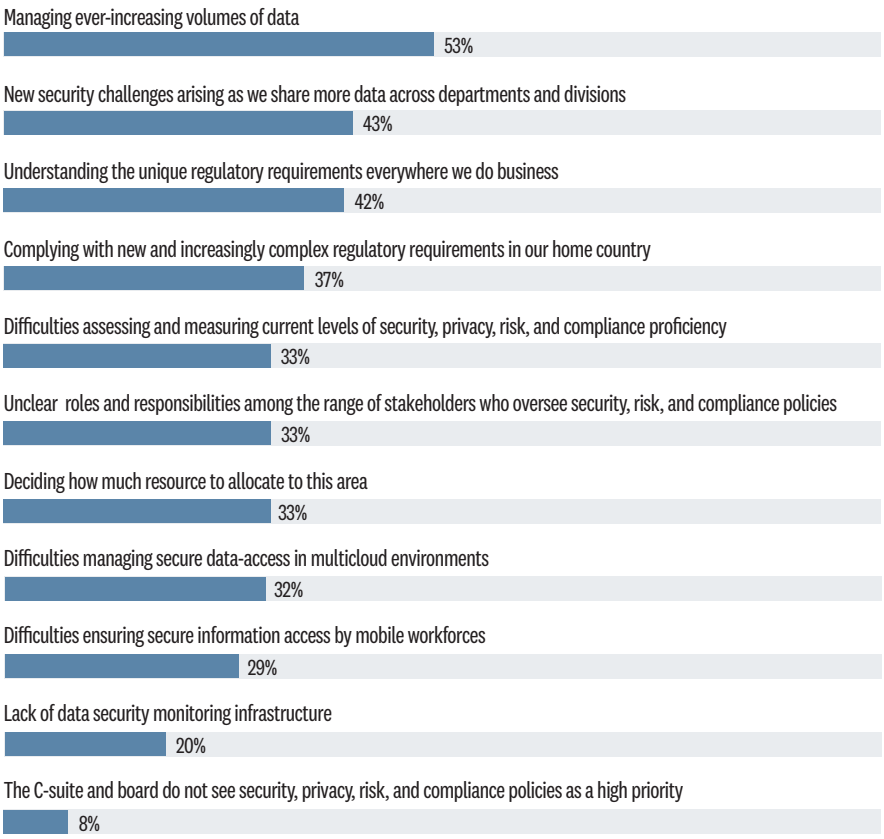
Executives reported **double-digit gaps between aspirations and results** when asked to rate their success in achieving each of the business goals related to data governance.

FIGURE 3

BURGEONING DATA AND NEW REGULATIONS PRESENT THE BIGGEST ROADBLOCKS

The pace of change creates unprecedented complexities.

What are the biggest challenges your organization faces related to managing data security, privacy, risk, and compliance?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, OCTOBER 2019

"As companies expand their digital transformation strategies, achieving security and compliance is becoming more complex," says Nikola Radonov, manager of service delivery at the Bulgarian offices of the global IT services company DXC Technology. "I've been in IT for 20 years, and I've never seen the rate of change be so rapid."

Executives even have trouble determining how well their data-governance efforts are working. The survey asked about some key performance indicators (KPIs) for data governance, including essentials like how long the IT department takes to apply protective security measures or remediate known vulnerabilities. More than 40% of the executives didn't know whether KPIs existed for these areas. The respondents were even more in the dark about pass rates for security and compliance audits and whether they were reducing fines from failed audits—more than half of the respondents say they were aware of audit-related KPIs.

Lack of clarity about individual performance metrics may be symptomatic of wider shortcomings. For example, before data-governance staffs can prioritize resources for securing and managing data, they must clearly understand their organization's appetite for risk—to general business systems and to critical assets, such as financial systems and customer records. Without this risk-tolerance foundation, executives can't accurately determine which resources require the highest levels of control. But more than a third (36%) of the survey respondents say senior executives can't agree on acceptable levels of risk. What's more, 63%

say the roles and responsibilities of stakeholders for security, risk, privacy, and compliance are not clearly defined, which leads to gaps in policy development and enforcement.

Data-Governance Leaders

Nevertheless, a select group of survey participants has found answers to data-governance challenges. The survey identified leading organizations as those that have attained two important maturity milestones: they're applying a strong data-governance framework across the entire organization, not just in some isolated departments, and they're accurately measuring the returns on data-governance investments. FIGURE 4 Together, these capabilities not only demonstrate strong commitments to a comprehensive data-governance strategy but also indicate that KPIs are in place to gauge the success of that effort.

Drilling into the survey results reveals how leaders are distinguishing themselves from less-mature peers. Security and compliance programs aren't recent developments for this group. Leaders have prioritized new approaches to managing data for at least the past two years. Seventy-nine percent of leaders have made fundamental changes to their operating models so they can use data more effectively. In addition, 55% of leaders have also updated their data-governance policies.

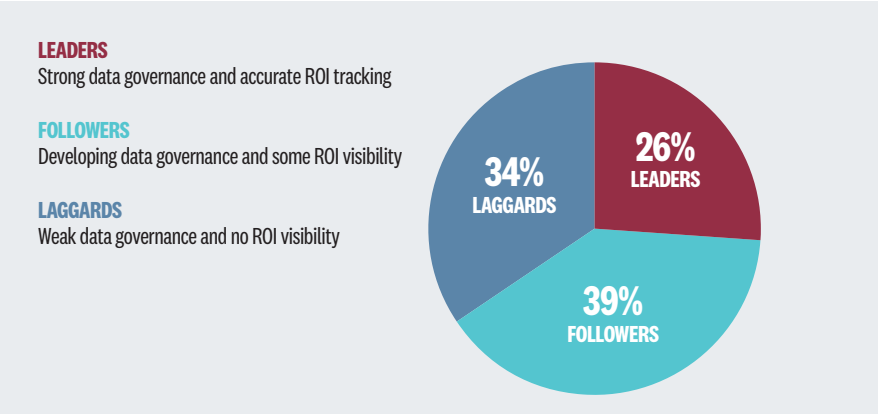
As a result, leaders are significantly more successful—by differences of 20% or more compared to the rest of the survey sample—in each of five core components of data governance: policies, culture, organization, technology, and people. In addition, nearly half (47%) of the leaders rate their organizations as being considerably ahead of rivals in data-governance capabilities.

The efforts of data-governance leaders are not only positioning them for business success, but also their actions may have larger social implications. "Industry surveys over the past few decades have shown that trust has been declining in institutions, while trust in businesses has remained fairly steady," says Paul Zak, professor of economic sciences, psychology, and management at Claremont Graduate University and author of the book *Trust Factor: The Science of Creating High-Performance Companies*. "There's a role for business to step in and be a trustworthy partner for citizens and communities."

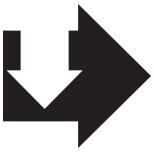
FIGURE 4

LEADERS FIND ANSWERS TO DATA-GOVERNANCE PROBLEMS

A select group combines strong strategies and ROI metrics.



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, OCTOBER 2019



"INDUSTRY SURVEYS OVER THE PAST FEW DECADES HAVE SHOWN THAT TRUST HAS BEEN DECLINING IN INSTITUTIONS, WHILE TRUST IN BUSINESSES HAS REMAINED FAIRLY STEADY." PAUL ZAK, PROFESSOR, CLAREMONT GRADUATE UNIVERSITY

INTELLECTUAL PROPERTY DATA REQUIRES HIGH LEVELS OF PROTECTION BECAUSE OF ITS ROLE IN CARVING OUT COMPETITIVE DIFFERENTIATION.

Six Steps to Better Data Governance

Leaders not only demonstrate impressive competitive advantages, but they also offer a model to help underperforming peers mitigate the new risks brought on by business transformation and the compliance gaps that explain why 60% of the enterprises surveyed have yet to apply a consistent data-governance approach across the entire organization. By following the guidelines of leaders, less-mature organizations can strengthen security and compliance capabilities to help improve business results, support data-driven operating strategies, and address increasingly complex regulations. The journey to data-governance maturity starts with six foundational steps.

1. Identify and classify all of the organization's data.

Before organizations can formulate specific policies for modern data governance, they must assess their current operations to determine where gaps exist and to prioritize the areas that must be addressed quickly. The process begins with data identification and classification, the first step in assessing risk. Not all data can or should be protected equally. Intellectual property, for example, requires high levels of protection because of its role in carving out competitive differentiation. By contrast, public resources, such as product brochures, need safeguards to guard against hackers, but the controls can be less rigorous. The audits should involve a cross section of stakeholders from IT and security, lines of business, legal departments, and senior executives to determine the relative criticality of various data resources and establish the organization's risk tolerance for each data type. By analyzing and categorizing internal assets, organizations can determine what controls are necessary to manage access and availability across the organization. In addition to identifying controls for security and privacy, the assessments also should examine processes for complying with government regulations in each of the markets where the organization operates.

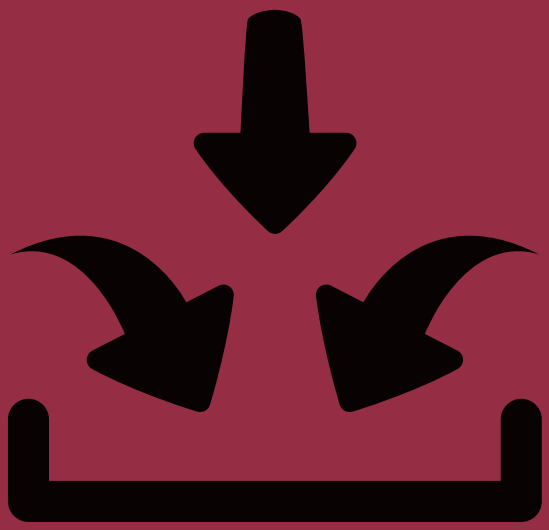
"Many large organizations don't have a clear picture about all the data they are collecting and what people throughout the organization are doing with it," says Ron Carucci, managing partner at Navalent, a consulting firm specializing in business transformation. "Executives need an understanding of everything regarding their information and the vital decision-making systems that information supports. They then need to make sure somebody is responsible for overseeing all the data initiatives that are underway, so they remain integrated. Fragmented data efforts can sometimes be worse than no data efforts."

With assessments as the foundation, organizations can tackle improvements in the five pillars of data governance.

2. Enhance data-governance policies to meet internal and governmental requirements for security and privacy.

When asked about the most important steps organizations are taking to demonstrate their commitment to improve data governance, more than half (54%) of the leaders say they are focusing on enforcing policies designed to prevent leaks of customer information. This result is higher by 20 percentage points or more than other choices and shows an acute awareness of insider threats—whether malicious or simply accidental breaches of internal policies. For many years, industry research into underlying causes of security and privacy breaches has named exploits of end users as the biggest source of threats.[2] The low-performing companies identified as laggards in the survey have yet to fully commit to this reality—only 39% name defenses against the unauthorized sharing of information as one of the most important data-governance steps they're taking.

Exacerbating efforts to stanch data leaks is the ongoing friction that end users feel between data governance and productivity. Almost two-thirds



"EXECUTIVES NEED AN UNDERSTANDING OF EVERYTHING REGARDING THEIR INFORMATION AND THE VITAL DECISION-MAKING SYSTEMS THAT INFORMATION SUPPORTS." RON CARUCCI, MANAGING PARTNER, NAVALENT

REGULATED INDUSTRIES TAKE THE LEAD IN DATA GOVERNANCE

The global survey by Harvard Business Review Analytic Services confirmed that executives across industry sectors understand the growing importance of strong data governance. But the research also found that some industries, notably the most highly regulated sectors, feel heightened pressure to bolster security and compliance efforts.

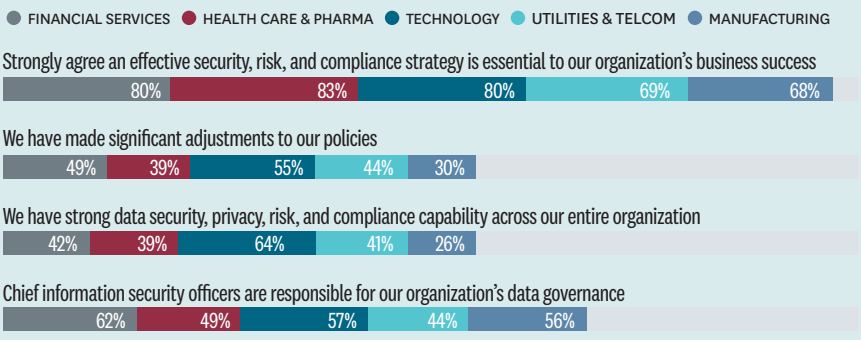
For example, 80% of executives from financial services and health care and pharmaceutical companies consider data governance essential for their success. FIGURE 7 Although not as highly regulated, technology companies feel similar pressures, which may be because many tech-industry business models depend on being trustworthy stewards of customer data. While also facing significant government oversight, utility and telecommunications firms don't see data governance in the same light as other regulated industries, perhaps because many are still transitioning to digital infrastructures and don't transmit as much internal data across internet-based systems.

Nevertheless, utility and communications companies are in the most active industries to have made significant changes to data-governance policies, outpacing their health care and pharma counterparts. The three highly regulated industries represented in the figure show similar success in implementing enterprise-wide governance strategies and matching rates reported by the full survey sample. At 64%, the technology industry clearly distinguishes itself in its ability to apply security and compliance policies throughout its organizations.

While manufacturing companies lag behind those in the other industries, they're showing a clear sign of progress that portends improvements in the near future. Second only to financial services, more than half (56%) of manufacturers strongly agree that having a chief information security officer (CISO) is the best way to drive a successful cybersecurity strategy.

DIFFERENT INDUSTRIES, DIFFERENT PERSPECTIVES

Executives adjust data strategies to unique requirements.



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, OCTOBER 2019

(64%) of all respondents acknowledge that employees are often tempted to skirt security and compliance policies because they believe the rules hinder productivity.

Leaders understand that crafting a policy framework for internal operations is only part of the data-governance puzzle. Half of the leaders are also looking outside their organizations and requiring partners to align with corporate security and compliance policies. A similar number (47%) are continuously monitoring the data access and usage behavior of partners to assess their data-management practices.

3. Create a culture of security and compliance by cultivating organization-wide awareness and responsibility about the proper handling of data.

Executives representing all three maturity levels—leaders, followers, and laggards—rely heavily on CIOs and chief data officers (CDO) to manage security and compliance.

To ensure that data-governance is seen as everyone's duty, however, leaders are much more likely to engage wider range of stakeholders in the effort. Two-thirds (65%) of leaders augment the work of CIOs and CDOs with governance, risk, and compliance (GRC) officers or equivalent titles. Nearly half of the leaders (45%) also involve line-of-business managers or department heads as formal participants in governance activities. By contrast, only a quarter of laggards make data governance a formal responsibility for heads of business operations.

The security staff at Hershey works closely with legal and business counterparts to develop governance rules. "We'll make recommendations about policies for information security, appropriate risk postures, and how to avoid theft of our intellectual property," Hendrie, the Hershey CISO, says. "Once policies are formulated, my team and I are responsible for implementing and enforcing them."

4. Creating new roles and responsibilities, to strengthen security, risk and compliance strategies.

Leaders are more likely than their peers to name a CISO to guide the formulation and enforcement of data policies. CISOs often also act as the point persons for identifying and managing appropriate data-governance KPIs. As the leader of cross-functional data-governance teams, CISOs also address a challenge that crops up when organizations enlist additional stakeholders, such as business managers, in data-governance efforts. Nearly two-thirds (63%) of the survey respondents overall say the responsibilities of stakeholders are not clearly defined, which leads to gaps in policy development and enforcement.

CISOs are making important contributions to their organizations by collaborating with IT, GRC, and business groups to blend relevant stakeholders into a cohesive team to ensure data security and compliance. But midsized and smaller companies may struggle to structure the security function. Capgemini's Chaya says, "This may leave a gap that makes companies more exposed to cybe rattacks. In the case of small and midsize businesses, statistics show that they are not only vulnerable to a breach, but that the consequences of such an event can be downright catastrophic."

5. Invest in new or enhanced technology to bolster security and monitor compliance with data-governance policies.

Organizations in each of the three levels of governance maturity have earmarked funds for technology over the past year—the top category for all organizations was new anti-malware programs, which offer the first line of defense against vulnerabilities introduced by end users. FIGURE 5

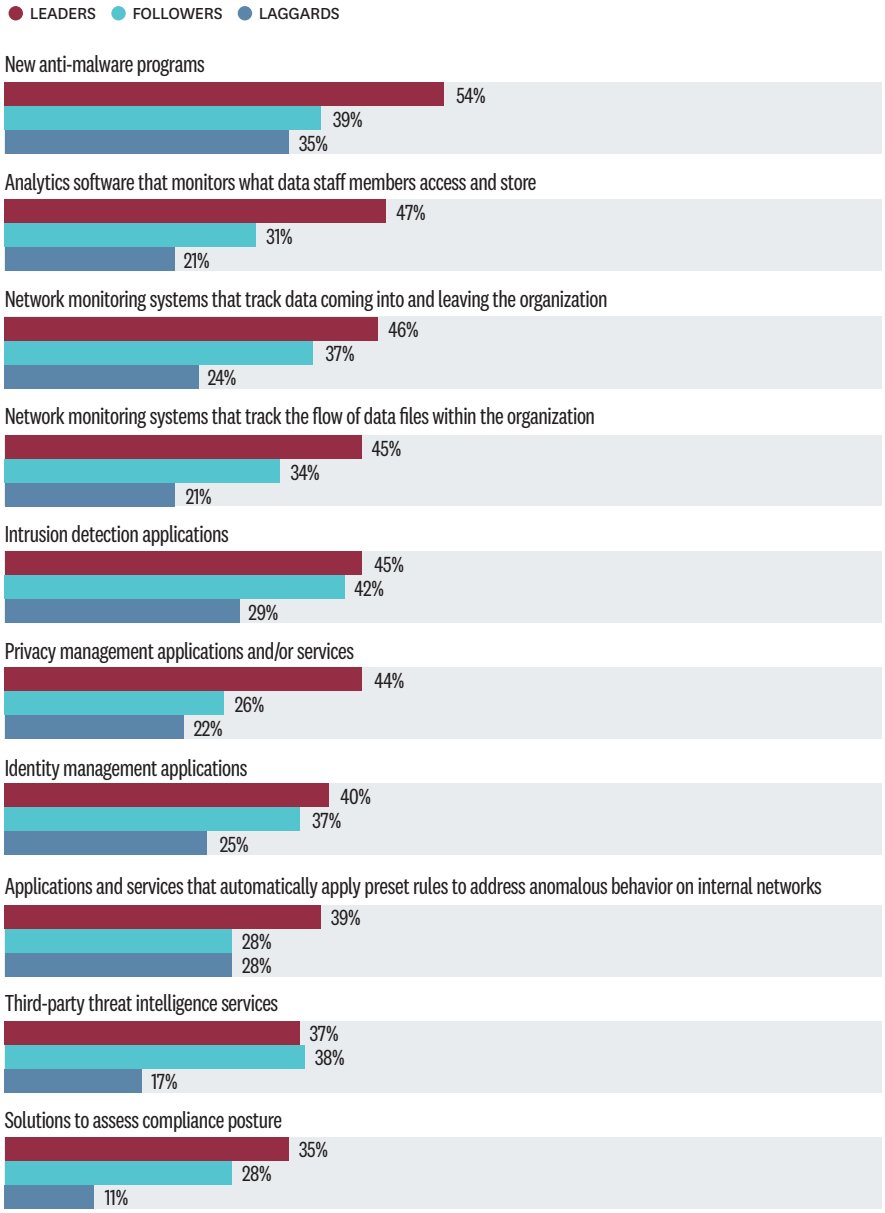
Beyond anti-malware software, leaders have prioritized spending much differently than their peers. Leaders are focusing more on tools for closely monitoring and analyzing data flows and the behavior of staff members.

FIGURE 5

LEADERS OPEN THEIR CHECKBOOKS FOR ANALYTICS AND MONITORING

Better insights lead to stronger policy enforcement.

Over the past year, what technology or cloud services has your organization acquired to better manage data security, privacy, risk, and compliance?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, OCTOBER 2019

“ORGANIZATIONS MUST CONSTANTLY EDUCATE THEIR EMPLOYEES ABOUT ALL THE REGULATORY REQUIREMENTS RELATED TO THEIR WORK.” DANIEL BONINI, ATOS

Three technology categories received nearly equal attention by leaders: analytics that monitor data accessed and stored by end users, monitoring systems that track data coming into and leaving the organization, and complementary tools for monitoring the internal flow of data. Together, this trio of applications and services directly addresses the biggest governance challenges that keep executives up at night: understanding the impact of rapidly increasing data volumes and the risks that arise when organizations share more data across departments and divisions.

"What data an organization has, where it's being stored, what information is confidential or trade secrets, and how it's being used are big challenges for large organizations," Exelon's Cavalcanto says. "New tools with machine-learning technology can assist in the classification of all this data, both structured and unstructured."

The technology is also important for finding specific data for e-discovery and other necessities. "We can search for a specific document type or phrase to find matches without needing humans for eyes-on reviews," says Starr.

By comparison, less-mature organizations have yet to significantly invest in governance-related analytics and monitors. For example, laggards have purchased these types of tools at about half the rate of leaders in the past year. That leaves those companies less able than leaders to quickly detect anomalies that may indicate breakdowns in security and compliance policies.

6. Commit more resources to workforce development, including training and skill development for executives and lower-level staff members.

Leaders appear to be well aware that even the most advanced security and compliance technology by itself won't strengthen data governance. "Many companies invest in expensive technology to keep them more secure, but they fail to also invest in expertise and training to optimize the new digital tools," Radonov says.

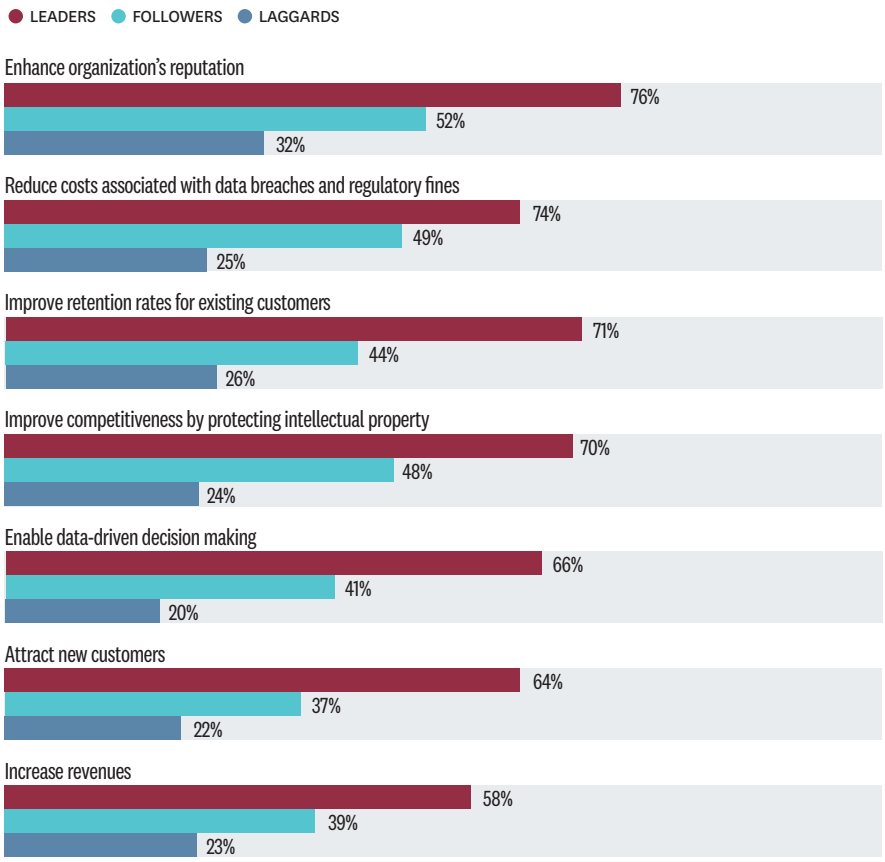
Everyone within the organization must understand how to capitalize on the tools and stay up to date on the latest security vulnerabilities and compliance trends. Leaders are outspending peers in training to heighten awareness of both business managers and employees about the importance of security and compliance. "Organizations must constantly educate their employees about all the regulatory requirements related to their work," says Daniel Bonini, IT systems architect in the Montevideo, Uruguay, office of ATOS, an IT services company. "Companies

FIGURE 6

THE BUSINESS BENEFITS OF GOOD GOVERNANCE

Leaders outperform peers in key business goals.

Rate your organization's success in achieving each of these business goals.



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, OCTOBER 2019

"Companies must demonstrate that they are **not only committed to protecting data**, but also that they have the systems in place to do that," says Jorge Osuna at Honeywell.

need a regulatory team in place to make sure people who are working on a project for a client in Europe, for example, must be aware of the General Data Protection Regulation."

Conclusion

By formulating a multipronged strategy that addresses technology modernization along with important policy, cultural, organizational, and workforce updates, leaders are outperforming peers and translating strong data governance into business success. For example, leaders far outperformed their peers in each of the business benefits that executives overall identified as being extremely important. FIGURE 6

Notably, data-governance efforts had the biggest impact on enhancing reputations, reducing costs, retaining customers, and boosting competitiveness—four critical areas that position companies for ongoing success in the months ahead.

"Companies must demonstrate that they are not only committed to protecting data, but also that they have the systems in place to do that," says Jorge Osuna, business director for Industrial Fire Protection for the Americas at Honeywell, an international manufacturer headquartered in Charlotte, N.C. "Organizations that successfully do that put themselves in a much stronger competitive position than others."

Endnotes

1 Picardo, Elvis, "10 of the World's Top Companies Are American," Investopedia, May 2019, https://www.investopedia.com/articles/active-trading/111115/why-all-worlds-top-10-companies-are-american.asp.

2 "2019 Verizon Data Breach Investigations Report," May 2019, https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/.

METHODOLOGY AND PARTICIPANT PROFILE

A total of 460 respondents drawn from the HBR audience of readers (magazine/ enewsletter readers, customers, HBR.org users) completed the survey.

SIZE OF ORGANIZATION

77%
10,000 OR MORE EMPLOYEES

22%
5,000–9,999 EMPLOYEES

SENIORITY

38%
MIDDLE MANAGEMENT

30%
SENIOR MANAGEMENT

16%
OTHER

15%
EXECUTIVE MANAGEMENT/ BOARD MEMBERS

INDUSTRY

9%
HEALTH CARE AND SOCIAL SERVICES

7%
IT CONSULTANCY/ SERVICES

7%
RETAIL FINANCE

6%
SOFTWARE

5%
CONSULTING

<5%
ALL OTHER INDUSTRIES

JOB FUNCTION

15%
OPERATIONS/PRODUCT MANAGEMENT

10%
HR/TRAINING

10%
IT

9%
CONSULTING

8%
SALES/BUSINESS DEVELOPMENT/CUSTOMER SERVICE

7%
GENERAL/EXECUTIVE MANAGEMENT

REGIONS

32%
NORTH AMERICA

31%
EUROPE

24%
ASIA

7%
MIDDLE EAST/AFRICA

7%
SOUTH/CENTRAL AMERICA

Figures may not add up to 100% due to rounding.

CONTACT US

hbranalyticservices@hbr.org