2018 CYBER GOVERNANCE SURVEY

Board Perspectives on Digital Transformation, Information Governance & Cybersecurity

BDO

Table of Contents

INTRODUCTION

Boards Are Striving to Keep Pace with Digital Transformation and Cybersecurity Imperatives

Technology is fundamentally changing the way we do business, introducing new opportunities and new threats. Succeeding in today's digital economy requires operating as a digital business. To be on the right side of disruption, digital transformation is essential to survival. The forces behind widespread digitization have put even the most conservative businesses on notice.

Digitization is a key way for organizations to increase profitability, enhance recruitment and employee engagement, encourage retention, and accelerate growth. True digital transformation, however, is a much bigger endeavor and fundamentally can serve as a catalyst for business transformation with proper board oversight. Along with digitalization comes the increasing need for information governance with a keen focus by directors on mitigating cyber risk and enhancing data privacy protections.

"BDO's 2018 Cyber Governance Survey reveals how public company board directors increasingly recognize the competitive advantages of embracing a digital transformation strategy and mitigating vulnerabilities related to cyber risk. Developing a strategic path for an organization's digital transformation and devoting company resources and board oversight to cybersecurity and data privacy are now necessities for businesses to survive and thrive during this time of intense change."

AMY ROJIK / BDO USA's National Assurance Partner, Communications and Governance

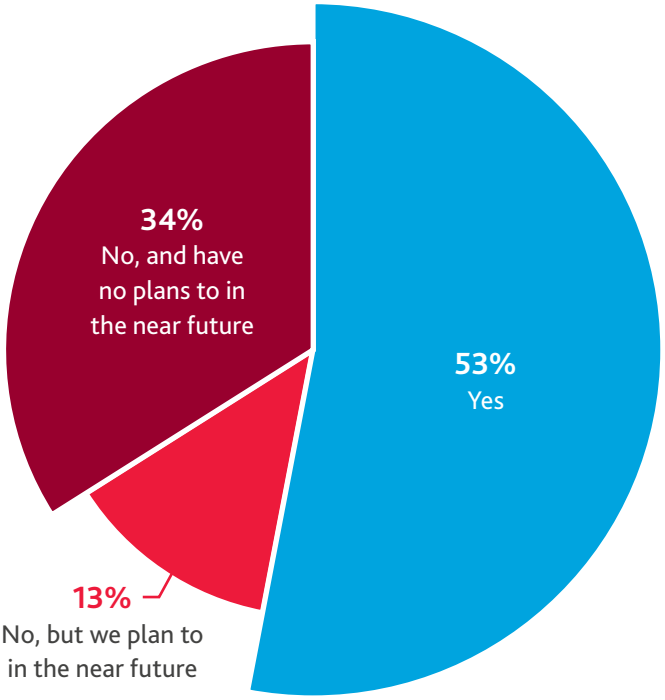
The 2018 BDO Cyber Governance Survey, conducted annually by the BDO Center for Corporate Governance and Financial Reporting, measures the opinion of public company directors on these issues, as well as other key governance concerns. This year's survey, conducted in July and August 2018, examines the opinions of 145 corporate directors of public company boards.

Digital Transformation and Disruption Driving New Value

In the world of business, the goals to "disrupt, innovate, and transform" have become daily pursuits of organizations, elevating the role of technology to the top of the board agenda.

Nearly two-thirds (66 percent) of public company board directors say their organization either has a digital transformation strategy in place or is planning to develop one, suggesting that digital transformation initiatives have transcended beyond the sole domain of IT to involve the entire organization. However, while they may be making ad-hoc investments in digital, many businesses have not yet set a digital transformation strategy into motion. About one-third of respondents (34 percent) say their organization has no digital transformation strategy currently and does not intend to develop one in the near future.

Does your organization have a digital transformation strategy in place?



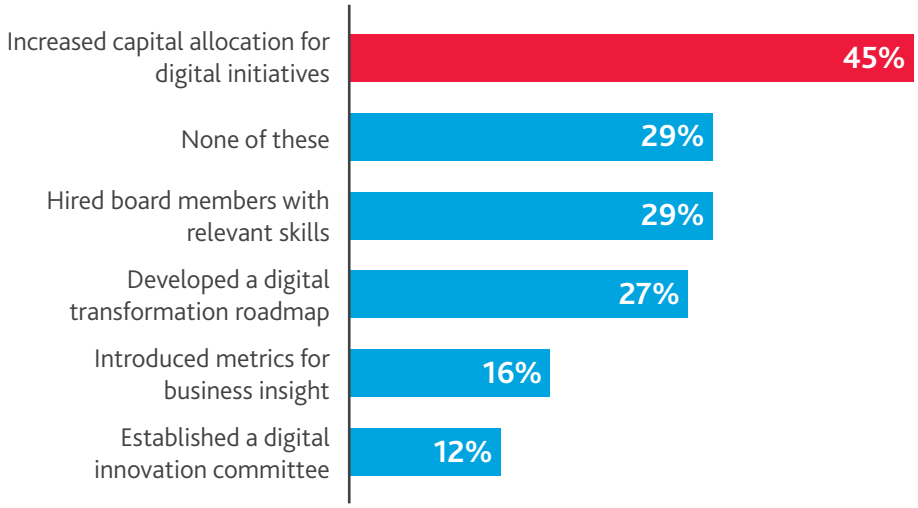
"Digital transformation is predicated on foresight: the ability to re-imagine business five years into the future—and then work backwards. Management naturally tends to focus on the short-term, so the board of directors plays a critical role in catalyzing strategic planning for the long-term view. And as the pace of change accelerates, the timeline of 'long-term' is shrinking. Organizations that live solely in the present are already operating in the past."

MALCOLM COHRON
BDO USA's National Digital Transformation Services Leader

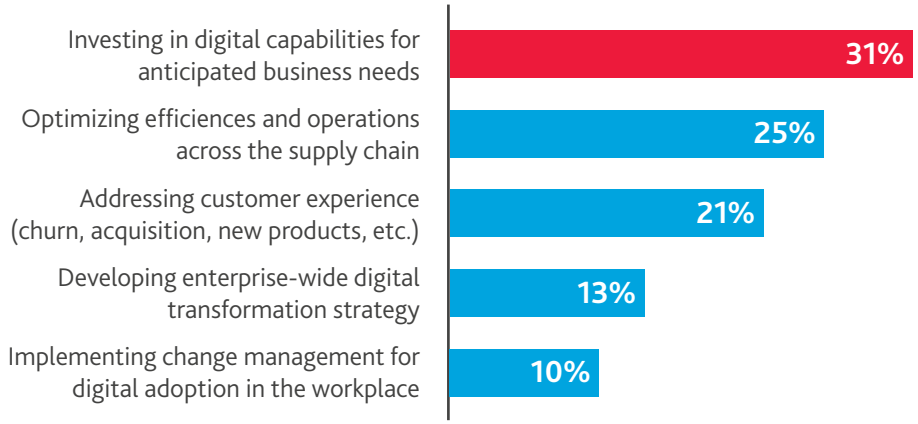
With or without a concrete strategy in place, boards are taking steps to address technology disruption. Nearly half (45 percent) have increased capital allocation toward digital initiatives; almost three-in-ten (29 percent) have hired board members with relevant oversight skills; and more than a quarter (27 percent) say the board has overseen the development of a digital transformation roadmap. Another 16 percent of board directors have introduced new metrics for enhanced business insight. Meanwhile, nearly one-third (29 percent) of respondents report they have not done any of these to address technology disruption, which may point to organizations overlooking significant opportunities and underestimating critical risks to their business.

The most important digital priority for directors serving on public company boards is investing in innovative digital capabilities for anticipated business needs, cited by 31 percent of survey respondents. This is followed by optimizing operational efficiencies (25 percent) and improving customer experience (21 percent). Only 10 percent of respondents are focused on implementing a change management program—a gap that may stymie business adoption and user enablement.

What steps has your board taken to address technology disruption?

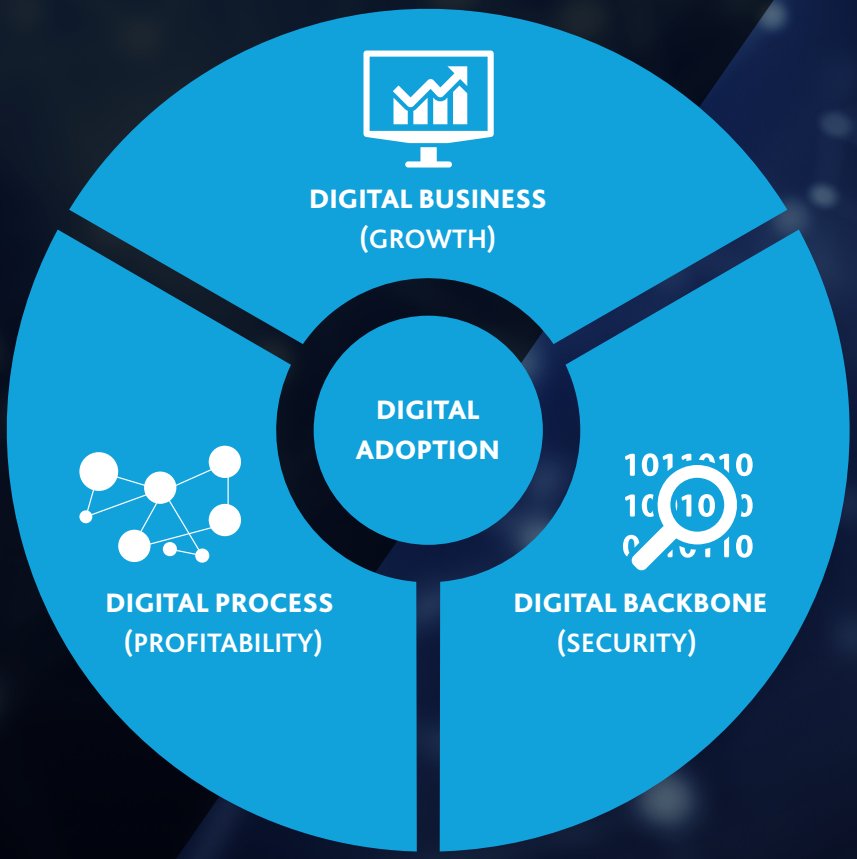


Which one of the following is the most important digital priority within your company?



BDO's Closer Look:

Digital transformation can be boiled down to three foundational areas of future value creation: Digital Business, Digital Process, and Digital Backbone. **Digital Business** is focused on creating new value, market differentiation, and revenue in the digital economy. **Digital Process** focuses on operational digital re-invention by optimizing end-to-end process performance and improving efficiency. **Digital Backbone** is the foundation on which all digital initiatives are built, centering on addressing or removing the IT complexities, risks, and barriers to innovation, to meet business and evolving market demands. These fundamental value drivers are interconnected—and will become even more intertwined as your organization becomes increasingly digital. BDO regularly produces resources to keep those charged with governance informed about the latest developments that may impact their business, including this article on how middle market organizations are re-imagining business and operations for the future digital economy: ***Digital Transformation: The Middle Market Goes "Back to the Future."***



Cybersecurity Continues to Be at the Forefront of Boards' Concerns

For all the doors digital innovation opens, it also invites a host of new threats in the form of increasingly sophisticated cyberattacks, such as zero-day exploits[1] against software flaws, botnets[2] capable of creating IoT "armies" to overwhelm servers, "cryptojacking,"[3] or the malicious mining of cryptocurrency by breaching systems and siphoning computing power. Hackers are not just stealing data; they are messing with democratic processes, releasing volumes of classified data, and threatening to bring organizations to a standstill. And as the cyber threat environment evolves, organizations will need to evolve their cybersecurity and data privacy programs, with significant oversight from the board.

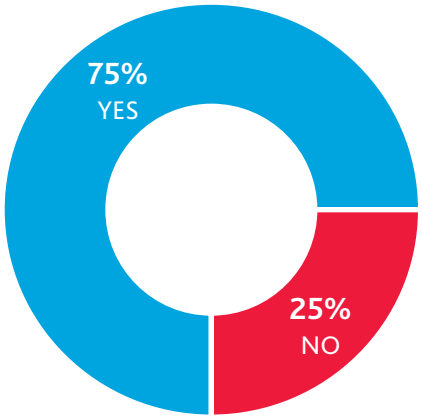
Common guidance given to the board is that cybersecurity investments should be concentrated on the organization's most valuable information assets. The problem with this approach is that what the organization deems most valuable may not be the prime target for a would-be-hacker. Instead of (or in addition to) focusing solely on protecting critical data assets or following the basic script of a generic cyber program, threat-based cybersecurity concentrates investments in **the most likely risks and attack vectors based on the organization's unique threat profile**. Corporate board members must ensure their organization develops a complete picture of its cybersecurity risks and adopts a threat-based cybersecurity strategy in alignment with an existing enterprise risk management framework.

While nearly eight-in-ten (79 percent) directors surveyed claim they have avoided a data breach or incident in the past two years, public company boards are becoming more involved in cyber oversight, with 72 percent of board members saying the board is more involved with cybersecurity now than they were 12 months ago.

With boards increasingly more involved in discussions around cybersecurity, especially due to regulatory changes and the potential for reputational damage, the cadence of reporting on cybersecurity is increasing, with nearly one-third (32 percent) of board members saying they are briefed at least quarterly on cybersecurity, while 54 percent are briefed at least annually. However, nine percent of boards indicate they are not being brief on cybersecurity at all. During the initial four years BDO conducted this survey, the percentage of directors reporting no cybersecurity briefings dropped consistently, and during the past year, that number has held steady. We strongly encourage all boards to reflect on potential cybersecurity risks and work with their management teams to foster communications in this area.

In terms of capital investments, three-quarters (75 percent) of directors say their organization has increased its investment in cybersecurity during the past 12 months. This is the fifth consecutive year that board members have reported increases in time and dollars devoted to cybersecurity.

Has your company increased its investment in cybersecurity during the past 12 months?



1 **Zero-day exploits**: Zero-day exploit refers to code that attackers use to take advantage of a zero-day vulnerability. They use the exploit code to slip through the hole in the software and plant a virus, Trojan horse, or other malware onto a computer or device. It's similar to a thief slipping through a broken or unlocked window to get into a house.

2 **Botnets**: Botnets are an army of IoT devices, "ro**bot**" and "**net**work."

3 **Cryptojacking**: The malicious mining of cryptocurrency by breaching systems and siphoning computing power.

Access to data is becoming increasingly boundaryless, as the scope of information sharing grows with an ever-expanding universe of vendors, contractors, partners, and customers. Striking the right balance between sharing and restricting information is becoming increasingly challenging. Every one of these digital relationships presents new potential attack vectors for bad actors. A majority of directors (73 percent) report their organizations require third-party vendors to meet certain cyber risk requirements, up 30 percentage points from when directors were last polled on this question in 2016. Nearly eight-in-ten (79 percent) companies have an incident response plan in place to respond to potential cyber risks.

"Clients, investors, regulators, and law enforcement officials expect organizations to be doing everything they can to protect sensitive information. In an environment where a data breach is an inevitability, a successful cybersecurity program is defined by the demonstrable effort made to minimize risk and increase the level of transparency and urgency in mitigating the fallout. The board should think of cybersecurity not only as a matter of compliance, but a matter of corporate ethics and trust."

GREGORY GARRETT
BDO USA's Head of U.S. and International Cybersecurity

BDO's Closer Look:

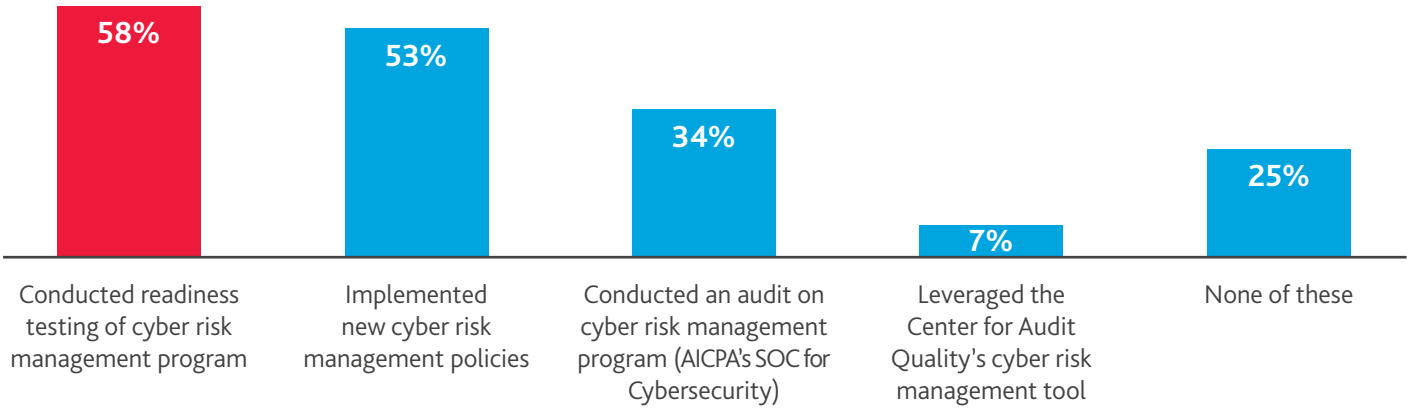
Data privacy regulations are driving more stringent governance requirements. At the center of these regulations is the ability for an organization to understand where its data resides, how it is managed, who can access it, and how it can be defensibly destroyed. Information governance is foundational to e-discovery directly impacting the cost, speed, and soundness of decision-making. Download BDO's fourth annual Inside E-Discovery & Beyond survey which examines the opinions and insights of more than 100 senior in-house counsel about changes in their approaches to e-discovery, information governance, compliance, and cybersecurity.

In BDO's Cyber Threat Insights - 2018 2nd Quarter Report, we report on a summary of trends, with a focus on the major events and campaigns that have made headlines in the healthcare industry and share our recommendations on how to mitigate vulnerabilities.

In February 2018, the SEC released **interpretive guidance** to assist public companies in preparing disclosures about cybersecurity risks and incidents. In response, more than half of board directors indicate their company has conducted readiness testing of cybersecurity risk management programs (58 percent) and implemented new cybersecurity risk management policies or procedures (53 percent). About a third of companies (34 percent) have conducted a formal audit of their cyber risk management program, but just seven percent have leveraged the **Center for Audit Quality's Cybersecurity Risk Management Oversight: A Tool for Board Members**.

Furthermore, a full quarter of organizations surveyed have taken no steps to address the SEC's guidance on cyber disclosure obligations. We urge management and board directors to familiarize themselves with such available guidance and tools, if they have not already, in considering and strengthening their cybersecurity risk management program and related cybersecurity disclosures.

What actions has your organization taken to address the SEC's guidance on cyber disclosure obligations and internal controls?



BDO's Closer Look:

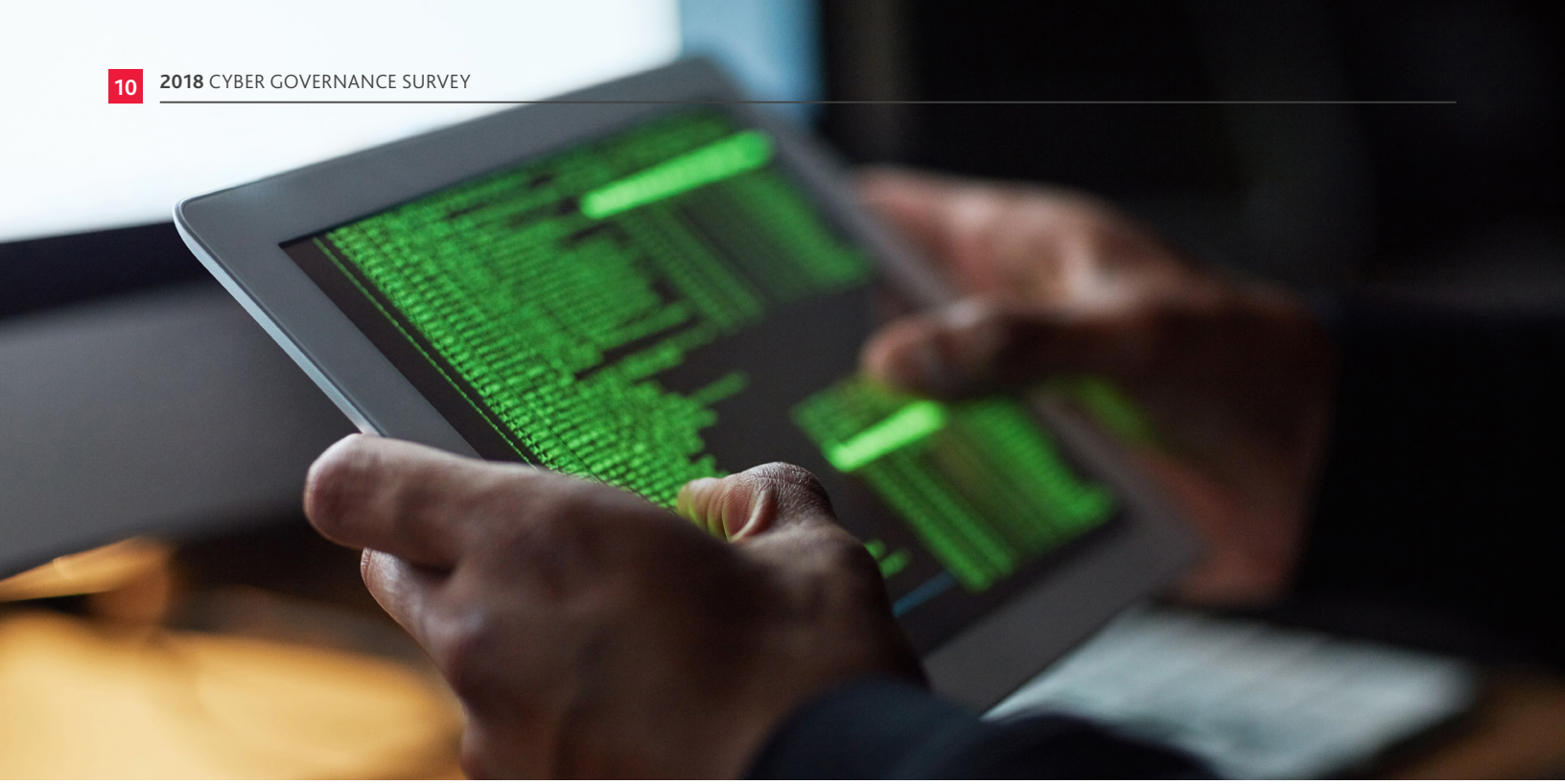
In BDO's publication, **Introducing SOC for Cybersecurity: Translating Cyber Risk for Every Stakeholder**, we highlight the AICPA's latest reporting framework for cyber risk management, first introduced in April 2017. Organizations can use the framework to design a comprehensive risk-based cybersecurity program, perform a cyber risk assessment and gap analysis, and/or undertake an examination-level attestation engagement.

In Spring 2018, the Center for Audit Quality (CAQ) released a new tool, **Cybersecurity Risk Management Oversight: A Tool for Board Members**, to assist board members in their oversight of data security and cybersecurity risks and disclosures by providing key questions board members can use in their discussions with management and auditors.

The tool further provides key resources from leaders in the area of cybersecurity. The goal of this tool is two-fold. First, it is intended to better educate board members and others charged with governance and provide discussion starters for them to properly evaluate their cyber risks. Second, it is meant to be a tool for auditors to help them assess how actively involved the board members and others charged with governance are in assessing these risks. BDO continues to provide financial reporting and governance resources, specifically related to cybersecurity, including our insights, events and webinars, website content, and CAQ materials that audit committees may find helpful.

"In the wake of this year's SEC guidance, we've seen an uptick in public company requests for independent cyber risk examinations. While the AICPA's SOC for Cyber Framework is relatively new and strictly voluntary, it addresses a critical gap in standardizing cyber risk reporting. Many of our public company clients anticipate increased regulatory scrutiny of their cyber risk and incident disclosures, and are using the SOC for Cyber reporting framework as a benchmark."

JEFF WARD
BDO USA's Third-Party Attestation National Managing Partner



A New Era of Data Privacy

In recent years, the explosion of data has created new, unprecedented business challenges, including increased risk and cost. Regulations are driving more stringent information governance requirements. Central to navigating these regulations is the ability for an organization to understand where its data resides, how it's managed, who can access it, and how it can be defensibly destroyed.

The **European Union's General Data Protection Regulation (GDPR)**, which went into effect on May 25, 2018, is the most significant overhaul to the EU's data privacy policies in over 20 years.

More than two-thirds (69 percent) of board directors said their company is not impacted by the GDPR. Chances are, many of them are wrong. More muted impact among corporate directors may reflect lack of awareness or misunderstanding that still underlies many aspects of this new regulation. Any U.S. company that deals with the personal data of EU citizens and residents could be subject to the GDPR's stringent requirements even if the company does not operate in any of the 28 EU member states.

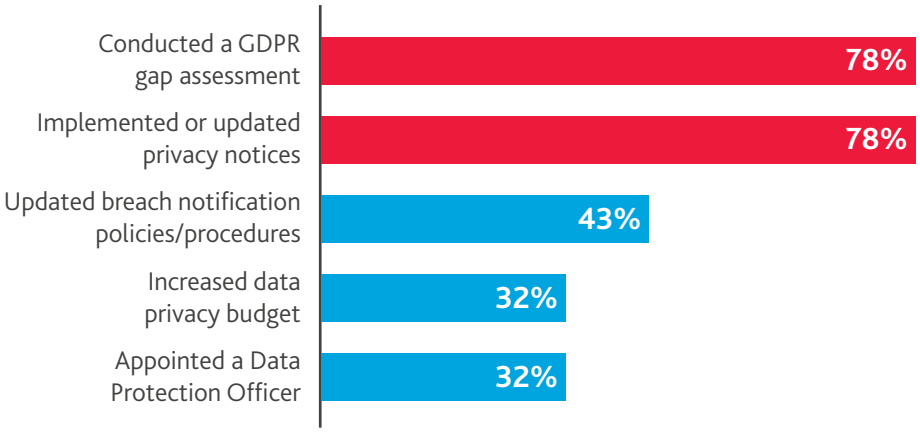
Clearly, there is a lot of confusion about the GDPR, not only because of its extraterritorial scope, but because of the ambiguity in the way it is written. There is a lot of room for interpretation—and a lot of potential downside for a bad interpretation.

Among respondents who say they are impacted, 78 percent report their organization has conducted a GDPR gap assessment; another 78 percent report that their organizations have implemented or updated privacy notices; and 43 percent have updated their breach notification policies. Just under a third (32 percent) report increasing data privacy budgets, while about one-third (32 percent) have appointed a Data Protection Officer, a requirement under the GDPR for organizations that engage in certain types of data processing activities.

The May 25th deadline to comply with the EU's GDPR may have come and gone, but the compliance journey is just beginning, as prudent and responsible data privacy governance goes beyond checking the box on implementation day. Data privacy governance is an ongoing process and a commitment to safeguarding personal data and other sensitive data that your organization collects, processes, transfers, or stores. The GDPR is designed with the evolving nature of data privacy in mind, and how it is monitored and enforced will change over time.

Data privacy regulation is also still evolving. The passage of the California Consumer Privacy Act, which goes into effect on January 1, 2020, is the first of what will likely be many new, more stringent rules governing data privacy at the state level. This privacy law contains a broader definition of personal data, establishes broad rights for California residents to direct deletion of data, establishes broad rights to access personal data without certain exceptions, and requires that organizations give consumers the right to know how their data is used and why it is being collected.

What steps has your organization taken to comply with the GDPR?



"GDPR was a shock to the system in the U.S. But beyond compliance, the regulation has served as a propeller for the U.S. to get privacy safeguards in line with global standards. Now, when boards consider how their organization can keep pace with mounting data-related challenges, their priority should be building a culture of privacy, with cybersecurity and regulatory compliance as critical components."

KAREN SCHULER
BDO USA's Data & Information Governance National Leader

The world of corporate directors at publicly traded companies is constantly in flux—never more so than in 2018, as boards face regulatory uncertainty, heightened cybersecurity threats, and disruptive changes in industry dynamics and business models. As overseers, the board must anticipate the rules that have yet to be written. The success of organizations ultimately hinges on having the agility and foresight to evolve and transform.

BDO's Closer Look:

The EU's General Data Protection Regulation, also known commonly as GDPR, applies to any organization that transfers data to, from, or within EU borders, impacting organizations in the U.S. and around the world. With the vast amount of data available to and within organizations, it is important to take the proper steps to protect and secure EU personal data to avoid the implications of non-compliance. BDO's Data & Information Governance professionals want to ensure your organization is taking in account the many ways to protect EU personal data. Download BDO's GDPR Checklist and refer to our September 2018 webinar for an in-depth look at how to mitigate risk for your organization.

BDO Board Survey

These are just a few of the findings of the 2018 BDO Cyber Governance Survey, conducted by the Corporate Governance Practice of BDO USA in July and August 2018. A companion report, the **2018 BDO Board Survey** on Corporate Governance and Financial Reporting, explores the board's role related to corporate governance, financial reporting, tax, sustainability, and diversity. These two annual surveys examine the opinions of corporate directors of public company boards regarding timely and relevant corporate governance and financial reporting issues.

BDO USA's Corporate Governance Practice is a valued business advisor to corporate boards. The firm works with a wide variety of clients, ranging from entrepreneurial businesses to multinational Fortune 500 corporations, on myriad accounting, tax, risk management, and forensic investigation issues.

About The BDO Center for Corporate Governance and Financial Reporting

BDO's Center for Corporate Governance and Financial Reporting provides numerous resources, webinars and live events designed to help board of directors, C-Suite executives, and financial reporting management stay on top of emerging issues and hot topics affecting both public and private companies. Visit the Center, and subscribe today to ensure you are receiving top of mind thought leadership.

About BDO USA

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 650 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 73,800 people working out of 1,500 offices across 162 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.


APARTMENT 201
LIVING ROOM 201
TERRACE 02.201

CONTACT

AMY ROJIK
617-239-7005
arojik@bdo.com

GREGORY GARRETT
703-893-0600
ggarrett@bdo.com

KAREN SCHULER
703-336-1533
kschuler@bdo.com

MALCOLM COHRON
404-979-7109
ccohron@bdo.com

STEPHANIE GIAMMARCO
212-885-7439
sgiammarco@bdo.com

JEFF WARD
314-889-1220
jward@bdo.com

CONTACT US:

First Name

Last Name

Title

Company Name

Email

Phone

Subject

Message

SUBMIT