

GDPR Preparedness: An Indicator of Cyber Risk Management



GDPR Preparedness: An Indicator of Cyber Risk Management

CONTENTS

- 1 An Overview of Survey Findings
- 2 Some Organizations Are More Prepared for GDPR than Others
- 3 A European Rule with Global Consequences
- 4 Encouraging Stronger Cyber Risk Management Practices
- 8 GDPR Compliance Does Not Mean Cyber Risk Management Excellence
- 10 An Opportunity to Strengthen Cyber Risk Management
- 12 Methodology/Survey Demographics

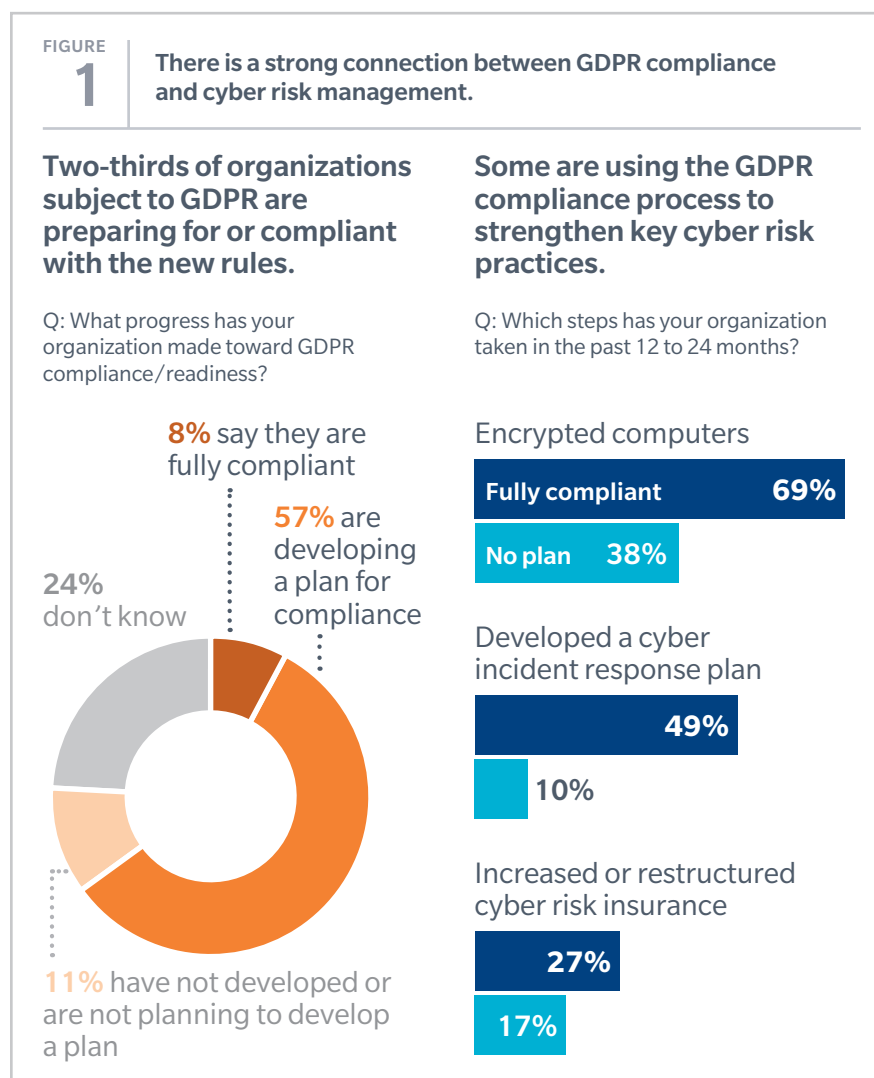
An Overview of Survey Findings

Cyber risk management is both a cause and consequence of GDPR compliance.

The EU General Data Protection Regulation (GDPR) is the most significant overhaul of privacy law in a generation, introducing sweeping changes to Europe's data protection and privacy rules. It establishes strict global requirements governing how organizations that do business in the EU must manage and protect personal data, while strengthening the privacy rights of individuals in the EU wherever they reside. It also serves as a force for growth and innovation, encouraging organizations that do business in the EU to adopt more rigorous data protection protocols and modernize their business practices for a data-driven world. As a result, one of the most noticeable knock-on effects of complying with the GDPR is not mentioned in the text of the new rules: an improvement in the ability to manage and respond to ever-evolving cyber risks.

This strong correlation was underscored by a recent survey of over 1,300 executives representing a range of industries and organizations worldwide. Respondents who said their organization was developing a plan or fully compliant with the new rules were more than three times as likely to adopt some cybersecurity measures — and more than four times as likely to adopt some cyber resiliency measures — as were those who had not started planning. Respondents with a higher level of GDPR readiness were also more than 1.5 times as likely to purchase or strengthen their cyber risk insurance, which can potentially help offset the financial impact of a cyber event (see Figure 1).

Cyber risk management is both a cause and consequence of GDPR compliance. Organizations with strong cybersecurity measures have a jumpstart on compliance since the GDPR strongly encourages certain practices, such as encryption. Likewise, practices such as cyber incident planning and cyber insurance are not explicitly required, but enable firms to quickly marshal the resources to meet the GDPR's 72-hour data



breach notification guidance. The GDPR is also spurring cyber readiness: A key provision states that the adoption of “appropriate technical and organizational measures” is foundational to ensuring a “level of security appropriate to the risk.”

So, how much progress have organizations made toward GDPR compliance? Among respondents at organizations subject to the GDPR, just 8% said they were fully compliant, 57% said their organization is developing a compliance plan, and 11% had yet to

start. Given the effort needed to comply, this suggests many organizations will face challenges to meet all requirements when the GDPR takes effect in May 2018.

Nevertheless, the GDPR is having a positive effect. Preparation alone is focusing executive attention on broader data protection and privacy issues and prompting related investments. Among respondents with a higher level of GDPR readiness, 78% reported an increase in cyber risk management spending, including on cyber insurance.



Some Organizations Are More Prepared for GDPR than Others

With only months remaining until GDPR enforcement begins, just 8% of survey respondents believed their organization was fully compliant. Nearly one-third (32%) said their organization had not yet developed a plan, or did not know if it had. What might explain this?

One possible answer is size. Broadly speaking, respondents at larger organizations were more likely to report higher levels of GDPR compliance (see Figure 2). These organizations have more resources to invest in compliance as well as the management infrastructure to support compliance measures. Many of these organizations also have significant operations in the US, where data protection practices and breach notification policies have been aggressively articulated and enforced for years. As a result, they have a head start since they are more likely to have a robust compliance infrastructure already in place – and can more easily adapt them to meet the demands of the GDPR.

Factors beyond size also contribute. Some organizations may be overwhelmed by the task at hand. The GDPR requires organizations to not just check-the-box, but to rethink data management practices. This

more holistic approach requires significant management attention and investment regarding the business implications of the new regulation, what activities may trigger it, and how it interacts with cyber insurance and other compliance requirements.

What's more, many organizations may not fully appreciate that the GDPR applies to them, especially in industries that do not traditionally see themselves as data collectors. For example, manufacturing-oriented businesses, such as in the automotive and chemical industries, report being less prepared than organizations in other sectors. The reality, however, is that almost every business today is data-driven. Even organizations that do not directly collect, hold, or analyze customer data could see their business severely disrupted through a cyber-attack on a key vendor or supplier.

Finally, many specifics of the GDPR need to be sorted out by national regulators. As a result, some respondents at organizations that are very far along in the GDPR compliance process may be reluctant to deem themselves fully compliant. Likewise, respondents at organizations that have yet to start planning may be waiting for additional clarity.

FIGURE
2

Larger organizations tend to be more prepared for GDPR.

Q: What progress has your organization made toward GDPR compliance?

KEY

- Organizations with more than \$5 billion in revenue (US dollars)
- Organizations with less than \$50 million in revenue

Fully compliant

29%

18%

Developing a plan

13%

27%

No plan

5%

55%

A European Rule with Global Consequences

Today, just about every organization collects, analyzes, or deploys data for all kinds of purposes. The potential opportunities are limitless, but so are the potential risks of misusing that information or having it fall into the wrong hands. The growing sophistication of threat actors makes the need for securing user data even more acute. It is not a matter of *if* an organization will experience a cyber incident but *when*. Indeed, our survey found that 23% of organizations that believe they are subject to GDPR had been victims of a successful cyber-attack in the last year (see Figure 3).

As part of its approach to protecting and strengthening individual privacy rights for EU citizens, the GDPR seeks to ensure that organizations holding or using personal data take the necessary precautions. It aims to modernize existing data protection rules, encourage the adoption of more rigorous data management practices, and impose

more stringent breach notification protocols should an organization experience a data compromise. But its impact will be much broader. Why?

First, the GDPR has relatively few explicit requirements, although national regulators may eventually provide additional guidance. To date, only a handful of provisions outline specific actions, such as requiring notification of regulators within 72 hours of a personal data breach or strongly encouraging encryption. This principles-based approach puts the onus on organizations to determine “appropriate” controls based on their risks. With no ready-made checklist, it effectively requires organizations to look comprehensively at business operations and revisit how they protect personal data. While complying with the GDPR is not the same as managing cyber risk, the two are inextricably linked.

Second, GDPR’s scope is extra-territorial, applying to all organizations that collect or process data on EU residents, no matter where they are headquartered or operate. Any company that offers products or services in the EU may be affected.

Third, organizations that run afoul of the rules will be held to tough sanctions. Policymakers hope to encourage compliance with fines that have no historic precedent, reaching to as much as 4% of an organization’s global turnover or EUR20 million, whichever is larger. According to Oliver Wyman research, fines and penalties in the first year¹ could exceed US\$6 billion in the UK alone for organizations in the Financial Times Stock Exchange (FTSE) 100.

The GDPR, in other words, is turning organizational attention to data protection and cyber risk management in far-reaching ways. As the rapporteur on EU data protection, Jan Philipp Albrecht, said, it will change “not only the European data protection laws, but nothing less than the world as we know it.”

EUROPEAN UNION GENERAL DATA PROTECTION REGULATION: WHAT IS IT?

The GDPR came into effect on 24 May 2016, with a two-year implementation period. It affects all organizations gathering data on EU citizens — not just European companies — and raises fines to the greater of EUR20 million or 4% of global turnover. Other key points:

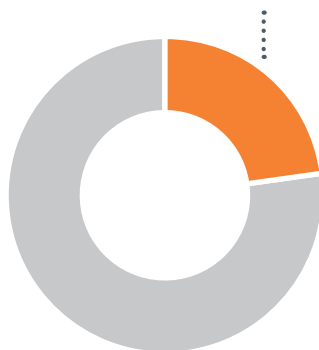
- Explicit consent required for collection of specific categories of sensitive personal information.
- New restrictions on the profiling of data subjects.
- Organizations must maintain an inventory of where personal data exists and be able to demonstrate compliance with the regulation.
- Requires the appointment of a data protection officer when core activities include the large-scale processing of special categories of personal data and/or criminal conviction information, or the systemic monitoring of data subjects.
- Data privacy impact assessments required for certain new or changed products and services.
- Organizations required to notify both the regulator and data subjects “without undue delay” and no later than 72 hours of a personal data breach.
- New and enhanced rights for data subjects, including the right to request access, correction, and deletion of personal data.
- Single lead regulator or enforcement action.

FIGURE
3

It is no longer if an organization will be attacked but when.

Q: Has your organization been a victim of a successful cyber-attack in the past 12 months?

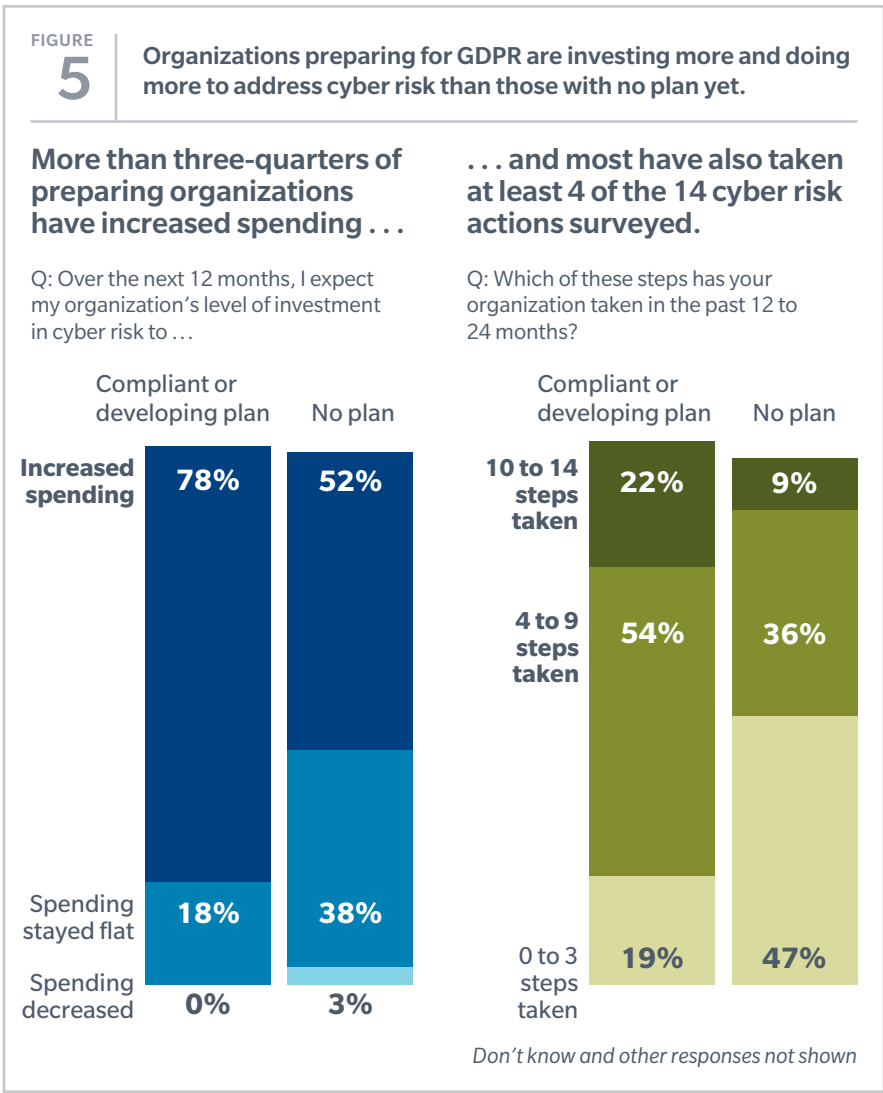
23% of those subject to GDPR were victims of a successful cyber-attack



Encouraging Stronger Cyber Risk Management Practices

The effort to comply with GDPR is already helping catapult cyber risk management to the top of the corporate agenda. Among respondents who said their organization was subject to the GDPR, 65% viewed cyber risk as a top-five risk management priority. Just 4% of respondents reported it as a low or non-existent priority (see Figure 4).

But awareness is one thing; action another. Our data suggests a correlation between being prepared for the new rules and strong cyber risk management practices. Not only were organizations preparing for or compliant with GDPR over 1.5 times more likely to report an increase in cyber risk management spending than those at organizations that had not yet started,



but they have adopted more cyber risk management practices overall (see Figure 5).

We asked our survey respondents to select among a variety of cyber risk management activities — ranging from the use of cyber risk assessment tools to the deployment of cybersecurity and cyber insurance strategies to the development of cyber resiliency protocols. Roughly 75% of respondents in

the “preparing” and “compliant” groups had engaged in four or more of these activities over the last 12 to 24 months. That compared to only 45% of respondents at firms that had not yet begun preparing for GDPR.

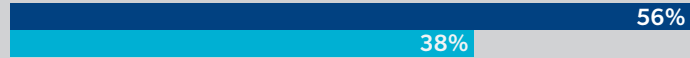
So, what cyber risk management practices are these organizations investing in (see Figure 6)?

FIGURE
6

Organizations that are compliant or developing a GDPR plan are more likely to adopt cyber risk management measures.

EXPLICITLY ENCOURAGED BY GDPR

Encrypted organizational desktop and laptop computers

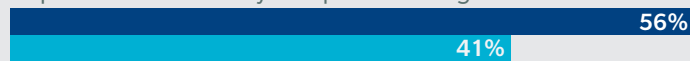


STRONGLY IMPLIED BY GDPR

Conducted penetration testing



Improved vulnerability and patch management



Identified external legal, public relations, and/or cybersecurity experts to provide support during a cyber incident



OTHER CYBER RISK MANAGEMENT ACTIONS

Conducted a cybersecurity gap assessment



Implemented/enhanced phishing awareness training for employees



Required multi-factor authentication for remote access to network



Made tangible improvements to cyber event detection



Developed a cyber incident response plan



Implemented a data loss prevention solution



Modeled potential cyber loss scenarios



Increased or restructured cyber risk management insurance coverage



Q: Which of these steps has your organization taken in the past 12 to 24 months?

KEY

■ Actions taken by organizations that say they are compliant or developing a GDPR plan

■ Actions by organizations with no plan

The adoption of cyber risk management measures makes GDPR compliance easier, while the process of achieving compliance has spurred organizations to adopt and improve cybersecurity, cyber risk mitigation, and cyber resiliency practices.

Of the information security activities we asked about, only one — encrypting organizational computers — is explicitly encouraged by GDPR. It showed very high levels of adoption among organizations preparing for or fully compliant with GDPR, with 56% of respondents at these organizations reporting that their computer systems were encrypted in the last two years. By contrast, only 38% of respondents whose organization had not yet started the GDPR compliance process reported encrypting their computers.

One explanation lies with the widespread adoption of cloud computing in recent years. As more organizations move critical data onto the cloud, they have been actively identifying and categorizing their data as part of the cloud implementation process, giving them a head start on requirements also outlined by the GDPR. What's more, many of the security controls required by the GDPR are similar to the controls expected by other data protection standards, such as the ISO 27018 cloud privacy standard. In fact, our survey found that of "compliant" or "preparing" organizations that encrypted their data, more than 85% reported using a cloud service (see Figure 7).

Besides encryption, several other cyber risk management measures showed high adoption rates. These include penetration testing, improved vulnerability and patch management, and the identification of external crisis management services (necessary for a timely mitigation and breach-notification response). While none are explicitly required by GDPR, its provisions strongly imply their need.

Not surprisingly, more than half of respondents at organizations preparing for or compliant with GDPR said they engaged in each of these activities within the last two years. That compares to about one-quarter of respondents whose organizations had not yet started planning for GDPR compliance.

In general, we found that the cyber risk management activities with the highest participation levels were cybersecurity measures focused on defense. For example, 67% of "preparing" and "compliant" respondents said that their organization had conducted a cybersecurity gap analysis, 56% reported their organization conducted penetration testing, and 66% reported their organization implemented or enhanced phishing awareness training for employees.

Given that cyber risk management has historically been the IT department's province (consider that 73% of respondents said that IT was the primary owner), most companies tend to focus on technical security measures designed to stave off a cyber incident rather than activities that help organizations respond when the inevitable happens. However, many of the organizations with the most sophisticated risk management programs view this exposure through an economic lens. They further maximize protection with a holistic approach that combines cyber insurance and cyber resiliency planning with traditional privacy risk mitigation and information security measures.

Organizations making the most progress on GDPR were more likely to share that

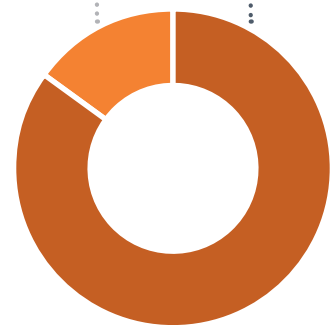
FIGURE
7

Using the cloud can be an effective way to encrypt data.

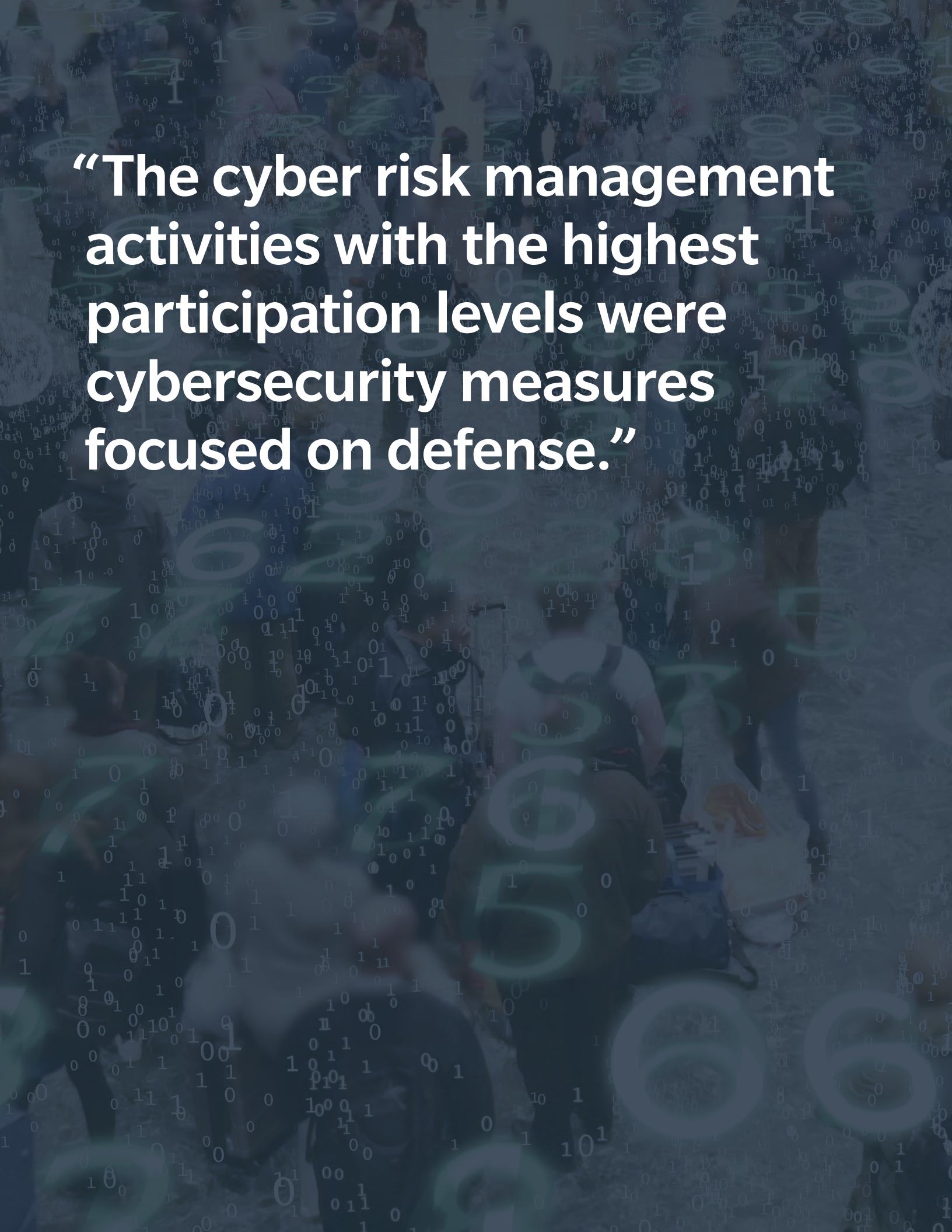
Q: Has your organization encrypted its computers in the past 12 to 24 months, and (if yes) does your organization use cloud services?

85% of organizations preparing for or compliant with GDPR that encrypted their data also use cloud services

15% do not use



philosophy. For example, GDPR "preparing" and "compliant" respondents were about twice as likely to purchase cyber insurance than those that had not yet started planning. Likewise, self-identified prepared and compliant respondents were 1.4 times more likely to benchmark their cyber risks against similar organizations and 3.9 times more likely to develop a cyber incident response plan.

A group of people are seated around a table in a meeting room, engaged in discussion. The image is overlaid with a semi-transparent grid of binary code (0s and 1s) in a light blue/green color. The text is centered in the upper half of the image.

“The cyber risk management activities with the highest participation levels were cybersecurity measures focused on defense.”

GDPR Compliance Does Not Mean Cyber Risk Management Excellence

Although the objectives may overlap, compliance with GDPR is not the same as excellence in cyber risk management. Even surveyed organizations with a higher degree of readiness — and that have adopted a number of best practices — may not be fully prepared.

Consider the use of cyber risk assessment tools. Only 53% of respondents who reported that their organization was preparing for or fully compliant with GDPR had estimated the financial impact of a cyber loss. Quantifying exposure provides a greater degree of precision, and enables more effective risk

management decision-making (see Figure 8). But just 24% of these respondents said their firms routinely express cyber risk exposure in quantifiable terms. Most rely on qualitative indicators — the green, yellow, red of a traffic light — to communicate the level of concern. As more cyber risk data becomes available in an increasingly standardized way, more organizations may find it less challenging to quantify the exposure.

Adoption of critical cyber risk management measures is similarly uneven. For example, 56% of “preparing” and “compliant” respondents said they encrypted their

computers. That means that 44% of those respondents either did not know if their systems were encrypted or had not yet done so. Meanwhile, respondents reported even lower levels of adoption for more expensive and complicated activities, such as reducing external system connectivity. Tellingly, none of the survey choices was close to 100% adoption.

Cyber insurance is another area with room for improvement. Only 65% of respondents “preparing” or “compliant” said their firm was covered by a cyber insurance policy, or that it intended to be within 12 months. About 12% of these respondents said their organization did not have or plan to purchase cyber insurance.

Adoption is even more uneven when viewed geographically. For example, cyber insurance adoption in the US is relatively high, largely due to regulatory requirements to report cyber breaches. In the rest of the world, take-up has been slower.

We believe the GDPR compliance process could accelerate broader adoption. That’s because one of the regulation’s main provisions gives organizations just 72 hours, with few exceptions, to notify both regulators and affected data subjects once they learn of a breach of personal data involving EU citizens. Businesses appear to be taking this requirement seriously, with our survey showing that 98% of “compliant” respondents said they had a data breach notification plan in place.

Putting a breach notification plan into action is expensive and logistically complex. Cyber risk insurance can help offset these costs, and give organizations that experience a data breach immediate access to some of

FIGURE
8

Only half of organizations preparing for GDPR estimate their financial exposure at all, and even fewer use robust means.

Q: Has your organization estimated the worst potential financial loss from a cyber incident?



Q: How does your organization measure its cyber risk exposure? (More than one choice allowed, not all choices shown)

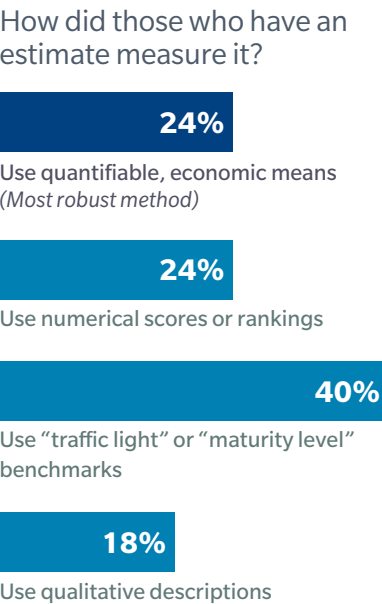


FIGURE
9

Organizations may still be vulnerable to third-party threats.

While 67% of organizations that are GDPR compliant or developing a plan say they assess third-party risks, there are gaps in how they do so.

Q: Which steps does your organization take to assess and manage the cyber risk posed by its suppliers, vendors, and other third parties?

17%

Analyze their financial strength to ensure their ability to compensate

20%

Require contractual language that specifies limits of liability for cyber losses

20%

Implement some form of continuous monitoring of vendors' cybersecurity posture

24%

Assess their cybersecurity posture and/or require independent attestation

34%

Take inventory of vendor/supplier relationships and data access privileges

the leading crisis management, legal, public relations, and cyber forensics firms. So, while not explicitly required by the law, cyber insurance is often a de facto solution.

Finally, even when organizations adopt all the measures to protect their boundaries from cyber risks, they may still be vulnerable to threats from third parties. Among

respondents who reported a higher degree of readiness, about 67% said they assess cyber risk posed by outside vendors. But the devil is in the tactical details: Only 34% of these respondents said their organization takes inventory of their vendor relationships and data management privileges. And only 20% said their organization reviews or continuously monitors their suppliers' cybersecurity posture (see Figure 9).



An Opportunity to Strengthen Cyber Risk Management

Organizations can leverage GDPR compliance to strengthen overall cyber risk management.

Complying with the GDPR by May 2018 is a business-wide challenge that will take time, tools, processes, and expertise. It may also require significant changes in an organization's privacy and data management practices. With under a year to go, more than two-thirds of our survey respondents said their organizations were still preparing for the new rules — or had yet to start.

But focusing on the scramble to comply with GDPR, while important, misses the broader impact that compliance efforts are having. In many organizations, GDPR has become a flashpoint, focusing senior leadership attention not just on specific sets of data or privacy protections, but on a broader, more strategic view of cyber risk management. After all, cybersecurity readiness is foundational to establishing that an organization has, as the GDPR puts it, “appropriate technical and organizational measures” in place. But as our survey data suggests, the most prepared organizations

use the explicit cybersecurity requirements of the new rules as a starting point — and adopt a broader set of cyber risk management best practices.

There is still much work to be done, and room for improvement. But what sets apart the organizations that have made the most progress?

First, they understand that cyber risk management is a shared responsibility that extends from the IT department to the executive suite. Regardless of size, many of these organizations have set up internal cross-functional task forces or steering committees led by senior executives — sometimes including or reporting to the CEO. These organizations are using the GDPR compliance process to look comprehensively at how they collect, retain, use, and manage data across the enterprise. They are exploring new tools, such as the use of cloud services; champion privacy rights; and have made

significant investments to ensure that any information they possess is secure. More broadly, they are reexamining their privacy and data protection practices to make sure that their people, processes, and technology are properly aligned.

Second, they treat cyber events as inevitable. Instead of focusing only on preventing cyber-attacks, they respond to incidents more quickly and reduce the potential damages. They view GDPR's data breach notification requirement as an opportunity to develop stronger incident management protocols — whether that means purchasing cyber insurance coverage with access to crisis management experts or encrypting their computer systems so that stolen data is rendered useless.

Finally, they take a quantitative and holistic approach. Because the GDPR compliance process requires organizations to implement measures that are appropriate to the potential threats they face, forward-looking organizations rigorously analyze their cyber risk exposures — both internal and external — and put a dollar amount on potential losses. As a result, they are not only investing in appropriate cybersecurity defenses, but they are strengthening cyber incident response plans as well as other risk mitigation and resiliency measures.

In other words, these organizations recognize the GDPR compliance process as a game-changing opportunity. In preparing for the new rules, they are strengthening their overall cyber risk management posture and turning what is often viewed as a constraint into a competitive advantage.



“In many organizations, GDPR has become a flashpoint, focusing senior leadership attention on a broader, more strategic view of cyber risk management.”

METHODOLOGY

This report is based on findings from the Marsh/Microsoft Global Cyber Risk Perception Survey administered between July 2017 and August 2017.

Overall, 1,312 senior executives participated in the global survey, representing a range of key functions, including information technology, risk management, finance, legal/compliance, senior management, and boards of directors.

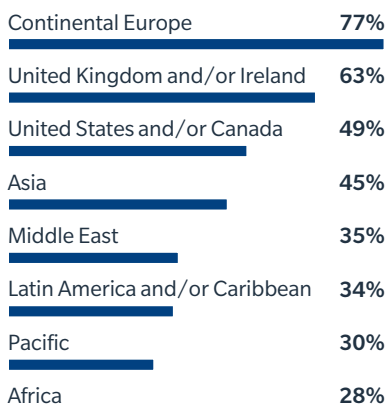
Of the survey participants, 41% came from organizations identified as being subject to GDPR rules. This was based on a series of questions that examined the activities in which their organization engaged as well as whether they offer goods and services to citizens of EU member states.

Respondents at organizations that are subject to the GDPR were split relatively evenly among eight major geographic regions and represented more than 25 industries. Of the 537 respondents at organizations subject to GDPR, 15% were IT professionals, 26% were in risk management, 7% were in legal and compliance, and 29% held other roles. Participants included 307 C-suite executives.

SURVEY DEMOGRAPHICS

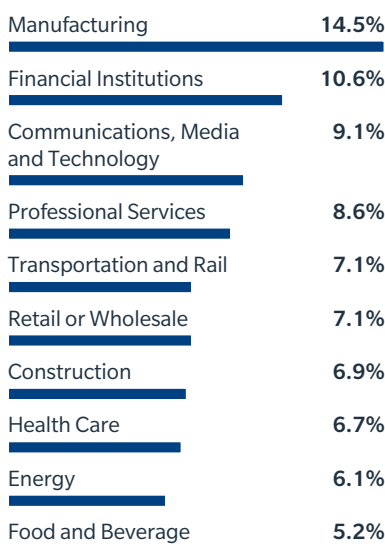
Business Geography

Where the organizations of the 537 respondents subject to GDPR offer goods or services:

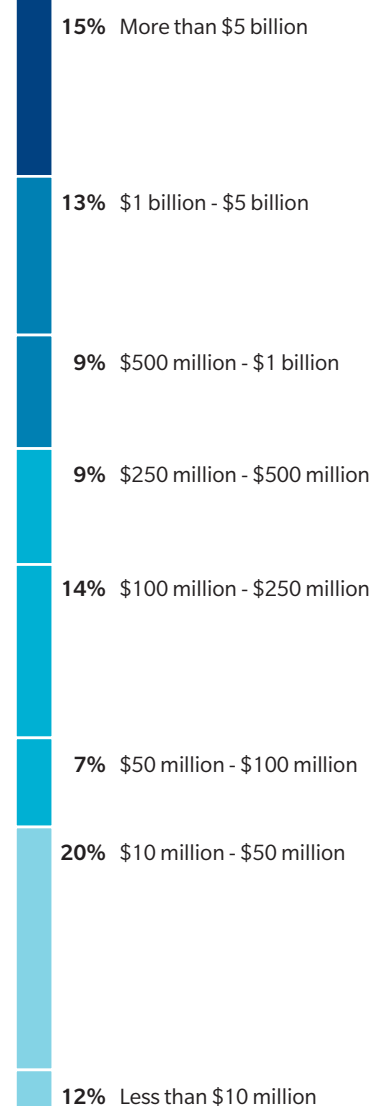


Industries

Largest industries represented among respondents subject to GDPR:



Revenue in US dollars



ENDNOTES

¹<http://www.oliverwyman.com/media-center/2017/may/ftse-100-companies-could-face-up-to-p5-billion-a-year-in-fines-w.html>



ABOUT MARSH

Marsh is a global leader in insurance broking and risk management. Marsh helps clients succeed by defining, designing, and delivering innovative industry-specific solutions that help them effectively manage risk. Marsh's approximately 30,000 colleagues work together to serve clients in more than 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and people. With annual revenue of US\$13 billion and approximately 60,000 colleagues worldwide, Marsh & McLennan Companies is also the parent company of Guy Carpenter, a leader in providing risk and reinsurance intermediary services; Mercer, a leader in talent, health, retirement, and investment consulting; and Oliver Wyman, a leader in management consulting. Follow Marsh on Twitter, @MarshGlobal; LinkedIn; Facebook; and YouTube.

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.

Copyright © 2017 Marsh LLC and the Risk and Insurance Management Society, Inc. All rights reserved. MA17-XXXXX USDG 21161