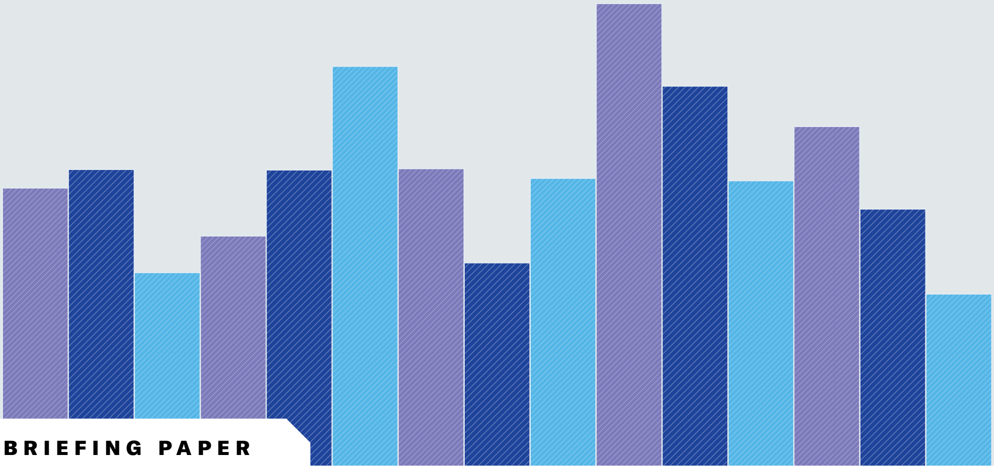
Harvard
Business
Review
ANALYTIC SERVICES



BRIEFING PAPER

Cyber Resilience in a New Era of Rigorous Compliance Mandates

Sponsored by

Commvault®

SPONSOR PERSPECTIVE

With the accelerating pressure of IT complexity, regulatory scrutiny, and ransomware attacks, investment in and executive support of an active enterprise compliance program is the leading indicator of readiness and cyber resilience. Companies must be proactive in their readiness, recovery, and resilience programs to achieve continuous business. Why?

Because the time to prepare for an emergency is before you're in one. Being cyber resilient means having three distinct teams ready to go. These three teams work simultaneously but separately:

1. Breach Response and Recovery Team
2. Regulatory and Legal Response Team
3. Business Readiness Team

Resilience is achieved through cross-functional collaboration, testing, and dynamic processes. Without a robust readiness program, a business is forever in catch-up mode, playing whack-a-mole in a breach, struggling to remove bad actors from systems, while trying to figure out what and when to communicate to customers and the market and how to abide by requirements with regulators. It is a perfect storm.

This comprehensive paper prepared by Harvard Business Review Analytic Services for Commvault details the cure to the chaos. This research underscores the necessity for continuous compliance to maintain economic viability and operational resilience, and explores the challenges of establishing a robust cyber resilience program and the importance of adhering to global regulatory requirements to protect data.

Featuring commentary and insights from industry leaders and experts, this report is a playbook for any organization navigating the complex landscape of cyber threats and regulatory requirements.

We hope this report becomes a in your journey to become proactive in compliance and resilience: We are all on the same team when it comes to safeguarding data and systems in today's digitally driven world.

Danielle Sheer
Chief Trust Officer
Commvault

Cyber Resilience in a New Era of Rigorous Compliance Mandates

THERE'S LITTLE MYSTERY about the mindset of risk, compliance, and security professionals. Data and cyber disruption have them spooked. In the 2023 Thomson Reuters Risk & Compliance Survey Report, released in October 2023, the Toronto-based information conglomerate found that 82% of risk and compliance professionals cited data and cybersecurity concerns as their organization's greatest risk—garnering nearly twice the response of the next most significant concern.[1] **FIGURE 1** Meanwhile, PwC's Global Crisis and Resilience Survey 2023, released by the London-based professional services firm in December 2023, found that 96% of organizations have experienced disruption in the past two years, with 76% saying the most severe disruption had a medium-to-high impact on operations.[2]

Such sentiment reveals what risk, compliance, and security professionals understand intimately: Businesses can't fall asleep on cyber resiliency—especially when preparing for cyber events is more complicated than ever. Welcome to the era of continuous compliance, when the world's economic viability demands endlessly available cloud services and uncompromising data protection, and while many firms are still figuring out artificial intelligence's (AI) ascending role in securing both, regulators on multiple continents have established strict digital safeguards that impose heavy noncompliance fines on organizations that fail to meet these rigorous requirements.

In fact, the most significant to cyber resilience will be the near eradication of significant business disruptions and AI's part in bringing that about, predicts Michael Rasmussen, a governance, risk, and compliance analyst with GRC 20/20 Research, a global market advisory firm based in Milwaukee. "Over the next three to five years, we can expect AI-powered services to become even more sophisticated, with advancements in machine learning enabling predictive security measures that can anticipate and neutralize threats before they materialize."

Organizations may already be familiar with legislative drafts aimed at either protecting data (the General Data Protection Regulation, the Data Governance Act, the European Data Act), safeguarding system and information security (the Network and Information Security Directive 2 (NIS2), the Cyber Resilience Act,

HIGHLIGHTS

By many definitions, resiliency demands that organizations gain the capacity to **anticipate human-made or natural disasters**, **survive disruptions with minor damage**, and **recover data and operations almost instantaneously** afterward.

Weaving new compliance functions into existing business process workflows is **particularly difficult for organizations that fail to foster a culture of compliance and that underinvest in continuous monitoring and improvement**.

Artificial intelligence research advancements could play a significant role in **helping organizations manage everything from threat prevention to the automatic preparation of compliance reports** that satisfy global regulatory requirements.

> "Over the next three to five years, we can expect AI-powered services to become even more sophisticated, with advancements in machine learning enabling predictive security measures that can anticipate and neutralize threats before they materialize," says Michael Rasmussen, a governance, risk, and compliance analyst with GRC 20/20 Research.

the Critical Entities Resilience Directive), or targeting specific use cases (the EU AI Act). These regulations set the stage for perhaps the most formidable compliance challenge: the European Union's Digital Operational Resilience Act (DORA), which mandates rigorous risk management frameworks, resilience testing, and incident reporting.

Organizations seeking to thrive in a globally connected digital economy must navigate this alphabet soup of regulatory complexity and build the resilience to withstand errors and attacks that not only disrupt their supply chains, data centers, networks, and cloud operations but harm their partners, customers, and shareholders. No matter the region or industry, the regulatory approach usually boils down to a basic concept: Bolster every link in the digital chain, from the resource-rich to the resource-poor, and hold organizations accountable for their actions.

"I think a lot of these regulations are seeking to ensure that society, given our tremendous economic interdependence, isn't impacted by entities who are not understanding or taking care of their own risk," explains Jonathan Fairtlough, principal at KPMG, a strategic consultancy based in London. Cyber risk, once delegated to computer teams, has become "a critical component in business planning, continuity planning, and assessing risk," Fairtlough says. "That's why you're seeing more and more boards put in place ways to oversee and understand cyber risk—because it touches on their fundamental role in the company."

In response to these current and pending regulations, organizations in North America, Europe, and Asia Pacific face mounting pressure to establish robust cyber resilience programs and invest in the right tools and talent to ensure both proper data handling and protection and the storage of sensitive data pertaining to their products, services, customers, partners, and employees. Meeting this mandate is no small feat. Establishing cyber resiliency is a high bar. By many definitions, resiliency demands that organizations gain the capacity to anticipate human-made and natural disasters, survive disruptions with minor damage, and recover data and operations almost instantaneously afterward. Meeting these high standards of operational resilience requires organizations to adopt best practices such as frequent recovery testing, cyber cleanrooms (isolated from external threats), better reporting capabilities, and robust cloud-native cyber defenses.

This paper will examine the essential components of regulatory compliance and cyber resilience in the digital age, highlighting the enormous challenges organizations all over the world face in attempting to cultivate resilience to potent and evolving threats, including new ones. It will also highlight the mounting regulatory oversight that threatens organizations with significant penalties for data mismanagement and careless actions that harm markets and supply chains. It will also explore how organizations can improve and fortify their operational resilience without compromising their business agility.

Costly Commercial Disruption

The coming and unprecedented regulatory wave, placed in an economic context, reflects widespread and concerted governmental interest in reducing, if not eradicating, the risk of costly commercial disruption. Among the most common problems are mismanaged cloud data centers and flawed cloud-based applications from software suppliers, which can result in harmful system failures and business interruptions, such as the pervasive CrowdStrike outage on July 19, 2024. A report prepared by Parametrix, a New York-based cyber insurer, shortly after the multiday outage estimated that the incident cost U.S. Fortune 500 companies $5.4 billion, not to mention possible brand reputational damage, litigation costs, regulatory penalties, or loss of shareholder value.[3]

To combat service disruption concerns and meet increasingly stringent data protection regulations, organizations must develop a comprehensive strategy that allows for greater operational resilience against both natural and human-made disruptions, including those involving data mismanagement. There is some urgency. The Cologny, Switzerland-based World Economic Forum's Global Cybersecurity Outlook 2023 report found that "cyber attackers are more likely to focus on business disruption and reputational damage." Pointedly, more than nine in 10 cybersecurity and business leaders who responded to the study believe that a “far-reaching, catastrophic cyber event is at least somewhat likely in the next two years.”[4]

According to GRC 20/20’s Rasmussen, “In a world where enterprise risks are increasingly complex and interconnected, being compliant and resilient means your organization can navigate regulatory pressures, protect critical assets, and ensure continuity and resilience in the midst of navigating the chaos of change in business.”

He sees strategic value in mastering this complexity. “Strategically, this [compliance effort] positions the organization as a trusted entity capable of delivering consistent value to customers and stakeholders while minimizing disruptions and the associated costs.”

High-Stakes Resilience

Cédric Burton, global co-chair and partner, data, privacy, and cybersecurity, in the Brussels office of the Palo Alto, Calif.-based law firm Wilson Sonsini, advises multinationals to treat cyber resilience as an imperative. “These days, if you want to be a successful company, you need to maintain healthy cyber practices, meaning you need to be cyber resilient,” he says. “Otherwise, you lose trust.”

No one disputes that cyber resilience is one of the essential building blocks of the global economy. But the cyber resilience game has changed. In the not-so-distant past, organizations focused primarily on quickly recovering from disasters rather than preventing them from occurring. Before the advent of the cloud, organizations shipped truckloads of data stored on tape reels for safekeeping at off-site warehouses. These tape backups weren’t indestructible and were virtually inaccessible—the antithesis of modern requirements for business resilience. While cloud operations present businesses with a myriad of attractive recovery options, such as global data redundancy, the cloud also complicates enterprise risk in the form of pervasive cyberattacks, including ransomware, where organizations must pay hackers up to millions of dollars for access to their stolen and encrypted data records.

Operating in the public cloud doesn’t mean offloading responsibility for operational resilience. Firms utilizing cloud service providers must also embrace the “shared responsibility model,” in which security is a shared effort, with the provider managing the infrastructure and networks and the customer monitoring its data security and applications. Customers operating in the cloud must formulate data protection and cyber resilience strategies with the shared responsibility model in mind.

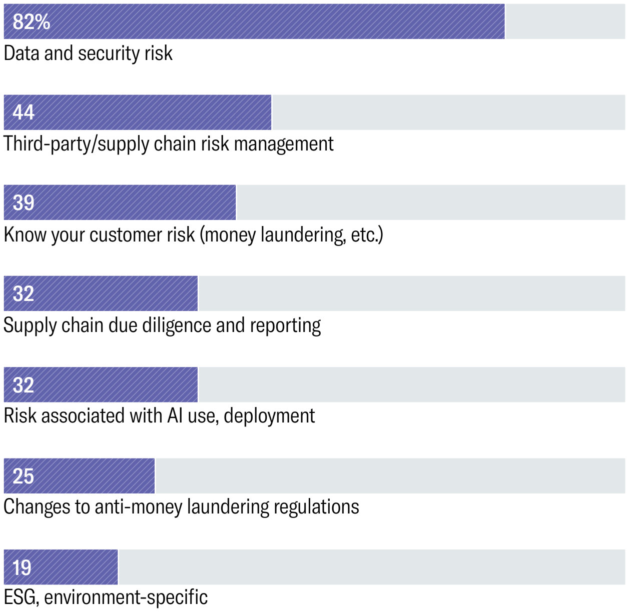
Businesses, particularly in regulated industries, face the looming threat of financial penalties and reputational damage for data privacy missteps in an era of stringent global regulatory controls. Clouds and software supply chains have become data management and regulatory minefields. Unfortunately, notes Rasmussen, “The shared responsibility model of cloud security can lead to confusion over who is responsible for what, increasing the risk of misconfigurations and data breaches.”

FIGURE 1

Risk Meets Compliance

Organizations believe data poses their most significant risk

Which of the following concepts constitutes your organization’s greatest risk?



Source: Thomson Reuters survey, October 2023

Resilience is a nontrivial investment that requires adopting proven technology frameworks and meticulous assessment of ongoing risks and opportunities. “Operational resilience is more than a regulation,” notes Rasmussen. “Every organization should be looking at integration risk” and assessing its “current compliance posture and resilience capabilities,” he adds. “This [assessment] includes mapping out their supply chains, identifying critical dependencies, and evaluating the potential impact of disruptions.“

When an organization identifies potential vulnerabilities, it should do a gap analysis between its current practices and the requirements of a governing regulatory framework, notes Wilson Sonsini’s Burton. “Once you identify the gap, try to remediate it by creating [or adopting] a framework which will allow you to comply and to bridge the gaps,” he advises.

Once those steps are completed, Burton recommends auditing, testing, and conducting an “ongoing review of your plan to ensure it keeps improving. The only way to be prepared is to practice.” One approach involves tabletop exercises—simulating the role each team member plays in response to a cyber emergency. Organizations can measure their improvement with key performance indicators such as mean time to recovery, system availability, team training, and the frequency of incident response plan updates. Another form of preparation entails cleanroom testing, a technique for identifying and eliminating flaws that can make software vulnerable to cyber threats. Cleanroom testing is an emerging, sometimes costly, and complicated practice that helps organizations demonstrate to regulators that they are taking appropriate data protection measures.

Yet most organizations have a "tendency to silo" the management of compliance and resiliency, explains KPMG's Fairtlough. This approach may result in a "gap of understanding how everything plays together." Conversely, those who view risk in holistic terms may communicate to their boards that while managing risk has a significant impact on the business, it "intertwines with existing business continuity and disaster recovery planning." As a result, he adds, integrating a holistic view of risk into organizational planning enhances an organization's capabilities of "meeting its production and contractual requirements" by eliminating information silos that impede compliance and cyber resilience best practices.

Gaining senior executive support and sponsorship for large-scale organizational projects has long been recognized for the way it can align divergent business units. Weaving new compliance functions into existing business process workflows is particularly difficult for organizations that fail to foster a culture of compliance and that underinvest in continuous monitoring and improvement. Adjusting to the demands of a complicated cloud architecture and a rapidly evolving regulatory and cyber threat environment isn't something you can simply hand over to the compliance team. It's an all-hands-on-deck company initiative involving considerable planning, investment, training, monitoring, and testing.

Building a successful compliance and resilience program requires an ongoing board commitment, notes Rasmussen. It also takes "a deep understanding of the evolving business environment and the risk/threat landscape and a culture that prioritizes risk and resilience management across all levels of the organization," he says. "The difficulty often lies not in the technology itself but in fostering the [continuous compliance] mindset and alignment across diverse business functions and keeping things current in a very dynamic and changing business environment."

Those who view risk in holistic terms may communicate to their boards that while managing risk has a significant impact on the business, it "intertwines with existing business continuity and disaster recovery planning," says Jonathan Fairtlough, principal at KPMG.

Risk Through a Cultural Lens

It's only natural but also perilous to assume that regulatory compliance and cyber resilience are defined or interpreted the same way by regulators around the globe. Fairtlough contends that U.S. companies often view compliance as a binary condition. "We focus on words like compliance, where we take a standard like NIST [the National Institute of Standards and Technology], work to meet that standard, and document extensively to show that we have met the standard." But, he says, EU compliance encapsulates a different perspective—demonstrating that you've properly studied the risk and have a plan to mitigate it. "It's not a checklist; it's risk analysis. What you need to show for compliance is subtly different," says Fairtlough. "That gets missed a lot. This issue, this cultural gap, is one of the areas that I find companies struggle with managing."

Developing individual operating frameworks for each country or applicable governing regulations wouldn't be a practical or cost-effective move, even for giant global organizations. "Companies can't just look at the EU in isolation," Burton asserts. "You can't implement a data protection framework for one country or one continent only. Threats come from all over the world, and data is global. So that adds a lot of complexity for companies."

On the other hand, Rasmussen believes that organizations should establish a "unified risk and resilience management framework that aligns with both global and domestic regulations." He says it should entail "leveraging technology for continuous monitoring and fostering a culture of compliance across the organization." As a practical measure, Rasmussen advises his clients to "embed compliance into their daily operations. Organizations [can] avoid penalties and strengthen their overall security posture, making them more prepared to respond to threats."

Companies operating in Asia Pacific nations such as China must also comply with new regulations concerning data protection, privacy, and anti-money laundering. Both Burton and Fairtlough caution that the world's second-largest economy sets compliance hurdles for any companies operating

"You can't implement a data protection framework for one country or one continent only. Threats come from all over the world, and data is global. So that adds a lot of complexity for companies," says Cédric Burton, global co-chair and partner, data, privacy, and cybersecurity, at Wilson Sonsini.

> “The sheer volume of data now available can overwhelm organizations that aren’t equipped to handle it, making it crucial to have the right tools and expertise to leverage AI and big data effectively,” says GRC 20/20 Research’s Rasmussen.

there. The “Chinese legal framework is very challenging to navigate,” says Burton. He cites data transfer restrictions as a case in point, noting, “When you touch certain data types in China, you need regulatory approval.” In China, for example, organizations can only use encryption if the government also has access to a key.

Despite regional differences, Fairtlough does find some consistency in the protections, the technologies, and the processes that organizations deploy globally. “The technical processes that you use to protect your data are, for the most part, going to be the same,” he says. “The difference will be set by regulatory or legal requirements like data localization—where you store that data. These regulatory differences also change the permissions required to enact some technical protections. As an example, certain types of data monitoring that a company can implement on its own in the United States may require the approval of a works council in Germany or France. You have to factor that [permission] into the overall risk analysis.”

AI Changes Everything

Cyber resilience isn’t just about surviving mistakes. It’s about ensuring business continuity and fast recovery when incidents occur.

AI can be an asset in this effort. “AI plays a critical role in protecting cloud data stores by enhancing threat detection, automating responses to incidents, and identifying vulnerabilities before they can be exploited” by bad actors, says Rasmussen. AI-driven tools, he says, have “absolutely” changed the complexities of managing cyber risk and regulatory compliance. “These technologies also require robust governance frameworks to manage the risks they introduce, such as algorithmic bias and data privacy concerns,” he notes. “Moreover, the sheer volume of data now available can overwhelm organizations that aren’t equipped to handle it, making it crucial to have the right tools and expertise to leverage AI and big data effectively.”

Despite its positive effects, AI also introduces new forms of cyber risk and presents organizations with vulnerabilities that can harm customer and partner relationships. While security and network teams tap AI-powered monitoring tools to detect cyber threats, the “threat actors have the same technology available,” notes Burton. “You know, on the one hand, AI is meant to protect a company network, but it’s also used by threat actors to create a new attack.” Deepfakes, in which a person’s face and body are digitally altered for malicious reasons, have emerged as “one of the key challenges for companies,” he adds. “It’s very easy to create a deepfake with the AI technology out there.” Burton believes existing regulations are “quickly outdated because of the fast-moving technology.”

The recently published EU AI Act proposes to govern everything about using AI systems within the EU. Like other EU regulations, such as DORA and NIS2, the act takes a “risk-based approach” that categorizes AI systems based on their potential risks. The riskier the application, the more stringent the controls; for example, the act bans manipulation of people and “voice-activated toys that encourage dangerous behavior in children.”[5] Among other things, the act sets standards for transparency and requires organizations to inform customers that they’re interacting with a chatbot rather than a human. The act’s provisions will phase in over the next three years, and it’s believed noncompliance fines may run up to €35 million or between 1% and 7% of annual sales, whichever is higher.

“AI is the hot topic right now from a regulatory standpoint,” says Burton. “Every single regulator in the world is trying to get a piece of it, and that’s true for antitrust, that’s true for privacy regulators in the EU, [and] that’s true for AI regulators with new AI regulations, as well.” He warns that it will become “really complex for an organization to identify every single regulation and make sure that it complies with [them].”

Steering clear of regulatory trouble requires planning. Laying the groundwork for using AI is similar to understanding your financial situation, says Fairtlough. “How can you engage in long-term financial planning if you don’t know what money you have, what accounts you have, what you’re owed, and what your receivables are, right?” he asks. “In concept, with data and with technology, these things produce value.” Fairtlough recommends that organizations determine how their data will be analyzed, where it will happen, and what the organization knows about its usage from a privacy standpoint. He suggests assessing the impact of potential problems such as a service interruption, a technical issue, or a regulatory hurdle.

“AI is the hot topic right now from a regulatory standpoint. Every single regulator in the world is trying to get a piece of it, and that’s true for antitrust, that’s true for privacy regulators in the EU, [and] that’s true for AI regulators with new AI regulations as well,” says Wilson Sonsini’s Burton.

KPMG's Fairtlough recommends that organizations determine how their data will be analyzed, where it will happen, and what the organization knows about its usage from a privacy standpoint.

According to Fairtlough, only after they've completed this assessment will organizations be adequately prepared to utilize large language models and tap their full capabilities, "because I know where to target my data and I know what data belongs to me," he explains. "And I'm able to put governance around that, knowing that I'm using data I was lawfully allowed to collect, that is part of my overall analysis set, and I can trust the results." Last, he would ask, "What steps am I taking to protect that data commensurate with the risk it poses to my business?" AI research advancements could play a significant role in helping organizations manage everything from threat prevention to the automatic preparation of compliance reports that satisfy global regulatory requirements. Rasmussen believes that AI and machine learning will do practical things for organizations in the next three to five years. "AI will play a key role in ensuring compliance, automating the auditing process, and providing real-time insights into an organization's security posture," he says.

Burton predicts AI tools will sharply enhance threat detection, offering organizations real-time analysis of impending danger. "You'll be more efficient in restoring a system because a lot of tasks will be automated," he says, and he anticipates automated "AI encryption as well—adapting your encryption model in real time depending on the type of threat you face."

Conclusion

The long road to cyber resilience and regulatory compliance begins with executive ownership of the problem, typically with board-level buy-in. Organizations that compete in global markets must adhere to a growing number of disparate regulations aimed at protecting data and keeping companies from disrupting supply chains and digital commerce—rules that seek to hold companies accountable for their actions or missteps.

However, it's not just the threat of stiff regulatory fines motivating organizations to beef up their resiliency and cyber defenses. There's also the cost of unplanned service disruptions, such as network or cloud outages, ransomware, and data loss, that imperils customer, partner, and stakeholder trust. The number one reason boards invest in enterprise resilience, agreed on by 49% of respondents in PwC's December 2023 survey, is to "reduce losses from future disruption."[6]

How will organizations respond to the rigorous demands of regulations such as the EU's NIS2, safeguarding security, and DORA, which concerns resiliency? Fierce testing, cleanrooms, and better risk management can move the needle to strengthen cyber resilience. But AI won't be an immediate panacea. There's a growing number of AI-related tools aimed at helping companies detect threats, butthere are also mounting governmental and industry concerns about AI cyber risk from deepfakes and errors. New EU regulations plus pending legislation in California aim to curtail algorithmic bias and limit data privacy harm.

While DORA, among other regulations, may impel some organizations to improve their cyber resiliency, it's also just good business sense to manage data and cyber operations as smartly as possible. "These regulations compel organizations to rethink their risk management strategies, focusing more on continuous monitoring, incident response, and recovery capabilities," explains Rasmussen. "Organizations should certainly adjust their posture—not just to meet compliance requirements but to exceed them. By doing so, they can future-proof their operations against new and unforeseen challenges, ensuring they remain compliant, robust, and adaptive in the face of evolving risks."

Endnotes

[1] Thomson Reuters, “The 2023 Thomson Reuters Risk & Compliance Survey Report,” October 13, 2023. https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/risk-compliance-survey-report-2023/.

[2] PwC, “PwC’s Global Crisis and Resilience Survey 2023,” December 2023. https://www.pwc.com/gx/en/issues/crisis-solutions/global-crisis-survey.html.

[3] Parametrix, “CrowdStrike’s Impact on the Fortune 500,” July 24, 2024. https://www.parametrixinsurance.com/reports-white-papers/crowdstrikes-impact-on-the-fortune-500.

[4] The World Economic Forum, “Global Cybersecurity Outlook 2023,” January 2023. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf.

[5] The European Parliament, “EU AI Act: first regulation on artificial intelligence,” June 8, 2024. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

[6] PwC, “PwC’s Global Crisis and Resilience Survey 2023,” December 2023. https://www.pwc.com/gx/en/issues/crisis-solutions/global-crisis-survey.html.

Harvard Business Review
ANALYTIC SERVICES

ABOUT US

Harvard Business Review Analytic Services is an independent commercial research unit within Harvard Business Review Group, conducting research and comparative analysis on important management challenges and emerging business opportunities. Seeking to provide business intelligence and peer-group insight, each report is published based on the findings of original quantitative and/or qualitative research and analysis. Quantitative surveys are conducted with the HBR Advisory Council, HBR's global research panel, and qualitative research is conducted with senior business executives and subject-matter experts from within and beyond the *Harvard Business Review* author community. Email us at hbranalyticservices@hbr.org.

hbr.org/hbr-analytic-services