Deloitte.

CEO and board risk management survey

Illuminating a path forward on strategic risk

Contents

Chuck Saia
CEO | Deloitte Risk and Financial Advisory

Foreword

One of my favorite things to do is coach my sons' sports teams. When I was their age, I preferred playing time over practice time. And no surprise, they feel the same way. But as a coach, I understand that practice pays dividends. It breeds competence—and confidence. I see it in the eyes of my sons and their teammates. They're prepared for the challenges that lie ahead.

It's the same in business. Practice not only builds confidence, but it can also create a culture of strategic thinking, allowing organizations to think beyond the crisis of the moment, embrace innovation, and even consider the unknown. Take cybersecurity, for example. Many organizations know there are risks related to cyber, but their solution for managing them is often to double down on technology. They believe a tech-centric threat calls for tech-centric investments. They may fail to view this strategic risk through the lens of governance, talent, and reputation. Senior leaders often view threats in a vacuum, acknowledging their existence but missing the mark on solving for them.

That mind-set is a key takeaway from **"Illuminating a path forward on strategic risk,"** Deloitte's 2018 CEO and board risk survey. In our survey, we wanted to explore leaders' risk posture and gauge their level of readiness. We focused on four strategic risks that are top of mind for our clients—brand and reputation, culture, cyber, and extended enterprise. When I meet with C-suite executives and board members, it's clear that these threats are the most difficult to understand, identify, and navigate. There's frustration in not having the right answers, but also in not knowing what questions to ask. They realize that their approach to strategic risks can be the difference between being a disruptor in their industries and being disrupted by a competitor.

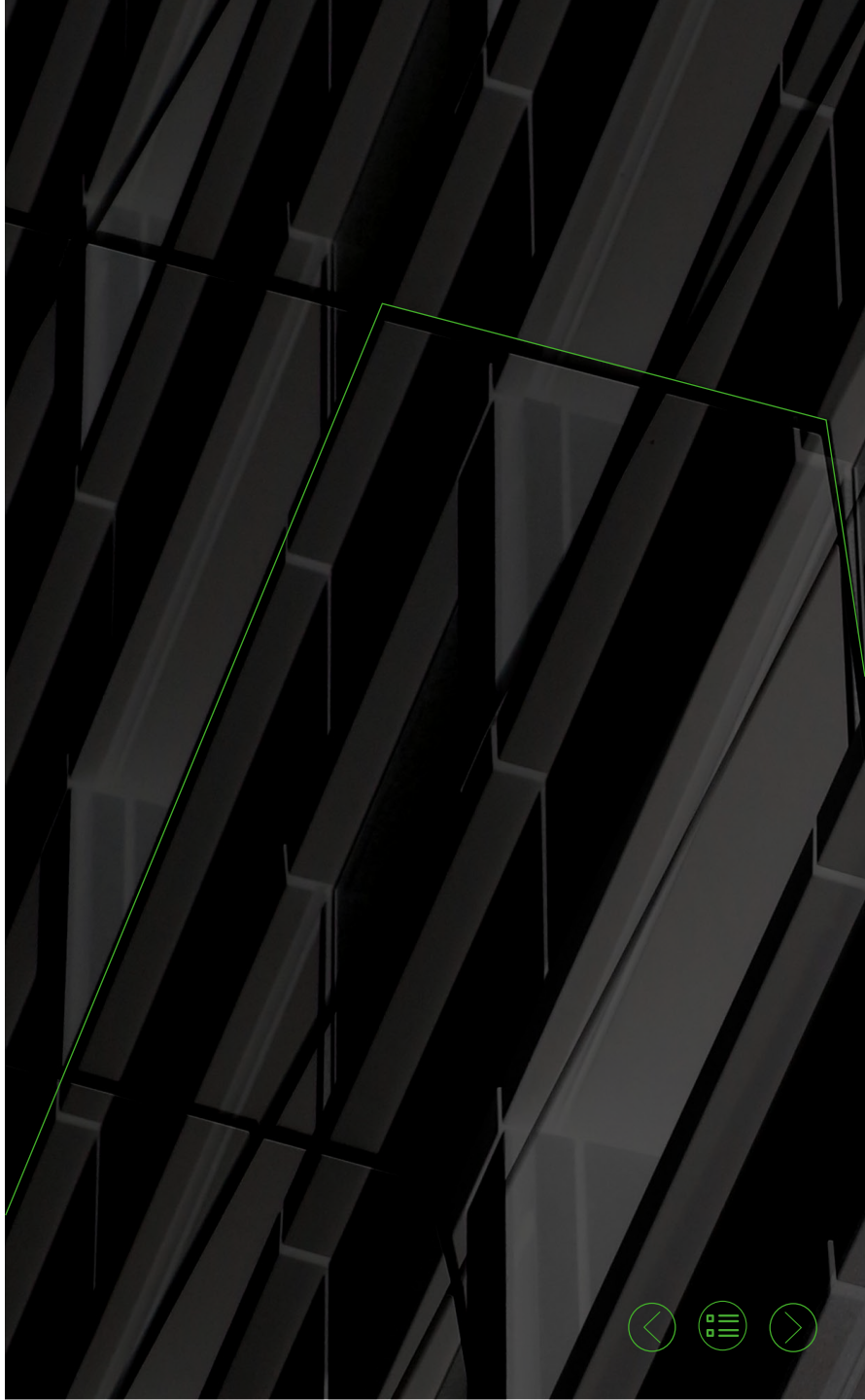
In our report, we surveyed 400 CEOs and board members from US organizations with at least $1 billion in annual revenue. We asked these leaders how they view strategic risk and how they're prioritizing investments to address these challenges.

We found that senior leaders know threats are on the horizon but, in many cases, are not managing them in a strategic way. They're not seeing these critical threats as interconnected, complex risks that, when managed correctly, could create opportunities for accelerating growth. Many admit that they're not fully preparing for threats or prioritizing the investments needed to identify, respond to, and mitigate these risks. Boards and management are often not aligned on key strategic risk decisions.

Looking at these risks strategically takes a shift in mind-set. It means challenging the status quo and being willing to take bold and innovative measures by doing things differently. Our goal with this report is to shed light on strategic risk management in today's complex world and offer insight into a path forward.

I hope this research helps you gain a deeper understanding of these interconnected strategic risks and the steps you can consider to position your organization to unleash its full potential and embrace the future. We may not always know what's around the corner, but we can be better prepared with a strategic mind-set. It's a good practice to get into.

Chuck Saia
CEO
Deloitte Risk and Financial Advisory



Executive summary

Managing risk is a critical facet of the roles of CEOs and board members. This is particularly true in today's environment of ongoing disruption, innovation, and technological change. Increasing disruption leads to greater risks—which become greater still because they're intertwined and interconnected. And because these risks don't occur in isolation, addressing them in silos can be an exercise in both frustration and futility.

Among all the risks that senior executives manage and board members oversee, strategic risks can pose the most significant threats as these risks can undermine the organization's ability to implement strategy and achieve performance goals. They can also cause major damage in a matter of weeks, days, or even seconds. What's more, investments in tools and technology aren't enough to "solve" strategic risks—unless leadership fully understands and embraces them.

In the face of these daunting challenges, how can leaders become more confident in their risk management capabilities? Deloitte surveyed 200 CEOs and 200 board members in organizations of more than $1 billion to find out. Our survey explores strategic risks in four areas that we believe are most critical to understand in today's marketplace:

This report sheds light on the need to take a more disciplined, direct, and calculated approach to strategic risk management.

Here are the key survey findings:

It may be inevitable. But are they ready?

Almost 100 percent of responding leaders believe their organizations will face serious threats or disruptions in the next two to three years. But are they prepared to manage those threats and disruptions? Survey responses reveal that many organizations are falling short in one or multiple areas: investment in technology that aligns with strategy, engagement from senior management and board members, alignment of risk and risk officers within an organization, and more.

- Leaders tend to focus on current, isolated, tactical risks rather than emerging strategic risks. And they generally take reactive rather than proactive measures.
- Leaders who manage strategic risks effectively are better able to navigate disruption, accelerate performance, and gain competitive advantage.
- To stay ahead, leaders need to:
  - Be aware of and position the organization to address these important risks
  - Apply the right technology to risk data, insights,and predictive analytics
  - Adopt integrated risk reporting and governance
  - Achieve greater CEO and board member alignment to drive informed decisions

Reputation risk may be flying under the radar.

Only half of organizations appear to recognize the importance of proactively managing reputation risk:

- About half of the surveyed leaders acknowledge that their organizations lack the ability to identify reputation-impacting events and to analyze incidents and predict effects.
- Less than half of the leaders have discussed the organization's reputation—and only about half have discussed how to address reputation risk—in the past 12 months.
- Due to a 24-hour news cycle, these risks stem from a broader range of events and sources in today's environment than in the past, including Internet sites, social media, and others.

Culture risk may be given short shrift.

Leaders may be overestimating the health of their organizational cultures or underestimating the forces that can undermine a sound culture:

- Culture risk is of the least concern to CEOs and board members, with only one in five citing it as a top risk. Yet it may be the area that leaders can control most directly.

- Culture risk can be quantified, but nearly two-thirds of organizations lack a process to identify signals of culture risk, which can be digitally detected and monitored.
- Surprisingly, less than 40 percent of CEOs have a plan to invest in a process for identifying and addressing culture risk in the next 12 months.
- A number of negative, very public incidents rooted in culture and conduct indicate a need for regular culture risk reviews, which less than one-third of organizations perform.

Cyber risk may be their greatest concern.

But only 38 percent of CEOs and 23 percent of board members are "highly engaged" in this area:

- To combat cyber threats, leaders are mostly aligned on the need for improvement and the areas of investment. In particular, they are more likely to invest in security operations and digital transformation, and less likely to invest in enhancing threat intelligence and analytics capabilities.
- Only 25% of organizations plan to invest in cyber war–gaming and scenario planning to combat cyber threats in the next 12 months, even though it's a leading practice to assess vulnerabilities and respond.
- Cyber risk reports often focus on technical details and technological risks. Yet CEOs and board members could benefit from—and be more engaged by—cyber risk reporting and assurance that focus more on business risks and impacts.

Extended enterprise risk may be underrated.

Most organizations don't hold third parties to the same risk standards they set for themselves:

- Sixty-two percent of CEOs view the policies of their third parties as being weaker than their own. But only 39 percent of board members share that view, indicating a need for greater alignment.
- More than 50 percent of organizations don't have a plan to establish formal risk-monitoring standards.
- Leaders plan to manage extended enterprise risk primarily in-house, with internal programs, new talent, and new technologies. But they've taken limited action. They may also be overlooking the value of today's managed services models.

This survey report reveals leaders' views on these four strategic risks, areas of alignment and divergence, current and future risk management and governance practices, and plans for related investments. To build on these findings, we also offer Deloitte's perspective on a path forward, including steps organizations can consider to enhance their approaches to managing strategic risks and questions leaders can ask to gauge their readiness for ever-evolving threats.

Gap analysis: Acknowledging and preparing for potential threats

Virtually all senior leaders—95 percent of CEOs and 97 percent of board members—believe that their organizations will face serious threats to their growth prospects in the next two to three years.

Leaders say new disruptive technologies and potential cyber incidents pose the greatest threats (see figure 1). They're concerned about the breakneck pace at which their organizations must develop, deploy, and manage new technologies. And they're keenly aware of technology's potential to disrupt business models, customer behaviors, and markets.

Cyber incidents are a major concern. The extended enterprise also poses significant risks—particularly in the view of board members, who rank it second among the four strategic risks.

Interestingly, reputation and culture risks are of the least concern to CEOs and board members. Yet these may be the risks over which they have the most control. And they may bear closer watching as they can also create or fuel cyber and extended enterprise risks. The need to be mindful of multiple strategic risks at the same time adds to the complexity.

For example, a cybersecurity incident is obviously a cyber risk, but it also could be a risk to reputation and culture. The interconnectedness of strategic risks (to a greater extent than traditional risks) needs to be acknowledged and understood. But our survey results indicate that risks posed by disruptive technologies and cyber may be overshadowing other risks on leadership agendas.

Figure 1. Areas that will pose the greatest threat to organizations' growth prospects in the next 2–3 years

The majority of CEOs and board members selected either disruptive technology or cyber as one of the greatest threats

> The interconnectedness of strategic risks needs to be acknowledged and understood.

Aligning risk strategy and investment priorities

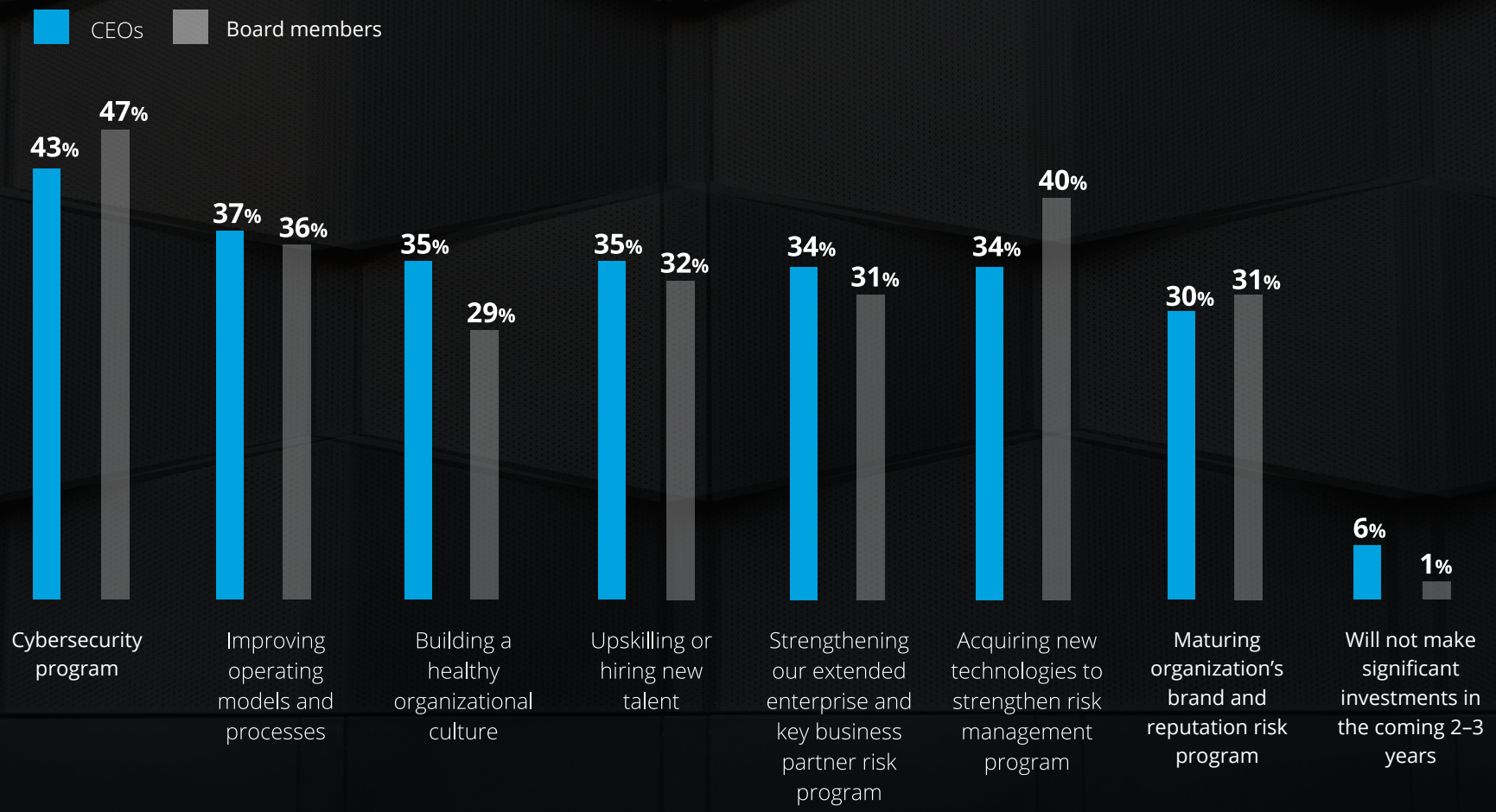
While both groups prioritize cybersecurity over acquiring new technologies to strengthen risk management, more board members than CEOs cite new technologies as a priority. CEOs are slightly more likely to prioritize investing in culture and talent (see figure 2).

A key task of the leadership team is understanding the impact of technology on strategies, business models, operations, security, culture, and reputation—and aligning risk strategy accordingly. Then leadership should invest in the right people, processes, and technology needed to address these impacts.

While CEOs and boards rank disruptive technologies and cyber incidents as posing the greatest risk, many may be "throwing money at the problem" as they continue to prioritize technology investment. Or they may need to better understand the broader impact of technology. Or both. With greater understanding, they are better positioned to establish risk governance and management structures to address cyber risks as well as all other risks to the organization—now and in the future.

With the right governance frameworks and risk management structures in place, leaders can position the organization to address the Internet of Things (IoT), wearable technology, and new technologies yet to be conceived. The organization can then be equipped to make the required investments in people and solutions to identify and address the full range of emerging risks, impacts, and opportunities. This is where organizations separate themselves from the pack. Having the confidence to strategically manage current and future risks is a game changer.

Figure 2. Areas where investments are expected to be made in the next 2–3 years



Reputation risk: A shortsighted view of an organization's most valuable asset

Reputation risk defined

Reputation is among an organization's most valuable assets. Reputation risks are interconnected threats related to a variety of factors, including ethics and integrity, security risks, product and service risks, culture risk, and extended enterprise risk. Reputation risk is created when performance doesn't match what customers expect based on the organization's communicated strategy, track record, and employee and leadership behavior.

Roughly half of CEOs and board members acknowledge that their organizations lack the ability to identify reputation-impacting events, analyze risks, and forecast impacts on brand and reputation (see figure 3). Separately, 59 percent of leaders lack a plan to develop or acquire tools to address reputation risks.

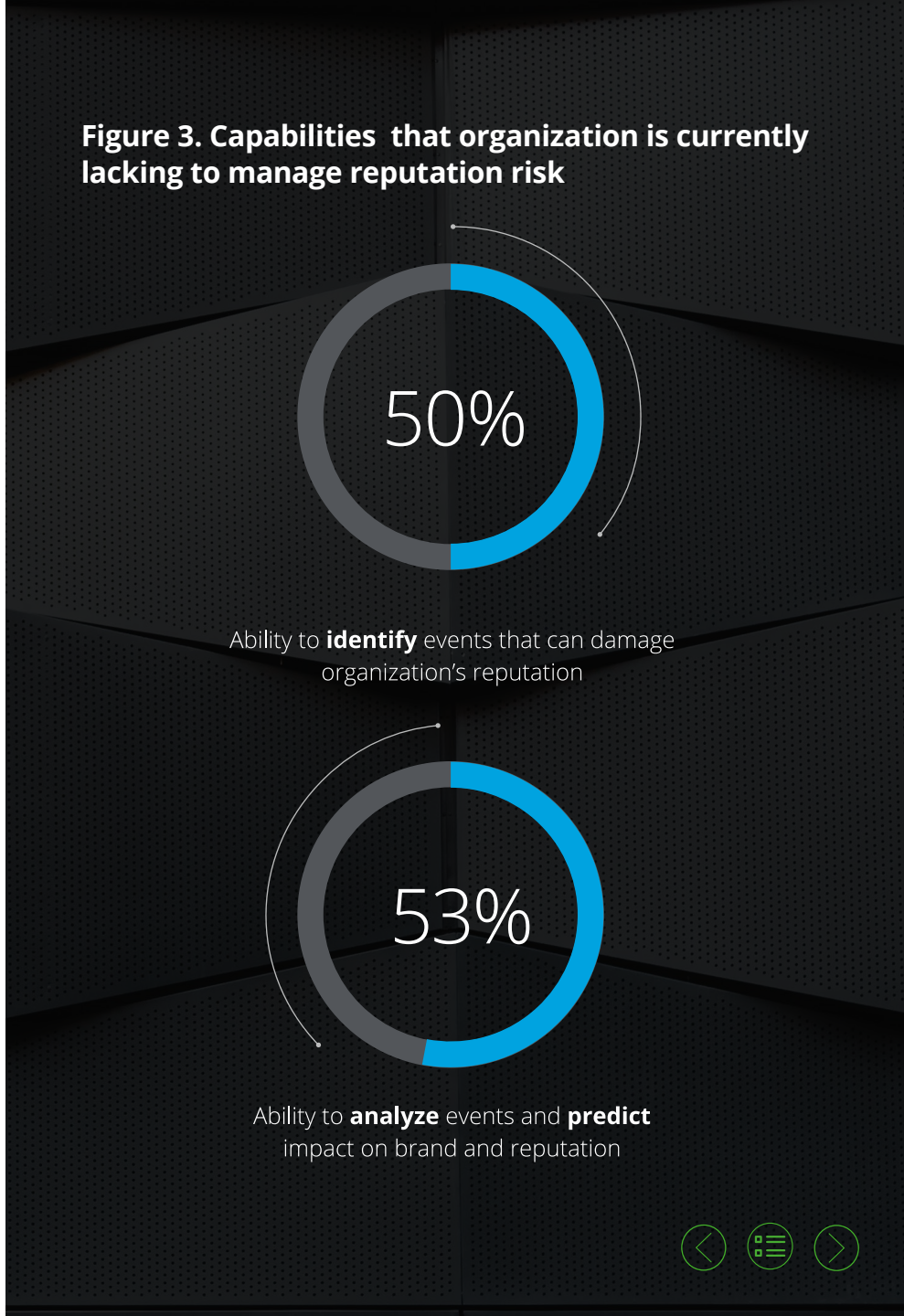
Reputation risks should be identified and analyzed as risks that can emanate not only from cyber incidents, crisis management, and conduct, but also directly from social media trends, Internet rumors, and other sources. Sophisticated risk sensing and predictive intelligence tools for monitoring and addressing reputation risks should be considered by the leadership of every organization.

Reputation risk should get onto boards' agendas

Fewer than half of CEOs and boards have discussed the state of the organization's reputation, and only about half have discussed how best to address reputation risks, in the past 12 months. Well under half have discussed how to best enhance the organization's reputation.

Perhaps many CEOs and board members don't realize that reputation risks stem from a much broader range of events in today's environment than in the past, due to digitalization and a 24-hour news cycle focused heavily on business. Or they may believe that risks to reputation arise only from other risks and can therefore be mitigated by simply managing those other risks well.

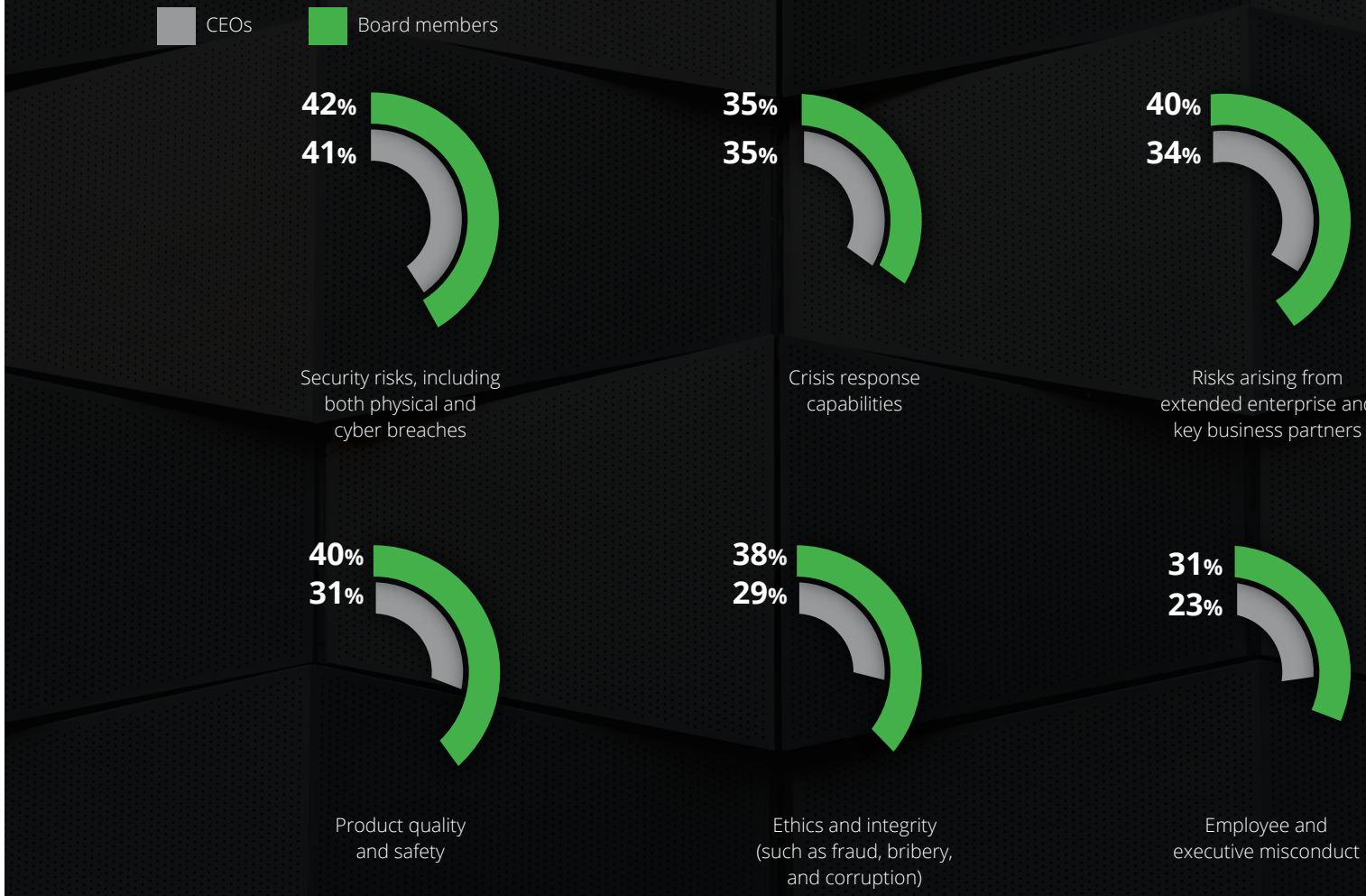
Figure 3. Capabilities that organization is currently lacking to manage reputation risk



CEOs and boards need to get on the same page

CEOs and board members are closely aligned on the top risks to the organization's reputation—cyber breaches and physical breaches—continuing the cyber-focused theme of their thinking (see figure 4). Both groups also see crisis response capabilities as a threat to reputation, followed by extended enterprise, product quality and safety, and ethics and integrity. Lack of consensus exists on some reputation risks, such as product safety and quality, ethics and integrity, and employee misconduct—areas where organizations might consider ways of providing greater assurance to the board.

Figure 4. Risks that pose the greatest reputational threat in the next 12 months



Our take

The relatively low ranking of ethics and integrity and employee misconduct among CEOs is interesting. It may reflect leaders' confidence—or overconfidence—in their abilities to manage and govern culture and conduct. This is also in line with the low overall priority respondents assigned to culture risk in this survey.

Yet managing and protecting reputation is a high-priority leadership responsibility. Reputation risks may not be subject to the patches and security measures that combat cyber risks, and they may not be as easy to identify. But like an organization's culture, reputation is arguably an area that can be managed most effectively by leadership (as opposed to, for example, cyber, health and safety, operational, and financial risks), in that it's an area that leaders directly impact.

Culture risk: Underappreciated, underestimated, and misunderstood

Culture risk defined

Culture is a system of values, beliefs, and behaviors that shapes how things get done within an organization. It aligns with and supports business strategy. It is also shaped by leaders' actions and decisions, sustained by employee behaviors, and reinforced by business and organizational systems. Culture risk is created when there's misalignment between an organization's values and leadership actions, employee behaviors, or organizational systems.

Culture risks are of the least concern to CEOs and boards, with only one in five citing it as a top threat to their growth prospects. Leaders may be overestimating the health of their cultures, or they may be underestimating the forces that can undermine even a sound culture, which is essential to implementing strategies and achieving goals. This view may also stem from a lack of culture risk sensing programs and regular reporting on culture. However, fewer than half of the surveyed leaders plan to invest in culture risk management processes.

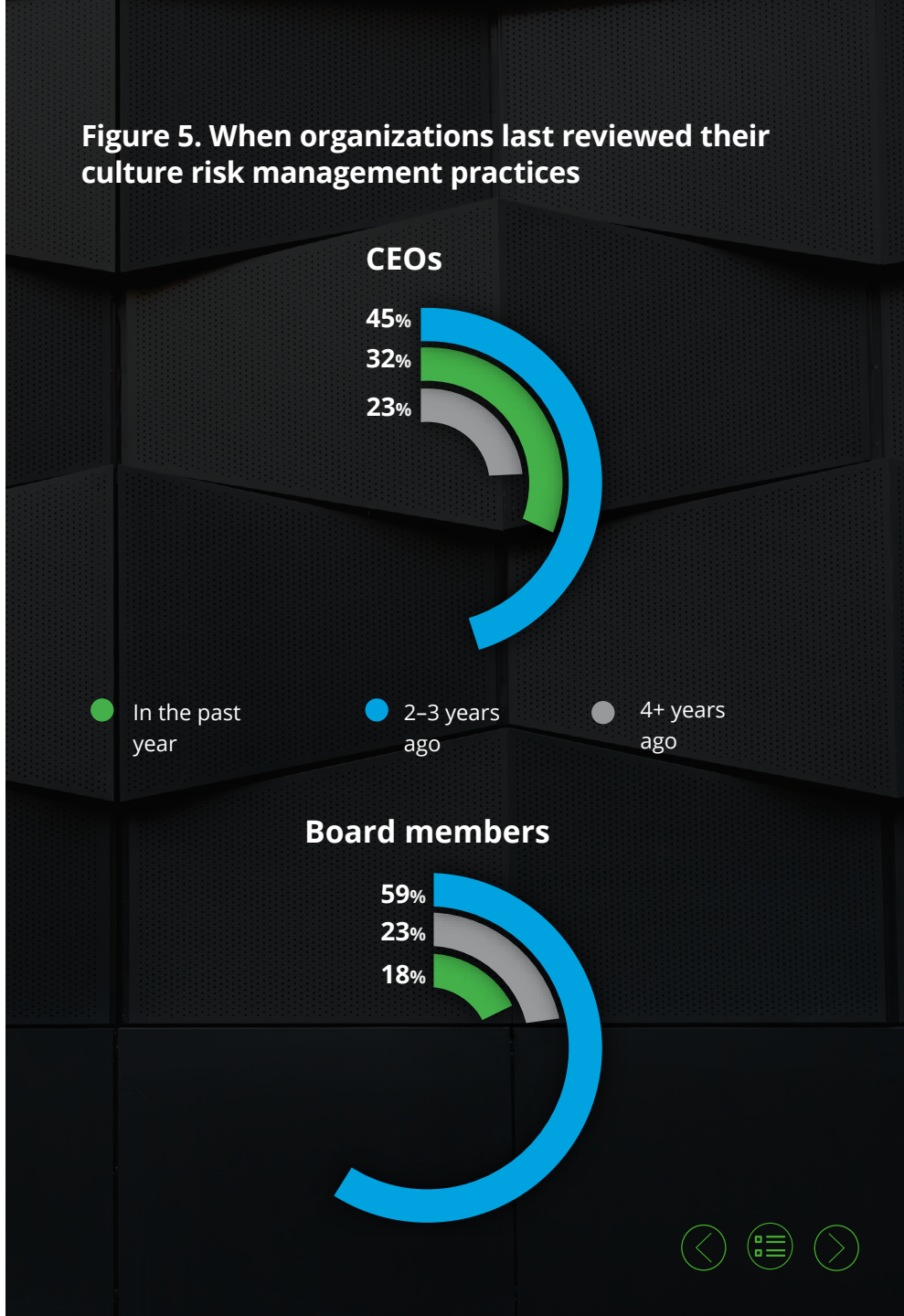
Sensing programs are underutilized

About two-thirds of CEOs and board members lack a process for identifying signals of potential culture risk. Only about one in three organizations plan to invest in these processes in the next 12 months.

Amplifying culture risk reporting and assessment to senior leadership

Only one in three organizations regularly report to the CEO and the board on culture and conduct risk. That leaves 70 percent lacking regular reporting to the leadership on this key risk. Similarly, only 32 percent of CEOs and 18 percent of board members report that their organizations have reviewed their culture risk management practices in the past year (see figure 5). The number of negative, high-profile, very public incidents rooted in culture and conduct over the past year alone would clearly indicate a need for ongoing reviews.

Figure 5. When organizations last reviewed their culture risk management practices



Fewer than half of organizations plan to invest in culture risk processes

Thirty percent of respondents indicate that their organizations will likely invest in processes to monitor employee behaviors in the next 12 months. The difference isn't a dramatic one, but organizations that conduct regular reviews of their culture risk practices are somewhat more likely to make such investments than those that don't conduct ongoing reviews.

Our take

How organizations invest in culture-related processes will likely determine their capabilities in this critical area. They should consider technologies, tools, and platforms that monitor external as well as internal culture risks. For example, insider threat programs that include risk-sensing platforms provide a broader picture of the risks to an organization.

CEOs and boards should also realize the upside to proactively managing culture—doing so can help create the effective culture an organization needs if people are to deliver on the strategy and the value proposition.

Cyber risk: More intensive engagement needed

Cyber risk defined

Cyber risk occurs when technological silos within organizations aren't connected through a broader strategy to defend what matters most to their mission, build awareness to know when a compromise has occurred or may be imminent, and reduce the impact when an incident does occur. The traditional discipline of IT security, isolated from a more comprehensive risk-based approach, may no longer be enough to protect organizations. To grow, streamline, and innovate, many organizations have difficulty keeping pace with the evolution of cyber threats.

CEOs and board members rank cybersecurity as their greatest concern, but only 30 percent on average describe themselves as highly engaged in the area. Increasing dependence on technology calls for more intensive leadership engagement through such practices as war-gaming participation, scenario planning, threat intelligence reviews, and a basic understanding of advanced analytics (see figure 6).

The need for leadership alignment on the most pressing issues

CEOs and board members differ a bit on the significance of specific cyber risks. Each group rated IoT as the most significant threat. But CEOs cite mobile platforms/cloud-based applications more often than boards do. Boards rate artificial intelligence technologies second (see figure 7).

Lack of CEO-board alignment on the most pressing cyber risks may signal the need for more robust cyber risk strategy, governance, and management frameworks. Senior leaders also need business-focused cyber risk reporting, rather than overly technical reports from the CIO and CISO. To engage senior leaders, those technical reports should be supplemented or replaced by cyber risk assessments from internal audit and external reviewers that focus on business impacts and risks.

Figure 6. Level of engagement among CEOs and board members toward cyber risk

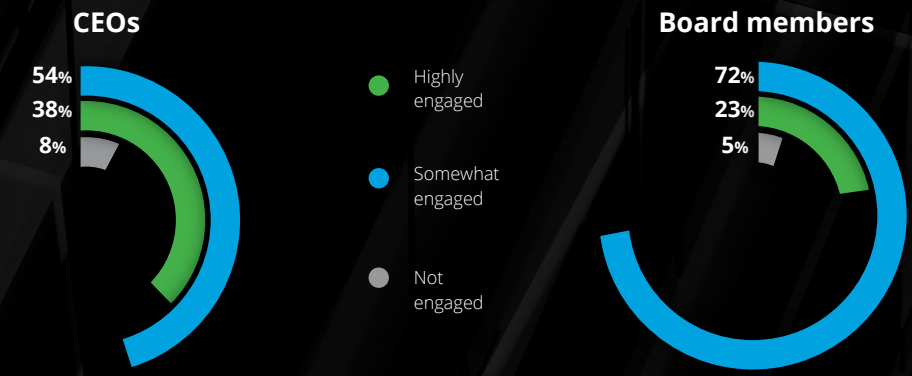
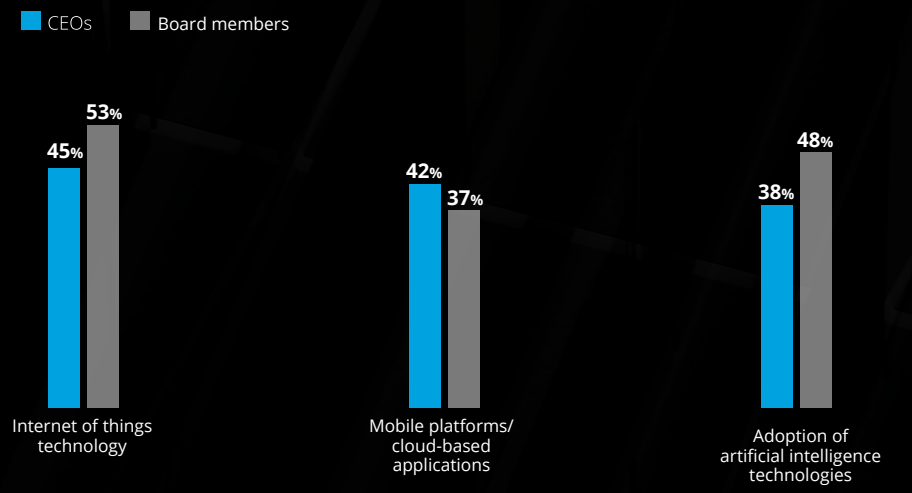


Figure 7. Areas that pose significant risk to organizations' cybersecurity programs



Missed opportunities in war-gaming and scenario planning

CEOs and board members agree that the top two areas needing improvement—and in which they'll invest—are security optimization services and digital transformation programs. The lower percentage citing war-gaming and scenario planning is concerning, as is the low percentage of CEOs citing threat intelligence and analytics solutions (see figure 8).

The capabilities that organizations say they will invest in are well—although not directly—aligned with the aspects of cybersecurity that are viewed as needing improvement (see figure 9). In general, the more closely leaders align investments with needs, the more likely they'll be able to allocate resources where they may be the most effective. Again, cyber risk assessments that focus on business impacts can help ascertain needs.

Figure 8. Aspects of organizations' cybersecurity programs that need improvement

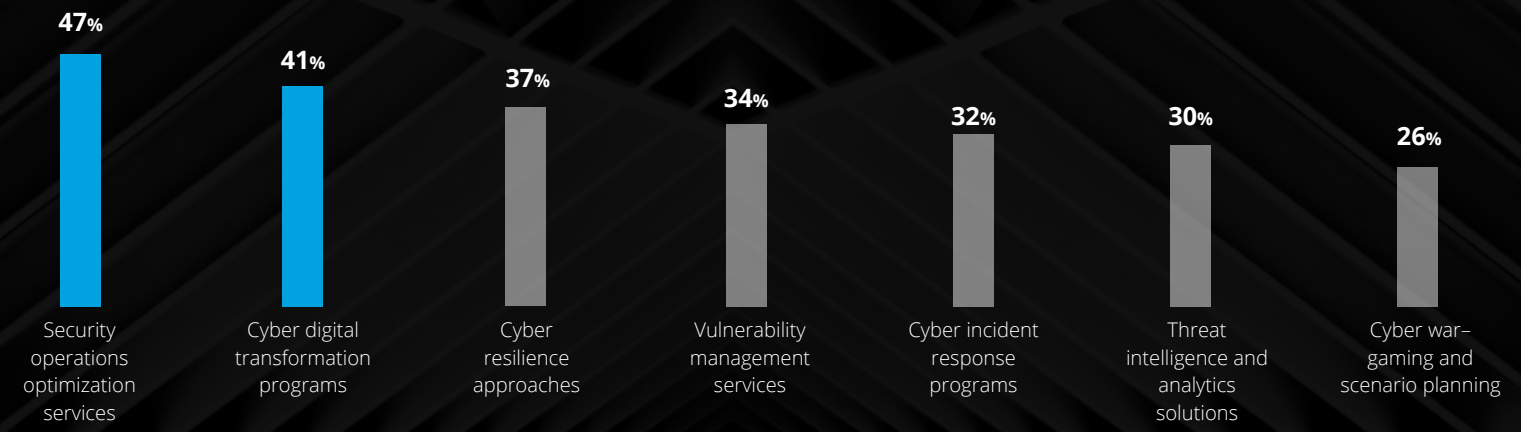
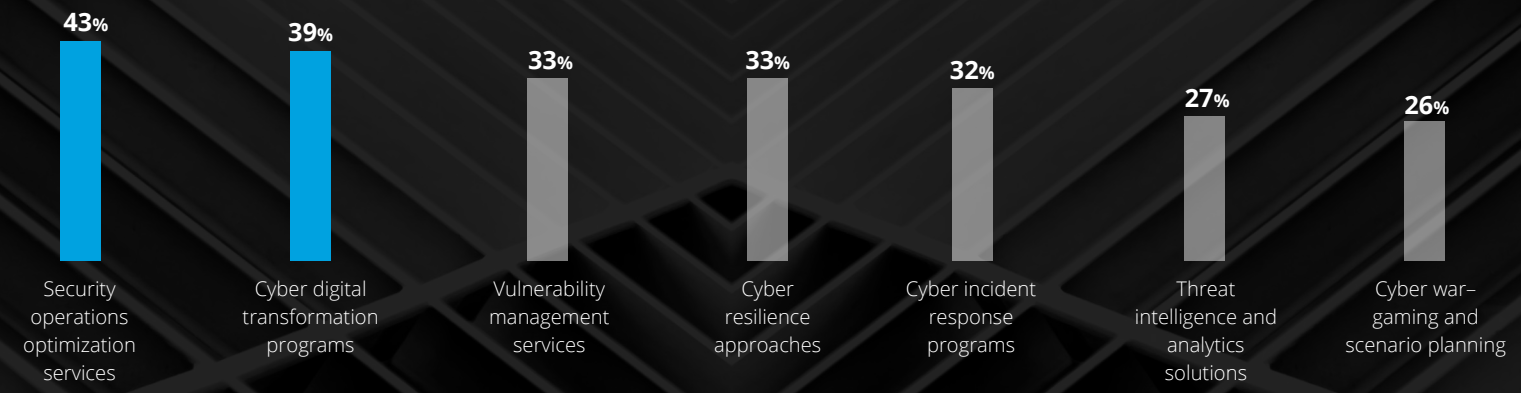


Figure 9. Capabilities organizations will likely invest in within the next 12 months to combat cyber threats



Our take

In our experience, war-gaming and scenario planning are among the leading methods of assessing vulnerabilities and improving resilience. Engaging senior leaders in these exercises is key to moving from simply identifying security threats and fixes to also defining business impacts, governance methods, risk escalation steps, and organizational responses.

Threat intelligence can help organizations proactively identify and monitor risks. Analytics solutions can assist in gauging the likelihood and potential impact of risks, as well as prevention and remediation steps. War-gaming, scenario planning, and threat intelligence can help provide the "outside-in" view needed to identify new threats and emerging risks.

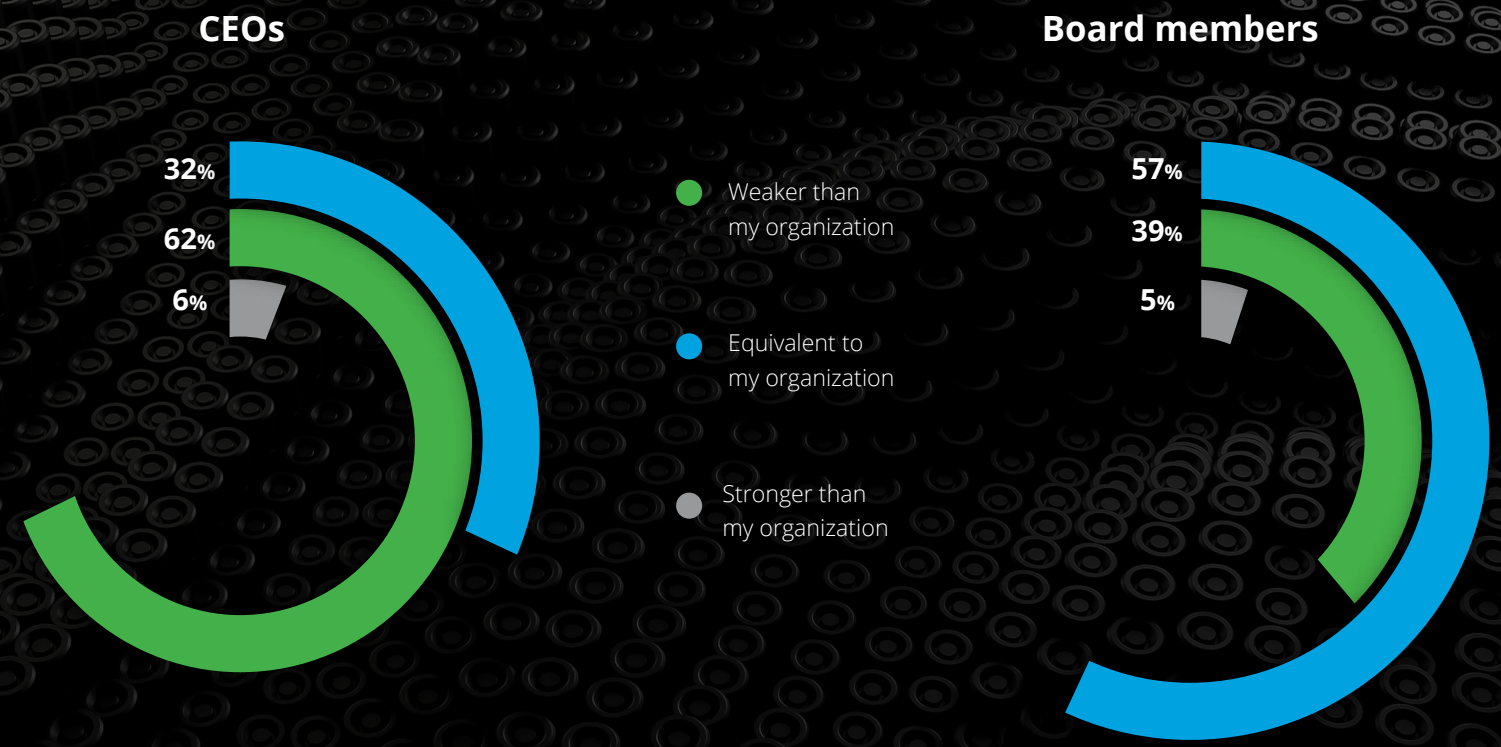
While cybersecurity operations are a priority, digital transformation presents greater opportunities to enhance performance and gain competitive advantage. Optimizing operations can generate efficiencies. But leaders who invest in digital transformation typically see opportunities to enhance current business models or adopt new ones, and to use risk to accelerate performance.

Extended enterprise risk: Third parties are a cause for concern

Extended enterprise risk defined

An extended enterprise is the collection of vendors, contractors, distributors, suppliers, and other third parties outside the main organization. Extended enterprise risk management (EERM) is the practice of anticipating and managing exposures associated with third parties across the organization's full range of operations, as well as optimizing the value delivered by the third-party ecosystem. Extended enterprise risk isn't a risk unto itself. Rather, it's a combination of diverse risks, and its various degrees of severity are based on the nature of the relationships an organization has with its third parties.

Figure 10. Perceived strength of extended enterprise risk management policies and standards relative to own organization's policies



Roughly two-thirds of CEOs and one-third of board members acknowledge that risk management in their extended enterprises is weaker than in their own organizations (see figure 10). The disparity between the two groups' perspectives—with many more CEOs taking a dimmer view than board members—should raise a red flag. Or at least a yellow one. This may reflect inconsistent reporting to the two sets of leaders and potentially a lack of alignment over risk strategy.

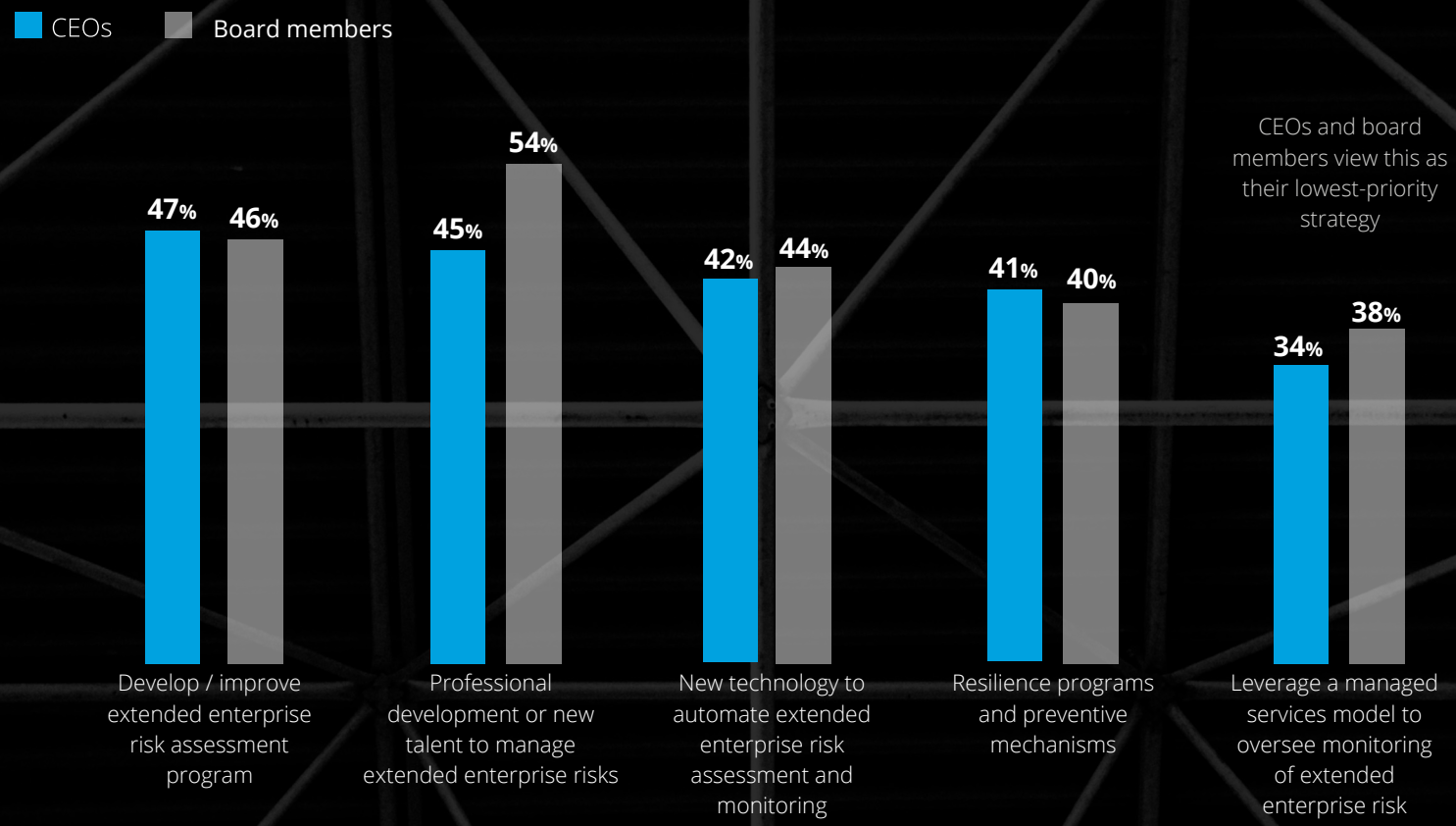
Third parties can create exposures as dangerous as those within the organization itself. So relationships with them need to be proactively managed across the life cycle, with mechanisms to ensure that all risks are identified, monitored, and mitigated.

Are managed services overlooked when managing third-party risk?

Five initiatives for managing extended enterprise risk were fairly evenly selected by survey respondents, with no single method standing out. Yet these responses may imply that organizations aren't taking key steps in this area. In order to adopt, enhance, and strengthen their partner ecosystem, organizations should have a defined risk management program that clearly outlines what's acceptable from third-party vendors. This can help ensure that third-party vendors are aligned to the organization's overall goals and adhere to its risk management policies.

Leaders are largely aligned on where they plan to invest over the next two to three years to manage this risk. Somewhat lower but significant percentages cite a managed services model—which may reflect a misunderstanding of today's approach to managed services and their benefits (see figure 11).

Figure 11. Investments organizations are planning to make in the next 2–3 years to manage extended enterprise risk



The managed services approach extends beyond traditional "outsourcing" to encompass highly specialized services, solutions, technology and talent to address specific needs. Potential benefits include lower required investment and lower risk than in-house initiatives, as well as industry and domain experience and knowledge transfer. The approach can be particularly useful during a major change, such as a move to a new business or operating model, or in a rapidly evolving area, such as advanced analytics.

Cyber theme continues with concern over IT vendors

Organizational leaders see IT providers as the third parties that pose the greatest threat, with two-thirds of CEOs and almost as many board members ranking them in the top three—and at the top of the list. No other type of vendor comes close. Clearly, respondents' overall cyber risk concerns may be carrying over to third parties, likely due to increasing dependence on IT service providers. These providers can expose the organization to cyber threats. But because they're external, they're beyond management's direct control.

Our take

It's critical that IT vendor risk is effectively managed. But leaders should avoid a cyber-centric-only view of extended enterprise risk. Regardless of the type of vendor, leaders should take the time and care to create an ecosystem of vendors that can be trusted; understands the organization's goals; and fits its risk profile, risk appetite, and risk management program.

Conclusion: Applying a forward-looking approach to strategic risk

Strategic risks should be managed strategically. A foregone conclusion? Perhaps, but our survey results demonstrated that many organizations are not truly embracing this approach.

An enterprise-wide strategic approach to risk management recognizes the danger these risks pose to the execution of strategy and achievement of goals. It harnesses technology in the right manner—to identify, measure, and monitor these risks. It also provides timely insight for better decision support, keeps risk on the leadership agenda, and engages leaders in their management and oversight.

> In all cases, leadership should take a balanced approach.

Strategic risks can elude traditional approaches to risk and, when managed ineffectively, they can impair performance and destroy value. Traditional approaches tend to be risk-specific and siloed. They rarely account for the interrelatedness of risks and knock-on effects of risk events. And they can undermine decisions related not only to strategy, but also to the business model, value proposition, mergers and acquisitions, funding, expansion, and R&D decisions.

As this survey indicates, many organizations should consider enhancing their management of these risks. This may come down to obtaining new information to identify and monitor these risks, reordering priorities, or overhauling approaches to risk governance and risk management. In all cases, leadership should take a balanced approach. Just as no risk occurs in isolation, no one risk should skew leadership's attention and investments. Leadership should also follow through, developing the information and platforms needed to implement such an approach.

This report is designed to illuminate not only senior leaders' views of these risks, but also to identify areas that may warrant greater understanding and additional attention to these critical areas. Only then can leaders assess their current risk profile; exploit untapped opportunities; and prioritize investments aligned to strategy, business goals, and growth objectives. In addition, initiatives aimed at addressing these four strategic risks—brand and reputation, culture, cyber, and extended enterprise—can bring greater rigor to risk governance and management and heighten risk awareness throughout the organization.

Is your organization ready to take a strategic approach to risk management?

We encourage you to share the results of this survey with your executive team and your board. The answers to these questions, particularly when discussed frankly among leadership, can help your organization identify and prioritize efforts to manage complex, interconnected, and potentially damaging threats.

Questions to evaluate strategic risk preparedness:

- Do we recognize strategic risk as a higher order of risk—as a risk that can undermine the ability of the organization to implement strategy and achieve our goals?
- Have we developed and implemented a specific approach to identify, analyze, measure, monitor, and manage strategic risks?
- Is our approach to strategic risk balanced? Or do we focus heavily on the risk of the moment as identified by the media or regulators?
- Is management receiving the information needed to understand and address strategic risks? Is the board obtaining useful assurance that these risks are being identified and managed?
- Are we bringing together the right talent, processes, and technology-enabled platforms to address strategic risks?
- What steps have we taken to ensure that our leadership team and our organization are prepared to proactively address these risks?
- Are management and the board fully engaged in the plan for strategic risks? Do they conduct war-gaming and scenario-planning exercises?
- How prepared is our organization to respond to a strategic risk event, from the standpoints of communications, planning, recovery, and resiliency?
- How good are we at identifying and exploiting strategic risks to create and build—as well as to protect and preserve—value?

Deloitte.