The risky six

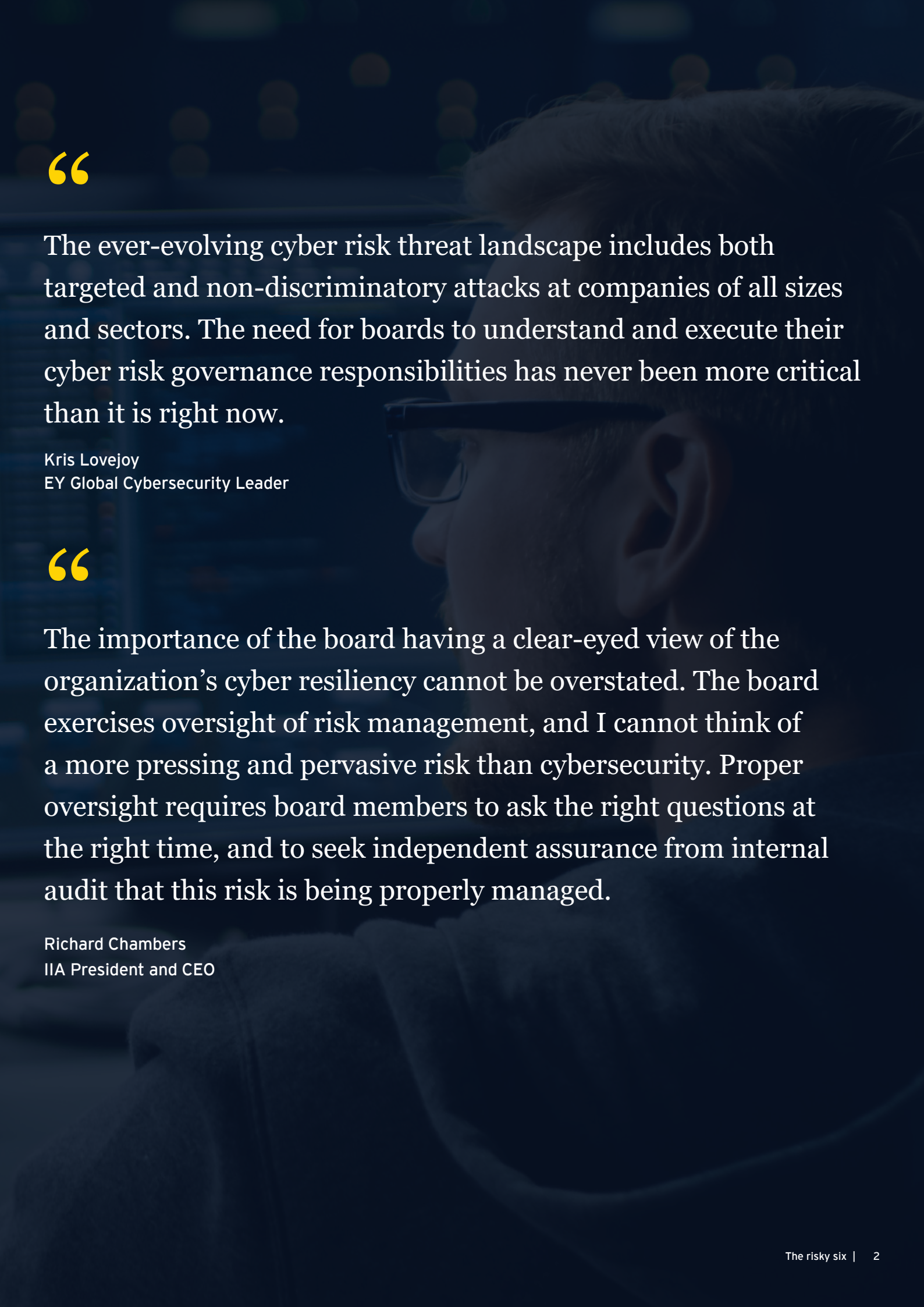
Key questions to expose gaps in board understanding of organizational cyber resiliency

EY
Building a better working world

The Institute of Internal Auditors

Contents

The risky six	03
Understanding risks one and two	05
Understanding risks three and four	07
Understanding risks five and six	09
Conclusion	10



“

The ever-evolving cyber risk threat landscape includes both targeted and non-discriminatory attacks at companies of all sizes and sectors. The need for boards to understand and execute their cyber risk governance responsibilities has never been more critical than it is right now.

Kris Lovejoy
EY Global Cybersecurity Leader

“

The importance of the board having a clear-eyed view of the organization’s cyber resiliency cannot be overstated. The board exercises oversight of risk management, and I cannot think of a more pressing and pervasive risk than cybersecurity. Proper oversight requires board members to ask the right questions at the right time, and to seek independent assurance from internal audit that this risk is being properly managed.

Richard Chambers
IIA President and CEO

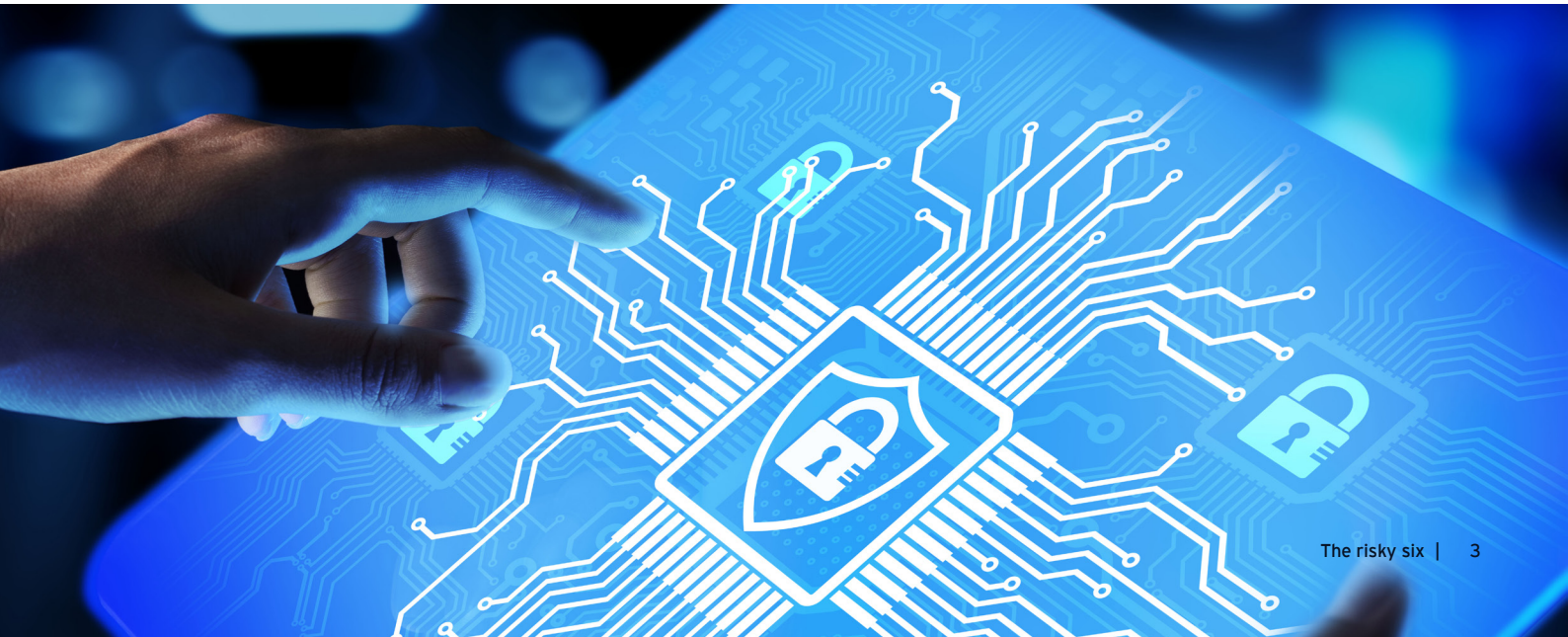
The risky six

A surprising phenomenon occurred in 2020. The unforeseen stressors of the COVID-19 global pandemic and a forced work-from-home (WFH) model exposed cybersecurity vulnerabilities in organizations around the globe as well as board and management overconfidence in the cyber resiliency of their companies. How could this happen in an age of acute cybersecurity sensitivity when boards have made the battle against cyberattacks a top priority?

The pandemic didn't create new vulnerabilities; it simply brought existing ones to light. It can be argued the fault is not on the boards or executive leadership alone, but in the fact every organization faces a myriad of ever-evolving risks. Yet, one thing is certain: the task of becoming and remaining cyber resilient is nearly impossible if boards do not have a clear-eyed understanding of their organizations' cybersecurity strengths and weaknesses.

Practitioners and researchers from Ernst & Young LLP or EY and the Institute of Internal Auditors (IIA) conducted extensive analysis to determine the root cause of how and why boards get a skewed picture of their organizations' ability to protect themselves from cyber-related risks. The team, which collectively has more than 100 years' experience managing cybersecurity risks within organizations in all industries, identified six key questions that if unanswered likely mean a disconnect exists.

The questions are rooted in the team's deep experience in the field, as well as cutting-edge research from EY and the IIA. The EY *Global Information Security Survey* (GISS) is greater than a two-decade-long examination of organizational efforts to safeguard their cybersecurity grounded in the firm's interaction with its global client base. The IIA's annual *OnRisk* survey, *EY Global Board Risk Survey*, *2020 EY Global Consumer Privacy Survey* and report combine the perspective of boards, executive management and chief audit executives (CAEs) about top-of-mind risks and provides in-depth analysis on how those views align and how that affects overall governance. Additionally, the IIA's annual *North American Pulse of Internal Audit* provides more than a decade of benchmarking data on risk assessments, audit plan allocation, and internal audit staffing and budgets.



The risky six

Review the following questions and ask if your organization can provide answers to all six with depth and understanding. If the answer is "no," to any or all of them, read further as a "no" to one question can greatly impact the responses to the others. The subsequent pages delve deeper into each question and explain how being able to answer each of them in the affirmative can help your board bridge gaps in their understanding of your organization's true cyber resiliency.

Six cyber questions every board should be able to answer "yes" to:

1. Has your organization conducted a recent enterprise-wide cyber risk assessment? □ **yes** □ **no**
2. Has your organization implemented a data governance program beyond basic classification? □ **yes** □ **no**
3. Have cyber risks and responses been incorporated distinctly into your crisis management program? □ **yes** □ **no**
4. Has your organization conducted a recent third-party and/or joint venture cyber risk assessment? □ **yes** □ **no**
5. Is cybersecurity included in the audit plan and/or is internal audit being leveraged as a tool to help your organization manage cyber risk? □ **yes** □ **no**
6. Is the effectiveness of cyber controls measured and reported in a consistent, meaningful manner? □ **yes** □ **no**

Understanding the risks

Question 1: Has your organization conducted a recent enterprise-wide cyber risk assessment?

For any organization, having a thorough understanding of the risks it faces is fundamental, and executing a sound risk assessment is critical. Because of the ubiquitous threat of cyber attack, boards must inquire about cyber risk assessments. Specifically, the board should ask several questions: In the past two years, has the organization conducted an assessment that identifies cyber risks related to people, processes and technology for all the business units, regions and groups? Have those risks been ranked based on impact should they occur and likelihood of them occurring as either inherent or residual risks? If so, who conducted the assessment — the CISO, the CAE, a third party engaged by IT? Did the assessment follow external guidance such as NIST SP 800-37 and CSF v1.1, COBIT 2019 (EDM03 and APO12) or ISO 31000? Is the CISO conducting periodic vulnerability scans and penetration tests and working with IT to resolve identified issues timely? If all of this has been done, how often are the assessments performed? When answers to these questions add up to a collective "yes," board members can begin to confidently say they understand the cyber resiliency of their organization.

However, data suggests most organization still struggle with cybersecurity. Results from the EY 2020 GISS report show 59% of organizations across the globe experienced a significant or material breach in the past 12 months. Additionally, one of the key findings in the IIA 2021 *OnRisk* report highlights critical knowledge deficits related to cybersecurity, data and new technology. Together, these data points suggest for most companies the collective answer to these questions is "no," and if the answer is "yes," too much time has gone by for the data to be useful to adequately protect the organization.

Why is the assessment question so important? Having this level of insight — a tailored and up-to-date understanding of the complete cyber risk profile of people, processes and technology — is the first step in understanding and managing the organization's cyber risk. Without it, efforts can be ad hoc and incomplete often only recognizing risk in more obvious forms. Take for example risks related to platform safety in the oil and gas industry. While personnel safety is critical and impact high, a major cyber incident can be just as financially impactful and much more likely to occur if management has not previously focused on mitigating that risk. If cyber is not included in a risk assessment, prioritizing efforts and reporting to a board on such risk management activities are often inaccurate. Having a clear and documented understanding of the impact and likelihood of cyber risks to your organization is a critical data set to properly manage and report on risk, yet it is something that many companies lack. EY professionals see this consistently while working with their clients across the globe, especially in industries where operational, health or environmental risks are present. These companies, mistakenly, often view cyber risks as secondary.

It seems simple to assess and document cyber risk. However, cost often is brought up as prohibitive, especially when it comes to the more technical assessments such as penetration testing. Cybersecurity typically is viewed as technical IT risks that require expensive specialized resources. While this is true in some cases, it is not in many others. Cybersecurity is as much business and process oriented as it is IT, and a simple cyber program or enterprise IT risk assessment is an ideal place to start the cyber risk management process. Such assessments identify IT and cyber risks throughout the business and prioritize them, providing a baseline not only to work from but also to report on. And with the constant evolution of the cyber risk landscape, it is recommended that such assessments be completed at a minimum every two years but preferably annually to remain relevant. Further, leading-class organizations are now embracing an ongoing risk assessment mindset. These assessments are considerably cheaper and more effective if performed by either internal audit or service firms and provide direction as to where more technical scanning or testing needs to be focused when finances permit.

EY Global Board Risk Survey reveals that only:

60% of organizations do not have a head of cybersecurity who sits on the board or at executive management level.

59% of organizations say that the relationship between cybersecurity and the lines of business is at best neutral, to mistrustful or non-existent.

So, after reading details on the first of the risky six, ask yourself: Does your company have this level of time-relevant granularity and understanding on how it goes about managing cyber risk? If not, this is the perfect place to start. Pick one of the better-known frameworks mentioned above, assess your organization and prioritize the risks. From there, the other five questions examined here will become much easier to answer "yes."

Question 2: Has your organization implemented a data governance program beyond basic classification?

Data privacy is a facet of cybersecurity where we've seen more confusion and immaturity than nearly any other. Just as Sarbanes-Oxley (SOX) emerged from trouble in the world of financial reporting, data privacy regulations are emerging from identity theft, rampant cybercrime, blithe sharing of information by companies and malicious use of that information. Almost in partnership with those troublesome realities is the lack of uniformity in national or provincial data privacy regulations. A confusing profusion of such regulations already exist, including the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), Argentina's Personal Data Protection Act (PDPA) and Brazil's General Data Protection Law. At least 10 US states are expected to follow California's lead soon with their own comprehensive consumer privacy regulations. Even countries within the EU have enacted additional regulations, such as Germany's Federal Data Protection Act.

This has created a compliance nightmare directly connected to cybersecurity risk. The trouble is most organizations outside of retail and healthcare typically adopt only basic data classification policies to govern internal handling/sharing, if that. Even more disturbing is the number of companies that are unaware of the type and location of sensitive information within their environments. This is especially concerning if they are subject to any of the above-mentioned regulations, some of which carry hefty noncompliance penalties as high as 4% of a company's annual revenues. Two of the key findings within the IIA's *OnRisk* report are directly related to data and its relevance in overall risk management. Additionally, the team of EY professionals consistently identify data privacy and related evolving legislation to be among the most transformstive types of cyber risks companies face, particularly in a post-pandemic work-from-home environment.

Being able to answer "yes" to question one above is important because it calls out the type of data at risk or that potentially requires compliance. It should be viewed as a first step. However, if no additional action is taken or no refresh or routine validation is performed, the likelihood of a data-related incident or breach remains high. In other words, if your company can answer "yes" to question one, but "no" to question two, there is still a great deal of risk present and much work to be done.

Just as in question one, budget and cost are often cited as obstacles to implementing a more robust data governance strategy. But just as with cyber risk assessments, sound data governance can be accomplished with support from internal audit or a third-party service provider, even as a carve-out effort done in unison with the risk assessments used to arrive at a "yes" for question one. Once the type of data needing protection has been identified, it is much easier to configure a technical scan to locate that data within an organization's environment.

Boards and executive leadership know cybersecurity is not a quick fix or one-solution-cures-all issue, but having a synchronized, documented and logical approach to data management instills appropriate confidence in boards and stakeholders alike. You're probably starting to see how these disconnects exist even with just these two questions. But to arrive at true confidence and understanding of an organization's resiliency, there are still more questions to answer.

Understanding the risks

Question 3: Have cyber risks and responses been incorporated distinctly into your crisis management program?

The most requested cybersecurity or IT internal audits seen by practitioners are for IT disaster recovery or cyber incident response. These audits have identified that cybersecurity is often not included in organizations' overall crisis management plans. Companies are rapidly realizing this is a major gap. Traditional incident response plans enable IT to recover or continue operations during or following a major weather event or other non-cyber-specific disasters. However, responding and recovering from a sophisticated cyber incident may require an entirely different set of activities and people. As such, cyber risk should have its own crisis management plan. Lacking a formalized plan can greatly reduce an organization's ability to respond and recover from such an event. Various kinds of disruptions (e.g., cyber, IT, natural, internal) should be identified and include their own playbook and routine tabletop exercises and testing for effectiveness.

Overconfidence from boards relating to this question is understandable. Business continuity planning and disaster recovery (BCP/DR) is a notion that has been around for decades and frequently includes IT in the context of redundant data centers, backups of critical data and more. Some CIOs even take the position that disaster prevention is the best strategy for business continuity. However, disaster prevention is not possible nor is it an appropriate response to business continuity and disaster recovery.

If humans could prevent disasters, there would be no need for disaster recovery programs, and while that would be nice, it is not realistic. Another problem with that approach is modern business relies heavily on third parties, and what happens within those organizations is often uncontrollable.

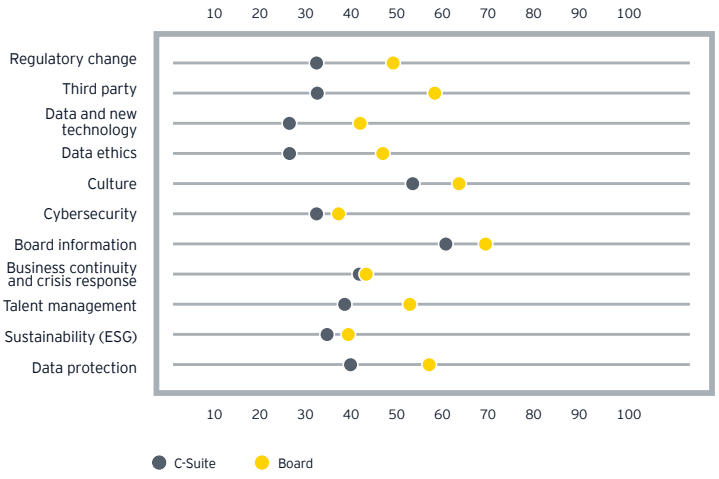
Another benefit of a thorough risk assessment (question one) is they can determine if gaps in disaster planning exist and identify what elements should be added to create a robust and complete crisis management plan that includes cybersecurity. Two common findings identified in assessments for questions one and two are:

- A lack of a business impact analysis of critical IT systems
- Not having the impacts of a data breach quantified

Without these, even basic incorporation of IT into crisis management strategy is ineffective. This is why it is important to be able to answer each question. Missing or skipping questions leads to weaker answers for the subsequent questions.

EY practitioners consulted for this article estimate more than three in four organizations that have performed cyber assessments answer "no" to questions one and two, yet most had disaster recovery programs that led their board to believe their organization would recover quickly from a cyber incident. This misplaced confidence in IT disaster recovery or cyber incident response is an example of board misalignment on major risks. Indeed, overall board misalignment on risk was one of the key findings in the IIA's 2020 *OnRisk* report (see Figure 1 below).

Figure 1: Organizational risk capability: board and C-suite perceptions



Question 4: Has your organization conducted a recent third-party and/or joint venture cyber risk assessment?

It is rare to find an organization that doesn't engage with third parties in some way. To everyone's defense, there is usually a contract arranged and signed by each party agreeing to terms that work for everyone involved — otherwise, why would they sign it? Unfortunately, this is where the praises end and the problems begin.

Once contracts are signed, they are rarely looked at again, and compliance to terms is not routinely checked unless mandated by a compliance-driven factor such as SOX reporting. Rarer still are routine checks to see if any new regulations, such as the ever-changing data privacy regulations mentioned in question two, should be incorporated into them. In addition, engaging third parties is often department specific, and IT is not always involved. This can lead to concerning gaps in cybersecurity. The *2020 EY Global Consumer Privacy Survey* reports 36% of organizations have had a data breach caused by a third party over the past two years with this trend on the rise in the remote working model. A massive contributor

to this is the lack of routine compliance checks. It is safe to assume third-party contracts do not allow breaching of one another's data, yet it happens constantly.

Third-party cyber risk assessment could be included in an organization's overall cyber risk assessment (question one), but it is such a large, important and complex component that it deserves to be called out as a stand-alone question and may require more frequent visitation depending on the rate of new third parties engaged by your organization. The IIA examined third-party relationships as 1 of 11 key risks in its 2020 *OnRisk* report (see figure 2 below). It found board respondents were generally more optimistic than executive management and CAEs about their organizations' ability to managing third-party risks.

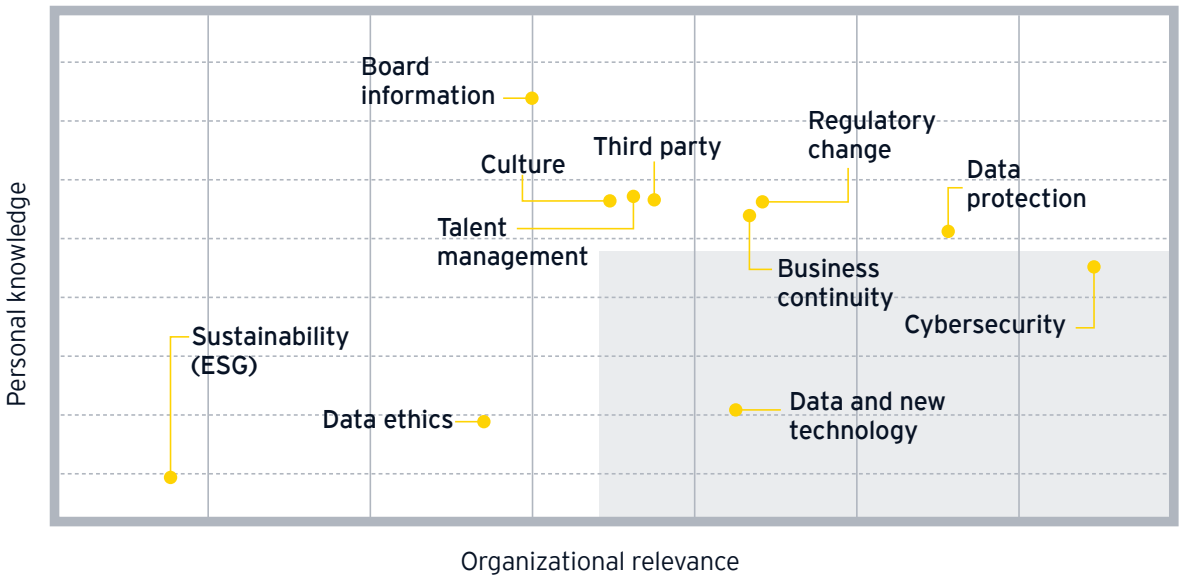
"This misalignment may stem from boards having a limited understanding of where and how organizations depend on third parties. Further, this misalignment may be fueled by the dangerous misconception that outsourcing processes includes the transfer of risks related to those processes," according to the *OnRisk* report.

Organizations with mature or sophisticated approaches to third-party contracts often mandate IT and/or security functions be involved in the entire life cycle of third-party engagements. However, getting to this level is not possible without assessing the risks specific to the third parties each organization is exposed to. The initial cyber assessment and risk documentation discussed under question one would likely highlight gaps, but a deeper dive into the organization's third-party relationships and the activities and data associated with each is the only thing that can enable architecting a proper risk management strategy.

> "The company overall needs to see the bigger picture and keep the bigger risks in the forefront of their mind. It's hard for departments to see beyond daily, weekly, and monthly functions.
>
> **Board Member, Global Technology Company**

Fortunately, there is plenty of guidance on this topic, so no one needs to start from scratch. The NIST CSF is probably the most straightforward place to start, specifically ID.GV-4, ID.RA, ID.RM, and ID.SC-1. So, if the answer to this question for your organization is an obvious "no," a look into this guidance is a great starting point to build toward an answer of "yes."

Figure 2: Personal risk knowledge risk relevance comparison, IIA OnRisk Report



Understanding the risks

Question 5: Is cybersecurity included in the audit plan and/or is internal audit being leveraged as a tool to help your organization manage cyber risk?

According to the *2020 EY Global Consumer Privacy Survey* report, 46% of boards involved in the study have engaged a third party to review the effectiveness of their organizations' cyber risk management program, 14% have not but intend to within the next 12 months, and 39% have not engaged a third party nor do they intend to.

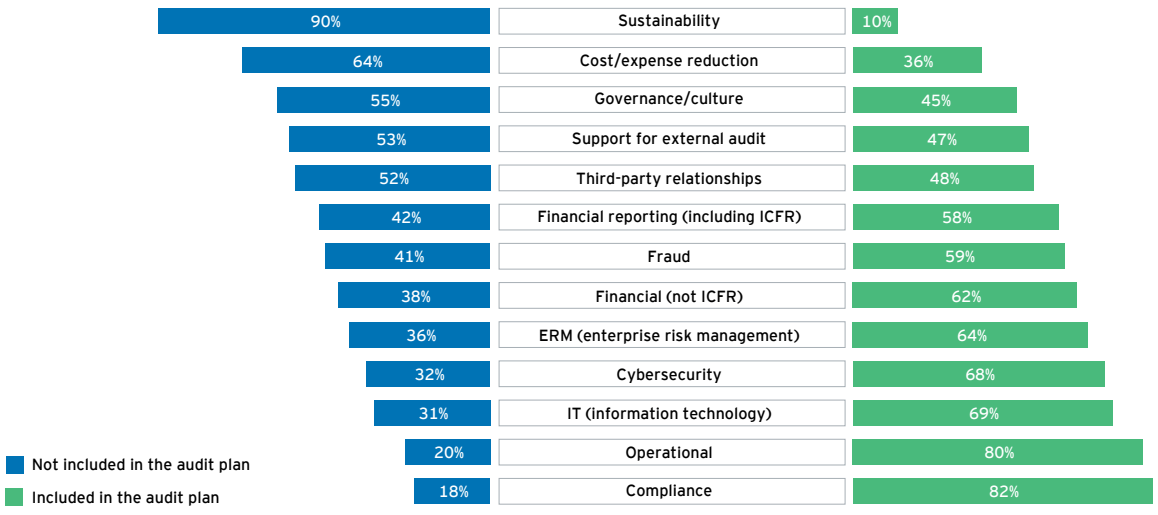
Though not specifically cited in responses to this question, cost is likely a factor for the 4 in 10 boards that have not engaged and have no plans to engage third-party services. As previously stated, cost is often cited for not being able to answer "yes" to many of these questions. Yet cost doesn't have to be an impenetrable barrier to improve cybersecurity. While engaging specialized third parties in many cases is the best course of action, an enormous amount of work can be done internally. This not only can reduce the cost of engaging a third party but also greatly improve that partnership if the need does arise in the future.

Question three addressed the frequency of requests for audits pertaining to IT/cyber disaster recovery—yes, audits. The group of practitioners involved in writing this article report they have seen cybersecurity-related audits grow from a rarity to a fixture. Just five years ago, only a select few organizations were doing such audits, but in the group's current portfolio of global clients, **every single one** has cyber built into its audit plan in some way or another. With IT audit-related expertise required in internal audit groups, boards are starting to recognize the crossover of skillsets applicable to some of the more non-technical cyber needs within organizations – and using it to build their understanding of their organization's cyber resiliency.

Growing understanding of the complexity of cyber resilience is reflected in risk rankings by CAEs in the IIA's annual *North American Pulse of Internal Audit* report. Between 2016 and 2020, cybersecurity, IT and third-party relationships ranked as the top three risks rated as "high" or "very high" by respondents. While the anecdotal evidence from EY practitioners is encouraging, *Pulse* data does not reflect whether the concern over cybersecurity, IT and third-party relationships has translated to significant allocation of internal audit resources in those areas. Audit plan allocation data for the same period shows IT holding steady at 9%, cybersecurity growing from 6% to 8% and third-party relationships mired at 4%. Even more troubling is data from the 2020 *North American Pulse of Internal Audit* found a disturbingly high percentage of internal audit functions did not plan to devote any audit plan allocation to cyber (32%), IT (31%), and third-party relationships (52%) in the ensuing 12 months (see figure 3 below).

This clearly mixed response to key components of cyber resiliency may reflect that some boards do not recognize or are not fully embracing internal audit as a resource in building their organizations' cyber resiliency. Leveraging internal audit as a tool to understand and help manage cybersecurity risk is an enabler that will help organizations answer "yes" to all six of the questions in this article. Based on what we are seeing in the marketplace, organizations that aren't doing this are often the ones with significantly less maturity in the cyber space.

Figure 3: Risk Coverage in audit plans (all respondents)



EY Global Board Risk Survey reveals that only:

20% of boards are extremely confident that the cybersecurity risks and mitigation measures presented to them can protect the organization from major cyber-attacks.

36% of organizations say cybersecurity is involved right from the planning stage of a new business initiative.

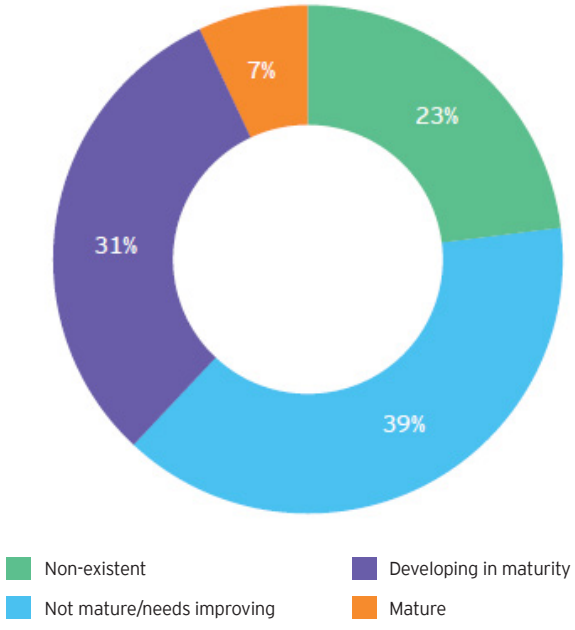
Question 6: Is the effectiveness of cyber controls measured and reported in a consistent, meaningful manner?

Answers to the preceding five questions for your organization may be a mix of "yes" and "no." Maybe the answers are "yes" to all, but if cybersecurity is not reported in an industry-accepted, standard way, the measurement can be lost or even become inaccurate and misleading.

According to EY's 2020 *Global Information Security Survey* results, only 7% of organizations report they have the ability to financially quantify the impacts of breaches (see figure 4 to the right). If such a small fraction of organizations can quantify the impact of cyber breaches, it stands to reason few can quantify the value of effort spent managing the risk. If neither are quantified, neither are reported with much granularity.

To our dismay, the answer to question six, for most organizations, is a relatively strong "no." This is of limited fault of any board. The true task of cybersecurity risk management at an enterprise level is tremendously complicated. It is an ever-changing, evolving and moving target. But arriving at a "yes" for these questions and building routines to instill assurance the answers will remain "yes" is the minimum a company should do to get a true idea of where its cyber resiliency stands.

Figure 4: Shortfall in security leaders' ability to quantify the financial impact of cybersecurity breaches



Conclusion

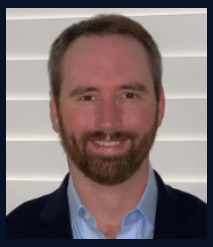
Organizations working toward a "yes" for any of these questions provides a narrative that is well received by stakeholders inside and outside the organization. It highlights the due care and diligence underway to battle cyber risk. However, it is plain to see how easily boards can develop false confidence if any of these six questions can't be answered in the affirmative.

EY Authors

Kris Lovejoy
Partner
Consulting
Ernst & Young LLP
kristin.lovejoy@eyg.ey.com

Lisa Hartkopf
Partner
Consulting
Ernst & Young LLP
lisa.hartkopf@ey.com

Matthew Randolph
Partner
Consulting
Ernst & Young LLP
matthew.randolph@ey.com



Austin George
Manager
Consulting
Ernst & Young LLP
austin.george@ey.com

IIA Authors

Richard Chambers
IIA President and CEO

David Petrisky
IIA director, professional practices (IT)

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

2102-3720723
ED None

ey.com