Governance Insights Center

Overseeing cyber risk: the board's role

Cyber risk management is no longer just about preventing breaches. A good program can also help a company get back on its feet and mitigate financial and reputational damage when a breach occurs. How do you know whether your company is doing all it should?

January 2024

pwc

Cyber threats are everywhere, and breaches make headlines on what seems like a daily basis. They also cost companies, in both dollars and in reputation.

The threat environment is becoming more complex with an increasing number of threat actors, including nation states, using new and more sophisticated tactics. Ransomware attacks continue to rise and make global headlines as threat actors' level of sophistication rises, and ransom demands become higher and higher. The proliferation of attacks is partly driven by the development of ransomware-as-a-service model that lowers barriers to entry and offers criminal clients help desks for support and professional negotiators. Add to this that the corporate world embarked upon a rapid digital transformation and many employees started working remotely over the last few years, increasing companies' digital footprint — and their cyber risk profile.

At the same time, expectations have risen. Even with a robust risk management program, a company may suffer a cyber breach or attack. Stakeholders demand that companies do everything in their power to protect consumer data and to recover quickly from a breach or critical disruption. And don't forget — data security and privacy are part of the "S" and "G" of ESG — an area of heavy focus from multiple stakeholders these days. Regulators have a heightened focus as well, with both the Cybersecurity and Infrastructure Security Agency (CISA) and the SEC issuing new rules related to cyber disclosures and incident reporting.

Addressing cyber risk may be a challenge for nearly any company and its board. While boards are more engaged in overseeing cyber today, it's still a complex, technical area with emerging threats occurring almost weekly. Most board members are not cyber experts, yet boards have an obligation to understand and oversee this significant risk. They need active engagement with leadership, access to expertise, and robust information and reporting from management.

This report outlines four key areas in which boards should take action to support their companies in establishing effective cybersecurity risk management programs.

49% of directors see cybersecurity as a significant oversight challenge

Source: PwC, *2023 Annual Corporate Directors Survey,* October 2023.

Table of contents

1. Work with management to embed cyber risk in strategic decisions — and the company's culture

Many strategic decisions have a cyber risk component. For example, adopting new technologies to innovate or better enable and connect a remote workforce changes the company's cyber risk profile. Cyber has to be a consideration when, for example, changing operations, entering new markets, developing new products and services, and when making acquisitions. It also should be considered when vetting what third parties the company partners with to both produce and distribute products and services. All of these scenarios can add cyber risk, particularly if the company is sharing personal information.

Of course, we should not forget the flipside — cyber can present opportunities for the organization and differentiate it in the market.

While the heavy lifting is done by the IT team, cybersecurity needs to be built into the culture of the organization. It is everyone's responsibility. To tackle cyber risk, the board of directors, CEO, management, business unit leaders, and the IT and security groups all need to address the cybersecurity implications of their business decisions and activities. The company's efforts to address cyber risk need to be coordinated and collaborated throughout the organization.

There's also another important group: the company's rank and file employees. They support IT security when they follow company policies, standards, and procedures, get training, and report suspicious activity. Messaging from senior leaders in the company should underscore the importance of being a cyber-aware organization and the critical role that employees play.

Next steps

- Give the chief information security officer (CISO) a seat at the table when addressing strategic decisions and the company's plan.
- Get metrics on the effectiveness of employee training and awareness for cyber risks as well as the remediation efforts for those that do not comply or lack understanding of the risks.
- Ask others outside of the CISO, like business unit and other functional leaders, how they address cyber risk in their departments and key product and service offerings.

2. Understand the cyber risk management program

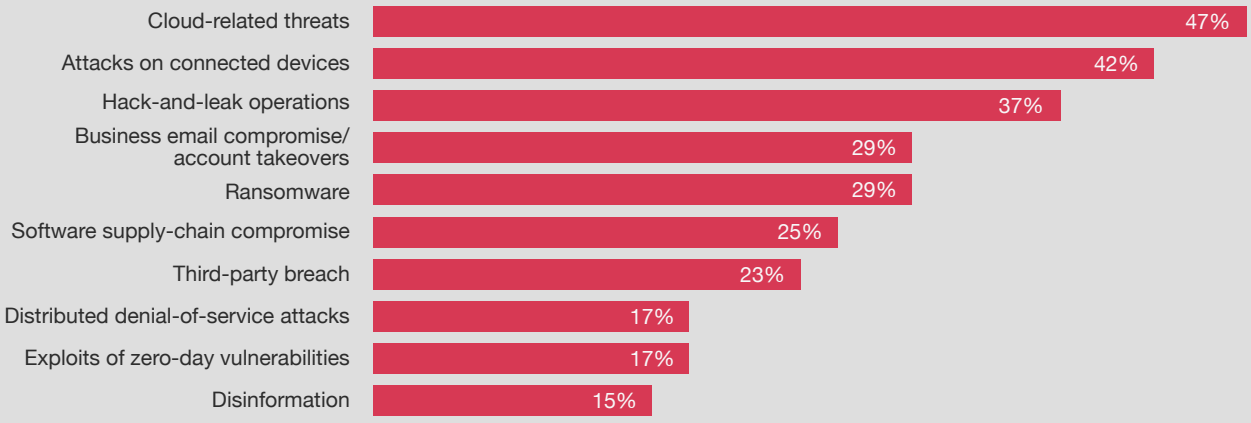
Boards want to know whether management is focusing on the right cyber risks, how management is addressing those risks and whether it's enough. This starts with understanding the company's cyber risk management program and cyber risk appetite.

Understand the company's risk posture

To do this, directors need to know the company's key cyber risks. Who are the main threat actors? What are their motives? What are they targeting and what is the potential business impact? Knowing this information can help zero in on the critical assets that need to be protected, identify potential vulnerabilities at the company and clarify the right steps for management to take to address them. Directors should understand first how the company is identifying the top risks and how that process is aligned with any existing enterprise risk management program. Next, directors should ask how management is mitigating these risks through implementation of processes and controls. What protections does the company have in place, and does the company layer those protections? More CISOs today are identifying metrics and quantifying cyber risks for better decision-making. These activities are helping to prioritize the most important cyber risks and aligning capital allocation needs against those risks. They help to make sure that cyber budgets are allocated to the most impactful areas for the company. Cyber risk quantification is an important area for organizations as their cybersecurity programs evolve.

Everything is connected, including cyberattacks

Top perceived cyber threats over the next 12 months



Q: Over the next 12 months, which of the following cyber threats is your organization most concerned about? (Ranked in the top three).

Base: All respondents = 3,876

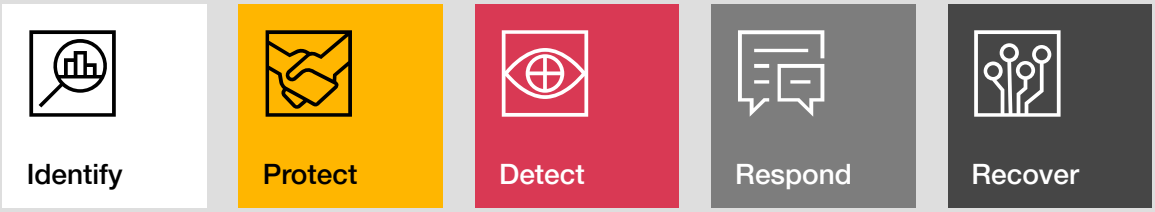
Source: PwC, 2024 Global Digital Trust Insights.

Ultimately, the level of cyber risk has to fit within a company's risk appetite. Some companies may draft formal cyber risk appetite statements. Even for companies with less specific or formal cyber risk policies in place, it's important for the board and management to be aligned on the scope of cyber risks and how they fit into the company's broader risk appetite.

Boards should also understand how the company's cyber program stacks up against a standardized framework such as the *National Institute for Standards and Technology Cybersecurity Framework (NIST CSF).* Directors will want to understand how management is leveraging a framework as a risk management tool. For example, directors should ask where there are gaps and how those gaps are being closed as part of enhancing the company's capabilities and maturity of the program. Many boards also receive information on how the company's maturity benchmarks against peers and the industry to understand any related risks that need to be addressed.

The NIST CSF is a widely-recognized and accepted set of guidelines and practices for managing and reducing cyber risk. It provides guidance on how directors can engage with company leadership around this critical issue.

The NIST CSF is organized into five "functions"



Refer to *A board's guide to the NIST Cybersecurity Framework for better risk oversight* for more information.

Cybersecurity risk assessment programs — what should directors know?

Regulators, investors and other stakeholders are seeking greater transparency as to how a company addresses its cyber risks. The SEC's new cyber disclosure rules, adopted in July 2023, will require companies to provide a description and other details about how they assess and manage their cyber risk. The new disclosures will significantly expand the information that companies provide today in this area. As companies get prepared for the expanded disclosures, the board can ask the CISO the following questions to better understand the company's process:

- Who in the organization "owns" the cybersecurity risk assessment program and who plays supporting roles? Who is responsible for managing operational technology cyber risk?
- How often is the assessment updated? Is it top-down or bottom-up? (ideally, the assessment should include both approaches)
- Does the third-party vendor/supply chain due diligence program include an assessment of cyber risk?
- Are there any risks that didn't make it on the assessment that should be included?
- Is the CISO comfortable that the security organization has the budget and resources to effectively execute on the risk assessment?
- How often does an external party assess the maturity of the cyber risk management program? If done, what were the most recent findings? What's being done to remediate any gaps?

Common cyberattacks

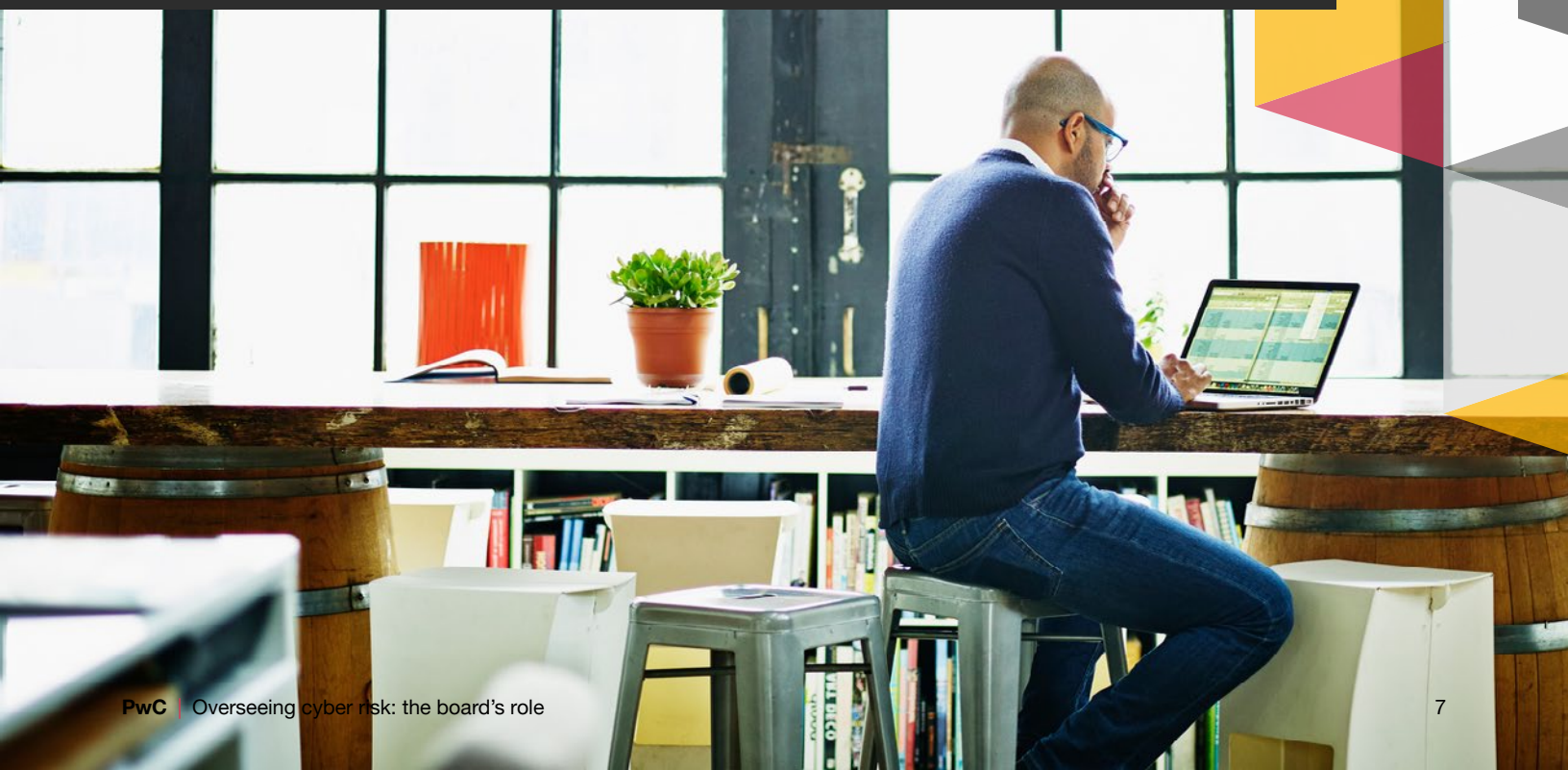
With rising cyberattacks, cloud breaches and social engineering schemes, below are the common ways that threat actors are launching their attacks.

Email: Spear phishing and business email compromises remain effective methods as employees/users fall for lures. Training and awareness of fraudulent campaigns for employees, contractors and third parties can help protect a company.

Software supply chain compromise: This refers to exploitation of a known vulnerability in a widely used piece of software that provides extensive access to systems within a network. Commercial and open source software can be targets. Companies will want to have an extensive software asset inventory and a "software bill of materials," which describes components in a piece of software, that enables them to quickly identify where to patch and monitor for impacted systems.

Account compromise: This refers to using brute force methods or credentials obtained from an external source. Threat actors are often successful due to the lack of use of multi-factor authentication by companies.

Ransomware: Ransomware is a major and growing danger, against which a company should strengthen defenses and develop an incident response plan along with an associated playbook for addressing a ransomware attack right now. Ransomware criminals are multiplying, attracting new cyber talent, innovating malware and acting with impunity. Leading companies are investing in cyber resilience capabilities that limit the potential impacts of ransomware and enable more effective recovery techniques.



Get the reporting you need

Cyber reporting to the board should be in jargon-free language so the board can easily get a snapshot of what's going on. Too often the chief information officer (CIO) or CISO provide the board with lengthy, detailed presentations that provide limited insights, and the format of these presentations change so it is hard for the board to get a consistent picture of what is happening with the cyber program. Board reporting will want to highlight how investments lead to cyber risk reduction.

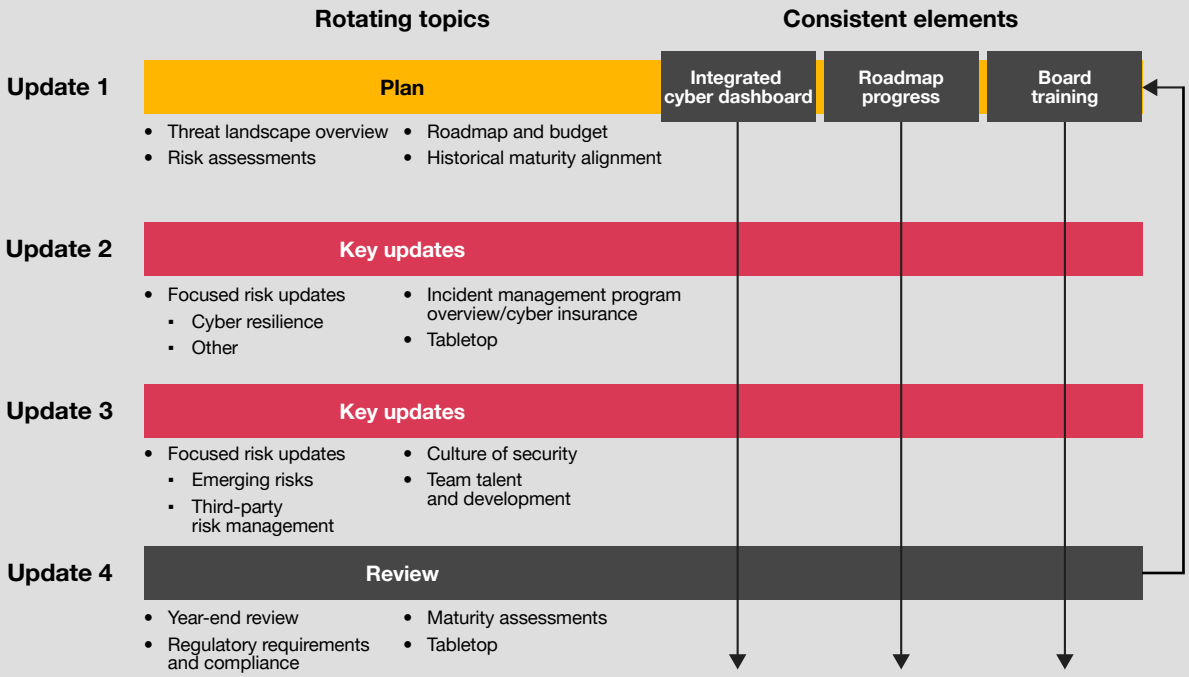
Many boards today are getting a cyber scorecard that can help address some of these concerns. A cyber dashboard or scorecard prepared by the CIO or CISO can help the board assess current risks and track progress. Clearly identified and quantified cyber-related metrics, as well as a consistent format, may help the board spot any trends that show the company improving or falling short relative to key risks.

Common elements of cybersecurity board reporting

- Multi-year strategic plan and current year business plan
- Cybersecurity resource allocation — funding and staffing
- Periodically updated inventory of mission critical systems that need to be protected
- Summary of key cyber risks impacting the company
- Dashboard or scorecard highlighting key cyber risks and metrics to address these risks
- Significant security incidents at the company
- Training and awareness program for employees
- Maturity assessment against a recognized framework (e.g., NIST)
- Third-party cyber risk management program
- Industry benchmarking against peers
- Significant legal and regulatory developments
- Incident readiness framework, including summary of the cyber insurance policy
- Lessons learned from external events in the market

Boards should also be getting information about the multi-year strategic plan, current year business plan, resources, cyber training program and other information about the company's cyber activities to get a holistic view. One way to do this is to have management take the board meeting dates for the year and map out what cyber board updates will be allocated to each session.

Annual cyber calender example to aid in oversight



Stay on top of legal and regulatory developments

As the threat and impact of cyber incidents grows, legislators and regulators have been active in trying to address this pervasive risk and its impact through regulation. Today, nearly all US states and many countries require entities to notify affected individuals of a security breach involving their personally identifiable information.

Both the Biden administration and the SEC have taken action recently. The SEC's 2023 cyber disclosure rules require more timely reporting of material cyber incidents and more specific risk management, strategy and governance disclosures. Also, the White House issued the Cyber Incident Reporting for Critical Infrastructure Act in 2022. Similar to other areas that require compliance focus, the board will want to understand how laws and regulations on data privacy and cybersecurity are changing, how the company is impacted and how management is tracking compliance.

Keeping up with regulations

SEC cyber disclosure rules finalized

The SEC approved new *cybersecurity disclosure rules* in July 2023. These *rules will require* more disclosure from public companies and in more places, compared to what's historically been provided. As part of the new rules, companies will have to disclose material breaches via a Form 8-K filing within four business days of determining an incident is material. The rules also will require companies to describe in their annual 10-K filings a description of their policies and procedures for the identification, assessment, and management of cyber risks and their governance processes. This includes the board's oversight of cyber risks and how the board is informed about cyber risks. Refer to Appendix A for more information.

Cyber Incident Reporting for Critical Infrastructure Act of 2022

Cyber Incident Reporting for Critical Infrastructure Act of 2022 *("the Act")* was signed into law in 2022, representing a step forward from the ad hoc, industry-specific voluntary disclosures that existed. For companies defined in critical infrastructure sectors, the Act will require that they report significant cyber incidents within set timeframes, offering protections to incentivize the reporting. For more information, see *Cyber breach reporting to be required by law for better cyber defense*.

Ask others for input

Most organizations have an enterprise-wide risk management program and cybersecurity should be part of it. Various groups in the company will be thinking about, reviewing and reporting on aspects of cyber risk. Boards will want to understand how those groups work together to have one integrated approach and avoid any risk silos.

Boards should also be hearing from groups such as internal audit about cyber risks. Many companies leverage the internal auditors to review cyber processes and controls, including resilience and response. External auditors can also provide a perspective on cybersecurity controls related to financial reporting processes.

Many boards seek external perspectives on the company's cybersecurity program for assurance on its maturity and the company's key risks. They want to hear a view independent from management. Oftentimes, management will hire external advisors to conduct activities like penetration tests, a cyber program maturity assessment or "red team" testing through which an unannounced ethical hacking takes place. This is an opportunity for the board to ask questions directly of these advisors and hear external advisors' unvarnished views.

Be transparent with stakeholders

As with many other areas of high risk, investors, regulators and other stakeholders are clamoring for more visibility into companies' strategy and risk mitigation plans for cybersecurity. Companies and boards can build trust with multiple stakeholders through greater transparency.

Interest in understanding more about a company's cyber risk management program and the board's oversight role goes beyond investors. Large proxy advisors are also starting to weigh cyber risk management into their governance ratings. These advisors are looking at public company disclosures for information security risk oversight data.

Next steps

- Understand the key cyber risks to the organization and how the executive team is managing these risks.
- Ask for cyber risk to be quantified to enable better risk prioritization and capital decisions.
- Understand how cyber risks fit within the company's risk appetite.
- Understand whether the company uses a standardized framework (e.g., NIST CSF) to benchmark its security program, and if so, how gaps are being closed.
- Discuss with management the need for external perspectives (e.g., third-party assessments for key risk areas, leading practices based on your industry and company size) and ask that findings be reported directly to the board.
- Take a fresh look at the board's cyber reporting and get consistent and holistic information to help the board make decisions.
- Understand significant new laws and regulations in the cyber/privacy areas and their impact on the business, and get updates on how the company is staying up to date with and meeting those requirements.
- Consider the transparency of cyber disclosures and the information that will need to be provided with the finalization of the SEC's cyber disclosure rules, and discuss with management how gaps are being addressed to meet the new requirements.

3. Monitor cyber resilience

Even with a robust risk management program, there still can be a successful breach and boards should focus their attention on resilience plans. The ultimate objective of resilience planning is to be able to detect and respond to cyber threats quickly to minimize business disruption and financial losses. A key to recovery is protecting the company's critical systems. This means limiting potential damage to systems from a cyber event and ensuring systems can recover from a cyber event.

Being well-prepared for a cyber crisis is critical. Boards will want to see that the company has documented crisis management, incident response and disaster recovery plans and that management periodically tests these plans through tabletop exercises. A focus on clear roles and responsibilities to reduce management's decision-making during a crisis event is the goal of these exercises. Another top focus is understanding the key provisions of the cyber insurance policy, importantly, what the policy does and doesn't cover. As this is a new model for many insurance companies and it is maturing, expect to see changes in policy coverage and premiums. Read *What you need to know about cyber insurance* for more details.

The SEC's 2023 cyber disclosure rules require that companies disclose a material cyber incident within four business days after determining that the incident is material. This short time frame spotlights the need for companies to have a robust process and framework in place for determining materiality of a cyber incident and escalating that decision in the company, when appropriate. The CISO, chief financial officer (CFO) and general counsel (GC) should weigh in on the quantitative and qualitative factors for assessing materiality. Boards will want to weigh in on the factors and process, particularly focusing on timely reporting of appropriate incidents to the board and to whom on the board this information will be reported.

Disclosure committees at the management level are used to address both the standard accounting and reporting disclosures and those arising from significant business and economic developments. With the SEC's new cyber disclosure rules requiring material incidents be disclosed in a Form 8-K filing, the board will want to understand how the CISO is connecting and engaging with the disclosure committee (or a member of it) to meet the new reporting disclosures.

How are companies thinking about materiality?

The SEC's focus on material cyber incidents isn't new — it was featured in the 2011 and 2018 guidance. And the definition of materiality hasn't changed; it's the same definition as securities law — what would a "reasonable investor" want to know. To apply this standard in the context of a cyber incident, companies should be prepared to conduct an objective analysis of both quantitative and qualitative factors, including evaluation of an incident's impact and reasonably likely impacts.

For more discussion on cyber incidents and materiality determination, refer to *Making materiality judgments in cybersecurity incident reporting*.

In addition to the broad questions the board should ask about resiliency, specific to a cyber breach, boards will want to:

- Understand how often back-ups are made of data in mission-critical systems and whether management tests those back-ups. Doing so helps the company get back to business operations more quickly in the event of a ransomware attack when systems are encrypted by a threat actor.
- Consider whether adequate resources are allocated to both protecting systems and to responding and recovering from breaches.
- Work with management to engage the right experts in advance of any event occurring. For example, companies will need someone familiar with security breaches, they may need an expert for negotiating with a threat actor, and they can benefit from having established relationships with government authorities (e.g., the FBI).

For a more in-depth discussion on crisis response plans, including broad questions for the board, read *Being prepared for the next crisis: The board's role*.

Next steps

- Oversee documentation of the company's incident response plan and understand how often it is tested by management.
- Participate in or get feedback on management's testing of the incident response plan.
- Discuss the company's internal escalation procedures for the reporting of an incident, including who will be engaged to assess materiality and ultimately how appropriate incidents are escalated to the board.
- Understand how the company is tracking immaterial incidents to identify potential related incidents. Note that the final SEC cyber rules require that events that are related — for example, the same malicious actor or that exploit the same vulnerability — be disclosed if a company determines they're material in the aggregate.
- Make sure management is maintaining contemporaneous documentation supporting the assessment of material and immaterial cyber incident decisions.
- Make sure the CISO is included in the company's disclosure controls and procedures process.
- Discuss lessons learned from other public security breaches with management and whether the incident response plan is updated for these learnings.
- Ask how the CISO collaborates with peers and competitors to understand the latest threat risks and resiliency issues for the industry.

4. Rethink the board's cyber oversight allocation

By now, all boards have allocated cyber risk oversight somewhere — either to a committee or the full board. But boards periodically should reassess their allocation to determine that it is effective. Current survey data indicates that 51% of S&P 500 company boards allocate responsibility to the audit committee. Given all the audit committee has on its agenda these days, boards should consider whether this committee has adequate time and the right skills to oversee this area. Some boards have deemed cybersecurity oversight a full board responsibility, taking it out of committee, while other boards have allocated this responsibility to a separate technology or cyber committee. However, only a very limited number of boards have these separate standalone committees. No matter where oversight sits if at the committee level, it's important that the full board gets regular and comprehensive updates.

The 2023 SEC cyber disclosure rules require disclosure of the board or committee responsible for oversight and the process for those board members to be informed about cyber risks.

With the increasing concern about cyber risk, many boards are engaging with the CISO (or other executive, such as the CIO or whoever is tasked with managing the company's cyber program) on at least a quarterly basis. This is a shift from the once-or-twice-a-year frequency of reporting that was common just a few years ago. Some boards today are also implementing private sessions with the CISO where they can ask about support from management and even adequacy of resources. The board should confirm it has adequate touchpoints with the CISO.

With the technical nature of cybersecurity and the evolving risk landscape, it's important that the board has the skills and expertise needed, or has access to skills and expertise, to oversee this area. The question of whether boards should fill a director seat with someone who has cyber skills is one that is determined by each board based on the company's industry and risk profile. While this decision may be appropriate for a particular board, it poses two risks to be mindful of:

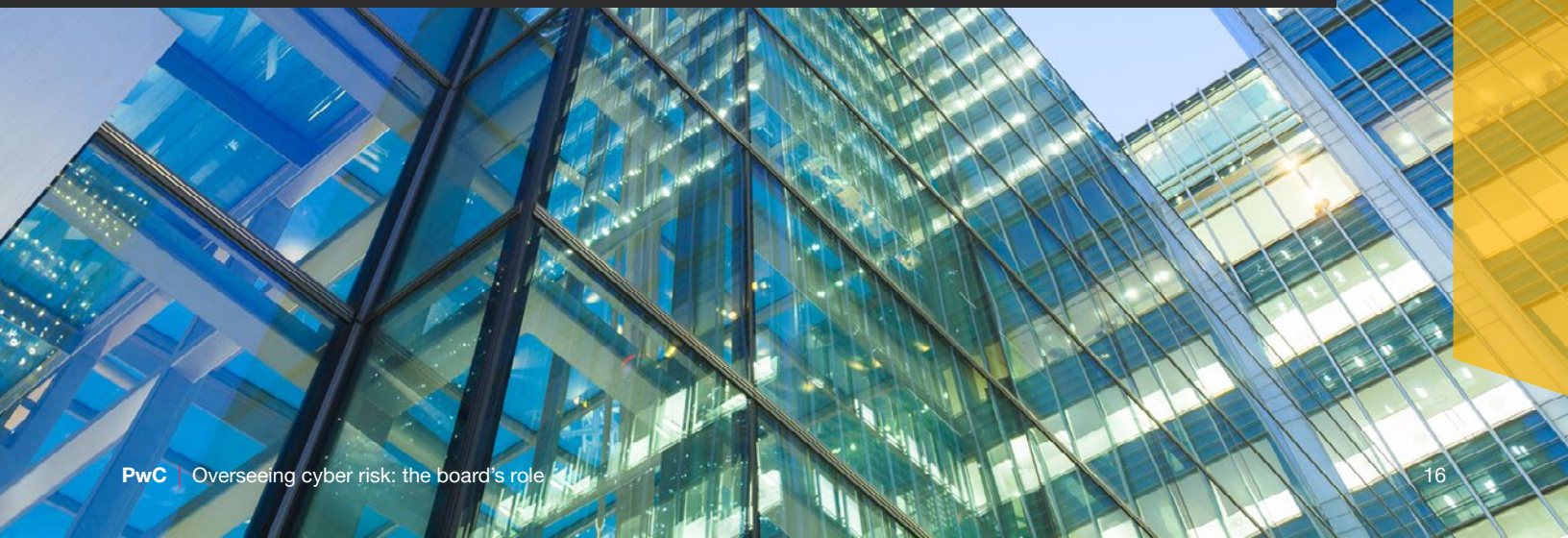
- Adding a director who has very narrow expertise and may not contribute to other board agenda topics
- Creating an authority bias among directors when it comes to cyber discussions and decisions — with a cyber expert on the board, other directors may be much less willing to voice their opinions on the subject

An alternative to adding a board director with cyber skills is upskilling the existing board or committee members. This can be done by having management deliver board education sessions. Some boards have the CISO walk through the top risks or mitigating program elements at every, or every other, committee and/or board meeting along with other upskilling opportunities. These can include hearing from external parties or organizations on the threat landscape and leading practices, obtaining board-level cyber certifications and attending external cyber programs.

Ultimately risk oversight is the responsibility of the entire board so all directors will need to consider how they are upskilling themselves in this area. Boards must think holistically about how they are seeking ongoing education.

How can directors improve their knowledge of cybersecurity?

- **Hold deep-dive discussions about the company's risk posture.** That could include the types of cyber threats facing the company, third-party risk mitigation plans and details on the company's cyber insurance policy, for example.
- **Attend external programs.** There are many conferences that focus on cyber risk oversight where directors can learn about new developments and get insights from experts on the topic.
- **Seek relevant certifications.** A number of cybersecurity certification programs exist through higher education institutions, governance providers and others.
- **Request presentations from law enforcement (e.g., the FBI) and other experts** on the threat environment, attack trends and common vulnerabilities. Then discuss with management how the company is addressing those developments.
- **Get opinions from peers and others.** Speaking to other directors outside the organization can offer the board different perspectives.



Next steps

- Reassess where cybersecurity oversight sits on your board and whether the board has cybersecurity skills/expertise, or has access to cybersecurity skills/expertise, to perform its oversight role.
- Take a hard look at your board/committee agendas and consider whether sufficient time is allocated to cyber and how often you are hearing from the CISO. Assess whether the information presented to the board is digestible and clearly articulates the company's risk profile and mitigation strategies.
- Evaluate how your board is continuing to get upskilled and educated on cybersecurity.
- Evaluate the need for private sessions with the CISO.
- Update the relevant charter with language that provides insight into the committee's responsibility, under the direction of counsel.

In conclusion

Cybersecurity may be an intimidating area for the board to oversee. However, a well-thought-out approach to oversight, robust reporting and a strong relationship with the CISO can pave the way for greater understanding and collaboration between the board and management on this critical topic.

Appendix A

SEC's Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure — July 2023

The SEC's 2023 rules require enhanced disclosure from organizations. At a high level, there will be additional information requested in the annual Form 10-K filing including details related to both the company's cyber risk management and assessment program and the board's oversight of cybersecurity. Additionally, companies will need to disclose material cyber incidents within four business days on Form 8-K once they determine that the incident is material. While the requirement to disclose material events isn't new — the timeframe for required reporting is.

Summarized below are the three central areas within the SEC's final disclosure rule.

Cyber incident reporting

- Report "material" cybersecurity incidents on Form 8-K within four business days of materiality determination
- An incident includes a series of related occurrences
- Describe the nature, scope and timing of the incident and the material impact or reasonably likely material impact on the registrant
- Extensions allowed if the US Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety

Effective date: On or after December 18, 2023 (smaller reporting companies on or after June 15, 2024)

The company's risk management and strategy regarding cybersecurity risks

Describe the company's process, if any, for assessing, identifying and managing material risks from cybersecurity threats, including:

- How cyber processes have been integrated into the overall risk management system
- Whether assessors, consultants, auditors or other third parties are engaged
- Processes to oversee and identify material cyber risks with third-party service providers
- How cyber risks have materially affected or are reasonably likely to materially affect business strategy, results of operations or financial condition

Effective date: For fiscal years ending on or after December 15, 2023 (for all registrants)

Cyber governance

Describe the company's governance of cybersecurity risks as it relates to:

- The board's oversight of cyber risk, including any board committee or subcommittee responsible for oversight, and the process by which they are informed about cyber risks
- Management's role in assessing and managing material cybersecurity risk and implementing cybersecurity policies, procedures and strategies, including specific disclosure of management positions or committees responsible and a discussion of their relevant expertise.

Effective date: For fiscal years ending on or after December 15, 2023 (for all registrants)

Appendix B

The World Economic Forum principles on cybersecurity

PwC served as the project advisor for the development of principles released by the World Economic Forum (WEF). *Principles for Board Governance of Cyber Risk* was developed to help boards know what to focus on when overseeing cybersecurity. The principles provide advice and key considerations to help a director understand the company's current cyber risk posture and exercise its oversight responsibilities.

The six WEF principles for board governance of cyber risk

Source: World Economic Forum, *Principles for Board Governance of Cyber Risk,* March 2021.

How PwC can help

To have a deeper discussion about how this topic might impact your business, please contact your engagement partner or one of the PwC specialists below.

Contacts

Maria Castañón Moats
Leader, Governance Insights Center
maria.castanon.moats@pwc.com

Sean Joyce
Global Cybersecurity & Privacy Leader, US Cyber, Risk and Regulatory Leader
sean.joyce@pwc.com

Mary Grace Davenport
Partner, National Office
mary.grace.davenport@pwc.com

Barbara Berlin
Managing Director, Governance Insights Center
barbara.berlin@pwc.com

Matt Gorham
US Cyber & Privacy Innovation Institute Leader
matt.gorham@pwc.com

David Ames
Principal, Cyber, Risk & Regulatory
david.m.ames@pwc.com

Catie Hall
Director, Governance Insights Center
catherine.hall@pwc.com