# Overseeing cyber risk: the board's role

Cyber risk is an enterprise-wide issue, and companies need to build resiliency to address the threat of a breach.

January 2022

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

pwc

Governance Insights Center

Nearly three quarters of US CEOs in PwC's *24th Annual Global CEO Survey* said they are "extremely concerned" about cyber threats. They even put it ahead of the pandemic and other health crises (46%). The focus is well deserved—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. Add to this that during the COVID-19 pandemic, the corporate world embarked upon a rapid digital transformation and many employees started working remotely, increasing companies' digital footprint—and their cyber risk profile.

The FBI's Internet Crime Complaint Center received over 2,000 ransomware complaints in the first seven months of 2021, a 62% increase over the same period in 2020.

At the same time, expectations have risen. Even with a robust risk management program, a company can suffer a cyber breach or attack. But stakeholders demand that companies do everything in their power to protect consumer data, and to also 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.

Addressing cyber risk is a challenge for nearly any company and its board. Cyber is 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 where boards should take action to support their company in establishing an effective cybersecurity risk management program.

### Trust in institutions is hard to earn—and easy to lose

Stakeholders want to know what companies are doing to protect personal data. The cyber oversight practices you choose and disclose as a board could impact how the company is seen.

### The World Economic Forum principles around cybersecurity

In 2021, PwC served as the project advisor for the development of principles released by the World Economic Forum. *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 directors understand their company's current cyber risk posture and exercise their oversight responsibilities. Refer to the appendix for more information on the report.

## 1 Ensure cyber risk is embedded in strategic decisions—and the company's culture

Many strategic decisions have a cyber risk component. For example, adopting new technologies to better enable and connect a remote workforce changes the company's cyber risk profile. Cyber has to be a consideration when 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. Don't forget the flipside as well—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 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.

### Aligning cyber with strategy

**42%**

of executives saw increased alignment of cyber and business strategy in their organizations over the last two years

Source: PwC, *2022 Global Digital Trust Insights*, October 2021.

## Next steps

- Make sure the chief information security officer (CISO) has a seat at the table when addressing strategic decisions and the company's plan.
- Understand how management embeds cyber risk as part of vendor management/third-party risk management programs.
- Get metrics on the effectiveness of employee training and awareness for cyber risks, and 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

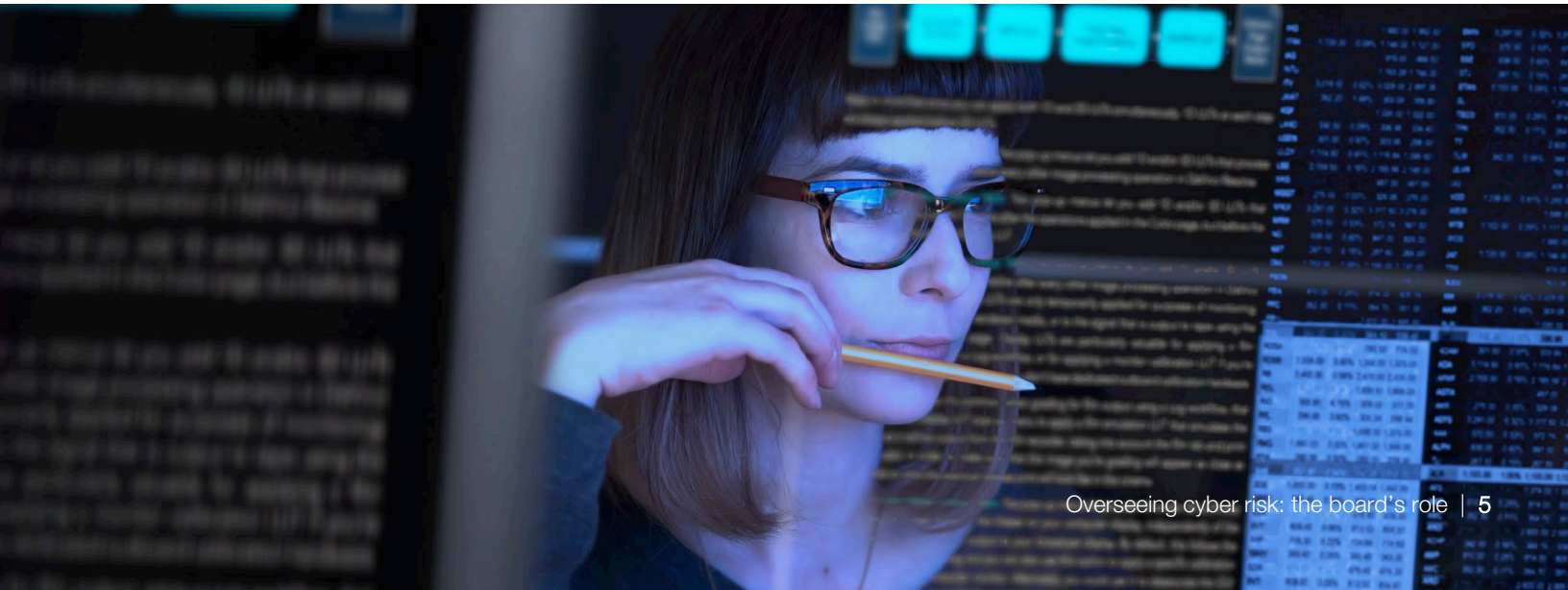
Boards want to know whether management is focusing on the right cyber risks, how management is addressing those risks, and whether it's enough. This starts with understanding the company's cyber risk management program and cyber risk appetite.

### 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 potential vulnerabilities at the company and clarify the right steps for management to take to address them. These key cyber risks can then be integrated into the company's enterprise risk management program.

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 cybersecurity organizations as their programs evolve.

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.



Only 33% of directors say they think their board understands the company's cybersecurity vulnerabilities very well

## 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: Exploitation of a known vulnerability in a widely used piece of software that provides extensive access to systems within a network. We have observed instances of both commercial and open source software being targeted. This requires an extensive software asset inventory and a "software bill of materials," which describes components in a piece of software, that enables you to quickly identify where to patch and monitor for impacted systems.

Account compromise: 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 companies must strengthen defenses and develop a response plan, 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.

## Review the reporting

Cyber reporting to the board should be in jargon-free language so the board can easily get a snapshot of what's going on. Many boards today are getting a cyber scorecard. A cyber dashboard or scorecard prepared by the CIO or CISO can help the board assess current risks and track progress. With clearly identified and quantified cyber-related metrics, as well as a consistent format, the board can spot any trends that show the company improving or falling short relative to key risks.

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 (NIST) Cybersecurity Framework. 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 improving the maturity of the program.

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 create a calendar that takes the board meeting dates and outlines the various cyber board reporting areas to help facilitate agendas and ensure all key areas are covered.

## Common elements of cybersecurity board reporting

- Multi-year strategic plan and current year business plan
- Cyber security resource allocation - funding and staffing
- Periodically updated inventory of mission critical systems that need to be protected
- 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

## Stay on top of legal and regulatory developments

As the threat and impact of cyber incidents grows, legislators 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 also taken action recently. For example, a May 2021 Executive Order on improving the nation's cybersecurity was released to galvanize public and private efforts to help identify, deter, protect against, detect, and respond to persistent and increasingly sophisticated malicious cyber campaigns. There have been a few recent SEC enforcement actions related to inadequate disclosure of breach information. Looking ahead, cyber disclosures are on the SEC's agenda for 2022.

Similar to other areas that require compliance focus, boards will want to understand how laws and regulations around data privacy and cybersecurity are changing, how the company is impacted, and how management is tracking compliance.

## 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 internal audit 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 where an unannounced ethical hacking takes place. The board will want to hear findings directly from any such advisors. This is an opportunity for the board to ask questions and hear external advisors' unvarnished views.

## Be transparent with stakeholders

As with many other areas of high risk, investors 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. Institutional Shareholder Services (ISS), for example, is looking at public company disclosures for information security risk oversight data and embedding this information into its *Governance QualityScore*. They have a list of data points that they use as part of the security risk assessment, including where oversight sits at the board-level, frequency of reporting to the board, third-party assurance, and breaches in the last three years. Glass Lewis, another large proxy advisor, announced a partnership in 2021 with BitSight. This deal will add BitSight's *Security Ratings* to Glass Lewis' proxy research reports.

### Next steps

- Make sure you have a clear understanding of 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 whether the company uses a standardized framework (e.g., NIST) to benchmark their security program, and if so, how gaps are being closed.
- Discuss with management the need for external perspectives (e.g., third-party assurance for key risk areas) and ask that findings be reported directly to the board.
- Understand how cyber risks fit within the company's risk appetite.
- Take a fresh look at the board's cyber reporting and make sure you are getting 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 meeting those requirements.
- Consider what cyber oversight practices are disclosed and whether any additional information should be provided.

## 3 Monitor cyber resilience

With the rise in ransomware attacks and increase in breaches, many boards focus significant attention on resilience plans. The ultimate objective is to be able to detect and respond to cyber threats quickly to minimize business disruption and financial losses. The 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.

Even with a robust risk management program, there still can be a successful breach, and companies need a playbook for how to recover quickly.

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*.

In addition to the broad questions the board should ask about a crisis response plan, 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. In our experience, companies that were well-prepared usually come out of a cyber crisis better than those that had to scramble.
- Make sure the company has the right experts engaged in advance of any event occurring. For example, they 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 the authorities (e.g., the FBI).
- Understand the key provisions of the cyber insurance policy at the company, 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.

## Next steps

- Review the company's incident response plan annually and understand how often it is tested by management.
- Participate in or get feedback on management's testing of the incident response plan.
- Understand when the board will be informed during the crisis escalation process and agree with management on the related triggers for communication.
- 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 it may be time to rethink that allocation. Current survey data indicates that 46% of S&P 500 company boards allocate responsibility to the audit committee. Given all the audit committee has on its agenda these days, some boards are considering whether a move to a separate cyber/technology or risk committee makes sense. And some boards have deemed cyber a risk that the full board needs to oversee, taking it out of committee. No matter what, if oversight rests with a board committee, it's important that the full board gets regular and comprehensive updates. Directors also need to maintain an adequate level of cyber knowledge to understand the nature of current risks and provide strategic direction in protecting the organization against them.

It is helpful to reassess the board's oversight approach periodically to ensure it is working effectively. Factors to consider include whether the current structure has the right board members engaged and whether they have adequate time to address the topic. It's also important to ensure your board has access to the expertise it needs on the subject. Many boards recruit a director with a cybersecurity background. This can be helpful, but it poses two risks to be mindful of. One is adding a director who has very narrow expertise and may not contribute to other board agenda topics. The other is 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.

### 34% of S&P 500 companies say their board includes a cyber expert

Another option is to upskill the board. Seek outside experts to help the board or committee understand and address cyber risk. A challenge here can be that the subject is so broad that there has to be a strategy for approaching board education sessions.

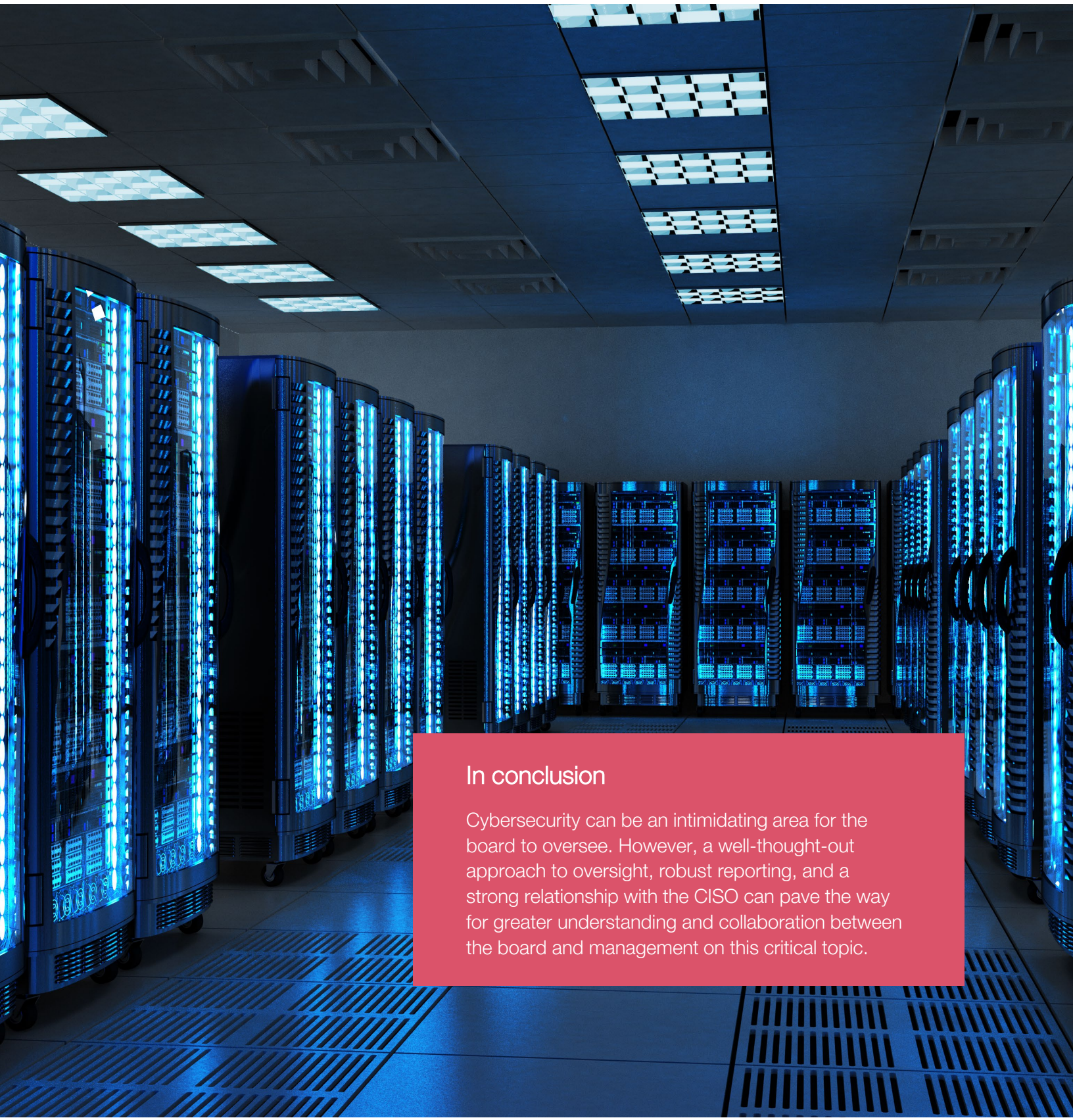
## How can directors improve their knowledge of cybersecurity?

- **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.
- **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.

With the increasing concern about cyber risk, some boards are engaging with the CISO (or other executive, such as the CIO, 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 ensure it has adequate touchpoints with the CISO and enough time for questions.

### Next steps

- Reassess where cybersecurity oversight sits on your board. Ensure that it aligns with your board's cybersecurity expertise. Review agendas and determine whether sufficient time is allocated to cyber to allow time for discussion.
- Evaluate how your board is expanding its knowledge of cybersecurity. Consider having the CISO walk through the top risks or mitigating program elements at every, or every other, committee and/or board meeting.
- Take a hard look at your board/committee agendas and consider the sufficiency of how often you are hearing from the CISO and whether the information presented to the board is digestible and clearly articulates the company's risk profile and mitigation strategies.
- Evaluate the need for private sessions with the CISO.



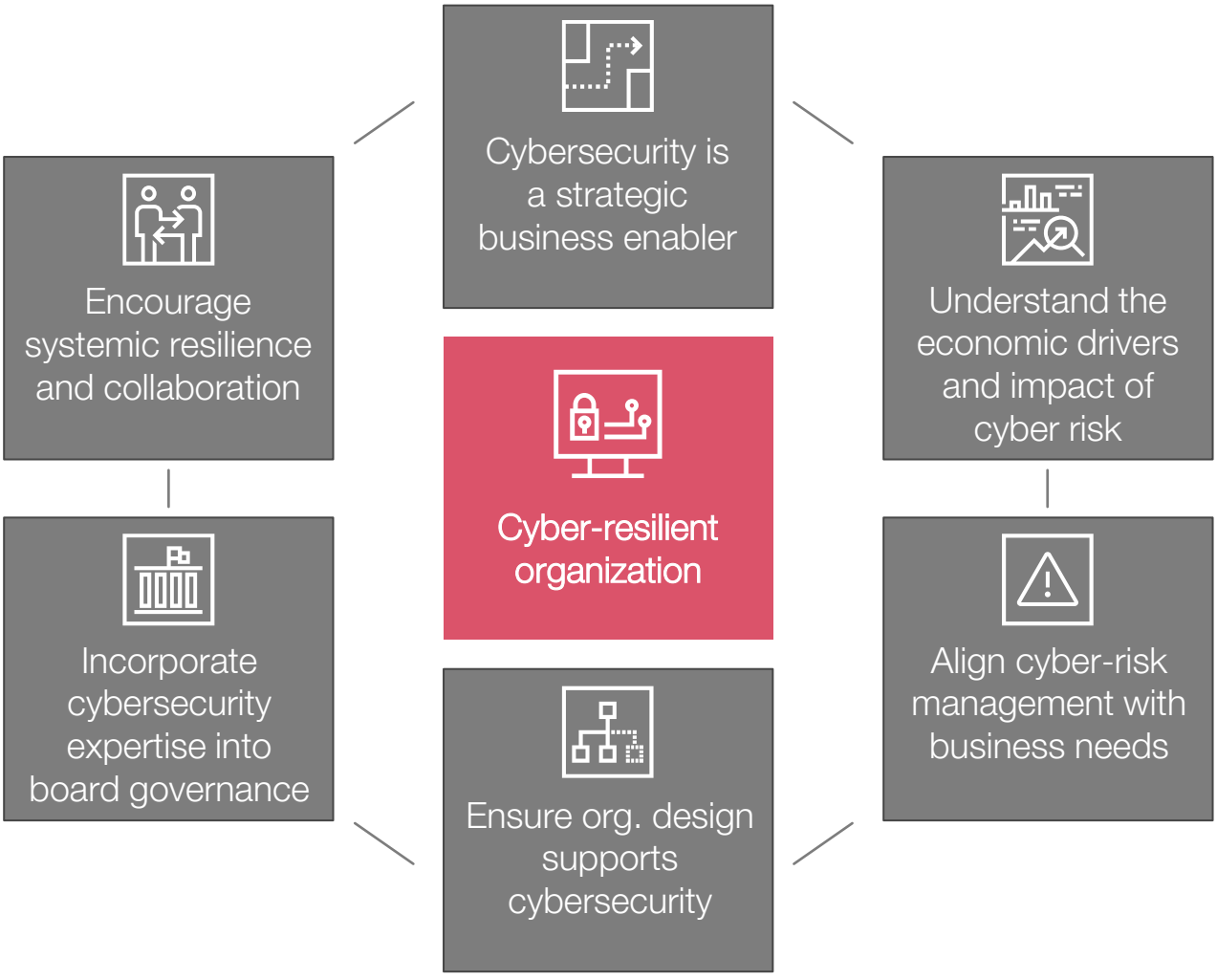
## In conclusion

Cybersecurity can 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

PwC worked with the World Economic Forum, the National Association of Corporate Directors, the Internet Security Association, and other WEF partners, to develop six consensus principles for cybersecurity board governance. The WEF document provides advice and suggests critical actions that directors may find useful as they seek to understand their organization's current position, exercise their oversight function, and set future goals.

## The six WEF principles for board governance of cyber risk




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

## Contacts

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.


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

**Sean Joyce**
Global and US Cybersecurity, Privacy and Forensics Leader
sean.joyce@pwc.com

**Joseph Nocera**
Cyber & Privacy Innovation Institute Leader
joseph.nocera@pwc.com

**John Oleniczak**
Partner, Governance Insights Center
john.oleniczak@pwc.com

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

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


pwc.com