Governance Insights Center
Risk Oversight Series

November 2018

How your board can better oversee cyber risk

Cyber risk is an enterprise-wide issue, and no company is immune to the threat of a breach.

Having a good cyber risk management program in place might help a company prevent some breaches. But more importantly, when a breach does happen, it can help companies get back on their feet faster and mitigate financial and reputational damage. How do you know whether your company is doing what it should to address the risk?

pwc

pwc.com/us/governanceinsightscenter

Cyber threats are everywhere, and breaches make headlines on what seems like a daily basis. They also cost companies—in money and reputation. The global cost of cyber crime is expected to reach $6 trillion annually by 2021.[1]

The threat environment is becoming more complex as hackers use sophisticated new tactics. The 2017 WannaCry and NotPetya attacks marked a new generation of cyberattacks—ransomware that spreads on its own, without human intervention. These attacks hijacked computers and data, paralyzing companies across the globe and causing extensive damage. In some cases, they exploited security gaps companies didn't even know existed, so-called "zero-day" vulnerabilities.

Tackling cyber risk is a struggle for companies, and overseeing it is just as difficult for boards. We outline the challenges and possible path forward for companies, as well as what directors can do to support their companies in establishing effective cybersecurity risk management programs.

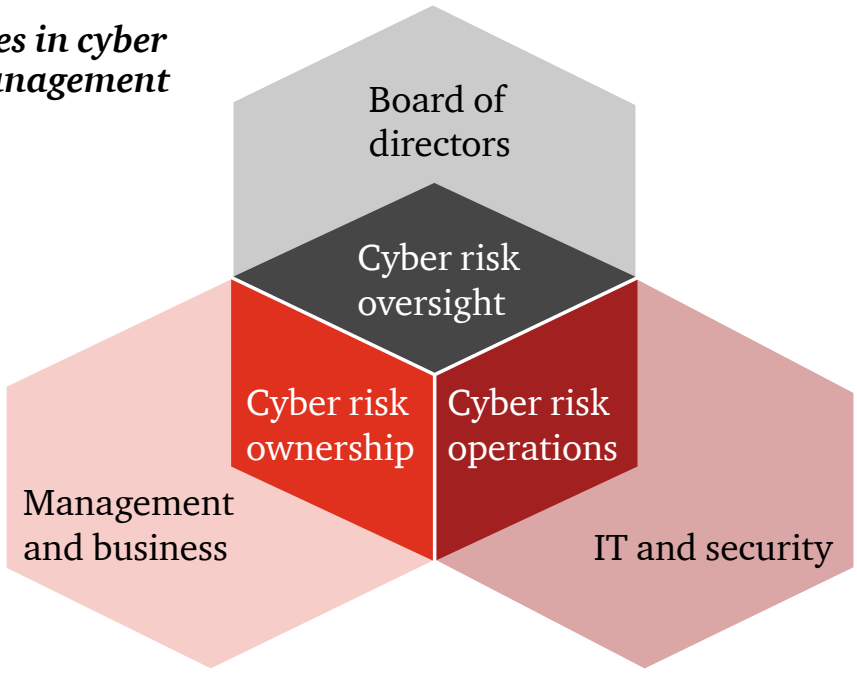
The cyber governance journey

Boards and management should recognize that addressing cyber risk isn't solely the IT department's responsibility. A chief information security officer (CISO) and his or her team can't do the job alone. To tackle cyber risk, the board of directors, management, business unit leaders, and the IT and security groups all need to be involved.

Of course, the heavy lifting is done by IT and management. And it doesn't get done overnight. It can be a journey for companies to establish a robust, working cybersecurity program. Different companies will be at different stages of maturity along this journey. And quite honestly, it's one that never ends, given the threat environment is continually evolving.

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.

Key roles in cyber risk management



1 Cybersecurity Ventures and Herjavec Group, *2017 Cybercrime Report*, October 2017.

Common challenges in getting cybersecurity right

There's no inventory of the company's digital assets

Only 37% of directors are very comfortable that the company has identified its most valuable and sensitive digital assets.[2]

The company doesn't know which third parties it digitally connects with

More than **half** of respondents to one survey say their companies don't keep a comprehensive inventory of the third parties they share sensitive information with, let alone whether those companies have proper controls in place to protect it.[3]

The company hasn't identified who is most likely to come after its data

Only 17% of directors are very comfortable their company has identified who might attack its digital assets.[4]

The company has poor cyber hygiene

93% of all 2017 breaches could have been prevented if companies had better cyber hygiene practices, such as regularly updating software, blocking fake email messages and training employees to recognize phishing attacks.[5]

The company hasn't patched known system vulnerabilities

According to one study, 57% of respondents who reported a breach said it was due to a vulnerability for which a patch was available but not applied.[6]

The company has a wide attack surface

As companies leverage "*internet of things*" (IoT) devices, their attack surface increases. 81% of business leaders say the IoT is critical to at least some of their business, but only 39% say they are very confident they are building sufficient "digital trust" controls—security, privacy and data ethics—into their adoption of IoT.[7]

Employees aren't trained on their role in security

Only 34% of executives say their company has an employee security awareness training program.[8]

The cyber environment is a fast-moving and dynamic one. What companies did yesterday to prepare for and battle cyber incidents may not work today, much less tomorrow.

2 PwC, *2018 Annual Corporate Directors Survey*, October 2018.
3 Ponemon Institute, *Data Risk in the Third-Party Ecosystem: Second Annual Study,* September 2017.
4 PwC, *2018 Annual Corporate Directors Survey,* October 2018.
5 Online Trust Alliance, *Cyber Incident & Breach Trends Report,* January 2018.
6 ServiceNow and Ponemon Institute, *Today's State of Vulnerability Response: Patch Work Demands Attention,* April 2018.
7 PwC, *Digital Trust Insights: The journey to digital trust,* October 2018.
8 Ibid.

Overseeing cybersecurity

A board should oversee cybersecurity just like it does any other significant risk to the company. That means discussing the top cyber risks with management. And understanding how management implements controls and other measures, such as cyber insurance, to bring the level of risk to an acceptable level, both for the company and the brand.

As your board oversees how management identifies, prioritizes and monitors cyber risk, here are seven key areas of focus.

1. Address cyber as an enterprise-wide business issue, not an IT issue
2. Have an oversight approach with access to cyber expertise
3. Understand legal and regulatory requirements
4. Discuss the adequacy of the cyber strategy and plan
5. Engage in discussions with management about cyber risk appetite
6. Get the right information to monitor the cyber and privacy program
7. Monitor cyber resilience

1. Address cyber as an enterprise-wide business issue, not an IT issue

Ideally, cybersecurity discussions should include business unit, technology and risk management leaders, as well as the CEO, CFO and other executive leadership. This shows that cyber is an enterprise-wide issue—and directors should expect everyone to be accountable for managing the risk. The discussion may also expose other areas where there are security gaps. For example, while a CISO will often cover IT, non-financial services companies often also need to protect the operational technology (OT) that directs what happens in physical plants or processes. So if the CISO isn't covering OT, the board needs to hear from whoever is.

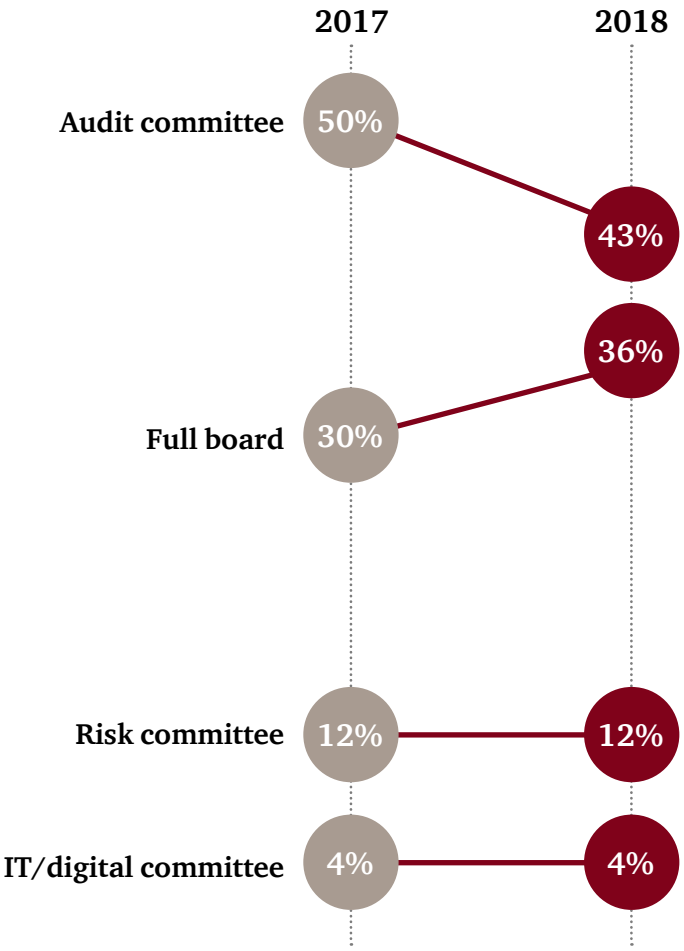
2. Have an oversight approach with access to cyber expertise

A critical first step is to determine if the entire board will oversee cyber risk or if it will delegate to a committee. While it appears more boards are tackling the area themselves, if oversight is done by a board committee, it's important that the full board get regular and comprehensive updates.

It's also important to ensure your board has access to the expertise it needs on the subject.

- Some boards recruit a director with a technology or cybersecurity background.
- Many boards get continuing education on the topic, from the company's CISO and/or from outside advisors. Boards can also take advantage of private sessions with the CISO for sensitive conversations.

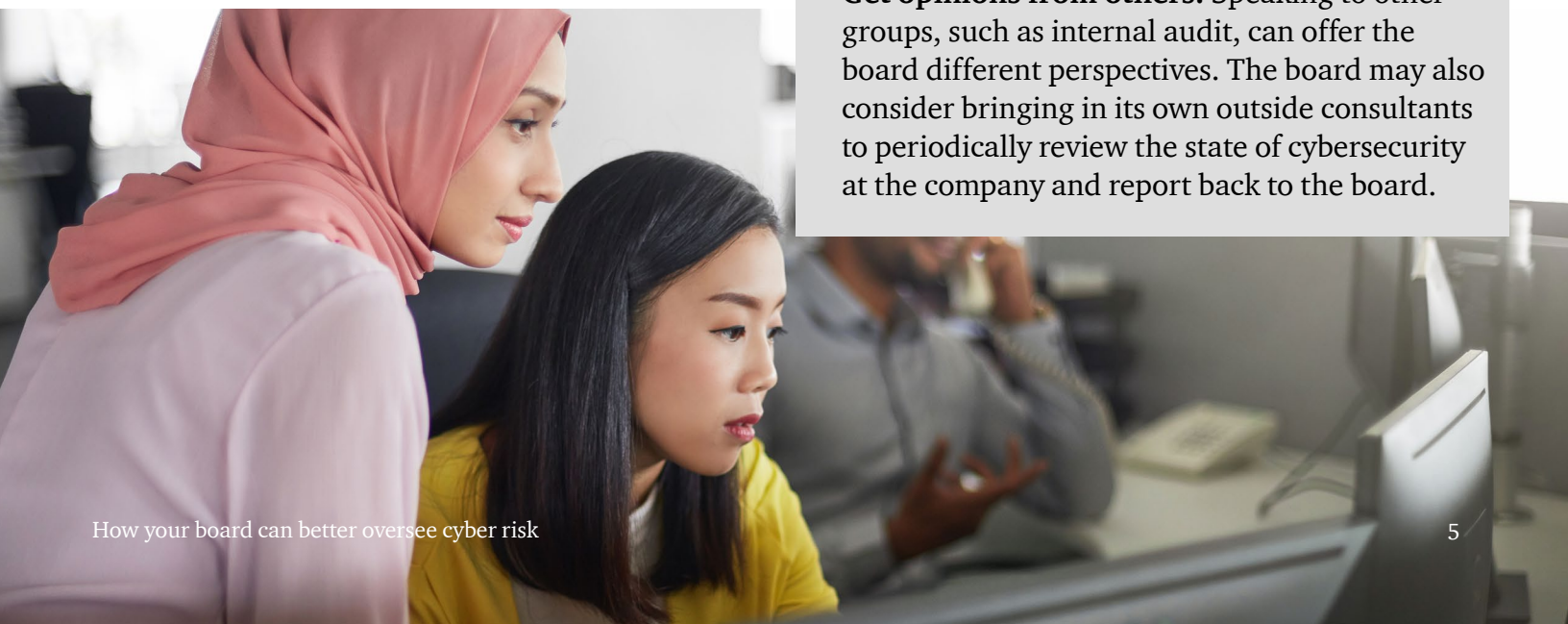
Who oversees cybersecurity?



Sources: PwC, *2018 Annual Corporate Directors Survey,* October 2018; PwC, *2017 Annual Corporate Directors Survey,* October 2017.

How can directors improve their knowledge of cybersecurity?

- **Hold deep-dive discussions about the company's risk posture.** That could include the company's cybersecurity strategy, the types of cyber threats facing the company, the nature of the company's "crown jewels" (its most important digital assets), the results of the most recent risk assessment and any planned mitigation actions. All of these should be weighed against the company's risk tolerance and appetite, which the company needs to reassess periodically.
- **Attend external programs.** There are many conferences that focus on cyber risk oversight and security where directors can learn about new developments and get insights from experts on the topic.
- **Ask management what it has learned from connecting with peers and industry groups.**
- **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 these developments.
- **Get opinions from others.** Speaking to other groups, such as internal audit, can offer the board different perspectives. The board may also consider bringing in its own outside consultants to periodically review the state of cybersecurity at the company and report back to the board.



3. Understand legal and regulatory requirements

Nearly all US states and many countries have laws requiring entities to notify affected individuals when there's been a security breach involving personally identifiable information. Some notification deadlines are as short as 72 hours. The data breach notification laws are not uniform and can change, making it a challenge to keep up to date. Plus, many states are now passing their own cybersecurity regulations. For example, the New York State Department of Financial Services' Cybersecurity Regulation requires all covered financial institutions to have a documented cybersecurity program, encrypt all data being sent externally and conduct a risk assessment of all of their third parties.

The penalties for noncompliance can be stiff. For example, the European Union's General Data Protection Regulation (GDPR) took effect on May 25, 2018. Businesses that fail to comply face potential fines of up to 4% of global revenues.

Boards will want to understand the basic regulations around data privacy and cybersecurity. But more importantly, directors will want assurance that management is tracking the evolving requirements and is able to comply—and that management has the resources it needs to do so.

4. Discuss the adequacy of the cyber strategy and plan

The board should be briefed periodically about the company's cyber strategy. Directors will want to know how the cyber strategy ties to the company's business objectives. Does the strategy protect the company's crown jewels, does it consider physical assets and is it enterprise wide? The board will also want to discuss whether the cybersecurity budget is sufficient to support the strategy.

In PwC's *Digital Trust Insights* survey, published in October 2018, most respondents responsible for communicating with the board on cyber and privacy risks say that their company has provided the board with strategies for cybersecurity (80%) and privacy (83%). But 30% of directors say their boards are not sufficiently or not at all engaged with overseeing/understanding the cybersecurity budget.[9]

Company CIOs and CISOs are often key to cyber strategies and plans. And 71% of the directors whose companies have a CIO say they communicate with that individual at least twice a year; 60% of directors whose companies have a CISO do likewise.[10]

5. Engage in discussions with management about cyber risk appetite

Risk appetite is the level of risk an organization is prepared to accept. While management sets risk appetite, directors should discuss it regularly as part of their risk oversight. A company can't get the risk level to zero, so boards will want to be comfortable that management is managing to a level of cyber risk that is appropriate for its business and circumstances—and that the program has adequate resources.

6. Get the right information to monitor the cyber and privacy program

The board should understand the company's IT environment and data assets. Board members should also understand the risk posture of the organization. With this background, management can provide updates on security projects, how well security efforts are working and how they are impacting the business. Boards should expect metrics that map to these areas.

9 PwC, *2018 Annual Corporate Directors Survey,* October 2018.
10 Ibid.

Of course, which metrics are available depends on the maturity of the security program and how controls are being implemented and managed. Management can report what they can measure today and, with board feedback, create a plan to add more sophisticated metrics over time. For example, directors might ask for metrics that gauge the business impact of security spending or the cost of addressing a security event.

In addition to internal metrics, the board should expect management to communicate how external factors—threats, third-party risk and regulations—affect overall risk posture and effectiveness of risk reduction activities.

Cyber reporting to the board should be in jargon-free language so the board can easily get a snapshot of what's going on. It should also be consistent so boards can see any trend lines on where the company is improving or falling short.

Unfortunately, only 37% of directors are very comfortable that the company is providing them with adequate reporting on cybersecurity metrics.[11]

7. Monitor cyber resilience

There are many aspects to being able to resist and recover from attacks. The keys are protecting the company's systems, limiting damage to systems from a cyber event and ensuring systems are able to recover from a cyber event. Cyber resilient systems have "built-in" security measures that allow them to withstand cyberattacks and continue to operate, ensuring the company can continue to do business.

The ultimate objective of cyber resiliency is to be able to detect and respond to cyber threats quickly to minimize business disruption and financial losses. The first step is for management to develop a plan that allows the company to get back to business as usual as quickly as possible.

Some of those plans might outline written, step-by-step responses or playbooks to help respond to and expedite the recovery. Those playbooks often describe who should be involved, what their responsibilities are and exactly what they should do if an incident occurs. This includes identifying any external resources on retainer that can support internal teams, as well as who the company will work with on the law enforcement side. The plan should outline the crisis escalation process, including when the board will be informed. It also needs to address how to respond to issues involving third parties.

Finally, after a breach, companies must consider what needs to be changed to adapt business processes and technical controls based on lessons learned.

Boards will want to regularly review cyber resiliency efforts. Often, security efforts focus on protective measures. Boards should discuss with management whether adequate resources are allocated to both *protecting* systems and to *responding, withstanding and recovering* from breaches.

Given how likely a breach is and how much companies need to do to respond, it's surprising that only 47% of directors say their company has a written crisis escalation policy in place.[12] That's pretty consistent with the 54% of executives who say their companies don't have an incident response plan.[13] Yet, in our experience, companies that respond well to a breach are those that were better prepared—and usually come out of a crisis better than those that had to scramble.

11 Ibid.
12 Ibid.
13 PwC, *The Global State of Information Security® Survey 2018,* October 2017.

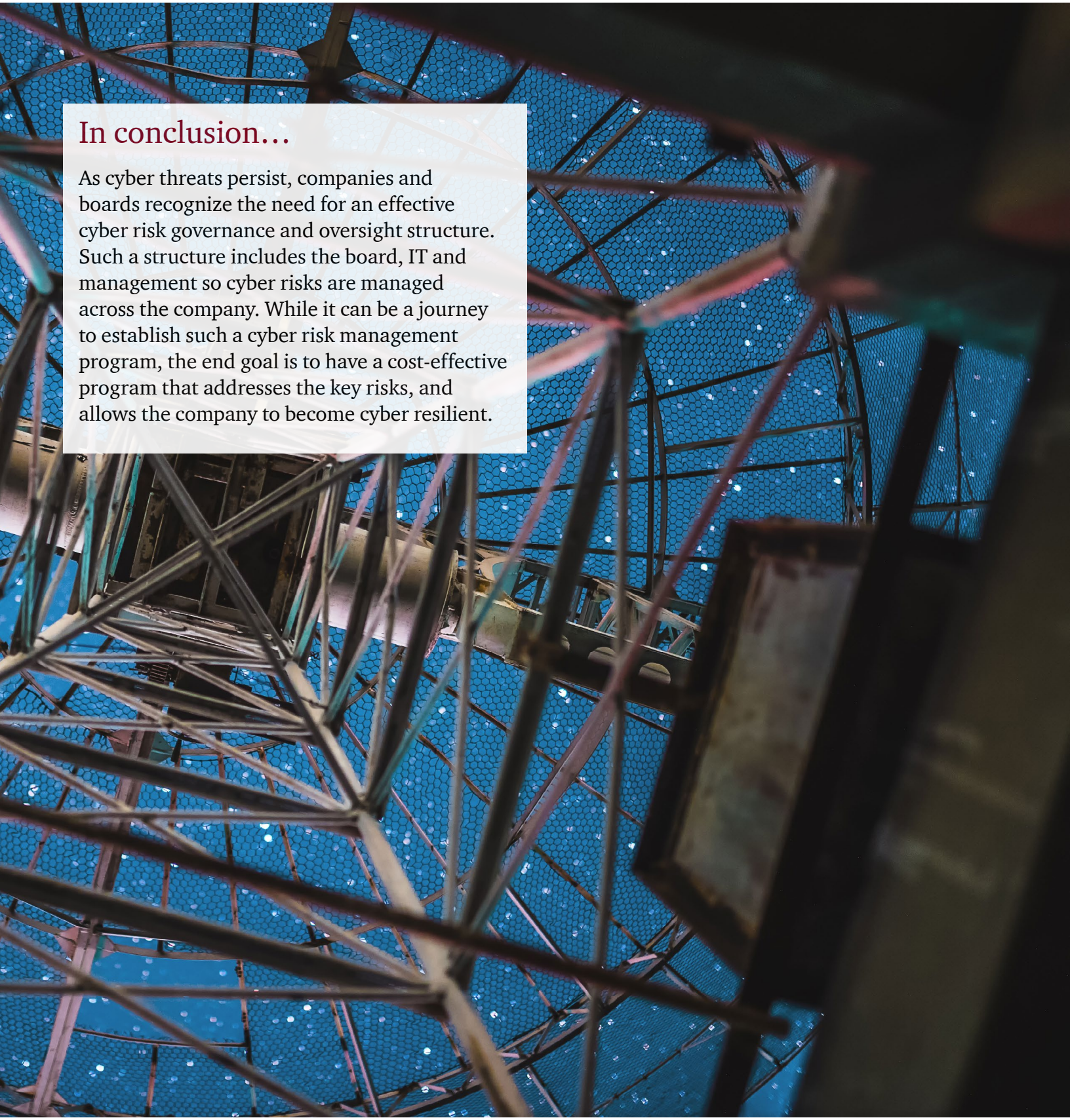
Because of the gravity of the issue, some companies are collaborating on cybersecurity issues and coordinating effective countermeasures. In fact, a number of global companies joined forces in early 2018, signing a Cybersecurity Tech Accord to foster collaboration on information security and advance online security.

Cybersecurity risk management tools: the NIST Cybersecurity Framework and capability maturity models

To strengthen cybersecurity, many companies are using leading risk management tools, such as the National Institute for Standards and Technology (NIST) Cybersecurity Framework.[14] NIST created the framework—with input from industry, and at the direction of the White House—to help critical infrastructure companies bolster their cybersecurity and resilience. Executive management can use it to identify gaps in their cybersecurity posture, set priorities for making improvements and assess progress toward the goals. Boards can use the NIST framework to understand cybersecurity problems more clearly and communicate with executives more effectively.

Executive management may also assess their cybersecurity program, assign maturity ratings and enable benchmarking against industry peers by using, alongside the NIST Framework, another tool known as a capability maturity model. Boards may find such benchmarking helpful when overseeing cyber risk management. A leading example of such a model is the Capability Maturity Model Integration (CMMI) approach.

14 NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, April 2018.



In conclusion…

As cyber threats persist, companies and boards recognize the need for an effective cyber risk governance and oversight structure. Such a structure includes the board, IT and management so cyber risks are managed across the company. While it can be a journey to establish such a cyber risk management program, the end goal is to have a cost-effective program that addresses the key risks, and allows the company to become cyber resilient.

Appendix

Questions boards can ask management about cybersecurity and cyber risk management

On how the company maintains its IT systems and updates its software patches:

- Do we patch all known vulnerabilities as soon as they're discovered?
- If not, how do we decide which ones to fix and when and what are the implications of such delays?

On dealing with employees, as one of the most critical components of protection:

- What are we doing to train employees about cybersecurity?
- What controls are in place to prevent an insider attack—and are they adequate?

On management's activities around cybersecurity:

- What is the company's overall cybersecurity strategy?
- Is the company looking at cybersecurity through an enterprise-wide lens?
- How is the company allocating resources to detection, prevention, protection and response?
- Is the company using a framework, such as NIST, or a maturity model to help with cyber risk management?

On connecting cybersecurity to both the company's strategic thinking and enterprise-wide risk management processes:

- How is the company managing cyber risk?
- What is the company doing to ensure it has durable networks?
- How is the company taking advantage of opportunities around digitization?
- What steps is the company taking to be cyber resilient? Is the board comfortable with this plan?

On the subject of the volume of data companies collect and store today, especially given expanding privacy laws, such as the GDPR, which took effect in May 2018 for all data impacting Europeans:

- Do we collect data we don't really need?
- How do we inventory and protect the data we collect?
- Do we have a data deletion policy, and if so, what does it entail?

On meeting with the CISO or the CIO:

- Which areas of cybersecurity should the board focus on?
- What information is most relevant to get from management? What else should the CISO/CIO provide updates about? What should be included on a cyber risk dashboard?
- Which of our networks or systems might be vulnerable? How so? What is the company doing to protect its most sensitive data?
- Have there been any breach attempts? If so, what has the company done in response?
- What are the company's policies and internal controls around multi-factor authentication and password use?

On the company's crisis management plan:

- What does the company's plan entail?
- How does the company plan to continue operating if something happens?
- How often does management test the plan and apply any lessons learned from that testing?
- Has management made any updates based on recent incidents at other companies?
- Does the plan include breach notification and escalation procedures? When will the board, regulators and other stakeholders be notified?
- Should the board participate in or observe tabletop exercises to better understand the response plan?
- If the company doesn't have a plan, why not? What is the company's timeline to develop and test one?
- Does the plan take into consideration pre-incident preparedness, actions during an incident and post-incident recovery efforts—so it is cyber resilient?

How PwC can help

For more information about the topics in this publication, please contact any of the following individuals.

Paula Loop
Leader, Governance Insights Center
paula.loop@pwc.com

Catherine Bromilow
Partner, Governance Insights Center
catherine.bromilow@pwc.com

Sean Joyce
Principal—US Cybersecurity and Privacy Leader
sean.joyce@pwc.com

Lisa Gallagher
Managing Director, Cybersecurity and Privacy—Strategy, Governance and Management
lisa.a.gallagher@pwc.com

Project team

Elizabeth Eck
Senior Manager, US Integrated Content Team

Chris Castelli
Director, US Integrated Content Team

Karen Bissell
Marketing Manager, Governance Insights Center

Erin Daylor
Marketing Manager, Cybersecurity & Privacy

Jyll Presley
Designer

Other "Risk Oversight Series" topics include:

- *Why your board should take a fresh look at risk oversight: a practical guide for getting started*
- *How your board can influence culture and risk appetite*
- *How your board can ensure enterprise risk management connects with strategy*
- *Why your board should refocus on key risks*
- *How you board can be ready for crisis*
- *How your board can decide if it needs a risk committee*
- *How your board can oversee third-party risk*
- *How executives and boards can get the risk information they need*

www.pwc.com/us/GovernanceInsightsCenter