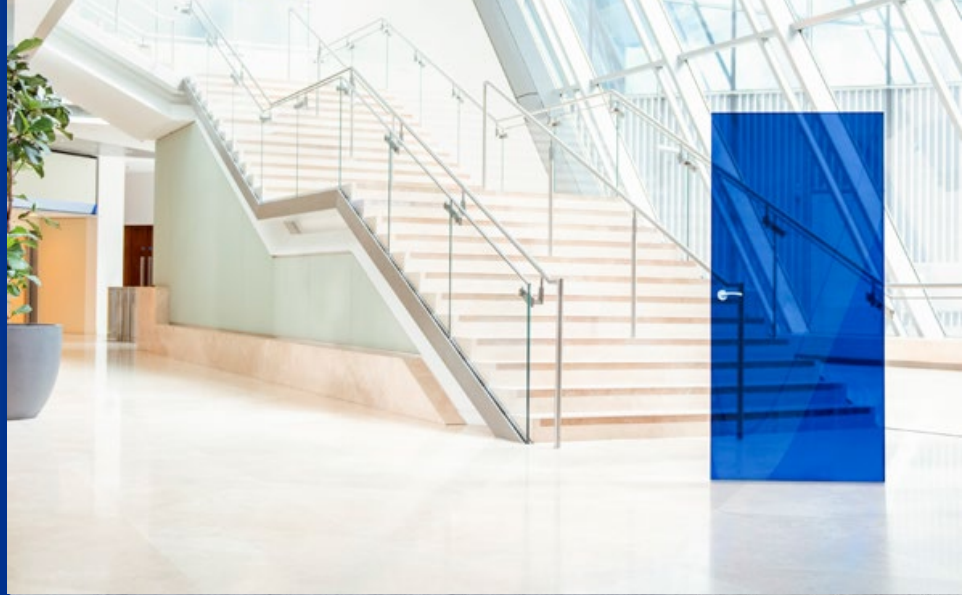
KPMG

Oversight of cybersecurity and data governance

KPMG Board Leadership Centre



The rapid shifts that companies made in 2020 and the first half of 2021 to keep their businesses up and running during the COVID-19 crisis – remote work arrangements, supply-chain adjustments, and increased reliance on online platforms – were a boon for organised crime, hacktivists, and nation-states. Cyberattacks of all types proliferated during the pandemic, and recent headlines of brazen attacks – from the SolarWinds[1] breach to the ransomware attack on the Colonial Pipeline[2] – with far-reaching implications for supply chains and the economy highlight the ongoing cybersecurity challenge facing companies.

Indeed, the acceleration of digital strategies, the likely continuation of remote work and hybrid work models, and increased regulatory scrutiny of data privacy continue to elevate cybersecurity and data governance on board and audit committee agendas. As boards refine their boardroom cybersecurity and data governance discussions and oversight processes, the following considerations may be helpful.

Periodically review management's cybersecurity risk assessment

Every company should be conducting cybersecurity risk assessments as a matter of course. What are the company's most valuable digital assets, and what are the greatest threats and risks to those assets? Are there security gaps?

How quickly can a security breach be detected? In a robust cybersecurity risk assessment, key areas of focus should include cybersecurity leadership and governance, human factors or "people risks," legal and regulatory compliance, business continuity, operations and technology, and information risk.

If the company has sufficient internal resources, the cybersecurity risk assessment can be conducted internally leveraging a standardised framework. However, as cyber threats become more sophisticated, the company may need to call on recognised security specialists for support.

Cybersecurity challenges and concerns: Through a boardroom lens

Our recent surveys of directors, including audit committee members, point to the continued and growing prominence of cybersecurity and data governance on board and audit committee agendas:

- The most important lessons learned – and significant changes made – as a result of the COVID-19 experience related to crisis readiness and digital strategy.[3]
- The top two global governance issues that directors cited as most relevant to their company's strategy in 2021 are cybersecurity and data privacy rules and practices.[4]
- Many audit committees continue to have substantial oversight responsibilities for cybersecurity (62 percent) and data privacy (42 percent).[5]

Indeed, third-party assessments and vulnerability management testing can be useful tools for assessing the robustness of cyber protections and whether existing processes are protecting the most valuable assets.

---

[1] SolarWinds Hack Victims: From Tech Companies to a Hospital, *Wall Street Journal*, December 21, 2020

[2] Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity, *New York Times*, May 14, 2021

[3] Views from the boardroom: 2021 pulse survey, KPMG Board Leadership Centre, January 2021

[4] Ibid

[5] Challenges presented by COVID-19: 2020 audit committee pulse survey, KPMG Board Leadership Centre, October 2020

Take a hard look at supply chain and other third-party vulnerabilities

Robust reporting of third-party risks – and close linkage with the company's risk management process – should be front and centre for the board. COVID-19 highlighted – and in many cases, accelerated – the heavy reliance on third-party relationships. How has the company's third-party risk profile changed as a result of COVID-19?

How has management's risk assessment changed to keep pace? Boardroom conversations should be particularly focused on whether the company's inventory of third-party risks is up to date and whether third parties' cybersecurity controls have kept pace with the changing risk environment. Most importantly, do they meet the company's own standards?

Make data ethics and hygiene a prominent part of the conversation

Beyond technical compliance with privacy laws and regulations – including global and/or national standards[6] – companies need to manage the tension between how they legally use customer data and customer expectations about how that data is used. As customers, employees, regulators, and other stakeholders pay greater attention to data privacy issues, this tension poses significant reputation and trust risks for companies. To that end, data hygiene should be a regular part of the data governance conversation: Are we collecting or holding data that we don't really need? Who has access to our data, including vendors and third-parties? A helpful touchstone for boards to keep in mind during data hygiene conversations: Just because we can, doesn't mean we should.

Insist on a cybersecurity scorecard

Many audit committees and boards review with management a cybersecurity scorecard showing (for the most recent period) the volume of identified cyber incidents, the materiality and nature of cyber incidents and how they are being managed, and key trends and developments in the external environment (e.g., in the private and public sector and on the legislative front). A cybersecurity scorecard can help to improve both the quality of cyber information and the quality of director dialogue regarding cybersecurity.

Understand the company's cyber-incident response plan

As one leading CIO recently told us, it's challenging to define a precise process or a set of concrete steps for managing a cyber incident because cyber incidents don't all have the same attributes and implications for the company or its customers. That said, incident management is a critical component of an overall cyber risk program and the effectiveness of the incident response plan depends on several factors. First, scenario planning is critical, and key players – including the communications, legal, and policy teams – need to be involved. Second, establish clear accountability. If you have a breach, who is responsible for doing what? The final piece involves decision-making – particularly if an incident has external implications (as many do). When third parties or customers might need to be notified, it's important to have a framework for making those decisions – sometimes very quickly.

Think carefully about the allocation of cybersecurity and data governance oversight responsibilities

Cybersecurity has evolved from being a fairly narrow IT/compliance-related matter typically on the audit committee's plate to a full board issue with the audit committee or another board committee conducting a deeper dive. Indeed, given the audit committee's heavy agenda, it may be helpful to have another board committee monitor cybersecurity and data governance issues and do the heavy lifting. While some boards have formed technology or risk committees to take on cyber-specific responsibilities, relatively few have standing committees devoted solely to cyber or technology issues.[7]

Where cybersecurity is addressed at the committee level depends on several factors, including the relative importance of cyber (and technology) issues to the company (i.e., is it central to the business or has the company experienced material failures related to cybersecurity?), the bandwidth of the existing committees, and the directors' skill sets. In short, recognise cybersecurity as a full-board responsibility and be clear and deliberate in allocating cyber-related responsibilities to board committees as appropriate to help bring the proper focus and oversight to the issue.

---

[6] For example, General Data Protection Regulation, and other relevant laws and regulations.

[7] According to the 2020 UK Spencer Stuart Board Index only five percent of the FTSE Top 150 companies have a board committee with "cyber", "technology", or "security" in the committee's name.

Reinforce the board's own cybersecurity protocols

In addition to greater vigilance regarding the security of board meetings and communications, directors' use of personal email, personal devices, or unauthorised software to conduct board business can present serious cyber risks. Has the general counsel or chief information security officer briefed the board on company cybersecurity protocols that apply to directors and employees in the context of the new operating environment? Companies with robust digital models that drive customer and supply chain channels, employee connectivity, and data-driven operations and insights are likely to fare best. That advantage going forward, however, will hinge on the underlying security and the company's overarching digital mindset.

Remember that cybersecurity is fundamentally a business issue

While a standardised or consistent way of discussing cyber risk and mitigation efforts is helpful, it's not uncommon for cybersecurity discussions to lapse into technical jargon. The board should insist that management (the CISO, CTO, chief data officer, etc.) discuss these issues with the board in plain English and in business context – i.e., the implications for strategy, risk, and reputation.

The KPMG Board Leadership Centre

The KPMG Board Leadership Centre offers support and guidance to non-executive directors, whether managing a portfolio non-executive career or embarking on a first appointment. Membership offers you a place within a community of board-level peers with access to topical and relevant seminars, invaluable resources and thought leadership, as well as lively and engaging networking opportunities. We equip you with the tools you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business.

Learn more at www.kpmg.com/uk/blc.

Contact us

Timothy Copnell
Board Leadership Centre
T: +44 (0)7801 520802
E: tim.copnell@kpmg.co.uk