KPMG

# Signals of change and the risk agenda

## March 2022: Cybersecurity

Chief Audit Executives (CAEs) continuously assess how to deliver on their objectives to maintain trust of shareholders and stakeholders. This includes considering signals of change in risks faced by their organization and, in turn, changing the focus of the Internal Audit plan needed. Our complementary series, "On the CAE agenda," provides a full view of top risks highlighted this period.

### Signals of change

Cybersecurity is seen in the spotlight across most organizations in recent times. From a rapidly evolving technological landscape to ever-changing threats, cyberattacks are now seen as one of the greatest risks to a company's health, and major cybersecurity investments are being made to protect organizations and maintain stakeholder trust.

According to the 2021 KPMG CEO Outlook, cybersecurity rose four places since 2020 and was selected as the greatest threat to an organization's growth over the next three years. KPMG also found that CEOs plan to spend more on digital in 2021, with 52 percent prioritizing data security measures.

### Risk considerations

- The adoption of cloud, the increase in demand for intelligent automation, robotics, and the rise of the Internet of Things have added new and more complex security risks to the business environment. Internal Audit will be challenged with assessing the cyber risks of these new and emerging technology areas.
- Ransomware has evolved to become increasingly prevalent, to the extent that organizations are developing stand-alone ransomware frameworks and asking Internal Audit to help them with the design and testing of effectiveness over ransomware-specific controls.
- Business change is impacted by technology change; regulatory environment changes; new business models; and the impact of mergers, acquisitions (M&A), or divestitures and initial public offering/special-purpose acquisition company transactions. Internal Audit will need to consider in depth the cyber risk and its associated impact related to these business changes.
- Some organizations have not been as prepared to address the changing regulatory landscape affecting every industry and, as such, have opened themselves up to the possibility of regulatory sanctions and fines. Internal Audit can play a key role in assessing the impact of new or existing regulations, as well as assessing the readiness of their organization in dealing with the new regulation, including assessing the first- or second-line cyber risk management and compliance capabilities.
- Increased reliance on third-party vendors has increased cyber risk by allowing third parties to access the organization's systems directly or through the processing of their private or confidential information or those of their customers. Internal Audit can perform assessments of their overall third-party program as well as perform detailed assessments of high-risk vendors.

### Questions to ask/actions to take

- Does the organization have a cyber risk management and assurance program? These programs provide a systematic and comprehensive approach to monitoring the extent to which cyber risks and stakeholder security requirements are being continually managed by the organization.
- Has the organization responded to the evolving ransomware threats? Have they developed and assessed a control framework and a response playbook to protect the organization? Has Internal Audit assessed the adequacy of these safeguards?
- Has a cyber maturity assessment been performed to review the organization's ability to protect its information assets and its preparedness against cyberattacks? Such assessments provide an effective framework for Internal Audit to consider follow-up deep dives into areas of higher risk.
- Internal Audit should assess the organization's overall strategy for dealing with emerging threats from a governance, architectural, operational, and technology perspective.
- Has the organization embraced security-by-design principles, and is the security organization undertaking design or technology reviews prior to final adoption and implementation of the technology?

## Contact us

**Richard Knight**
**Principal, Technology Risk Management, IT Internal Audit Solution Leader**
**E:** raknight@kpmg.com

**Learn more by visiting**

Building stakeholder trust through cyber security assurance (kpmg.us)

Evaluating cyber risk with internal audits (kpmg.us)

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

**kpmg.com/socialmedia**