



Technology companies lean on cyber to go faster and gain trust

Culture and technology are both crucial to a resilient cyber strategy

kpmg.com/techinnovation

Foreword

Tech company leaders name cyber security as both the greatest threat and greatest operational priority. In response, they are investing in skills, culture, and technology to build cyber resiliency, accelerate digital and business model transformation, and foster stakeholder trust.

Technology companies continue to provide the products and services that have powered digital transformation throughout the COVID-19 pandemic and allowed the wheels of global industry to keep turning. Yet this digital acceleration has also caused an explosion in the number of potential cyber vulnerability points due to an immediately virtual workforce, increased cloud adoption, hastily reworked supply chains, and new business partnerships. The rapid integration of new technologies also created an avalanche of new data to be stored and protected.

While some of these trends were already underway, the pandemic dramatically accelerated them. Technology companies were forced to react quickly like all others. In this new reality, technology company CEOs rank cyber risk as the greatest threat to their organization's growth over the next three years, higher than even supply chain disruption, climate change, or talent risk.¹

They also cite cyber security resiliency as their most important operational priority.¹ Additional research indicates the average cost of a data breach involving one million compromised records is \$52 million, and the cost escalates from there. When more than 50 million records are compromised, the average cost of the breach is \$401 million.²

Yet technology company leaders also recognize that opportunity exists. A strong cyber strategy enables a company to maximize the fullest benefits of digital transformation to quickly grow the business while knowing risks are managed. Sixty-one percent actually view their information security as a competitive advantage. More than half (57 percent) say their cyber security strategy is integrated with their growth strategy.³

The vast majority (77 percent) of tech CEOs believe a strong cyber strategy is critical to engendering stakeholder trust.¹ A strong cyber strategy incorporates both people and technology. The ongoing shortage of cyber talent dictates that all employees across all functions improve their cyber proficiency. Chief Information Security Officers (CISOs) are also stepping up—expanding their role to increase collaboration and their influence with other business unit leaders. From a technology standpoint, company leaders are increasing their investments in a variety of solutions to enhance organizational safeguards.

Cyber security has expanded beyond its traditional risk management and compliance focus to become a competitive advantage that enables stakeholder trust and fosters organizational resiliency. It is no longer exclusively an IT issue — it is a strategic priority that needs to be embedded throughout an organization's culture, technology, and operations.

1. KPMG CEO Outlook 2021, n=120.

2. IBM, Cost of a Data Breach report 2021.

3. KPMG Technology Industry Survey 2021, n=802.

Key findings

KPMG canvassed opinions on cyber security issues from tech company CEOs and senior executives in two separate global studies: the Technology Industry Survey and the CEO Outlook. Key findings include the following:

#1

Cyber security risk is the top threat to growth.

74%

say they are prepared for a future cyber attack.

#1

Cyber resiliency, with emphasis on cyber skills and culture, is the top operational priority.

61%

feel information security is a strategic function and a potential competitive advantage.

87%

think building a cyber security culture is just as important as building technological controls.

57%

believe their cyber security strategy is integrated with their growth strategy.

Sources: KPMG CEO Outlook 2021, n=120; and KPMG Technology Industry Survey 2021, n=802.

Investing in skills and technology

Building a human firewall

Technology CEOs recognize the threat environment changes constantly, and sophisticated solutions can be the foundation of a cyber security program. However, technology cannot protect everything. It needs to be reinforced by human behavior.

Many studies show that a large percentage of reported breaches include some element of human error. That makes it critical for businesses to develop and maintain a comprehensive cyber security strategy that incorporates skilling the workforce.

Human firewalling allows companies to move beyond cyber awareness and build an integrated, holistic approach to employee communication and training around cyber security — elevating employee behavior from a conscious choice to an ingrained habit. Tech CEOs recognize this and cite skills and culture as the top actions they are taking to build cyber and digital resiliency over the next three years.

Key steps tech companies plan to take to build digital resilience over the next three years.

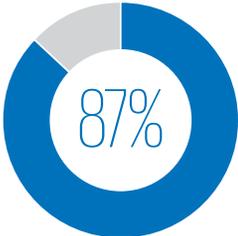
1 tie	Focus on improving skills in cyber security and other areas of technology risk
1 tie	Establish a strong digital and cyber risk culture, championed by senior leaders
2	Strengthen governance around operational resilience and the ability to recover from a major incident
3	Invest in a secure and resilient cloud-based infrastructure

Source: KPMG CEO Outlook 2021, n=120.

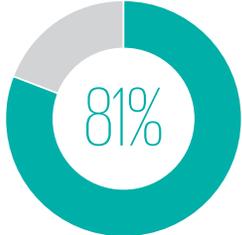
Tech companies are also part of a complex ecosystem of suppliers and partners, tied together through shared data and shared services. Traditional contracts and liability models seem ill-suited to this rapidly evolving supply chain. The cyber education, behavior, and culture within these partners must change too in order to bring security to all parties.

Tech CEOs report high agreement with the following statements, reinforcing that proficient cyber skills and culture are critical requirements, and companies must work with their partners and ecosystem to create a truly holistic defense plan.

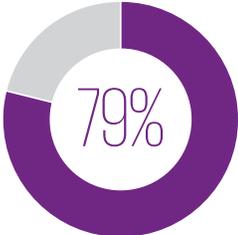
Building a cyber security culture is just as important as building technological controls.



It will take an industry-wide approach to properly address the issue of ransomware demands.



Protecting our partner ecosystem and supply chain is just as important as building our own organization's cyber defenses.



Source: KPMG CEO Outlook 2021, n=120.

Investing in skills and technology (continued)

Cyber security requires a technological village

Enterprises have long recognized that one technology or process is unable to mitigate cyber risk by itself. They need to invest continually and broadly to identify emerging threats, improve the organization’s response capabilities, and increase efficiency within their security function and business units. Tech leaders also feel that while cyber tools are necessary to enable enterprise success, they cannot be so intrusive that they hinder operational efficiency or growth.

When asked about specific security investments, tech firm executives confirmed they plan high investment across multiple areas over the next three years. Investment in automation, specifically, can reduce the manual workload,

ease skill shortages, foster greater efficiency, and help meet growing compliance requirements in a consistent and repeatable way. It can also help embed security and improve the user experience, as well as reduce the time to respond to a major cyber incident.

We are heading toward a further hyperconnected future in which the Internet of Things (IoT) and 5G networking will massively increase efficiency and enable radically different business models. But this also opens up organizations to new attack vectors and privacy concerns — demanding a shift to new, data-centric security models such as [zero trust](#). Another KPMG study – [The Data Imperative](#) – found that 44 percent of respondents believe an effective data strategy would have a high impact in improving cyber security.

Expected level of investment by technology companies over the next three years.



Source: KPMG Technology Industry Survey 2021, n=802. Percentages may not equal 100% due to rounding.

Cyber investment yields optimism

Technology company leaders are optimistic overall about the state of their information security function, as well as the degree to which it is integrated with their broader risk management efforts, third-party partnerships, and business unit leadership. Nearly three-quarters (74 percent) of tech CEOs say they are prepared for a future cyber attack, compared to 58 percent across all industries.⁴

They believe their increased investments and focus have yielded sufficient enterprise capabilities to largely mitigate cyber risks. This confidence, and the investment required to achieve it, is necessary because 77 percent of tech CEOs also believe that a strong cyber strategy is critical to engendering trust with key stakeholders.⁴



4. KPMG CEO Outlook 2021, n=120.

Technology company executives who agree with the following statements:

My company views information security as a strategic function and a potential competitive advantage.

61%

My company's cyber security risks are incorporated into its overall enterprise risk planning.

60%

My company is prepared to manage third-party risks from vendors that provide critical services and/or have access to sensitive data.

58%

My company's cyber security strategy is integrated with its growth strategy.

57%

Source: KPMG Technology Industry Survey 2021, n=802.

The redefined CISO

With technology companies blending on-site and remote workers, IoT devices, third-party partners, and service providers in dynamic teams and ecosystems, the CISO is taking a broader role in not only maintaining cyber security, but also overall organizational resilience.

As threats and regulatory expectations evolve, CISOs are taking on increased responsibilities and building relationships with a wide range of functions and business unit leaders. The CISO's role is moving beyond "protect and detect" to enabling the business to get up and running quickly after an incident, as well as helping the CEO preserve trust with customers, suppliers, regulators, and other stakeholders.

CISOs are interacting more with CEOs and boards, providing consistent updates on emerging threats and mitigation efforts, while maintaining their traditional relationships with Chief Technology Officers and Chief Information Officers. They are helping to integrate security into governance and management processes, education, and awareness, plus establishing the right mix of corporate and personal incentives to do the right thing.

CISOs are also leveraging this opportunity to enhance organizational resilience by working to embed security- and privacy-focused design principles throughout their companies' digital infrastructures. This expanded scope allows organizations to enhance their ability to mitigate cyber, regulatory, and business risks more effectively.

Seven steps that CISOs should consider to enhance their role.

1. Speak the language of the board

by thinking in terms of customers, revenue, costs, and return on investment.

2. Focus on operational resilience

like keeping the lights on and getting back to normal quickly following a crisis.

3. Invest time in building a network

within your organization, visiting different functions, learning how they operate and gaining trust.

4. Think about shaping the

workforce to the cyber needs of the business — as opposed to permanent roles and structures. Consider the ratio of employees to contractors and gig workers.

5. Build a business case for

automation, reflecting the efficiencies it brings and the value added from workers who are freed up for higher-level tasks.

6. Work out what zero trust means

for your business and see this as an ongoing philosophy rather than a one-off program.

7. Find ways to reach out

to peers in your sector, by joining existing industry bodies or forming less formal groups.



[Read more here on the evolving role of the CISO.](#)



Key considerations for company leaders in 2022



Expand the strategic security conversation

Change the conversation from cost and speed to effective security to help deliver enhanced business value and user experience.



Exploit security automation

Gain a competitive advantage through smart deployment of security automation.



Develop critical talent and skill sets

Transform the cyber security team from enforcers to influencers.



Protect the privacy frontier

Move to a multidisciplinary approach to privacy risk management that embeds privacy and security by design.



Adapt security for the cloud

Enhance cloud security through automation — from deployment and monitoring to remediation.



Secure beyond the boundaries

Protect the organization by encouraging the broader supply chain to be cyber secure.



Place identity at the heart of zero trust

Put identity and access management and zero trust to work in today's hyperconnected workplace.



Reframe the cyber resilience conversation

Broaden the ability to sustain operations, recover rapidly, and mitigate the consequences when a cyber attack occurs.

 [Read more about these considerations here.](#)

About the authors



Alex Holt is the global head of Technology, Media & Telecommunications (TMT) for KPMG and is based in Silicon Valley. A highly accomplished executive with over 20 years' international experience, Alex joined KPMG in 2012 as the chief operating officer in the U.K., taking up the leadership of the U.K. TMT sector in 2015. Alex relocated to the United States, joining KPMG in the U.S. in 2018 as the global account executive for several leading technology companies based in Silicon Valley. In 2020, he took on greater responsibility running the multibillion-dollar global TMT practice, leading thousands of KPMG professionals who serve clients across the TMT sector with a wide range of advisory, tax, and audit services. alexanderholt@kpmg.com



Mark Gibson is the Technology, Media & Telecommunications national sector leader for KPMG in the U.S. During his 30 years in public accounting and advisory, he has served clients in the technology, consumer products, and retail industries, as both an audit and advisory partner. Prior to his current role, Mark was the Seattle office managing partner. He serves as the account executive for several large clients in the Seattle and Silicon Valley markets and as global lead partner for a leading technology company, where he works with KPMG professionals from audit, tax, and advisory in more than 15 countries. mgibson@kpmg.com



Vijay Jajoo is a principal in the KPMG Cyber Security Services practice. He is an accomplished technology and management leader with over 20 years of experience specializing in IT strategy, enterprise security architecture, solution implementation, identity and access management, cloud security, and enterprise governance, risk, and compliance. Vijay helps global tech companies transform by establishing trust and embedding cyber security and privacy into product and service design. He drives cross-functional alignment to develop innovative solutions with advanced analytics and correlates siloed data sets to provide insights for effective risk mitigation decisions. vjajoo@kpmg.com

Contributors

Danny Le

Principal, Cyber Security Services
KPMG LLP
dqle@kpmg.com

Rik Parker

Principal, Cyber Security Services
KPMG LLP
rikparker@kpmg.com

Deepak Mathur

Managing Director, Cyber Security Services
KPMG LLP
deepakmathur@kpmg.com

Austyn McLoughlin

Managing Director, Cyber Security Services
KPMG LLP
austynmcloughlin@kpmg.com

How KPMG can help

KPMG firms can help you create a resilient and trusted digital world — even in the face of evolving threats. KPMG cyber security professionals can offer a multidisciplinary view of risk, helping you carry security throughout your organization so you can anticipate tomorrow, move faster, and get an edge with secure and trusted technology.

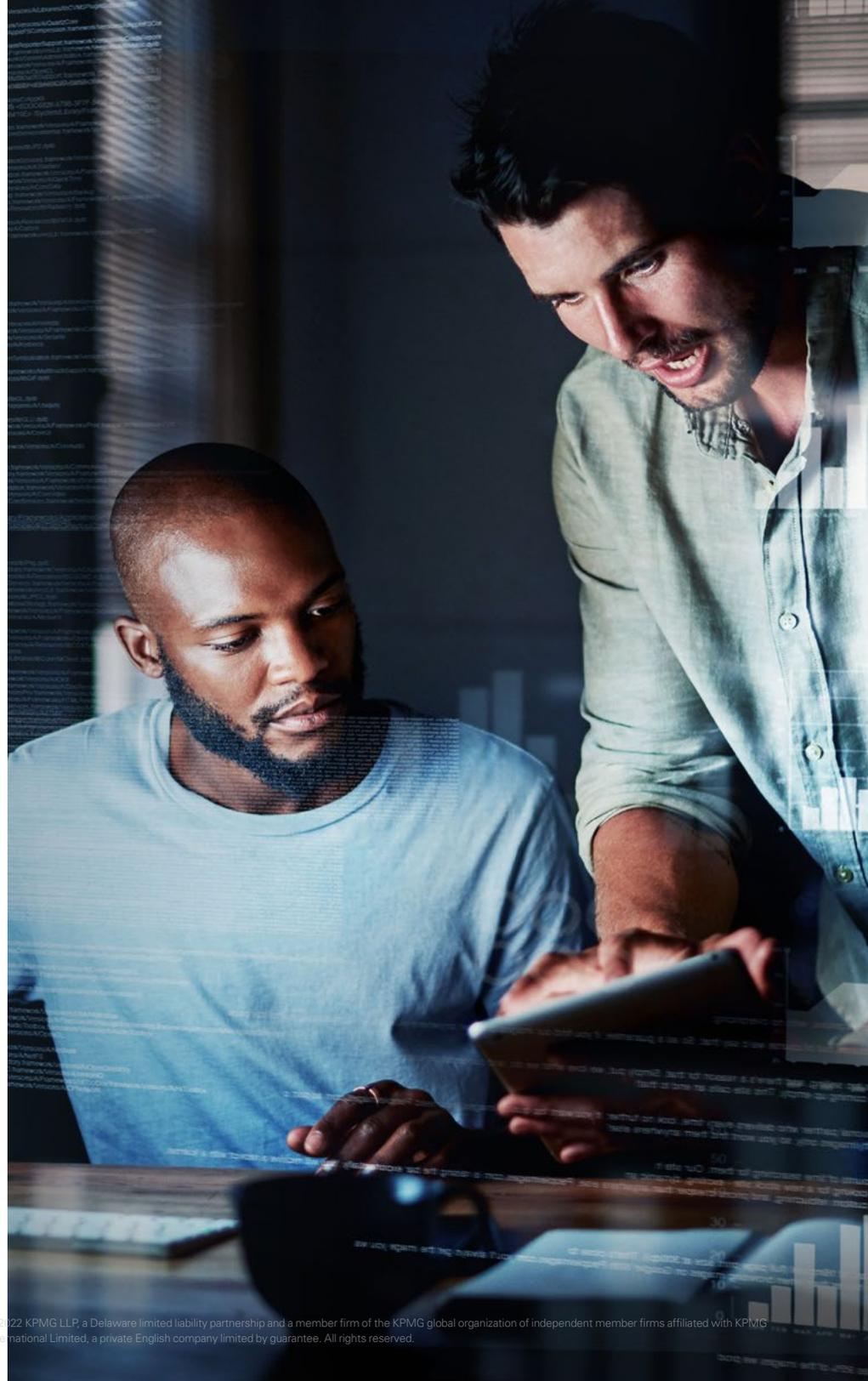
No matter where you are on your cyber security journey, KPMG firms have extensive experience and resources across the continuum — from the boardroom to the data center. In addition to assessing your cyber security and aligning it to your business priorities, we can help you develop advanced solutions, assist with implementing them, advise on monitoring ongoing risks, and help you respond effectively to cyber incidents.

KPMG firms bring an uncommon combination of technological specialization, deep business knowledge, and creative professionals who are passionate about enabling you to protect and build your business. We will help you create a trusted digital world, so you can push the limits of what's possible. Learn more [here](#).

About the research

The KPMG Technology Industry Survey, now in its ninth year, included responses from more than 800 global executives at technology companies. Twelve countries were included in the online survey, and about two-thirds (65 percent) of the respondents were C-level executives. The data collection for this publication was completed in the third quarter of 2021.

The KPMG CEO Outlook asked 1,325 CEOs to provide their outlook on the economic and business landscape, as well the impact the ongoing COVID-19 pandemic will have on their organizations' future. The survey was conducted from June 29 to August 6, 2021, and included leaders from 11 countries and 11 industries. There were 120 respondents from technology companies.



Related material



Human firewalling

Human firewalling allows companies to overcome the human risk factor in cyber security. This report explores the five steps organizations should take to increase awareness and build an integrated, holistic approach to employee communication around cyber security — elevating employee behavior from a conscious choice to an ingrained habit.



From enforcer to influencer

CISOs and cyber security teams are now responsible for building trust and resilience, forging a pragmatic security culture, and helping embed secure by design thinking into the digital infrastructure and data. To do this, they must see themselves as enablers and facilitators. This report identifies seven actions that CISOs should take to help keep organizations resilient and competitive.



Cyber security considerations for 2022

Looking beyond the digital shifts created from the pandemic, this hyperconnected world will likely face expanding cyber risks on multiple global fronts. This report identifies eight considerations that leaders should prioritize to help mitigate and minimize the impact of cyber attacks while protecting customers, data, and sustainability.



The Data Imperative

Digital transformation accelerated at most companies during COVID-19, resulting in tremendous new quantities of data that companies are not fully utilizing. This report outlines how data strategies must be prioritized and rewritten to capitalize on digital transformation investments.

Your contacts in Switzerland

KPMG AG

Badenerstrasse 172
PO Box
8036 Zurich

Dr. Matthias Bossardt

Partner
Head of Cyber Security &
Digital Risk Consulting

+41 58 249 36 98
mbossardt@kpmg.com

Dr. Thomas Bolliger

Partner
Cyber

+41 58 249 28 13
tbolliger@kpmg.com

Nicolas Tinguely

Director
Cyber

+41 58 249 21 44
ntinguely@kpmg.com

Yves Bohren

Director
Cyber

+41 58 249 48 95
ybohren@kpmg.com

[kpmg.ch/cyber](https://www.kpmg.ch/cyber)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence. If you would like to know more about how KPMG AG processes personal data, please read our Privacy Policy, which you can find on our homepage at www.kpmg.ch.

© 2021 KPMG AG, a Swiss corporation, is a subsidiary of KPMG Holding AG, which is a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.