KPMG

KPMG Cyber trust insights 2022

Building trust through cybersecurity and privacy

KPMG International | kpmg.com/cybertrust

Contents

Overview

Five crucial steps to building trust through cybersecurity and privacy

To today's businesses, trust is everything. In an uncertain, constantly shifting environment, customers, employees and investors look for organizations they can depend on. But building and protecting that sense of trust requires every part of the organization to work together to deliver a consistent, unified vision.

Now that we live in a digitized world, every part of the business depends on fairness, integrity and transparency in the way information is collected and processed. Systems should be resilient, dependable and able to respond quickly in the face of disruption. Whether you are a customer or client who wants to feel safe when transacting with the organization, or part of the broader ecosystem of partners, investors, regulators and society which surrounds every organization — digital trust matters.

Cybersecurity and privacy have a key role to play in building and maintaining that trust. Businesses are ramping up data collection, expanding the use of artificial intelligence (AI) and machine learning (ML) technologies and embracing the environmental, social and governance (ESG) agenda, all while facing increasingly exacting regulatory standards.

In the KPMG Cyber trust insights 2022, we surveyed 1,881 executives and conducted a series of discussions with corporate leaders and professionals from across the world to explore the extent to which the C-suite recognizes this, how they are meeting the challenge, and what they need to do next. We also explore the key role that chief information security officers (CISOs) can play in helping them do so. We identify five crucial steps towards building trust through cybersecurity: **treat cyber and privacy as a golden thread woven into the business; build internal alliances; reimagine the CISO role; secure leadership support;** and **reach out to the ecosystem.**

Key findings

Data deluge

Businesses are mining data at scale. Raising concerns over how data is protected, used and shared.

A majority of respondents have engaged in more extensive collection or analysis of customer data over the past year.

Investment in data-driven activities is increasing in priority for organizations.

Challenges of AI and ML

There are growing societal and business concerns over the ethics, security and privacy implications of adopting AI and ML solutions for big data analysis.

78% agree that AI and ML bring unique cybersecurity challenges.

3 in 4 say AI and ML raise fundamental ethics questions.

Value and trust

Trust matters more than ever — and is not just about reputation. Boosting trust creates competitive advantage and adds to the bottom line.

More than 1/3 of organizations recognize that increased trust leads to improved profitability.

But 65% report that information security requirements are shaped by compliance needs rather than long-term strategic ambitions.

Rising regulation

Regulators are paying greater attention to these issues, and many organizations are concerned about navigating an increasingly complex global regulatory landscape.

36% worry about their ability to meet existing or new cybersecurity regulation when activities are outsourced to digital service providers.

34% worry about corporate-reporting disclosures related to cybersecurity.

Trusted communities

External partnerships are expected to also be vital to success in hyperconnected ecosystems, but practical barriers stand in the way of collaboration.

79% say constructive collaboration with suppliers and clients is vital, but only 42% report doing so.

60% admit their supply chains are leaving them vulnerable to attack.

Evolving CISO

Do organizations recognize the role the CISO can play in helping them embed an organization-wide approach to digital trust?

1/2 of executives doubt that the relationship between the board and the CISO is characterized by 'high trust.'

1/3 say the CISO is not viewed as a key executive and has less influence than they need to protect the organization and its data.

Trusted purpose

Have businesses recognized the connection between digital trust and their environmental, social and governance (ESG) agenda?

Less than 1 in 5 say the CISO team is an integral part of the ESG team.

50% report that the CISO team plays a very limited role or no role in ESG.

Source: KPMG Cyber trust insights 2022

1

Digital evolution

The business case for investing in trust

What do we mean by trust?

A clear definition of trust can help companies take an active role in measuring it, increasing it, and unlocking a broad range of tangible potential benefits.

Digital trust is the confidence stakeholders have in the ability of an organization to harness digital technology to protect their interests and uphold societal expectations and values.

While each organization is likely to have differing priorities and may use different language to describe aspects of digital trust, the concept typically covers:

Security and reliability

Aiming to ensure that an organization's technology and data is well-protected, while operating as designed.

Inclusive, ethical and responsible use

Aiming to ensure an organization designs, builds and operates its technology and data as a steward for people, society at large, its environment and other stakeholders.

Accountability and oversight

Aiming to ensure an organization clearly defines responsibilities for trustworthiness and assigns and tracks those responsibilities.

Why it matters: Increased trust can increase profits and customer loyalty

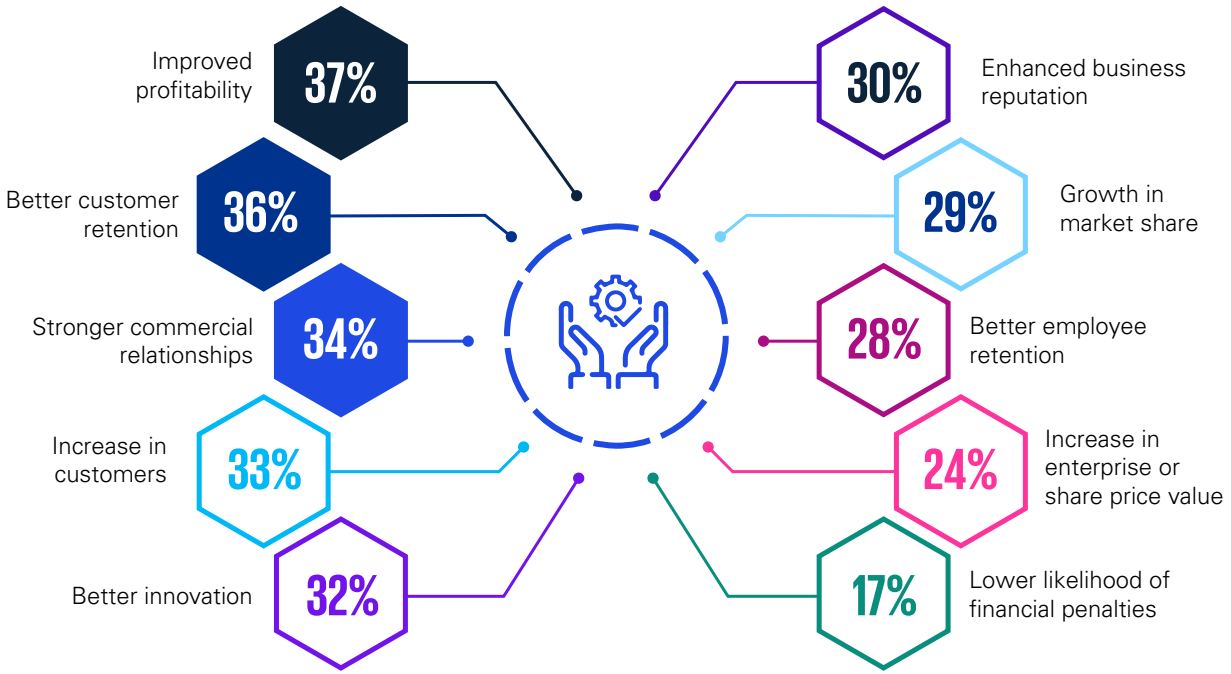
According to our respondents, the top three expected benefits of increased trust are:

1. Improved profitability
2. Better customer retention
3. Stronger commercial relationships

Other potential gains include enhanced innovation, improved employee retention and a bigger market share.

The top benefits of increased trust

Chart shows percentage of respondents who selected each option in their top three.



Source: KPMG Cyber trust insights 2022

Businesses are investing in data and focusing on the customer experience

Digital transformation is well underway: across every industry, businesses are overhauling their technology and placing advanced data and sophisticated analytics at the heart of their operations. Over the next 3 years, organizations plan to make a series of investments in digital tools to power their growth, optimizing their customer and client interactions, streamlining business operations and unlocking the value in their data. Each new data activity exposes companies to potential vulnerabilities and reputational risk that should be guarded against to maintain trust.

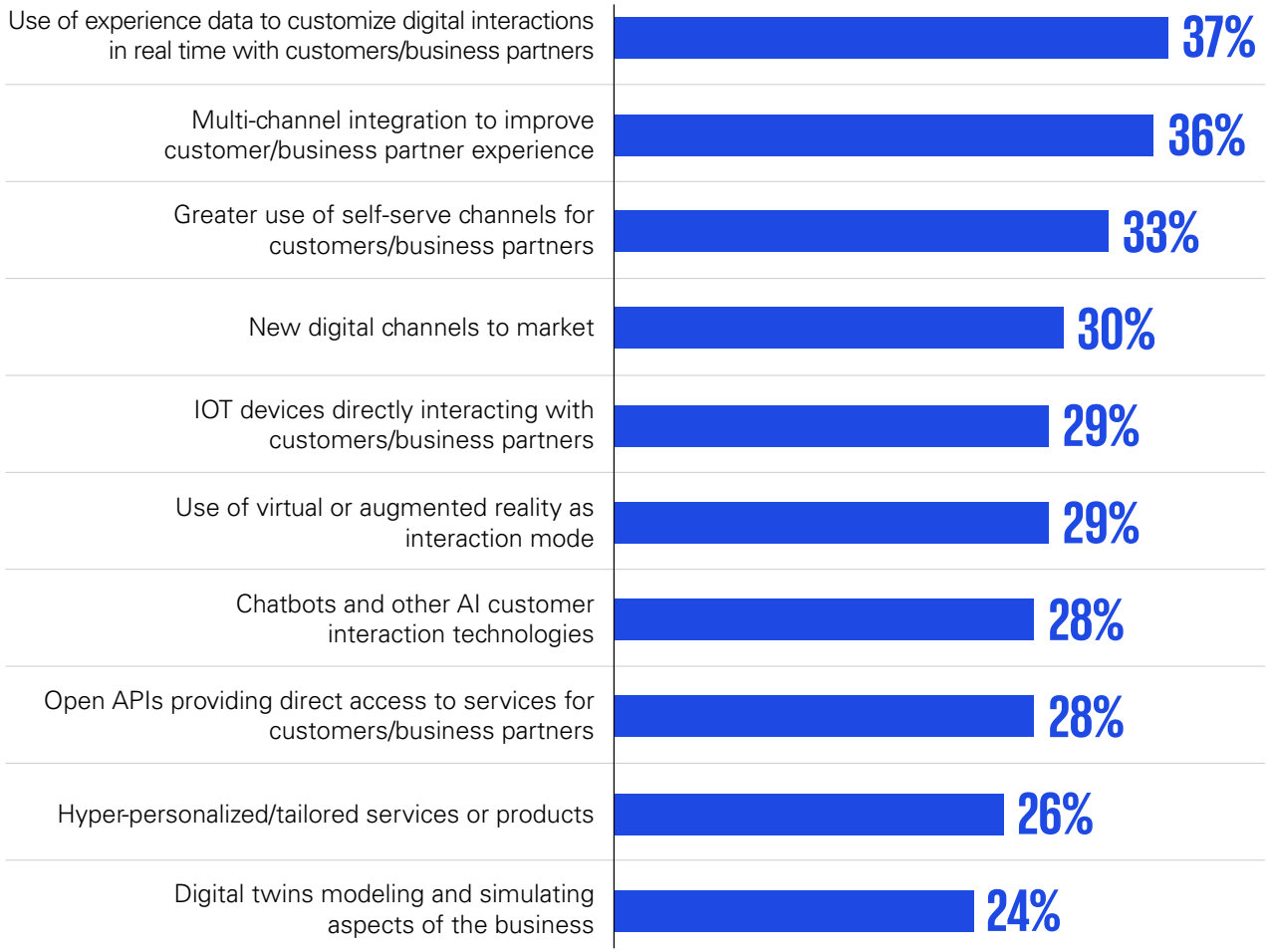
According to KPMG's Global Tech Report, **61 percent of businesses expect to embrace disruptive new tech platforms within 2 years** and, over the next 3 years, say they will increasingly ramp up their investment in internet of things (IoT), edge computing and 5G and, to a lesser extent, virtual reality (VR) and augmented reality (AR).

In the same KPMG report, **the digitization of customer channels is cited as the second-most serious cybersecurity challenge faced by organizations**, just behind the adoption of hybrid working environments. We asked businesses where they were investing in their digital experience. Thirty-seven percent of businesses are focused on the use of experience data to customize digital interactions in real time, while 36 percent are investing in multi-channel integration to improve the customer experience.

As these trends gather pace across industries, the privacy expectations of customers are also changing. Increasingly, users expect to be able to customize privacy controls across their devices and channels, requiring organizations to engineer flexible controls into the design of future products and services.

The top areas of digital experience investment

Chart shows percentage of respondents who selected each option in their top three.



Source: KPMG Cyber trust insights 2022

> **Protecting client trust is what drives our investments in cybersecurity and privacy."**
>
> **Bashar Abouseido**
> SVP and CISO, Charles Schwab

Cybersecurity is changing and data matters more than ever

Against this backdrop, companies must now strengthen their safeguards in the areas that are crucial to securing stakeholder trust. Over 80 percent of our respondents recognized the importance of improving cybersecurity and data protection including increased transparency around data use. In particular, 51 percent regarded the protection of IT assets from attack as being extremely important.

As organizations drive digital transformation, budgeting for cybersecurity and privacy investment should follow, and increasingly be seen as integral to those strategic initiatives. "The success of transformational digital services will likely depend on whether organizations can weave security and privacy into their design and implementation," says Allan Cockriel, CISO at Shell. He further notes, "we're really focusing on what we call 'secure by design standards' in the way we build technology. We want those standards to be transparent to our customers because our obligation is to maintain and enhance trust."

"Protecting client trust is what drives our investments in cybersecurity and privacy," says Bashar Abouseido, SVP and CISO at Charles Schwab. "We go above and beyond to maintain the trust we have with our clients through both proactive, continuous improvements to privacy controls and transparency around how we protect their data."

KPMG perspective: Trust is becoming fundamental to the success of emerging technology

Emerging technologies such as distributed ledger technology (DLT), quantum computing, 5G networks, AI/ML, and augmented and virtual reality are developing rapidly, and promise to transform the way businesses operate.

Yet the successful rollout of future applications (connected economy, smart systems, NFT, metaverse, etc.) that rely on these technologies will likely be governed by an organization's ability to instill trust across multiple dimensions. This means embedding security and privacy controls with transparency, reliability and integrity.

Atul Gupta
Partner and Head of Digital Trust and Cyber Security Services
KPMG in India

2

Trends in digital trust

Understanding the drivers of trust

Facing the ethical challenges of AI

The growing use of AI and ML technologies in many businesses is creating a new (and, to date, ill understood) set of trust issues. KPMG's research shows that businesses are determined to embrace AI and ML, with expected benefits ranging from increased efficiency and productivity to improved ability in generating predictive insights into customers and markets.

The danger is that these technologies, if badly handled, raise cybersecurity and privacy risks with potential for reputational damage and regulatory sanction.

Organizations are starting to recognize these risks. More than three-quarters of our respondents (78 percent) agree that AI and ML bring unique cybersecurity challenges.

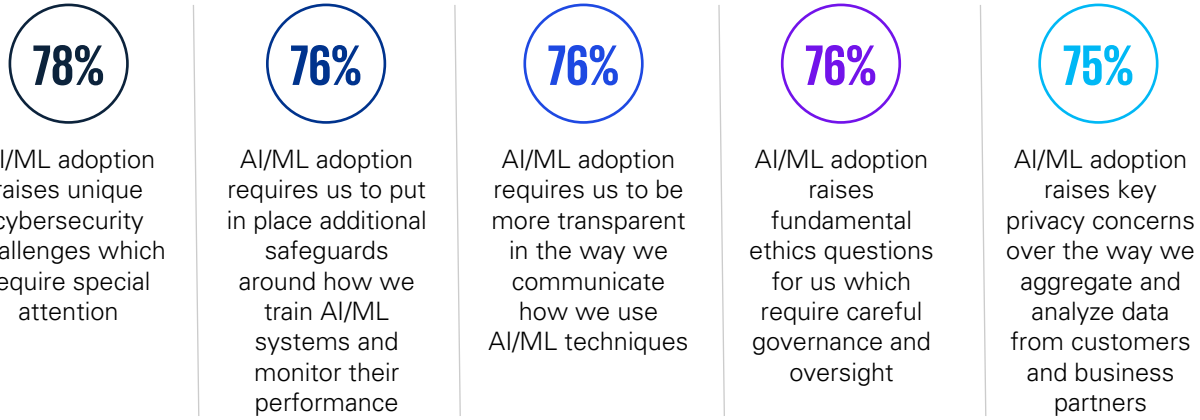
Almost as many believe there are fundamental ethical questions to resolve as they adopt these technologies and say organizations will need to communicate more openly about how they are managing those issues.

All of which underlines the important role cybersecurity and privacy teams play in helping shape the ethical debate and managing risks.

"We're doing a lot of work on adversarial AI — things like data poisoning, machine drift, AI attacks — because we believe that will be the next wave of attack," says Ann Johnson, Corporate Vice President, Microsoft Security Business Development.

AI and ML create new challenges for the information security team

Chart shows percentage of respondents who agree or strongly agree.



Source: KPMG Cyber trust insights 2022

KPMG perspective: Ethical AI

Organizations know they must become data-driven or risk irrelevance. Many are scaling AI to automate data-driven decision-making, but AI brings new risks to brand and profitability. The technology has the potential to drive inequality and violate privacy, as well as limiting the capacity for autonomous and individual decision-making.

You can't simply blame the AI system itself for unwanted outcomes. Trustworthy, ethical AI is not a luxury, but a business necessity. Growing numbers of business leaders recognize this — but trust is not secured without effort or challenges.

Not least, what is considered ethical and trustworthy in one sector or region may not hold in another. There is no one-size-fits-all solution and copying existing frameworks is ineffective. Trustworthy AI can only be achieved with a holistic, technology-agnostic and broadly endorsed approach to awareness, AI governance and risk management.

For example, AI impact assessments should involve the right stakeholders to identify risks. AI needs to be aligned with organizational and stakeholder values. Organizations should carefully assess compliance with laws and regulations, as well as AI return on investment. Decisions need to be traceable and auditable. And all these protections must be implemented without impeding innovation.

Sander Klous
Partner, D&A Business Development
KPMG in the Netherlands

> **"We're doing a lot of work on adversarial AI because we believe that will be the next wave of attack."**
>
> **Ann Johnson**
> Corporate Vice President
> Microsoft Security Business Development

The regulatory outlook

As societal concerns over digital trust grow, so too does the interest of lawmakers and regulators, with greater demands for transparency and oversight. According to the KPMG Cyber trust insights 2022 survey:

36%

of respondents worry about their ability to meet existing or new regulation of cybersecurity when activities are outsourced to digital service providers.

34%

worry about corporate-reporting disclosures related to cybersecurity.

31%

worry about the growing demands around critical infrastructure, which is the subject of increasing regulation in the UK, the EU and the US.

To add to the burden, international organizations must cope with an increasingly complex, diverse and sometimes contradictory tapestry of extra-territorial regulation. "One challenge for CISOs is that stakeholders in different regions construe different meaning from the same regulations," says Ulrich Baisch, CIO, Bechtle, one of Europe's largest IT providers. "You need to have a clear concept of what you can and can't do."

KPMG perspective: Regulatory drivers

Globally, growth of cybersecurity and privacy regulation is accelerating. More than 137 countries now have some form of data-protection regime, often claiming extra-territorial jurisdiction over services offered into the country or the data of citizens of that country. More mature privacy regimes are moving into a second generation of regulation while confronting new privacy challenges driven by technology adoption. For example, discussions about the regulation of AI are now being formalized in draft legislation.

In addition, countries are implementing increasingly strict critical infrastructure cybersecurity regulations as concerns grow around attacks on industrial control systems. These regulations are moving from self-assessment to more directive control frameworks, including mandatory incident reporting and external audit.

Regulators are also being more prescriptive in their control frameworks, while also seeking to reinforce the independence of the CISO and their role in setting internal control standards. More holistic resilience requirements, focusing on business recovery in extreme but plausible scenarios, are also emerging in sectors such as finance.

Corporate requirements for transparency over cyber risks are under debate, along with growing requirements for the disclosure of ransomware incidents. Companies should invest to automate compliance monitoring and reporting; maintain a regulatory watch; and consider privacy and security regulatory trends when developing new services and products.

David Ferbrache
Global Head of Cyber Futures
KPMG International

Looking beyond regulation

Digital trust should be part of the ESG agenda, and of course cybersecurity and privacy will likely be part of that. "ESG is integral to the business as a whole, but naturally the CISO plays a key role, in particular when it comes to social and governance-related issues," says Bechtle's Ulrich Baisch.

But more work is needed to make that a reality. Fewer than one in five organizations describe security as an integral part of the ESG team — and the majority report that it plays a very limited role. Organizations also need to recognize the social imperatives and growing expectations around these topics.

Within organizations, those individuals responsible for ESG should work collaboratively with those responsible for cybersecurity (often, the CISO) and data privacy (often, the DPO).

> **"ESG is integral to the business as a whole, but naturally the CISO plays a key role, in particular when it comes to social and governance-related issues."**
>
> **Ulrich Baisch**
> CIO, Bechtel

KPMG perspective: ESG and societal responsibility

Organizations that truly embrace the ESG agenda can earn the trust of their customers and reinforce the strength of their brands. In today's digital world, boardrooms, investors, regulators, customers, and the wider public expect transparent reporting on the organization's cybersecurity and privacy posture. Stakeholders want to feel confident that boards and executives appreciate the social implications of striving to ensure the resilience and integrity of critical services, while protecting the information they hold in trust.

Key considerations for these stakeholders include:

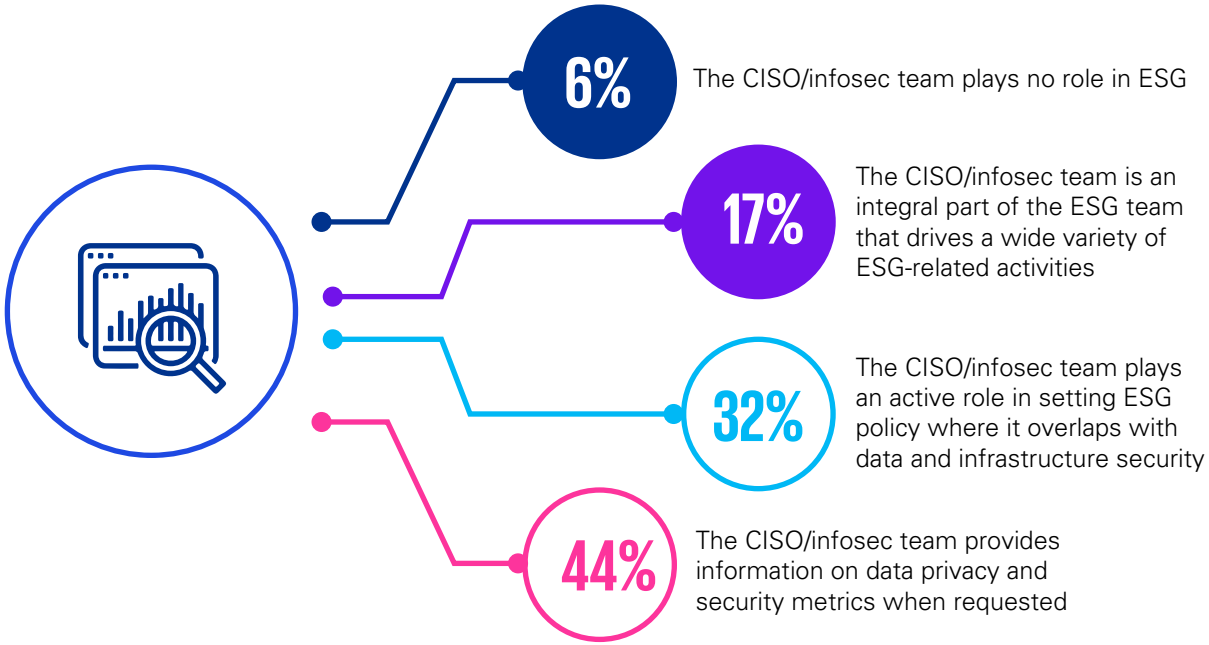
- Proactive monitoring of digital assets to help ensure access to safe and reliable content in a time of increased online exploitation and weaponization of information through 'fake news' and 'deep fakes'.
- Helping protect customers, particularly those below the cyber poverty line, against cyber-enabled fraud and identity theft.
- Aiming to ensure ethical adoption of technologies such as AI and ML, which gather and analyze customer data.
- Maintaining the reliability, integrity and availability of the digital services that we, as a society, have come to rely on.
- Demonstrating a broader commitment to building cyber skills and capacity, within their supplier ecosystem and beyond.

Srinivas Potharaju
Partner, Digital Trust
KPMG in India

Siddharth Durbha
Director, Digital Trust
KPMG in India

Most CISOs are only passively involved in ESG policies and activities

Chart shows percentage of respondents who selected one option as their top choice.



Source: KPMG Cyber trust insights 2022

KPMG perspective: Driving trust by going beyond the regulatory minimum

Forward-thinking organizations are incorporating data privacy metrics into ESG reporting frameworks.

This enables them to build trust while helping to ensure regulatory requirements are, at a minimum, being met. Often, as part of driving stronger trust, organizations are proactively seeking to exceed regulatory minimum standards, so stakeholders feel more confident that their personally identifiable information is being appropriately collected, used or disclosed — not only from a legal perspective but from a perspective that fits within the organization's articulated ESG narrative."

Sylvia Klasovec Kingsmill
Global Privacy Lead
KPMG International and Partner
KPMG in Canada

3

Building a community of trust

The power of collaboration and partnership

Today's digitizing businesses do not operate in a vacuum; increasingly, they are active members of broader partnerships and collaborations. This adds to the challenge facing cybersecurity teams: they should build faith in the ecosystems their organizations inhabit, by collaborating with partners to help secure mutual trust — and trust in the ecosystem as a whole.

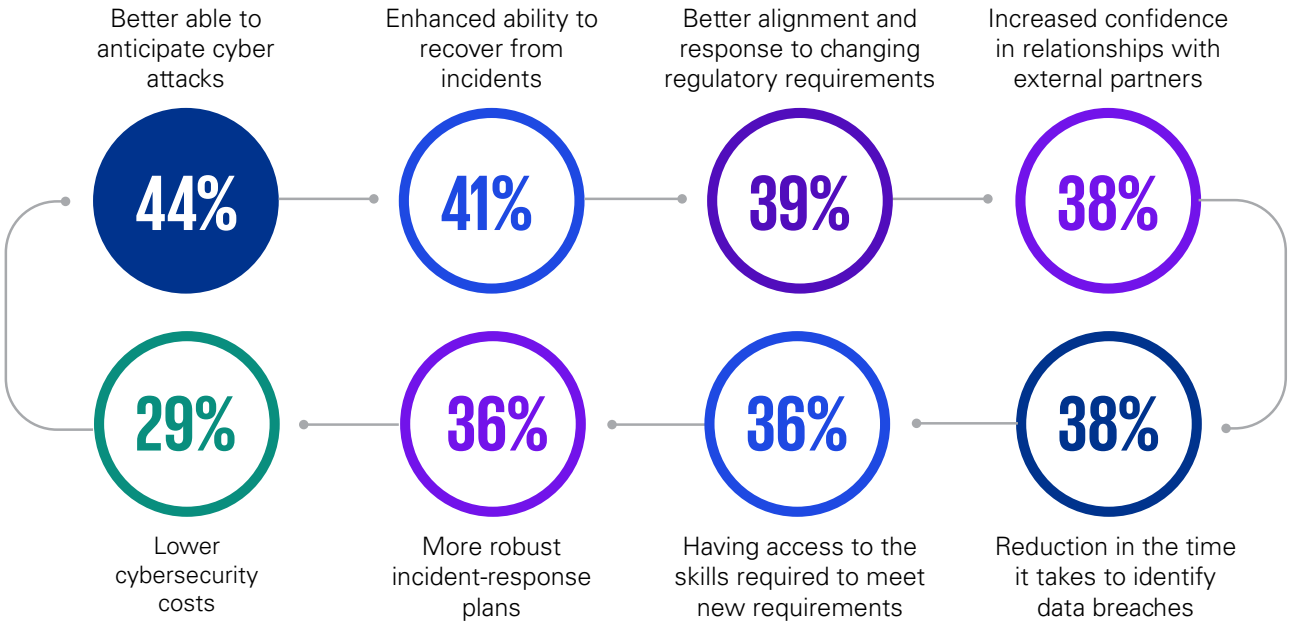
There is strength in numbers. In the KPMG Cyber trust insights 2022 survey, almost half of our respondents (44 percent) say that collaboration on cybersecurity across the broader ecosystem will help them anticipate attacks, for instance.

Although collaboration may be desirable, it's not always straightforward. More than one-third of respondents (38 percent) say that privacy concerns stand in the way of external cybersecurity partnerships, and 36 percent worry about revealing too much about their own security arrangements. Other problems include regulatory restrictions, lack of support from the C-suite and lack of resources.

> **Having a standard, and saying your firewall rules meet that standard, is a completely different data point that generally doesn't give away intricate details and helps enable trust.**
>
> **Mark Thompson**
> Chief Strategy Officer, International Association of Privacy Professionals (IAPP)

Collaborating on cybersecurity across the broader ecosystem can help organizations anticipate and recover from attacks

Chart shows percentage of respondents who selected each advantage in their top three.



Source: KPMG Cyber trust insights 2022

There are practical solutions, according to Mark Thompson, Chief Strategy Officer at the International Association of Privacy Professionals (IAPP). "If I gave you my firewall rule parameters, there is a risk you could see a vulnerability or a gap," he says. "But having a standard, and saying your firewall rules meet that standard, is a completely different data point that generally doesn't give away intricate details and helps enable trust."

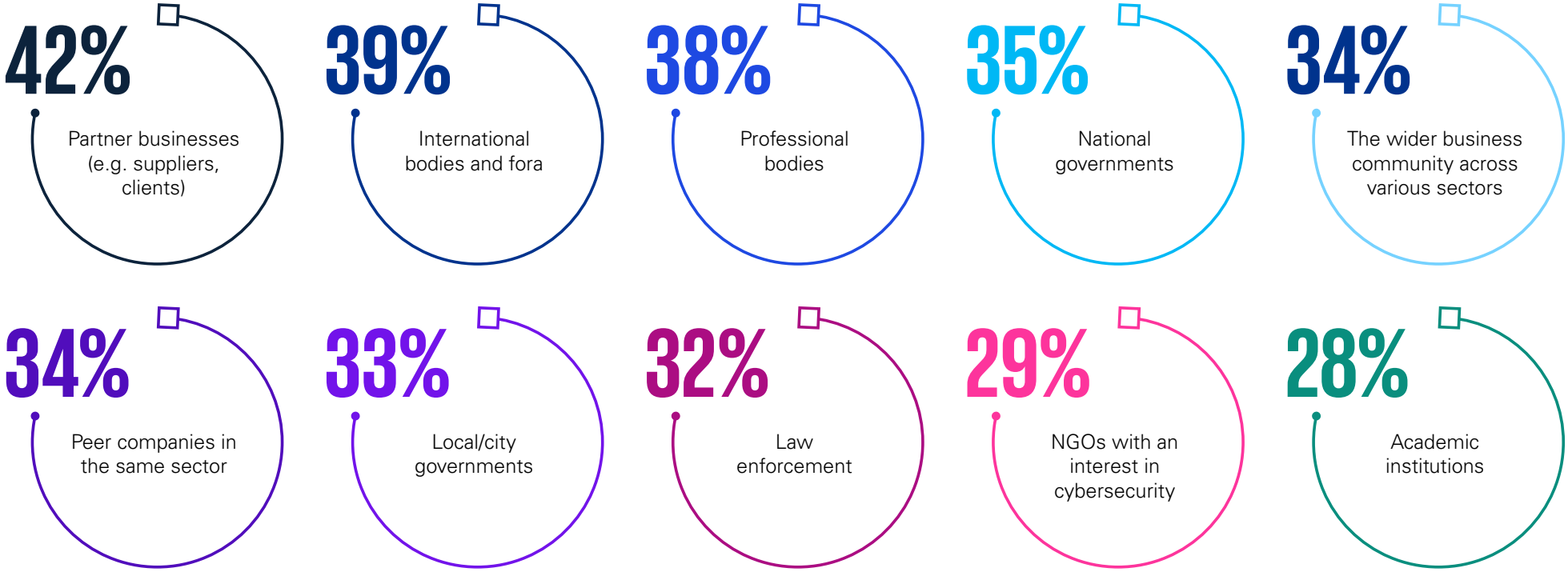
The immaturity of standards and best practices for information sharing may help explain why fewer than half of companies are collaborating or exchanging information with key partners. Even though 79 percent say that constructive engagement of suppliers is vital to effective cybersecurity, only 42 percent of respondents say they are actually working together to achieve it.

But this reluctance could cause serious harm. More than half of companies admit they do not know whether their defenses are strong enough to stop attackers from exploiting procurement and supply chain vulnerabilities.

This more limited approach to collaboration cannot continue; it fails to offer sufficient protection to either individual organizations or their ecosystems, undermining trust in both. More than half of our respondents (53 percent) worry that their organizations are not proactive enough in their cybersecurity collaborations — they may well be right.

More cybersecurity partnerships are needed across the ecosystem

Chart shows percentage of respondents who selected all that apply.



Source: KPMG Cyber trust insights 2022

KPMG perspective: The value of unity

Effective community building is vital in addressing cybersecurity challenges: individual organizations should work together. However, significant questions regarding risk management, reputation, law, and strategy can still impede that goal.

No organization can address these challenges alone, so it's important to combine resources and coordinate effectively. Working in concert, both public and private organizations can secure additional efficiencies, perspectives and resources.

To build trust and community, each party should recognize what is possible, where the barriers are, and how to overcome them. For example, some organizations are using existing protocols, such as the NIST cybersecurity framework, to create a common language and terminology when partnering with other organizations. Others are focusing on how to help ensure proprietary information stays within the organization. Cooperation agreements based around common operating principles can help organizations develop relationships and support digital infrastructure, while maintaining privacy and strengthening mutual trust among partners.

There is also a need to recognize that the traditional security paradigm is less relevant in such an interconnected landscape. Instead, a focus on resilient thinking makes more sense. Rather than attempting to defeat bad actors solely by isolating and controlling systems, there is a need for a more coordinated and cooperative approach.

Prasad Jayaraman
Principal, Cyber Security Services
KPMG in the US

4

The evolution of the CISO

The contribution of the CISO to building trust

Enter the CISO

Sometimes seen as putting the brakes on innovation and growth initiatives, CISOs are now in a position to play a crucial role as enablers. By operating as one of the organization's ultimate guardians of trust, they can be a driving force of its success.

"CISOs can really enhance and improve trust, but often what they do is generally driven by their organizational priorities," says IAPP's Mark Thompson. "There is a need for them to start stepping into that space — to help the organization drive and change the dynamic."

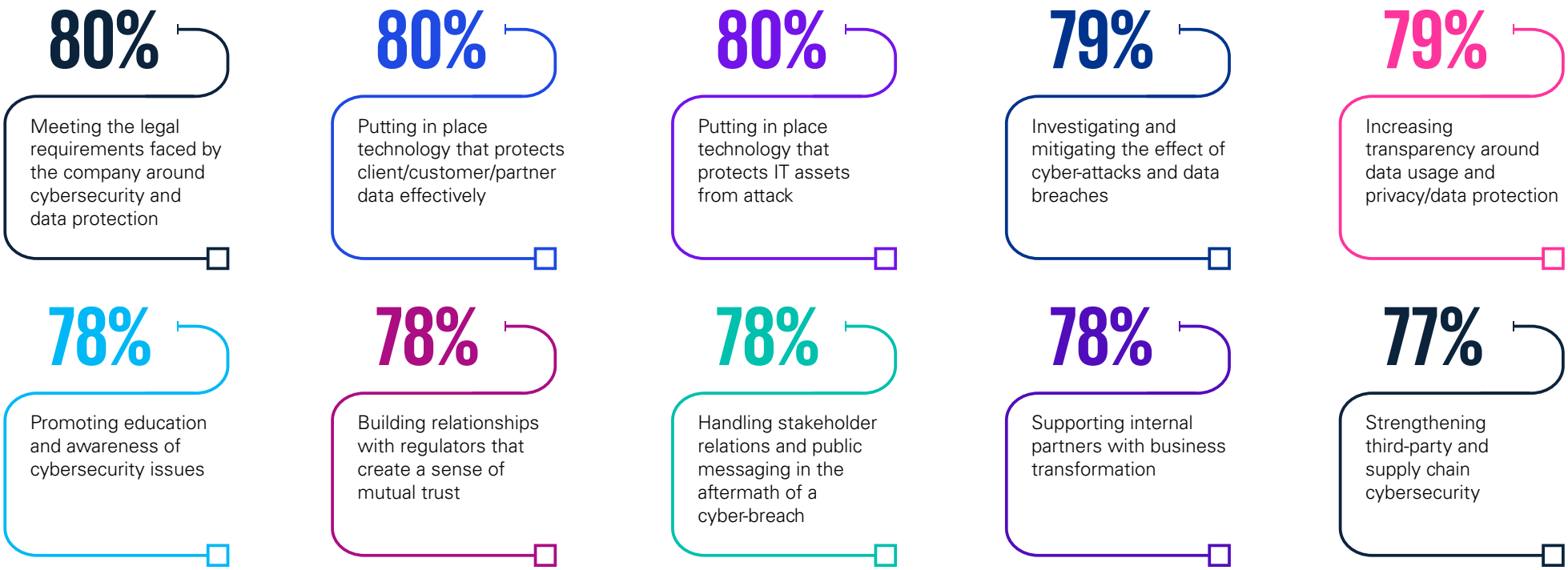
CISOs themselves recognize what is at stake. More than three-quarters of respondents (77 percent) say increased trust is a key objective of their cyber risk programs.

And organizations display high levels of confidence in their cybersecurity capabilities: 74 percent claim to have seen cybersecurity improvements over the last 12 months — with more than one in four saying significantly so. This confidence is combined with a strong belief in the CISO's ability to deliver on crucial tasks.

But do CISOs feel able to meet those expectations?

Organizations display high levels of confidence in the CISO

Chart shows percentage of respondents who rate each activity as 'effective.'



Source: KPMG Cyber trust insights 2022

It's interesting, then, that many CISOs are struggling to secure a mandate to pursue their objectives. There can often be difficult conversations, says Microsoft's Ann Johnson. "What data are we going to share? How are we going to store it? How are we going to use it from an AI-ML standpoint? How are we going to protect it? The CISO has to be involved in every single one of these conversations, and they are not easy conversations to have," Johnson adds.

Almost two-thirds of respondents (65 percent) say information security is seen by their organizations as a risk-reduction activity, rather than a business enabler. Moreover, 57 percent say senior leaders do not understand the competitive benefits of enhanced trust enabled by better information security. Does this disconnect suggest the CISO needs to do more to deliver a cybersecurity reality check?

Build a relationship with senior leaders

It would be unrealistic and unfair to expect CISOs alone to push the trust agenda across cybersecurity and data privacy. Their interactions with colleagues such as the chief data officer and the chief privacy officer will likely be crucial. If they collaborate effectively, this trio can begin to make practical changes to enhance trust.

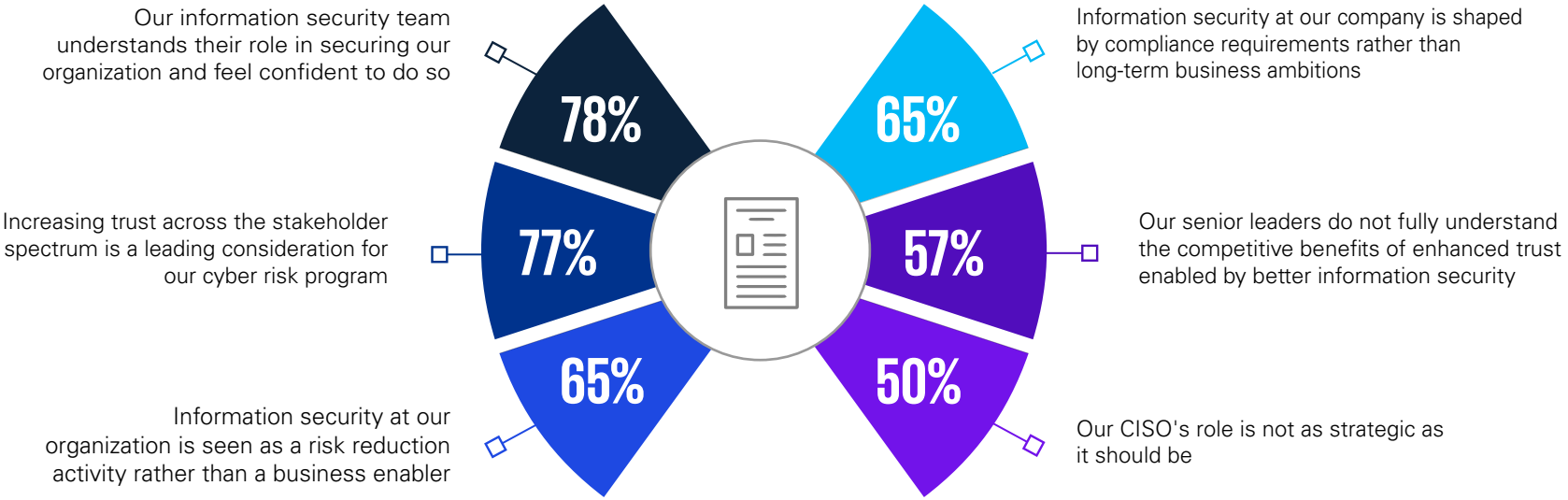
The good news is that organizations' most influential leaders believe CISOs and the broader cybersecurity function should be involved in transformation from an early stage.

Forty-five percent of C-suite respondents now see the CISO as a key executive and the profile of the CISO role has grown rapidly over the last 5 years driven by digital transformation, growth in cyber crime, and rising regulatory expectations.

One way for CISOs to change that perspective may be to shift the focus away from more technical issues — after all, more than half of C-suite respondents say that boards do not understand them anyway. The challenge of stepping into that strategic role remains for CISOs. Companies are demanding they engage at a senior level, focus on the needs of the business, and aim to ensure cyber is seen as a golden thread that runs through every aspect of business strategy, planning, investment and delivery.

CISOs are ready to step up — but are they being allowed to?

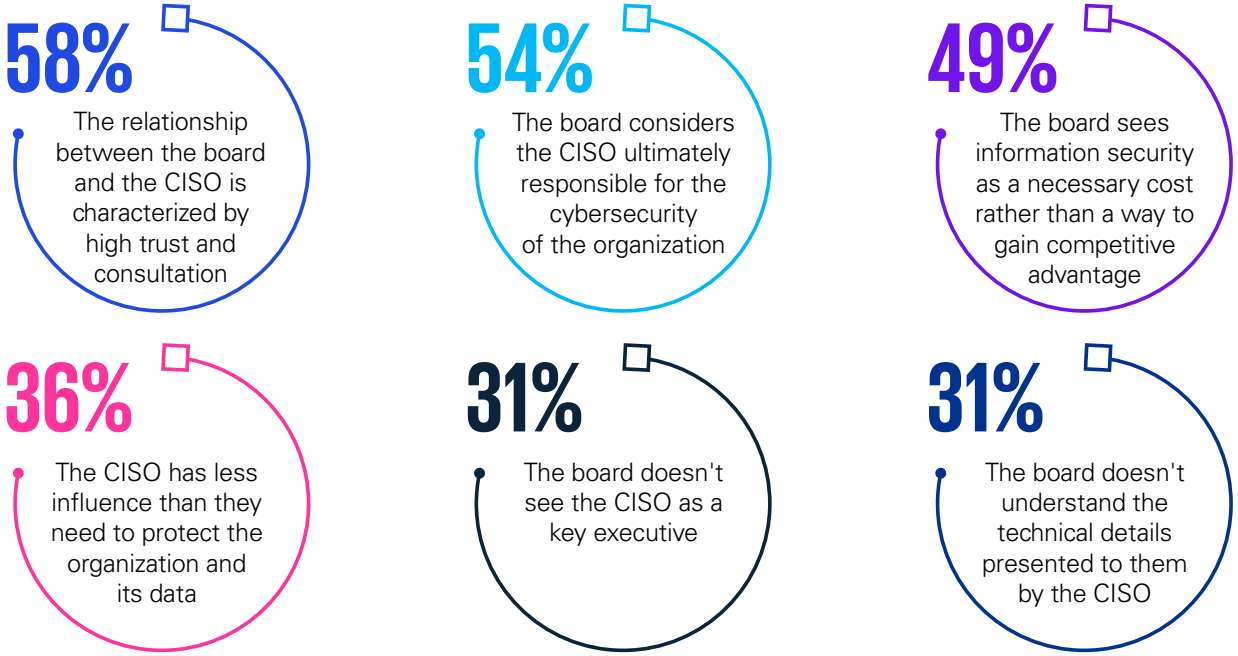
Chart shows percentage of respondents that agree or strongly agree.



Source: KPMG Cyber trust insights 2022

Boards have mixed opinions of CISOs' influence

Chart shows percentage of respondents who indicated statements are true.



Source: KPMG Cyber trust insights 2022

The challenge of quantifying risk

Many organizations are making good progress on risk modeling and assessment in an area that has been notoriously resistant to analysis. Three-quarters of organizations say they have implemented risk modeling to quantify and visually report cyber risk to the board, yet only 58 percent describe their approach to quantifying cyber risks as 'robust' and agree that their cyber risk scenarios are tailored to business needs.

More positively, more than two-thirds of respondents (69 percent) believe they have a robust approach to valuing digital trust, rather than seeing it as just an abstract concept. And 65 percent say that risk modeling drives investment in cybersecurity improvements, with clear links between projects and risk reduction.

So, CISOs need to do more of what they do today, but they also need to recognize the evolving nature of their job, broadening their reach into areas where there is potential to help drive trust in their organization and beyond.

KPMG perspective: In praise of cyber risk quantification

Careful modeling and quantification work can help decision-makers understand the organization's true level of cyber risk exposure. This can help management understand which controls contribute most to reducing certain cyber exposures — and, therefore, helps ensure they are focusing their resources in the areas of greatest return.

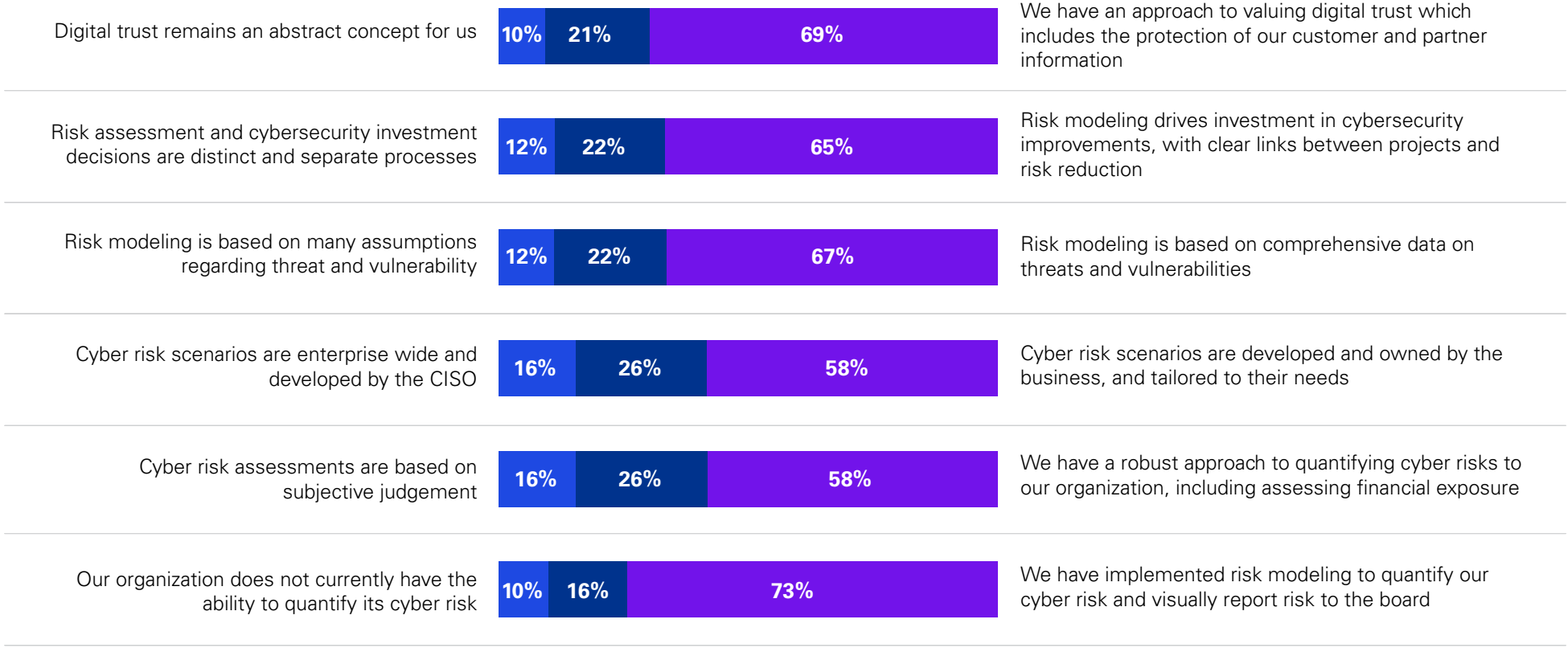
To get this right, organizations should follow five principles:

1. Ensure alignment of the risk model with organizational risk frameworks.
2. Be consistent in the definition of cyber risk as potential loss events to the business (scenarios are a great way to do this).
3. Take a threat-led approach to modeling, using attack-path modeling to de-construct how these risks can materialize.
4. Use real-world data in calculations — likelihood and impact estimates should be informed by internal and external empirical data (you have more than you think).
5. Understand the benefits and limitations of the model and be transparent about them.

James Hanbury
Director, Cyber Security Services
KPMG in the UK

Many organizations are struggling to model and assess cyber risk

Chart shows percentage of respondents who indicated the statements most closely reflected their organizations.



Source: KPMG Cyber trust insights 2022

5

Mission achievable

How organizations can drive trust via the CISO

Executives understand why it's important to increase trust in their organizations and their ecosystems, and they're looking to the CISO to be one of their champions in doing so. Cybersecurity and privacy are key elements in driving trust in the minds of customers, regulators and the public through the ESG imperative.

CISOs themselves recognize their responsibility for driving the enterprise's pursuit of that goal, and so do their colleagues in other parts of the business. However, our research shows that many are struggling to fulfill this responsibility — perhaps because they lack a clear vision of what digital trust really means and their part in achieving it.

Not that this is work any CISO can do alone. They need stronger support from senior leadership, more collaboration from other functions and productive cooperation with external partners and third parties.

Still, the CISO is a vital champion. Explicitly defining trust can be a good starting point, followed by using cybersecurity and privacy as a way to reinforce trust in the organization, with all the competitive advantages that brings.

How should they go about this?

Five crucial steps to building trust through cybersecurity and privacy

01

Treat cyber and privacy as a golden thread

Weave cybersecurity and privacy into the business processes, governance and culture of the organization — making it integral to business rather than a compliance-driven overhead.

02

Build internal alliances to drive trust

Work with colleagues such as the chief data officer and the chief privacy officer to help establish, embed and sustain digital trust.

03

Reimagine the CISO role

Embrace a broader agenda and recognize the ability to make wide ranging contributions in areas ranging from ESG to the ethics of AI.

04

Secure leadership support for investment in trust

CISOs who win the support of the C-suite and the board will likely find it easier to help drive the trust agenda. This means transforming the CISO from a narrow technical role to a strategic enabler within the organization.

05

Reach out to the ecosystem

Identify key partners within the organization's ecosystem and collaborate closely with them to help improve trust and resilience.

Methodology and acknowledgments

About the KPMG Cyber trust insights 2022

The KPMG Cyber trust insights 2022 survey, conducted by KPMG International between May and June 2022, surveyed 1,881 executives and interviewed five corporate leaders from across the world to explore the role that cybersecurity and privacy play in building and maintaining trust.

A significant proportion of the sample surveyed is composed of senior leadership: 42 percent are board or C-suite members. Respondents included leaders from 31 markets (24 percent from ASPAC, 50 percent from EMA, 16 percent from North America and 10 percent from South America) and six key industry sectors (energy and natural resources, financial services, life sciences and pharmaceutical, media, entertainment and technology, public sector, telecommunications).

All respondents have annual revenues over US$100M, 45 percent have annual revenues over US$500M, 23 percent have revenues over US$1B and 7 percent have revenues over US$5B.

KPMG would like to thank the following for their contributions:

- Bashar Abouseido, SVP and CISO, Charles Schwab
- Ulrich Baisch, CIO, Bechtle
- Allan Cockriel, CISO, Shell
- Ann Johnson, Corporate Vice President, Microsoft Security Business Development
- Mark Thompson, Chief Strategy Officer, International Association of Privacy Professionals (IAPP)

About KPMG

KPMG firms can help you create a resilient and trusted digital world — even in the face of evolving threats. KPMG cybersecurity professionals can offer a multidisciplinary view of risk, enabling you to 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 cybersecurity journey, KPMG firms have expertise across the continuum — from the boardroom to the data center. In addition to assessing your cybersecurity 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 professionals harness constantly evolving technologies that can connect and power businesses forward — building trust and creating and protecting value, while bridging the gap between past and future.

Let's create a trusted digital world together.

Author and contributors

Akhilesh Tuteja
Global Cyber Security Leader
KPMG International and Partner
KPMG in India
E: atuteja@kpmg.com

As a passionate leader of the Global Cyber Security practice, Akhilesh is committed to helping organizations use cybersecurity to build trust and protect their futures. He has advised numerous clients on cybersecurity, IT strategy, and technology selection — helping them realize the business benefits of technology.

Akhilesh has played an instrumental role in supporting the industry and is widely recognized for his strong blend of business and technical skills. He's a frequent contributor to business and technology publications and is a notable speaker on cybersecurity and its impact on enterprise businesses.

Siddharth Durbha
Director, Digital Trust
KPMG in India

Prasad Jayaraman
Principal, Cyber Security Services
KPMG in the US

David Ferbrache
Global Head of Cyber Futures
KPMG International

Sylvia Klasovec Kingsmill
Global Privacy Leader
KPMG International and Partner
KPMG in Canada

Atul Gupta
Partner and Head of Digital Trust and Cyber Security Services
KPMG in India

Sander Klous
Partner, D&A Business Development
KPMG in the Netherlands

James Hanbury
Director, Cyber Security Services
KPMG in the UK

Srinivas Potharaju
Partner, Digital Trust
KPMG in India

Contacts

Akhilesh Tuteja
Global Cyber Security Leader
KPMG International and Partner
KPMG in India
E: atuteja@kpmg.com

Prasad Jayaraman
Americas Cyber Security Leader
and Principal
KPMG in the US
E: prasadjayaraman@kpmg.com

Dani Michaux
EMA Cyber Security Leader
and Partner
KPMG in Ireland
E: dani.michaux@kpmg.ie

Matt O'Keefe
ASPAC Cyber Security Leader
and Partner
KPMG Australia
E: mokeefe@kpmg.com.au

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

Designed by Evalueserve.

Publication name: KPMG cyber trust insights 2022 | Publication number: 138298-G | Publication date: October 2022