KPMG

Cyber trust insights

Board Leadership Center (India)

Overview

In the times of uncertainty, trust is everything for businesses. In the constantly changing environment, customers, employees, and investors look for organisations they can depend on. But building and protecting that sense of trust requires every part of the organisation to work together to deliver a consistent, unified vision.

Now that we live in a digitised 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 be able to respond and recover quickly in the face of disruption.

Whether you are a customer or client who wants to feel safe when transacting with the organisation, or part of the broader ecosystem of partners, investors, regulators, and society which surrounds every organisation - 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.

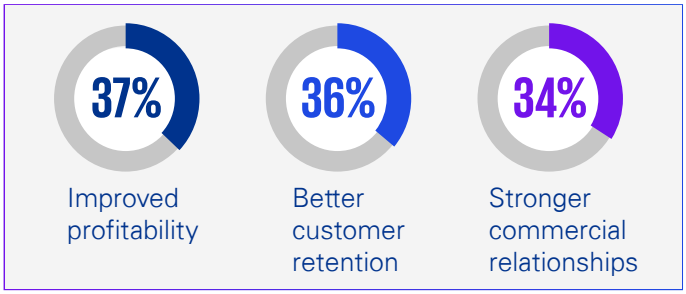
What do we mean by trust?

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 organisation to harness digital technology to protect their interests and uphold societal expectations and values.

Increased trust can increase profits and customer loyalty

According to the Cyber trust insights 2022 survey, the top three expected benefits of increased trust are:



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

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

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.

Source: Cyber trust insights 2022

Rising regulation

Regulators are paying greater attention to these issues, and many organisations 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.

Source: Cyber trust insights 2022

Understanding the drivers of trust

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. According to cyber trust insights 2022 survey, 80 percent of our respondents recognised the importance of improving cybersecurity and data protection including increased transparency around data use.

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. Cyber trust insights 2022 show 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 regulatory outlook: As societal concerns over digital trust grow, so does the interest of lawmakers and regulators, with greater demands for transparency and oversight.

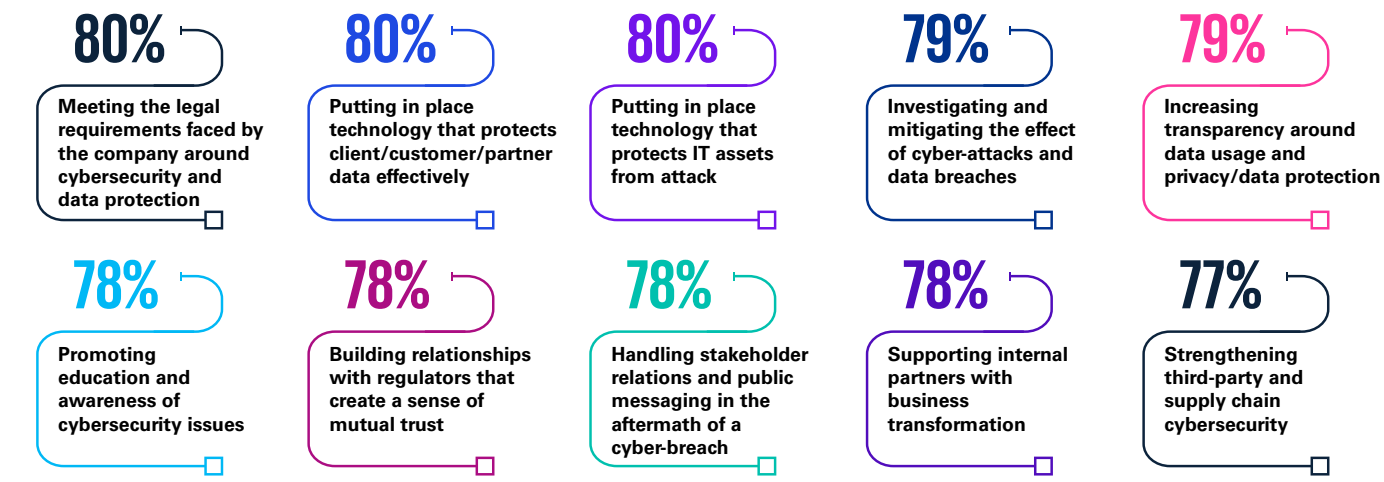
Looking beyond regulation: Digital trust should be part of the ESG agenda, and of course cybersecurity and privacy will likely be part of that. Fewer than one in five organisations describe security as an integral part of the ESG team and the majority report that it plays a very limited role. Organisations also need to recognise the social imperatives and growing expectations around these topics. Within organisations, those individuals responsible for ESG should work collaboratively with those responsible for cybersecurity (often, the CISO) and data privacy (often, the DPO).

The contribution of the CISO to building digital trust

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 organisation's ultimate guardians of trust, they can be a driving force of its success. CISOs themselves recognise what is at stake. According to the cyber trust insights 2022, more than three-quarters of respondents (77 percent) say increased trust is a key objective of their cyber risk programmes. And organisations 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 will CISOs be able to meet those expectations?

Organisations display high levels of confidence in the CISO

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

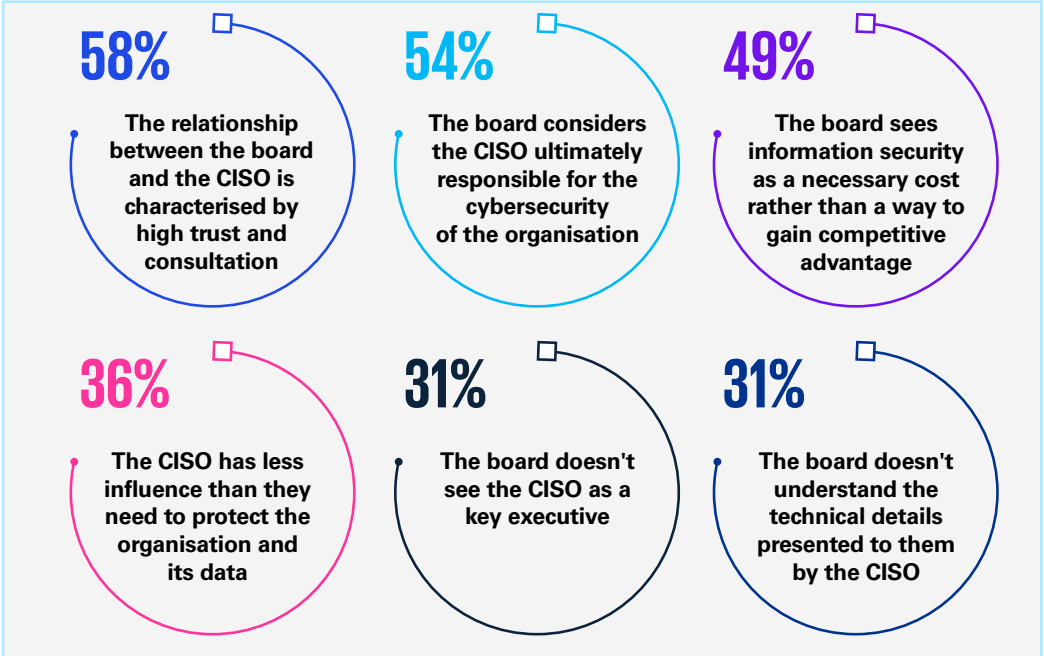


Source: Cyber trust insights 2022

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 organisations' most influential leaders believe CISOs and the broader cybersecurity function should be involved in transformation from an early stage. The CISO is a key executive and the profile of the CISO role has grown rapidly over the last five years driven by digital transformation, growth in cyber crime, and rising regulatory expectations.

Boards have mixed opinions of CISOs' influence

Chart shows percentage of respondents who indicated statements are true



How organisations can drive trust via the CISO?

Executives understand why it's important to increase trust in their organisations 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 recognise their responsibility for driving the enterprise's pursuit of that goal, and so do their colleagues in other parts of the business. They need stronger support from senior leadership, more, collaboration from other functions and productive cooperation with external partners and third parties.

How should they go about this?

Treat cyber and privacy as a golden thread: Weave cybersecurity and privacy into the business processes, governance and culture of the organisation making it integral to business rather than a compliance-driven overhead.

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.

Reimagine the CISO role: Embrace a broader agenda and recognise the ability to make wide ranging contributions in areas ranging from ESG to the ethics of AI.

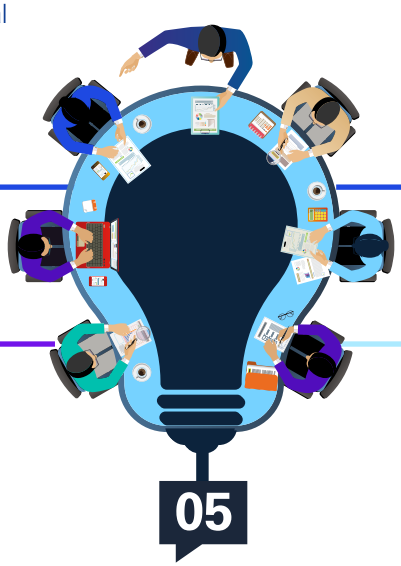
Secure leadership support for investment in trust: CISOs who win the support of the C-suite and the board will likely find it easier to help drive the trust agenda. This means transforming the CISO from a narrow technical role to a strategic enabler within the organisation.

Reach out to the ecosystem: Identify key partners within the organisation's ecosystem and collaborate closely with them to help improve trust and resilience.

Boardroom questions:

01 Are cybersecurity and privacy critical in establishing and maintaining trust in your business relationships? Is digital trust still an abstract concept in your organisation?

02 Why is the trustworthiness of digital technologies an essential requirement today - why does it matter to the future success of businesses in every sector?



03 How can we build partnerships across the ecosystem to 'rebuild' digital trust in terms of cyber-security?

04 Does your organisation consider digital trust as a part of the ESG agenda and privacy?

05 Do you think your CISO is a strategic enabler within your organisation?

About Cyber trust insights 2022

Cyber trust insights 2022, we surveyed executives and conducted a series of discussions with corporate leaders worldwide. The survey explored the extent to which the C-suite recognises the importance of maintaining digital trust, how they are meeting the challenge, and what they need to do next.

Read full report here - **Cyber trust insights 2022**

KPMG in India contacts:

Ritesh Tiwari
Partner,
Board Leadership Center, (India)
E: riteshtiwari@kpmg.com

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

Atul Gupta
India Cyber Security Leader and Partner,
E: atulgupta@kpmg.com

home.kpmg/in/socialmedia