Cyber security – what does it mean for the board?

Board Leadership Center (India)

April 2023

Cyber security as a golden thread

Globalisation has made the world borderless and interconnected — a reality made only too evident by the disruption to global supply chains brought on by the pandemic.
To create lasting relationships with customers (whether B2B or B2C), organisations must establish and maintain digital trust.

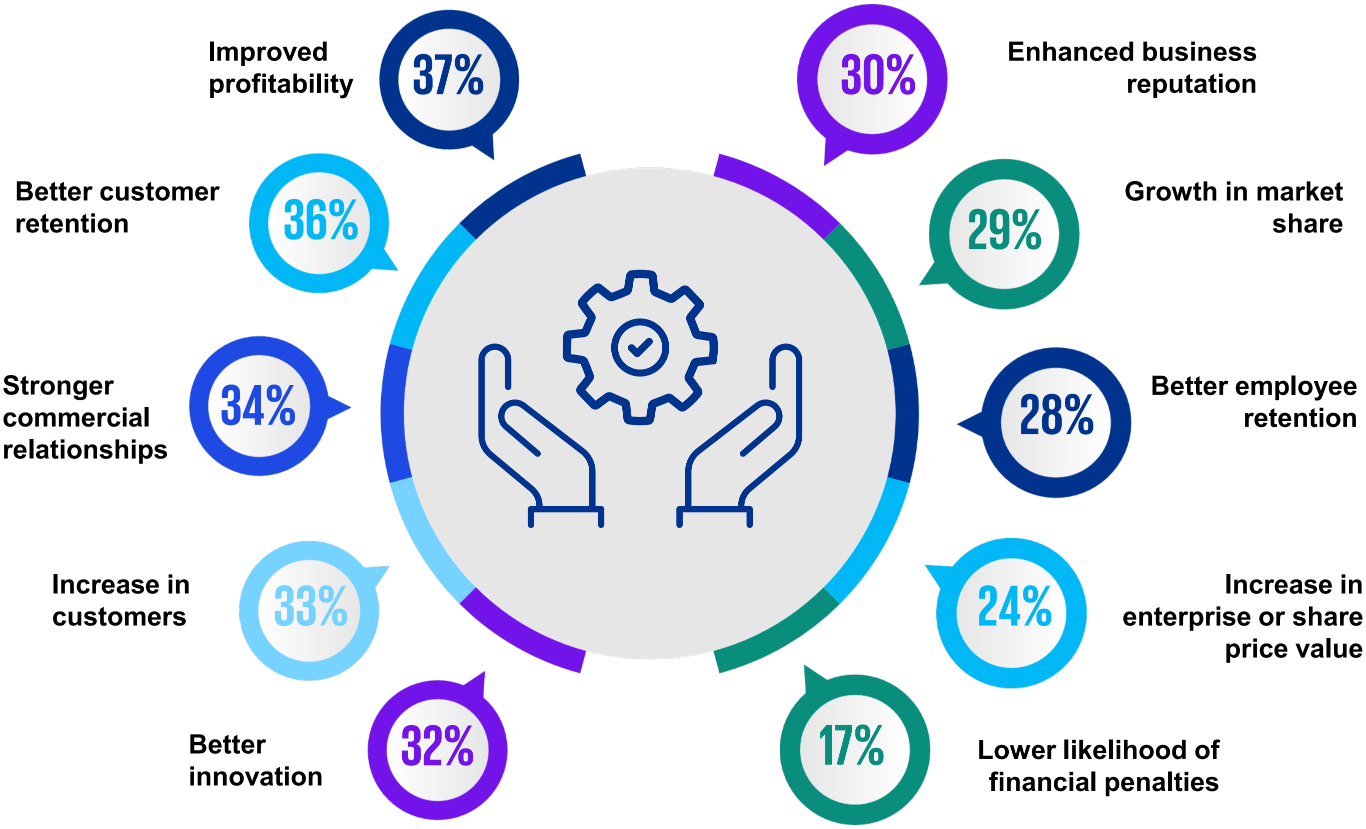
The success of any digitally enabled business is built on digital trust — cybersecurity and privacy being the vital foundations for that trust. And is not just about reputation. Boosting trust can create competitive advantage.

However, according to the KPMG International's Cyber trust Insights survey of 2022*, 49 per cent of respondents believe that the board of directors see security as a necessary cost rather than a way to gain competitive advantage. 65 per cent of the executives also feel that information security requirements are shaped by more compliance needs and are a risk reduction activity rather a strategic business enabler.

This is where the role of Chief Information Security Officers (CISOs) becomes significantly prominent. A big part of a CISO's job today is to be a communicator and to articulate across the enterprise the potential business impact of a breach and the value of keeping cybersecurity top of the mind. CISOs must be able to explain to the board and other corporate leaders that the investment is not just another new technology but a new way of thinking that is designed to support a secure, perimeter-less future.

Growing numbers of senior leaders recognise the benefits of digital trust, with 37 per cent seeing improved profitability as the top commercial advantage of increased trust. Cyber security is no longer just a technology matter, but a golden thread that runs through an organisation to enable it to operate with greater effectiveness, efficiency, and security. The benefits of increased trust have been enumerated in KPMG International's Cyber trust insights survey exploring the extent to which the C-suite recognises the importance of building cyber trust.

***Cyber trust insights 2022** — KPMG International surveyed 1800+ executives and held a series of discussions with corporate leaders and professionals from across the world to explore the extent to which the C-suite are recognizing and meeting the cyber security challenge, and what they need to do in the near- and long-term future.



Source: KPMG International's Cyber Trust Insights survey | 2022

8 key cyber security considerations for 2023

This report identifies eight considerations that organisations should prioritise as they seek to accelerate recovery times, reduce the impact of incidents and aim to ensure their security plans enable their business. The report explores the key actions CISOs should take to meet the challenges ahead and to help ensure security is the organisation's golden thread, woven into the business across the board — providing the basis for trust.

1. Digital trust: A shared responsibility

Digital trust is finding its way on to board agendas as privacy, security and ethics debates gain momentum — partly driven by regulation and partly by public opinion. The future success of any digitally enabled business is built on digital trust. CISOs must be prepared to help the board and C-suite create and maintain the trust of their stakeholders if they are to create a competitive advantage. Realising this potential requires a collective commitment from all stakeholders

2. Unobtrusive security drives secure behaviours

Embedding security within the business in a way that helps people work confidently, make productive choices, and play their part in protecting the organisation must be a key, albeit often elusive, CISO objective. It's too easy for people to see security as an impediment, and only by considering security from both human and business-centric perspectives can CISOs hope to change this mindset.

3. Securing a perimeter-less and data-centric future

It's no surprise that business operating models have fundamentally changed over the last decade — becoming more fluid, data-centric, connected ecosystems of internal and external partners and service providers. In this distributed computing world, to help reduce the blast radius of any potential outages or breaches, CISOs and security teams must adopt very different approaches, such as zero trust, Secure Access Service Edge (SASE) and cybersecurity mesh models

4. New partnerships, new models

Gone are the days when security teams focused solely on the security of their organisation's IT systems. CISOs need to understand when to hit the brakes and when to press go for outsourcing cybersecurity efforts and determine what skills to keep in-house today and in the future. Security has become a business priority, delivered through a shared responsibility model between the organisation and service providers.

5. Trust in automation

In the race to innovate and harness emerging technologies, concerns over security, privacy, data protection and ethics, while gaining more attention, are often ignored or forgotten. Left unchecked, this negligence could lead businesses to sabotage their potential, especially with new AI privacy regulations on the horizon.

6. Securing a smart world:

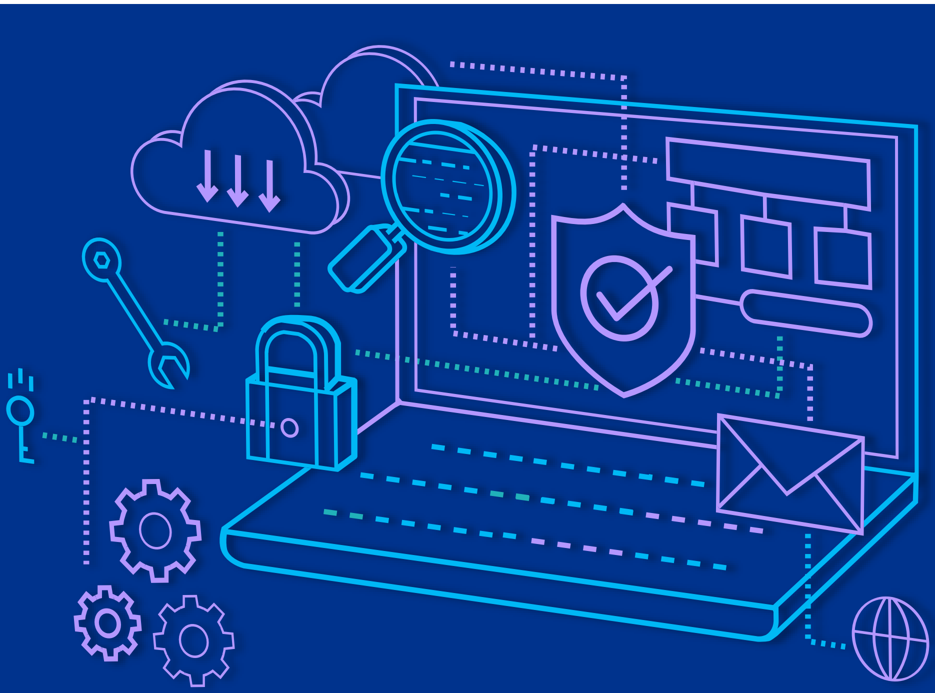
Businesses across virtually every industry are shifting to a product mindset — focusing on developing network-enabled services and managing their supporting devices. CISOs and their teams are getting pulled into discussions with engineering, development and product support teams as organisations realise product security matters too.

7. Countering agile adversaries

The time from initial compromise to enterprise-wide ransomware activation is shrinking. Increasingly, rogue and state-sponsored attackers can penetrate systems with automated tooling and accelerate the exploitation of systems. Security operations should be optimised and structured to fast-track the recovery of priority services when an incident occurs, which can reduce the impact on clients, customers and partners.

8. Be resilient when — and where — it matters

Every security system is flawed. There is an air of inevitability that, at some point, an organisation will suffer an incident, large or small, and likely more than one. Regulators are increasingly focusing on plausible scenarios and pushing companies — particularly those in strategically important industries like energy, finance, and health care — to be resilient and position themselves to recover.



Boardroom questions

Boards are today well aware of the complex tapestry of interconnected ecosystems and information infrastructures in which organisations operate. Breakthrough technologies also pose new security challenges and raise fundamental questions about trust in digital systems.

Following are some of the key areas of potential impact and possible implications that boards are focusing on as they help organisations thrive and innovate proactively rather than retrospectively.

- Has the cyber risk been assessed holistically and is it quantifiable?
- What are key cyber risk indicators board should be reviewing to understand effective, or proactive mitigation and remediation measures?
- Does the board have access to cyber expertise it needs? Is cyber being addressed by senior executives in organisation that also provides ongoing updates at board meetings?
- Is cyber security aligned to organisation’s overall business strategy?
- Does cyber coverage include all connected technology assets across the organisation, or this is limited to traditional IT environment?

- Do we have the right governance capabilities and mechanisms to make suitable decisions on how to manage cyber risk?
- Is my organisation cyber resilient and agile to minimise disruptions in the event of a cyber attack?
- How does the changing regulatory landscape impact the organisation?
- Is our organisation’s cybersecurity programme ready to meet the challenges of today’s and tomorrow’s cyber threat landscape? How does the changing regulatory landscape impact the organisation?
- Is there a cyber security incident response plan? How often are cyber drills conducted with near real life situation?

- Is there a communication plan to be enacted during cyber crisis situation? How is brand value protection being factored upon?
- How is the ecosystem of organisation being covered in security programme? Does the framework cover all relevant supply chain partners, including cloud based services?
- How are cyber threats and risks assessed while adopting new technologies such as machine learning (ML) and other forms of artificial intelligence (AI)?
- Is there a cyber responder service available with the organisation?
- What form of cyber intelligence is being received by orgnanisation? Does this include generic intelligence or contextual to organisation?

- How can organisations keep security, privacy and resilience at the forefront in an environment where outsourcing and managed services are a growing priority?
- What portfolio of capabilities are we investing in to protect the data across enterprise? Is there a data governance programme in the organisation?
- Is there a technology platform, which provides a single view of cyber risk and also provides dashboards for right decision making?
- Are there adequate mechanisms deployed to manage digital identity in the current hyper connected environment?
- Are we seeing cyber as a risk mitigation measure or Digital Trust as a business growth driver?

KPMG in India contacts:

30 years and beyond

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

Atul Gupta
Partner and Head,
Digital Trust
E: atulgupta@kpmg.com

kpmg.com/in

kpmg.com/in/socialmedia

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.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi,
Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only. (004_BRO0423_KK)