Key cyber security considerations for 2024

Board Leadership Center (India)

April 2024

kpmg.com/in

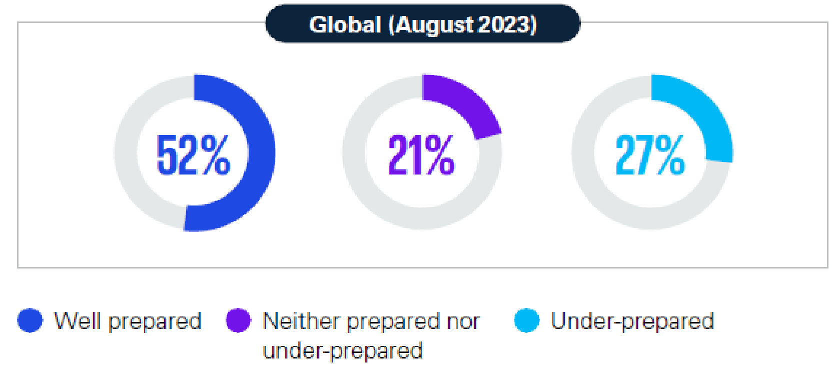
KPMG. Make the Difference.

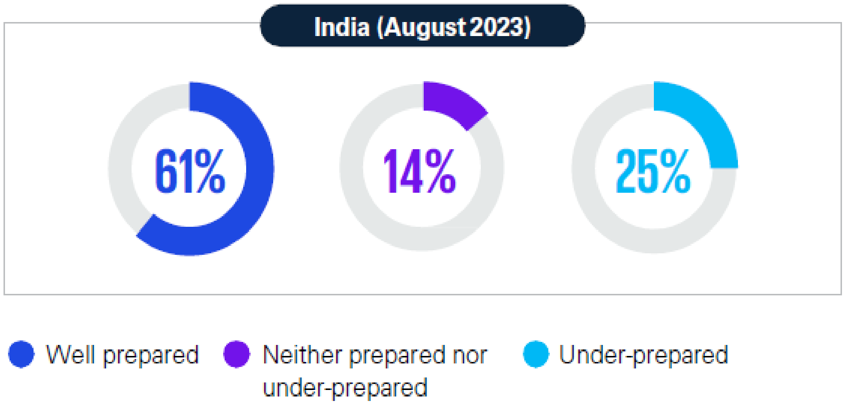
Technology innovations demand strategic pragmatism!

As 2024 unfolds, organisational leaders, from the CEO down, have much on their plates. They are contending with diverse challenges around achieving sustained growth, navigating the impact and risks of emerging technology, and attracting and retaining talent, to name just a few.

CEOs globally and in India are continually exploring the potential of generative AI and increasingly making it a top investment priority considering its indispensable benefits such as increased efficiency, productivity, and profitability. While CEOs in India and globally recognise the potential benefits of AI in detecting cyber-attacks, they also acknowledge the potential risks associated with its use.

Comparison of CEOs in India and globally on preparedness of cyberattacks





Despite these concerns, a higher number of CEOs in India at 61 per cent compared to 52 per cent CEOs globally, feel confident in their organisation's preparedness for potential cyber-attacks[1].

This evolving threat landscape requires organisations and their business leaders to view security through a new and more pragmatic lens. More than ever before, the need is to balance cyber security and privacy with the broader objectives of the business. From a cybersecurity perspective, the impacts of societal, economic, political, and regulatory developments are more consistently felt today.

Cybersecurity is now being viewed as an ever-evolving ongoing endeavour. The more organisations accept cyber incidents as inevitable yet manageable, the better their chances of achieving that balance between preparation and resilience.

[1] KPMG India CEO Outlook, KPMG in India, August 2023

© 2024 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and 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.

Given this scenario, there are eight cyber security considerations for the year 2024 that we emphasise on to ensure there is a sense of digital trust and harmony that prevails through the organisations:

1. Meet customer expectations, improve trust

With cyber threats and data privacy concerns increasing, there is a need for the organisations to be working closely with their stakeholders to maintain trust and ensuring the organisations are well-prepared to handle the crisis situations that may emerge due to imminent cyber threats.

CEOs in India as well as globally are starting to see ESG as an essential component of their corporate strategy, that helps generate long term growth. 54 per cent CEOs in India, have fully embedded ESG into their business[2] as a means for value creation. ESG covers wide agenda, while environmental aspects have garnered most attention, the need is to enhance governance elements such as cybersecurity and privacy. With cyber threats and data privacy concerns growing, enhanced governance shall lead to business operations being more resilient and necessary continuity plans are readily deployable. Further, through protecting data (including customer data), organisations increase chances of maintaining their reputations and drive trust, even in the event of a major breach.

2. Embed cybersecurity and privacy, for good

The organisations across the globe have rapidly gone through a massive shift in the operating model due to significant role played in enabling "digital transformation" along with accelerated pace of innovation. Organisations have gone through a major shift in the business model with significant investments being made in AI during last 12-18 months, to enable in providing products and services that could drive efficiency, optimisation, and smarter operations. Constantly evolving model with heightened dependence on digital systems exposes organisations to dynamic threat landscape and there is an increased need to build trust across digital channels, considering that any cyber-attacks shall have impact across business processes. Embedding security into broader business should be viewed as an exercise in driving operational excellence.

3. Navigate blurring global boundaries

For years, the global regulatory landscape has been very disjointed, however more recently common themes have started emerging, which are driven due to cyber threat not being differentiated by geographical boundaries. This is making organisations have adequate frameworks & cyber controls not only to meet the local requirements across data privacy and protection but also address the global requirements. Similarly, cyber incident reporting is a common theme emerging, whereby organisations need to be prepared for compliance with local and global requirements.

[2] KPMG India CEO Outlook, KPMG in India, August 2023

© 2024 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and 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.

Beyond regulations, the world is also dealing with complexities due to changing geopolitical situations, that could lead to impact on supply chain across business processes including cyber.

A central consideration that organisations must examine is to most effectively navigate the increasingly complex global business landscape to ensure operational resilience.

4. Modernise supply chain security

Today's operating model requires the industry to operate in an ecosystem which has complex supply chain ranging from product components to intricate exchange of information through APIs and constant interaction with multiple other virtual technologies. This dependence has been exposed to have operational impact across industry segments including critical infra and consequently there are expanding compliance requirements. There have been multiple cyber incidents that has brought this threat to the forefront, with far-reaching impacts. As the world gets hyper connected, adversaries have been exploiting weak links in supply chain to infiltrate across organisations.

Organisations should establish more strategic supplier partnerships focused on continuous monitoring of changing risk profiles across the suppliers that shall enable in taking proactive measures and also enable in strengthening operational resilience.

5. Unlock the potential of AI – carefully

The concern over business outcomes and the need to foster trust among employees and customers, specifically, and society, in general, has sparked a broad ethical debate around how AI can be controlled and deployed responsibly, transparently, and with integrity. 77 per cent CEOs in India compared to 82 per cent CEOs globally view generative AI as a double-edged sword, as it can both enhance cybersecurity efforts and create new vulnerabilities for adversaries to exploit[3].

The organisations should ensure they have a thorough understanding of the complexities involved and accordingly plan to adopt AI.

6. Supercharge security with automation

Digital agendas are proliferating at a massive rate, which is also making many organisations to see themselves as tech companies, regardless of their core business. As operating models digitise leading to wider attack surface area, cyber is actively contributing by accelerating the automation of security processes to deal with complex adversary and ever growing threat scenarios.

Security automation is becoming time critical across domains. Automating scheduled procedures and updates play a key role in ensuring defences are resilient and trusted to address the attacks emerging from organised and rogue bad actors. Automation is also enabling in near real time addressal of risks emerging in third-party ecosystem, vulnerabilities and weak links across vendor and supplier ecosystems.

[3] KPMG India CEO Outlook, KPMG in India, August 2023

© 2024 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and 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.

7. Make identity individual, not institutional

The current digital age has created a connected world where machines are connected and constant automation is enabling them to perform multiple activities (some of them are very close to activities which were performed by humans in past). Average enterprise has more machine identities than human ones, and some organisations don't even know the exact number of machines and their identities. In addition, the emergence of online platforms, social media, and digital communication has resulted in a ubiquitous presence of customer identities across multiple channels. This has given rise to a fragmented and intricate experience, which, if not appropriately addressed, can lead to data breaches and security risks.

Given the fast-evolving need, the overall identity model is evolving to manage digital identities and user access across a hybrid environment (Cloud, digital channels, enterprise applications, mobility, etc.).

Organisations need to transform identity and access management journey, covering employees, machines/ bots, third party and consumer, which shall enable in maintaining a robust security posture.

8. Align cybersecurity with organsational resilience

Cyber incidents in the digital world are becoming inevitable and organisations are working on strategy to ensure continuity of business operations through organisational resilience. When a data breach or ransomware attack occurs for any organisation, trust is the first asset to be impacted (internally and externally as well). How well organisations are prepared and how quickly they can respond, and recover are key determinants in restoring customer and, for public companies, investor trust. When organisations commit to earning — and re-earning — the trust of these vital stakeholders, they place themselves firmly on the path to operational resilience.

Globally regulations have been established for critical industry sectors which require organisations to have operational resilience addressing cyber threats/ incidents. In some cases, rebuilding trust is about rapid technical recovery; in others, it's about identifying alternate ways of delivering services. In every instance, it's about identifying vulnerable and/or impacted stakeholders, expeditiously addressing their needs and minimising disruption.

© 2024 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and 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.

Key areas for 2024

Board members and the wider organisation leadership plays a critical role in embedding culture of cyber being a cornerstone that not only enables in adequate protection but also provides an opportunity to competitively differentiate through establishing digital trust.

Following are the key areas which are extremely relevant for leaders in the current age of digital technologies to enable the business rather than expose to cyber risks:

1. Bring a new perspective on what could disrupt the business and what should be done to manage those risks without impacting experience across key stakeholders (business teams, customers, regulators, capital markets, etc.)
2. Enhance transparency to build trust across global supply chains through an approach of considering them as an extension of organisation rather than treating third, fourth, and fifth-party supplier relationships solely as transactional and contractual
3. Gain visibility across data (with focus on business-critical data)— both structured and unstructured — and establish adequate measures to protect data confidentiality and availability
4. Speed of change is significantly high, which requires cyber to be powered by adequate technology thereby enabling the orgnisational environment to align the pace with emergence of threat adversaries
5. Maintain an understanding of the global regulatory landscape, specifically an understanding of the relevant rules at a granular, jurisdictional level. Sharpen global regulatory intelligence around cyber and privacy to ensure timely compliance and reporting. Drive common measures to address common requirements (global and local), thereby in duplication of efforts and optimise resource deployment
6. Intelligence is time-critical in cyber, and the need is to have adequate sources that shall enable in driving cyber measures proactively
7. Fast-paced emergence of new technologies creates a massive business opportunity, however, it is important to adopt the new and emerging tech in a manner that shall be sustainable and also not impact on 'trusted' approach of use of tech
8. Establish a single view across the threat, risk and compliance status covering all ecosystem (Cloud, mobility, digital channels, supply chain partners, regulatory requirements, enterprise standards, industry practices and global frameworks)
9. Increasing resilience through cyber awareness (specific focus on new threats, such as deep fake based financial crimes, identity masquerading methods used for launching cyber attacks, etc.) and regular cyber drills across the organisation (board and leadership, management team and operational teams) continue to be an impactful measure and need to be enhanced to ensure that they create right impact
10. Proactively develop right ecosystem to address situations that may emerge during a cyber incident, including having an incident responder, appropriate coverage of cyber insurance, pre established communication channel and clarity on roles and responsibilities of crisis management team.

© 2024 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and 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.

Boardroom questions

Following are key areas that boards are focusing on as they help organisations thrive and innovate proactively:

- What role is Cyber Governance playing as part of ESG (Environmental, Social, and Governance), and how is organisation ensuring that security and privacy align with broader social responsibility goals?
- What considerations are being factored regarding the changing landscape of cybersecurity regulations, data privacy laws, and the impact on global business operations and supply chain security?
- Are the measures for cyber and data security embedded in the business processes thereby addressing strategic imperatives that are aligned with business objectives or they continue to be considered as compliance requirements and applied reactively?
- How is organisation collaborating across industry forums, research agencies and trusted technology ecosystem partners to bring in insights that shall enable in not only protecting the stakeholder value but also uniquely position the organisation?
- How prepared the organisation is to navigate the complexities of global regulatory requirements, data localisation, and data transfer considerations to ensure efficient, cost-effective, and compliant cybersecurity practices across different jurisdictions?
- What strategies are being employed to strike a balance between business enablement, value creation, regulatory compliance, and maintaining a strong cybersecurity posture in an increasingly interconnected and regulated business environment?
- How is organisation leveraging on fast paced changing and emerging technology (such as AI, blockchain, quantum) to address constantly evolving cyber threat and risk environment?
- Are there measures being taken up by management on preparing the organisation to manage exigencies caused due to cyber threats and respond as well as recover from it effectively?
- Is cyber and its associated business impact covered as part of the organisational resilience methods? These are vital for maintaining business operational capabilities, safeguarding customer trust, and reducing the impact of future attacks.
- Have organisations established strategic supplier partnerships and thereby creating a 'trusted' supply chain that strengthens operational resilience?

© 2024 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and 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.

KPMG in India contacts:

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

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

kpmg.com/in

Follow us on:

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.

© 2024 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

This document is for e-communication only. (010_BRO0424_SP)