



Cyber security - what does it mean for the Board?

Key cyber security considerations for 2022

Board Leadership Center



Why cyber security risk is an everyday business consideration?

Organisations across industry sectors have accelerated digital transformation in the past 24 months, and there is increased pace to further enhance the digital quotient. While this is a reality across businesses, simultaneously it's also raising a question on having strong cyber strategy which is critical to engender trust among key stakeholders in this hyper connected world.

From the board to the C-suite and from front office to back, cyber controls should be in place to protect the organisation's and clients' high-value assets, the proverbial 'crown jewels.' Over the years - and particularly as a result of the pandemic - it has been found that a lack of preparation and being overly reactionary is far more detrimental than the actual event.

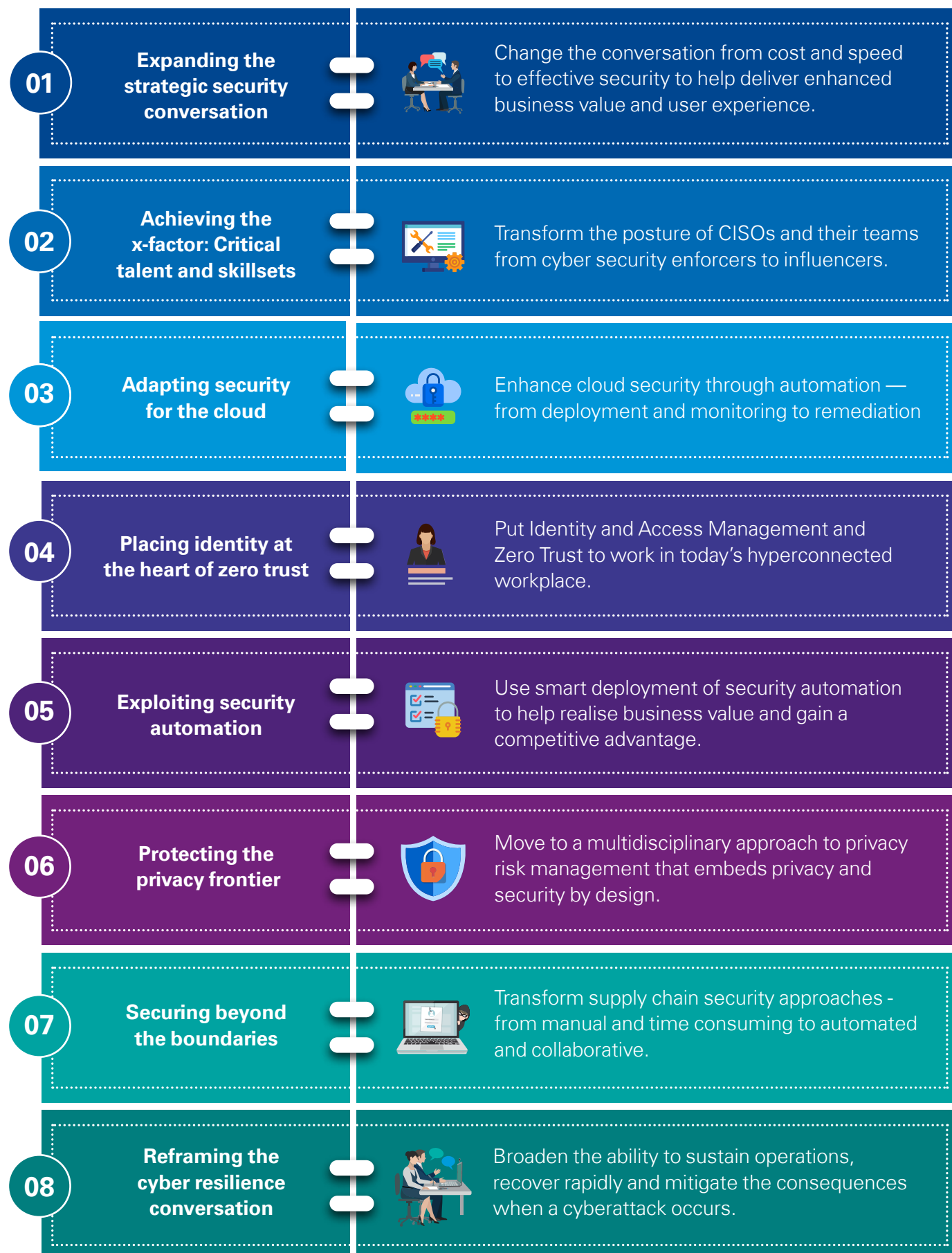
The ever-increasing threat landscape isn't making it easy for security teams to prepare for the inevitability of a cyber event and it's, in fact, compelling security teams to prioritise cyber response through regular testing across different scenarios and understand the depth and breadth of potential cyber incidents.

At the same time, investors, governments and regulators are increasingly challenging Board members to actively demonstrate diligence in this area. Regulators expect personal information to be protected and systems to be resilient to both accidents and deliberate attacks.

This is an opportunity for organisations across virtually every sector to reimagine and reposition their cyber strategies.



Eight key cyber security considerations for 2022



Potential impact and possible implications for Boards



Business disruption of an organisation's operations, and impact across multiple dimensions including financial impact



Reputational losses causing the market value to decline, loss of goodwill and confidence by customers and suppliers



Leadership time focused on recovery processes and investigating the implications of incident, keeping shareholders advised and supporting regulatory authorities (financial, fiscal and legal)



Penalties, which may be contractual or regulatory fines for data privacy breaches and customer and contractual compensation, for delays



Intellectual property losses including patented and trademarked material and commercially sensitive data



Legal recourse emerging due to cyber incidents



Administrative recourse to correct the impact such as restoring client confidence, communications to authorities, replacing property and restoring the organisation to its previous levels.

Boardroom questions

Board is aware of the cyber risks and constantly changing threat landscape. Following are the key areas where the board is focused, which supports in taking control of cyber risk in a unique and positive way.

1. Is cyber part of the organisation's strategy discussions and when was the threat last examined upon by the leadership?
2. Is the organisation's cyber security programme ready to meet the challenges of today's and tomorrow's cyber threat landscape, specifically considering rapid digital adoption and associated transformation?
3. How is the organisation keeping abreast of new cyber security threats and risks, and understanding its effects on the organisation?
4. Key risk indicators that should be reviewed by senior executives and Board to ensure there is effective cyber risk management and resilience built upon?
5. Is there a visibility of digital risk (including cyber) as the organisation pivots to the next wave of digital tech adoption, including next generation technologies?
6. Does the organisation understand all obligations (regulatory, contractual, etc.) related to cyber and data security risk? Also, is there a compliance framework to track compliance against these obligations?
7. Are we investing enough to position cyber as a competitive differentiator?
8. Is the cyber talent/skills a concern area? If yes, then how are we dealing with it?
9. Do we have enough protection for cyber risks emerging from supply chain ecosystem?
10. Does the organisation have defined response and recovery mechanism from cyber incidents?



Contacts:

Ritesh Tiwari

Partner

Board Leadership Center

KPMG in India

E: riteshtiwari@kpmg.com

Akhilesh Tuteja

Global Cyber Security Leader

KPMG International

and Partner, KPMG in India

E: atuteja@kpmg.com

Atul Gupta

Partner and Head

Digital Trust

KPMG in India

E: atulgupta@kpmg.com

home.kpmg/in

#KPMGjosh

Follow us on:

home.kpmg/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.

© 2022 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.(001_FLY0422_AR)