Guide

Top 10 Cyber Security Questions for Executives

Simplified Cyber Security for Boards

Huntsman®
Defence-Grade Cyber Security

Does your risk management framework adequately deal with cyber security?

> "Digital risk, including cyber risk, is a pervasive and potentially existential concern. Leaders need to understand and take account of cyber risk in their strategic decisions."
>
> *World Economic Forum*

With cyber security and risk reporting now being adopted as a normal part of the board agenda, it demands serious accountability and management.

The cyber security challenge for organisations is a continuous issue:

- Cyber threats are evolving and increasing all the time
- Customers' expectations of trust are growing
- Digital transformation increasingly relies on secure and interdependent technological environments

Often, senior stakeholders don't appreciate the scale, number, likelihood and impact of security risks. Blind faith and an over-reliance on security "experts", or a poor understanding of cyber security governance, is no longer acceptable.

With the shift in accountabilities, boards and senior executives need ongoing visibility to cyber risks, alignment between their organisation's risk management framework and risk appetites and measurement of the effectiveness of their cyber security efforts.

The recent report "Principles for Board Governance of Cyber Risk" from the World Economic Forum highlights six very clear points:

- Cybersecurity is a strategic business enabler
- Understand the economic drivers and impact of cyber risk
- Align cyber-risk management with business needs
- Ensure organisational design supports cybersecurity
- Incorporate cybersecurity expertise into board governance
- Encourage systemic resilience and collaboration

These form the basis of a "cyber resilient" organisation.

There are a growing number of checklists available from Government, regulators and professional bodies advising boards and directors how to better understand and manage cyber security risk.

Most, however, don't provide an obvious starting point from which to benchmark your state of play and measure the establishment of your cyber security improvement program. To help, we have compiled the following Top 10 Cyber Security Questions for Executives and their operational teams to collectively improve their management of this growing scourge of the digital world.

https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk

> A quick cyber security risk assessment is a practical way to gather some valuable insights into your current cyber maturity level.

1	What are your highest priority cyber security risks?
2	Do you know what your "crown jewels" and key digital information assets are?
3	Where are these assets located and who has access to them?
4	Are they accessed by, received from, sent to, or shared with third party suppliers?
5	What controls or strategies are in place to protect data from being comprised, destroyed or stolen and are they effective? Consider: Prevention, Limitation and Recovery
6	Do you have a defined security governance program or use a recognised security control framework?
7	Are the controls you have in place (technology and process) operating effectively and how are they measured and reported on?
8	Are regular risk assessments to understand and mitigate control deficiencies conducted as part of a continuous improvement program?
9	Are security outcomes (of audits, reviews, incidents, processes) and risks objectively and quantitatively reported to IT and senior executive teams to inform risk management decisions?
10	Which roles are responsible for cyber security governance and effective ongoing cyber security performance? How do they report up to your Board?

Every question you can't confidently answer highlights a weakness in your cyber security delivery or reporting capability and hence a risk to your business operation.

A quick cyber security risk assessment is a practical way to gather some valuable insights into your current cyber maturity level. By measuring your cyber security controls against a recognised cyber governance framework, you can gain significant intelligence about the maturity of your security systems and controls.

By benchmarking and regularly measuring your security risk metrics with Huntsman Security's Essential 8 Auditor, you will receive status reports on your cyber security maturity and identify any weaknesses in IT governance efforts that require attention.

Huntsman®

Want to find out more?

Download our Essential 8 Auditor brochure.

Download

Or contact your local Huntsman Security office (listed below) to talk to one of our team today.

About Huntsman Security

Huntsman Security's technology heritage lies in delivering cornerstone cyber security risk management, monitoring and response technology to some of the most sensitive and secure intelligence, defence and criminal justice environments in the world.

Huntsman®

HUNTSMAN | TIER-3 PTY LTD

ASIA PACIFIC

t: **+61 2 9419 3200**

e: **info@huntsmansecurity.com**

Level 2,
11 Help Street
Chatswood NSW 2067

EMEA

t: **+44 845 222 2010**

e: **ukinfo@huntsmansecurity.com**

7-10 Adam Street,
Strand
London WC2N 6AA

NORTH ASIA

t: **+81 3 5953 8430**

e: **info@huntsmansecurity.com**

GINZA EAST SQUARE 4F
3-12-7 Kyobashi Chuoku, Tokyo
Japan 104-003

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman