CYBERSECURITY TOOLKIT FOR ENTERPRISE LEADERS
EXECUTIVE SUMMARY

The benefits of digital transformation can be fully reaped when enterprises invest in cybersecurity. Cybersecurity is a critical enabler for businesses – business leaders should view cybersecurity as a competitive advantage, especially in industries where trust is key to business relationships.

CYBERSECURITY IS A BUSINESS INVESTMENT – IT WILL PAY FOR ITSELF OVER TIME

KEY REASONS TO INVEST IN CYBERSECURITY

Cybersecurity is Critical for Digital Transformation

Reap the full benefits of digital transformation when you invest in cybersecurity.

Cybersecurity is a Competitive Advantage

Investing in cybersecurity helps you to establish trust in business relationships.

The Cybersecurity Toolkit for Enterprise Leaders is targeted at larger enterprises that adopt a two-tier corporate hierarchy with a Board of Directors and a top management C-suite team. This toolkit will help enterprise leaders understand the five fundamental areas that an organisation should consider to ensure cybersecurity is adequately addressed:

1. CULTIVATE CYBERSECURITY LEADERSHIP IN YOUR ORGANISATION

Cybersecurity is about risk management, and not just a technical issue. It requires the Board and top management to make trade-offs between security, usability of systems and cost. Such trade-offs require an executive decision, and will depend on the risk profile of your organisation, and the environment it operates in. This is a decision for the Board and top management, rather than IT or security experts.

Enterprise leaders should:
- View cybersecurity as a business investment.
- Ensure governance and oversight from top management.
- Establish a cybersecurity strategy and roadmap.

Organisations should:
- Ensure risk management practices for cybersecurity are in line with the risk profile of your organisation.

2. EDUCATE YOUR EMPLOYEES ON CYBERSECURITY

One of the biggest threats to cybersecurity in any organisation comes from its employees, whose actions may inadvertently result in a cybersecurity incident in your organisation. An organisation can reduce its risk by building a culture of cybersecurity, where employees are aware of the potential cybersecurity issues and align their behaviour to mitigate the risks.

Enterprise leaders should:
- Lead by example and champion cybersecurity within your organisation.
- Ensure investment is in place for cybersecurity training and awareness of employees.

Organisations should:
- Drive cybersecurity as a top-down approach/ cultivate a cybersecurity culture.

Updated: 7 October 2021

3. PROTECT YOUR INFORMATION ASSETS[1]

Knowing the information assets involved in your daily business operations helps you plan more effectively for your information security risk management and resource allocation. This can help to reduce the chance of data misuse, breaches and operational disruption.

Enterprise leaders should:

- Establish and endorse an information asset management programme.

Organisations should:

- Identify what are your business-critical information assets.
- Implement security controls for protection of information assets.
- Establish a data backup strategy.
- Drive the importance of regular system/application updates and manage the risks of using outdated systems and applications.

4. SECURE YOUR ACCESS AND ENVIRONMENT

Implementing good cybersecurity measures can help secure your organisation and reduce the likelihood of a significant cybersecurity incident. You can secure your organisation through managing and controlling the access of every account and individual within your environment, including third parties. Additional cybersecurity measures such as usage of passphrases and Multi-Factor Authentication (MFA) can further secure your organisation's environment.

Enterprise leaders should:

- Establish and endorse a user access management programme for systems and data.
- Establish and endorse a third-party cybersecurity risk management programme.

Organisations should:

- Drive the importance of using strong passphrases and MFA.

5. ENSURE YOUR BUSINESS IS CYBER RESILIENT

In an increasingly volatile business environment, organisations not only have to prepare for cybersecurity incidents, but expect them. For your organisation to be cyber resilient, it must have the ability to respond and recover from a cyber attack with as little business disruption, regulatory conflict and reputational impact as possible.

Enterprise leaders should:

- Ensure you have a cybersecurity Incident Response Plan.
- Ensure cybersecurity is integrated into your Business Continuity Plan (BCP), Disaster Recovery Strategy and Plan (DRP), and Crisis Management Plan (CMP).

Organisations should:

- Establish and endorse a cybersecurity incident response plan.
- Maintain oversight of regular crisis management, BCP and DRP exercises.

[1] An information asset refers to anything that has value to an organisation, including hardware, software, and data supporting business operations.