Board Toolkit: Executive summary

The NCSC's Board Toolkit helps boards to ensure that cyber resilience and risk management are embedded throughout an organisation, including its people, systems, processes and technologies.

This document summarises the contents of each section of the Board Toolkit.

Introduction to cyber security for board members

An introduction to cyber security, explaining the fundamental concepts that boards should be aware of, and why cyber security is a board-level issue.

Part 1: Create the right environment

Embedding cyber security into your organisation

Cyber security is not just 'good IT'. It should be integrated into organisational risk management and decision making, and all the business units in your organisation should be clear about their cyber security obligations and responsibilities. Done well, cyber security will enable your organisation's digital activity to flourish, adding value to your business. It's also a team sport, and as Board Member, it's vital that you empower everyone.

Developing a positive cyber security culture

Security culture refers to the values that determine how people are expected to think about and approach security in an organisation.
A positive cyber security culture is essential because it's people that make an organisation secure, not just technology and processes. If this is in place, people view security as a collective and collaborative endeavour that supports and is supported by their everyday work.

Growing cyber security expertise

As the demand for cyber security professionals grows, senior leaders should ensure that recruitment and training meet their cyber security needs. This will include a combination of investing in your people, bringing in external expertise, and developing a pipeline of talent. The assessment of cyber skills might be an activity within the people planning part of the business, and the board should have sight of this.

Part 2: Get the right information to support decision making

Identifying the critical assets in your organisation

Understanding how technical assets are critical to your organisation's objectives is key to effective risk management. This means having a good understanding of your technical estate, and being able to identify which are the critical assets upon which your key business objectives depend. The board will therefore need to communicate key objectives so technical experts can focus on protecting the things that ensure these objectives are fulfilled.

Understanding the cyber security threat

Understanding the threats faced by your organisation will enable you to tailor your organisation's approach to cyber security investment accordingly. You need to prioritise what threats you are trying to defend against, otherwise you risk trying to defend against everything (and doing so ineffectively). Threats will evolve over time, so it's important to stay up-to-date and regularly perform threat assessments.

Risk management for cyber security

Every organisation has to make difficult decisions around how much time and money to spend protecting their technology and services; cyber risk management should inform and improve these decisions. Many of your operational and organisational risks will have a cyber component to them. Cyber security risk should therefore be integrated within your overall approach to risk management, and not be dealt as a standalone topic (or considered simply in terms of 'IT risk').

Part 3: Take steps to manage those risks

Implementing effective cyber security measures

Implementing effective cyber security measures will help reduce the likelihood of a significant incident. Even basic cyber security measures can reduce your exposure to cyber attacks, and lessen the associated reputational, financial and legal impacts. With a baseline of controls in place to mitigate against the most common cyber attacks, you should then tailor your defences to mitigate your organisation's highest priority risks.

Collaborating with your supply chain and partners

Many organisations rely upon suppliers to deliver products, systems, and services. Supply chains are often large and complex, and effectively securing the supply chain can be hard because vulnerabilities can be inherent, introduced or exploited at any point within it. Building a clear picture of your suppliers (and working with them to establish their sub-contractors) is essential if you are to gain assurance that threats from the supply chain are understood, and risks mitigated.

Planning your response to cyber incidents

Cyber security incidents can have a huge impact on an organisation in terms of cost, productivity, reputation and loss of customers. Being prepared to detect and quickly respond to incidents will prevent the attacker from inflicting further damage, and can reduce the financial and operational impact. Having a well-prepared cyber incident response approach is essential for cyber resilience.

National Cyber Security Centre
a part of GCHQ

@NCSC @cyberhq ncsc.gov.uk National Cyber Security Centre