National Cyber Security Centre
a part of GCHQ

Guidance (/)

10 Steps: A Board Level Responsibility

Created: 29 Sep 2015
Updated: 08 Aug 2016
Part of: 10 Steps to Cyber Security (/guidance/10-steps-cyber-security)

Why protecting your information is a board-level responsibility.

Cyberspace has revolutionised how many of us live and work. The internet, with its more than 3 billion users, is powering economic growth, increasing collaboration and innovation, and creating jobs.

Protecting key information assets is of critical importance to the sustainability and competitiveness of businesses today. Companies need to be on the front foot in terms of their cyber preparedness. Cyber security is all too often thought of as an IT issue, rather than the strategic risk management issue it actually is.

Companies benefit from managing risks across their organisations - drawing effectively on senior management support, risk management policies and processes, a risk-aware culture and the assessment of risks against objectives. There are many benefits to adopting a risk management approach to cyber security, including:

Strategic Benefits

Corporate decision making is improved through the high visibility of risk exposure, both for individual activities and major projects, across the whole of the organisation.

Financial Benefits

Providing financial benefit to the organisation through the reduction of losses and improved “value for money” potential.

Operational Benefits

Organisations are prepared for most eventualities, being assured of adequate contingency plans.

We have therefore produced a set of questions for you which we believe will assist and support your existing strategic-level risk discussions, specifically how to ensure you have the right safeguards and cultures in place.

Key questions for CEOs and boards

Protection of key information assets is critical

1. How confident are we that our company’s most important information is being properly managed and is safe from cyber threats?
2. Are we clear that the Board are likely to be key targets?
3. Do we have a full and accurate picture of:

- the impact on our company's reputation, share price or existence if sensitive internal or customer information held by the company were to be lost or stolen?
- the impact on the business if our online services were disrupted for a short or sustained period?

Exploring who might compromise our information and why

1. Do we receive regular intelligence from the Chief Information Officer/Head of Security on who may be targeting our company, their methods and their motivations?
2. Do we encourage our technical staff to enter into information-sharing exchanges with other companies in our sector and/or across the economy in order to benchmark, learn from others and help identify emerging threats?

Pro-active management of the cyber risk at Board level is critical

1. The cyber security risk impacts share value, mergers, pricing, reputation, culture, staff, information, process control, brand, technology, and finance. Are we confident that:
    - we have identified our key information assets and thoroughly assessed their vulnerability to attack?
    - responsibility for the cyber risk has been allocated appropriately? Is it on the risk register?
    - we have a written information security policy in place, which is championed by us and supported through regular staff training? Are we confident the entire workforce understands and follows it?

Topics

Risk management(/topics/risk-management)
Cyber attacks(/topics/cyber-attacks)

Was this guidance helpful?

We need your feedback to improve this content.

Yes No