‘Cyber security 101’ for board members

Effective governance of any organisation requires board-level understanding of cyber security. Without it, no organisation can be confident that all risks are being adequately addressed.

This document provides a **sample script** of questions to discuss at your next board meeting. It will help you to find out whether you - as a board member - have enough cyber security knowledge to ensure:

- **you** can have constructive discussions with key staff
- **your organisation** has appropriate plans in place to mitigate threats

These questions are designed to encourage productive cyber security discussions between boards and key stakeholders in your organisation (such as your legal, procurement, HR as well as technical teams). The questions are designed as a ‘starting point’, rather than a checklist that’s simply to be worked though.

This sample script is taken from the NCSC’s Board Toolkit. Each section in the toolkit contains a full set of questions (with possible answers) that you can use to help evaluate your organisation’s performance.

Questions for board members

1. Is a cyber strategy in place?

A cyber strategy that supports your wider business strategy helps your organisation to reduce risk, financial impact and reputational harm. A cyber strategy is a plan of **high-level actions** to improve the resilience of your organisation and should cover your highest priority critical concerns (for example, unpatched software or obsolete devices) through to ongoing projects. As a minimum it should also include:

- planning your response to an incident
- exercising incident response procedures
- detecting, responding to and recovering from a cyber attack
- employee cyber awareness training

The board should receive management information on how the cyber strategy and plan are being delivered, and this should be reviewed at least annually.

2. Can board members name the top cyber security threats, and outline the measures that are in place to mitigate their impact?

An easy indicator for whether your organisation has clearly articulated the key cyber security threats is whether these issues have been communicated to the board.

For instance, for many organisations, ransomware attacks by cyber criminal groups at (or near the) top of the list. Board members should understand the nature of these threats, the risks they pose to your business, and how the organisation is addressing them.

3. Do we have an effective approach to managing cyber risks?

The board need assurance that a **cyber** risk register is in place, as part of the overall organisation risk register. It should cover risk ownership and an escalation mechanism for the whole extended enterprise, including front line business units, subsidiaries, suppliers and partners, and in some cases customers. This should involve all of the key stakeholders in the organisation and reflect the agreed priorities and tolerances endorsed by the board. The NCSC's detailed Risk Management guidance includes advice on choosing suitable frameworks for your organisation.

4. Does the board understand the overarching purpose of the cyber security measures in place?

Typically there are many technical details involved in assessing threats and risks, and the measures that protect against them. However, if the overarching approach to cyber security measures can be easily explained (and is understood by the board), that is a good sign that an effective approach is being taken.

5. Does your organisation have an incident response plan in place, and do you regularly rehearse it?

Board members should expect direct sight of the plan. Rehearsing your plan by running exercises will identify improvements, and are a far better way to ensure people know what they are expected to do, compared with reading documents. The board should expect to see reporting on the exercises conducted, and lessons learned. If an exercise has recently taken place against the cyber risk scenarios defined in the risk register, this suggests that the key processes will be fresh in the minds of both the board and the workforce, and you are well set up for incident response.

6. Are products/ services provided by partners/suppliers documented?

There should be evidence that external data processing arrangements have been documented, including the security of **all** data that has been shared (not just personal data). Critical dependencies on external services (not just IT services) should be mapped ensuring the risk around external failure is within the board's appetite (or that there are credible measures in place for redress if a supplier lets your organisation down). For more information you can refer to the NCSC's guidance on How to assess and gain confidence in your supply chain cyber security.

7. Do your organisation's security metrics focus on success rather than failure?

Metrics express the organisation's values, and if you appear to value the absence of reports of problems, you incentivise people to keep quiet about issues. Consider how you can formulate your security metrics in terms of successes. For example, as well as measuring how many people clicked on a phishing email, focus on how many people reported it.

8. Are your HR team identifying - and addressing - any cyber skills gaps in your organisation?

Whoever reports to the board on HR matters should be able to report on the specific skills gaps that the organisation is facing with a **plan** in place to develop cyber expertise where required. The board should be supporting this both in terms of investment and broader resources.

© Crown copyright 2023. Photographs and infographics may include material under licence from third parties and are not available for re-use. Text content is licenced for re-use under the Open Government Licence v3.0.