10 questions your board should ask about cybersecurity

Under NIS2, the management body approves and oversees the cybersecurity measures and can be held liable. These ten questions help directors check whether cybersecurity is really under control.

NIS2 Aware · nis2aware.eu · November 2026

1. Are we in scope of NIS2, and are we an essential or an important entity?

Why it matters: Your obligations, supervision and fines depend on it, and nobody will tell you: you must assess it yourselves.

A good answer: A documented analysis of sector and size, reviewed when the organisation changes (acquisition, new activity).

2. Are we registered with the CCB, and are our details up to date?

Why it matters: Registration on Safeonweb@Work is mandatory, and the CCB uses those contacts in a crisis.

A good answer: Registration confirmed, with named contacts who are still with the company.

3. What are our five biggest cyber risks, and what would they cost us?

Why it matters: The board cannot oversee what it cannot see. Risks expressed in business terms make decisions possible.

A good answer: A short risk register with impact on operations, revenue and reputation, updated at least once a year.

4. Which measures have we approved, and how do we know they work?

Why it matters: The board must approve the measures and oversee their implementation. Approval without follow-up is not enough.

A good answer: A plan of measures with owners and deadlines, and regular reporting with a few simple indicators.

5. If ransomware hit us tomorrow, how long until we are back up?

Why it matters: Backups and recovery are what make the difference between a bad week and a bankruptcy.

A good answer: Offline or immutable backups, a tested restore and a realistic recovery time for critical systems.

6. Who decides, and who notifies the CCB within 24 hours?

Why it matters: The early warning is due within 24 hours. In a crisis there is no time to find out who does what.

A good answer: A written incident procedure with names, phone numbers and decision rights, tested in an exercise.

7. Which suppliers could bring us down, and what do we require from them?

Why it matters: Many incidents start at a supplier. NIS2 requires you to manage supply chain security.

A good answer: A list of critical suppliers with security clauses, notification duties and periodic checks.

8. Is multi-factor authentication enabled everywhere it matters?

Why it matters: Stolen passwords are the most common way in. MFA stops most of these attacks.

A good answer: MFA on email, remote access, cloud services and all administrator accounts, with no exceptions.

9. Have the board and staff been trained, and can we prove it?

Why it matters: Training of the management body is a legal obligation, and people are the first line of defence.

A good answer: Board training completed, a yearly awareness programme for staff, and attendance records.

10. What is our budget and roadmap for the next 12 months?

Why it matters: Cybersecurity is a continuous effort. Without budget and targets, it stays on paper.

A good answer: A target (for example a CyberFundamentals level), a roadmap and a budget approved by the board.

> **How to use it:** put two or three questions on the agenda of each board meeting, and ask for the answers in writing.

General information on the Belgian NIS2 framework as of November 2026, not legal advice. Always check the latest guidance from the CCB (ccb.belgium.be and atwork.safeonweb.be).