Cybersecurity in the Boardroom: the Importance of a Warm Handshake

A unique international study on cybersecurity reporting to boards of directors.

The increasing cyber threats make proper reporting on cybersecurity to boards of directors increasingly important. A new international report, a collaboration between the Centre for Corporate Governance in St. Gallen, Switzerland and the Centre for Cybersecurity Belgium, provides directors with a framework to better fulfil their role in cybersecurity governance. "It's crucial to create a warm handshake between board and management," says Chris Verdonck, initiator of the project.

Cyber threats on the rise

"The threat of cybercrime is increasing significantly. Cyber activism, espionage, and sabotage are also becoming more real due to the geopolitical situation," warns Miguel De Bruycker, Director-General of the Centre for Cybersecurity Belgium (CCB). Belgian companies are certainly at risk. "Cybercrime doesn't respect national borders or sectors. Anyone who can be hacked and where ransom can be demanded is in the crosshairs. Our essential services in particular are definitely targets."

A unique study

The report is the result of a unique international study surveying 67 large companies in Belgium, Switzerland, and Australia. Of those companies, 63% were publicly listed, with an average market capitalisation approaching 20 billion. The researchers spoke exclusively with board members and analysed dozens of sanitised cybersecurity reports.

The handshake as a crucial moment

Before the project began, many board members expressed discomfort discussing cybersecurity during board meetings. That handshake between board and management takes place when cybersecurity is on the agenda and a report is presented. A warm handshake requires engagement from both sides.

Work to be done

Only 65% of interviewees indicated they had the right information to make properly informed decisions. Reporting often lacks consistency, is too technical, and misses the link with business risks.

Three key points from the framework

1. Know your environment: Understand your organisation’s risk level and cybersecurity maturity.
2. Organise your board: Structure how cybersecurity is discussed at board level.
3. Adapt your reporting: Align reporting with the organisation’s cybersecurity maturity.

Boards often don't know what to ask

A clear framework helps board members feel more confident, better informed, and more comfortable asking questions.

Report availability

The report entitled *Cyber Security Board Reporting - The Board's Perspective* will be available mid-April via www.cybersecurityboardreporting.com. Pre-registration is already open. Use promotion code **CyberBoardReporting** to receive a 15% discount. This offer is exclusive for Guberna members and valid until the end of 2025.