WHAT THE BOARD SEES
Board Reporting
THE EVIDENCE IT RESTS ON
Benchmarking | Research

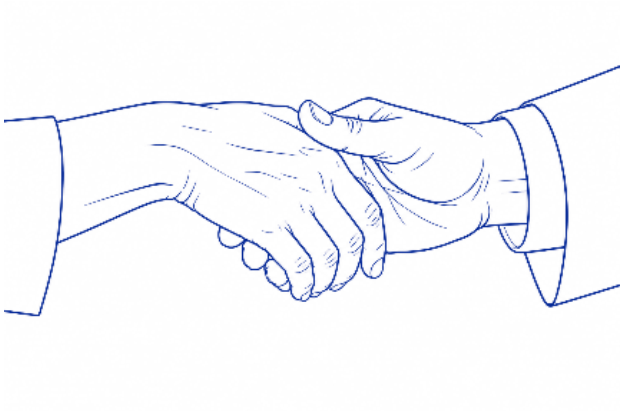
Cybersecurity Board Reporting 2026

The Two Sides of the Handshake

Published 29 October 2026 · Chris Verdonck, Maya Bundt, Tommy Viljoen

Two sides of one handshake

- Every Board discussion of cybersecurity is a meeting between two parties who see the subject differently
- The Executive responsible for cybersecurity knows the exposure in operational detail
- The Board carries the accountability for the decisions that follow
- The 2026 report calls that meeting the handshake
- For the first time, the same questions were put to both sides
- This document previews what the report contains and a selection of what it found



The report in numbers

The report

110+
pages

50
figures

19
tables

26
moves a Board can make

1
standard report

The evidence

78
Board Directors interviewed, one hour each

13
countries

35
Executives responsible for cybersecurity surveyed

11
sanitised Board documents from 7 organisations

What was done: data sources

1 Board Director interviews

78 Directors in 13 countries, one hour each, through a structured questionnaire. Conducted by the founders and 5 country fellows, February to August 2026.

2 Executive survey

35 Executives responsible for cybersecurity, 26 with a CISO or equivalent title and the rest CIOs, CEOs and a CTO, answering many of the same questions in the same words. Approached separately from the Directors.

3 Interview notes

Sixty-five Directors gave notes beyond their survey answers, producing 634 coded observations and the quotations in the report.

4 Sanitised Board documents

Eleven documents from 7 participating organisations, each coded against the survey's content categories before the Director's answers were examined.

Eleven judgement questions, each out of 10. Quality, the information it gives and the willingness to recommend it are averaged into a reporting score used throughout. Findings describe the population studied, not any individual Board, and practices that occur together, not causes.

What the report contains

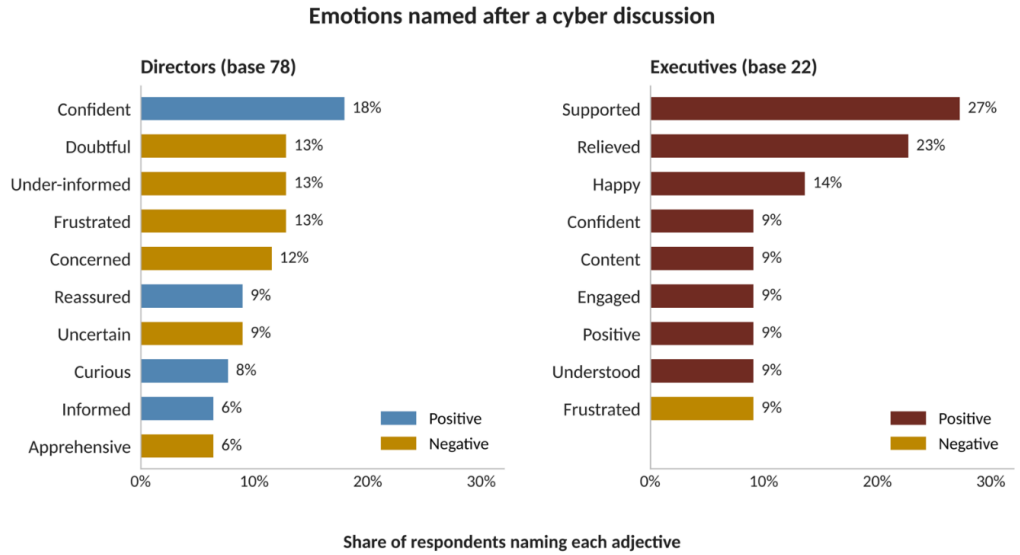
Executive summary	The argument in short, and the findings of each chapter on three pages.
1. The handshake and why it is often cold	Where the two sides describe the same exchange differently: who the Board hears from, what cyber risk means, what each believes the pack contains, and how each feels afterwards.
2. Board-level Governance	Where cybersecurity sits, how much time it gets, who presents, what the Board is equipped to do, how risk appetite and budget are handled, and whether anything is decided.
3. Board Reporting	Whether the information arrives as one assembled overview, holds its shape over time, can be believed, contains what it should, and asks anything of the Board.
4. What a warm handshake looks like	The Digital Profile, three factors that set the level an organisation needs, and a map of where the 78 Boards sit on governance and reporting.
5. What can be done	Twenty-six moves, grouped by handshake, governance and reporting, and two exercises a Board can run in a single meeting.
6. Closing	What the evidence adds up to, and the question each Board can put to itself.
Annex A. A standard cybersecurity Board report	One structure for every Board, in three layers and six content areas, sized to the organisation's Digital Profile. Written for the Executives who produce it.
Annex B. What the regulatory frameworks require of Boards	What the regimes in the main countries studied have in common at the level of the governing body.
Annex C. Methodology	Samples, the reporting score, the statistical approach and its limitations.

Why the handshake is often cold

−53
Net Promoter Score, Directors

−34
Net Promoter Score, Executives

- **Neither side would recommend the reporting.** Only 19 of 78 Directors rate their decision information at 8 out of 10 or higher
- **They leave the room feeling differently.** 20 of 22 Executives named a positive emotion; over a third of Directors named doubt
- **Not all Boards know their CISO.** 21 of 78 Boards have no working route to the security function



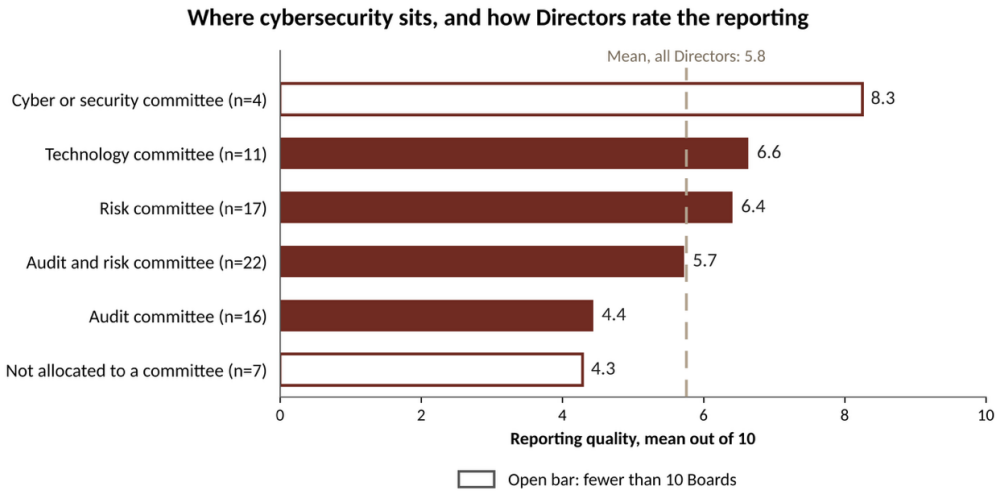
Emotions named after a cyber discussion, Directors and Executives (Figure 12 in the report).

Governance: where the topic sits matters

4.4
out of 10, audit committee alone

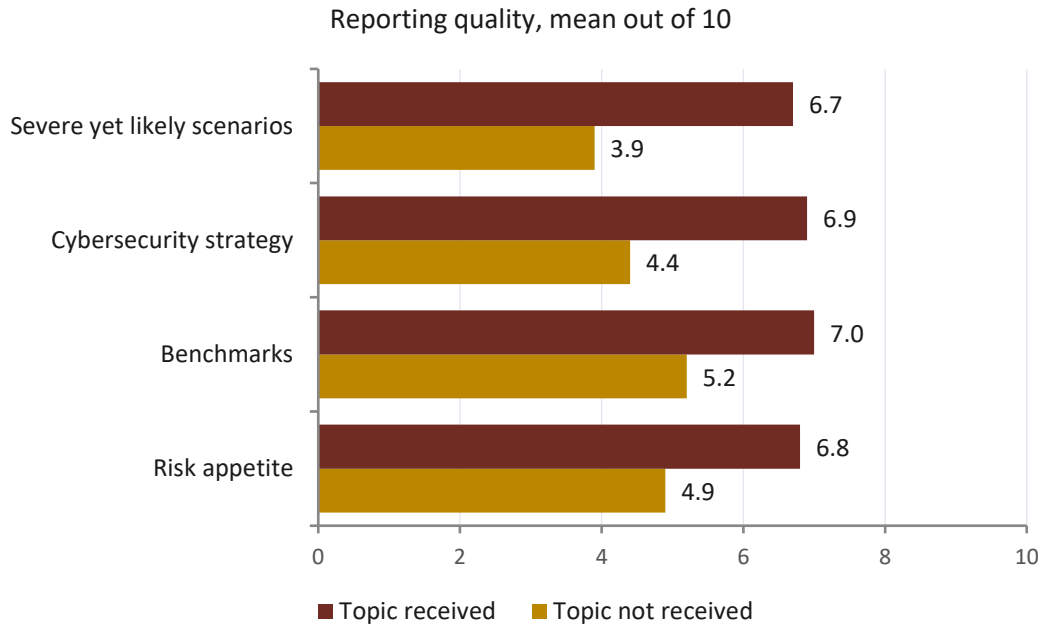
6.4
out of 10, risk committee

- **One hour a year.** The median Board gives cybersecurity one hour at Board level, 3 hours with committee time
- **Repetition beats a single session.** Annual training and crisis simulations go with reporting rated about 2 points higher
- **Ten of 11 governance practices** go with better-rated reporting, and most are decisions a Board can take on its own



Where cybersecurity sits, and how Directors rate the reporting (Figure 18 in the report).

Reporting: what reaches the Board, and how Directors rate it



Directors' rating of reporting quality where the topic is received and where it is not (Sections 2.6 and 3.4 in the report).

23

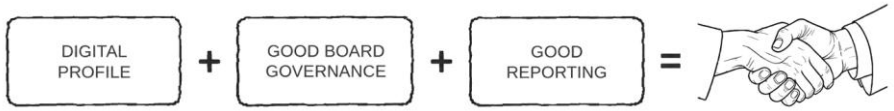
topics tested, in 6 content areas

7.4

out of 10 with 19 or more topics; 3.7 with 12 or fewer

- **The report does this for all 23 topics:** how many Boards receive each, and how Directors rate the reporting with and without it
- **The least supplied topics** are the ones that require a measurement, a comparison or a decision before they can be reported
- **No sign of information overload.** Within this sample, Boards receiving more topics rate their reporting higher, not lower

The Handshake Model: the level a Board needs



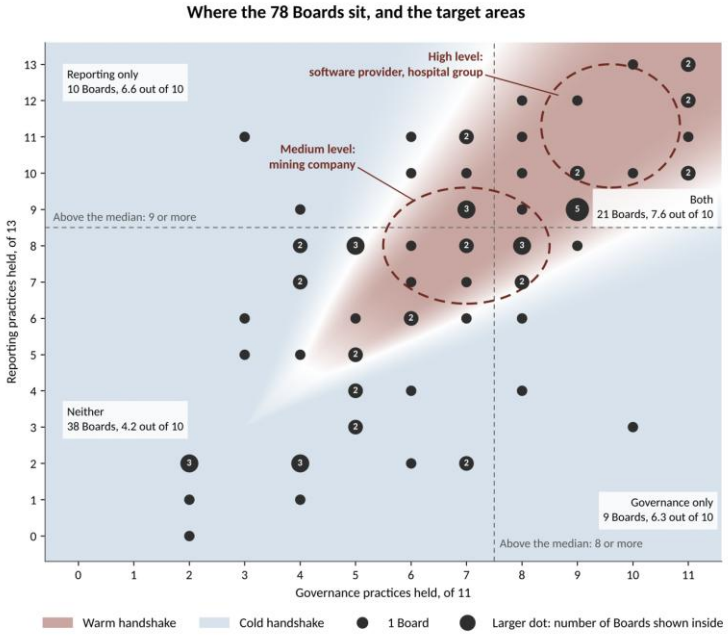
7.6

out of 10, above the median on both dimensions

4.2

out of 10, at or below on both

- **The Digital Profile** sets the level an organisation needs from 3 factors: risk, regulation and opportunity
- **Two dimensions,** measured by 11 governance and 13 reporting practices, behave separately
- **Nineteen Boards** are strong on one dimension only, and land in between



Where the 78 Boards sit, with the warm and cold zones (Figure 50 in the report).

What can be done: 26 moves, and where to start

3

Where to start

- Agree the level the organisation needs before judging where it stands
- Build governance and reporting together
- Take the next step rather than adding more of the same

6

Moves on the handshake

- Establish a route to whoever owns security
- Compare the two descriptions of the same pack
- Say what you want to see

8

Moves on governance

- Give the committee a forward-looking remit
- Agree how much risk the Board will carry, and in what terms
- Rehearse or train regularly, not once

9

Moves on reporting

- Ask for one assembled overview
- Discuss one severe yet likely scenario each year
- Require a decision at the end of the cyber paper

Two exercises close the chapter. A 12-question condition map the Board can complete in one agenda slot, and the two descriptions, where the Executive and the committee chair each write down what they believe the pack contains, and discuss only the differences. Most moves need a conversation or a decision rather than new resources.

What the annexes add

Annex A

A standard cybersecurity Board report

One structure for every Board: 3 layers, 6 content areas, a one-page position and a calendar across the year, sized to the Digital Profile. Written for the Executives who produce the reporting.

Annex B

What the regulatory frameworks require of Boards

What NIS2, DORA and the regimes in the main countries studied have in common at the level of the governing body: accountability, approval, training and notification.

Annex C

Methodology

Samples, the 11 judgement questions, the reporting score, the correction for multiple comparisons, and 7 limitations stated in the order of how much of the report they qualify.

'If you had asked me at the beginning of the interview, I would have said eight, now I am saying six. If it was worse than six I would have to ask more questions.'

A Board Director

Who the report is for, and what to do with it

Who it is for

- **Board Directors,** in particular Chairs and members of audit, risk and technology committees, who want to know where their Board stands and what to ask for
- **CISOs and other Executives responsible for cybersecurity,** who produce Board reporting and want a structure that both sides of the exchange can agree on
- **Advisers to Boards,** company secretaries, auditors, regulators and educators who support Boards on cyber governance

What a reader can do with it

- Understand where your Board stands on cybersecurity governance and reporting, compared with 78 Boards in 13 countries
- See the exchange from the other side: what Executives believe they deliver, and what Directors say they receive
- Establish what level of oversight your organisation actually needs, rather than measuring against a single standard
- Identify the one or two next steps that are likely to make the largest difference for a Board in your position
- Give the Board and the Executive a shared language, and a structure for the reporting, that both can agree on

If you have only 30 minutes, read the Executive summary, the closing section of each chapter and Chapter 5.

WHAT THE BOARD SEES
Board Reporting
THE EVIDENCE IT RESTS ON
Benchmarking | Research

Purchase and enquiries

info@cybersecurityboardreporting.com

www.cybersecurityboardreporting.com

Published 29 October 2026

Cybersecurity Board Reporting is an independent, self-funded research initiative founded and run by three equal partners: Chris Verdonck (Belgium), Tommy Viljoen (Australia) and Maya Bundt (Switzerland). It sells no security products and holds no commercial relationship with any vendor.

The 2026 report is the second study, following The Boards' Perspective in 2025.

Five country fellows contributed to this year's study, and the research is supported by the International Center for Corporate Governance in St. Gallen and the Centre for Cybersecurity Belgium.

Benchmarking will be available as of January 2027.