BOARD BRIEFING · CYBERSECURITY

Cyber terms for the boardroom

Most cyber briefings are written for the SOC. This one is written for the board. Thirteen terms, defined for oversight, each paired with **the single question to put to management before the next incident, not in the post-mortem.**

■ CORE VOCABULARY ■ ACUTE BOARD EXPOSURE

1 Ransomware ■

Malware that locks or steals your data, then demands payment. Modern crews do both: encrypt and threaten to leak.

Stake: Paying may be illegal if the group is sanctioned. Not paying may halt operations for weeks.

ASK

Have we decided, in advance, whether we would pay — and confirmed it is legal?

2 Phishing / social engineering ■

Tricking a person into clicking, paying, or handing over access.

Stake: Most breaches still start with a person who clicked, not a flaw no one knew about.

ASK

When did we last test our own people, and what share failed?

3 Multi-factor authentication ■

A second proof of identity beyond the password. A code, a key, a prompt.

Stake: The highest-return control there is. Insurers now refuse to cover firms without it.

ASK

Is MFA enforced everywhere, including admins, vendors and legacy systems?

4 Zero trust ■

Trust nothing by default. Verify every user, device and request, every time.

Stake: The architecture regulators and insurers now expect. Network location no longer earns access.

ASK

Where are we on the zero-trust roadmap, and what still runs on implicit trust?

5 Attack surface ■

Everything an attacker could reach. It grows with every cloud app, vendor and remote device.

Stake: You cannot defend what you do not know you own. Shadow IT widens it silently.

ASK

Do we have a current inventory of everything internet-facing?

6 Supply-chain risk ■

Your security now depends on your vendors' security. SolarWinds and MOVEit reached thousands through one supplier.

Stake: You inherit every breach upstream of you, and the regulator still asks you.

ASK

Which third parties can reach our most sensitive data, and how do we assure them?

7 Patch management ■

Closing known holes before attackers use them.

Stake: Most intrusions walk through a known door a patch already existed for.

ASK

What is our mean time to patch a critical vulnerability?

8 Business email compromise ■

Impersonating an executive or supplier to redirect a payment.

Stake: The FBI ranks it the costliest cybercrime by dollar loss. No malware required.

ASK

What stops a spoofed CEO email from authorising a wire transfer?

9 Endpoint detection & response ■

Continuous monitoring on every device, with the ability to isolate and respond.

Stake: The gap between break-in and detection — dwell time — decides whether it stays an incident or becomes a catastrophe.

ASK

How long could an intruder sit in our network before we noticed?

10 Encryption ■

Scrambling data so it is useless without the key, at rest and in transit.

Stake: Many breach laws offer safe harbor if the stolen data was encrypted. Key control is the catch.

ASK

Is our sensitive data encrypted, and who holds the keys?

11 Incident response ■

The rehearsed plan for the breach you will eventually have.

Stake: Under 30% of firms are confident in their incident response (Barclays, 2026). Confidence comes from rehearsal.

ASK

When did this board last sit through a breach tabletop?

12 Breach disclosure & materiality ■

The legal duty to tell regulators and markets when a material incident happens.

Stake: US public companies must disclose a material incident within four business days of deciding it is material (SEC, 2023).

ASK

Who decides materiality here, and could we file within four days?

13 Cyber insurance ■

Transferring some of the financial risk of a breach to an insurer.

Stake: Policies now demand MFA, EDR and tested backups, and exclude acts of war. Coverage you cannot claim is not coverage.

ASK

What does our policy exclude, and do we actually meet its control requirements?

> Strong security posture produces compliance as a by-product. The reverse never works.

Sources: NIST Cybersecurity Framework 2.0 (2024) · Verizon Data Breach Investigations Report · SEC Form 8-K, Item 1.05 (2023) · FBI IC3.

FOLLOW FREDRIK LINDSTROM FOR MORE

Fredrik Lindstrom

AI and cybersecurity governance for boards, CISOs and senior leaders. 25+ years in enterprise security.

Every promise. Every risk. The truth.

ARTICLES & BOARD ADVISORY
fredriklindstrom.info
Long-form governance analysis and toolkits

LINKEDIN
in/fredriklindstrom
Daily commentary and article launches

YOUTUBE
@Promise-and-Risk-AI
AI education without the hype or fear

COMPANION SITE
promiseandrisk.ai
Episode notes, sources and explainers

NEWSLETTER
The Governance Memo
Monthly, board-facing. Subscribe at fredriklindstrom.info