Security metrics: which few numbers show the board whether you're getting safer?

This quarter, pick about seven measures tied to how attacks start, count each one against your full inventory and have management agree a target and tolerance for each. Then report them on one page every quarter with trend, target and the decision you need, and drop any measure that hasn't changed a decision in a year.

Reviewed	Next review	Version
5 Nov 2026	**5 Dec 2026**	**1.0**

Written for

CISOs and security and IT leads in EU organizations who report to management and boards, including management bodies with NIS2 or DORA duties

Latest version

sheets.einblick.dev/security-metrics/

If you only do five things

1. **Count outcomes, not activity.**
   Report what an attacker would find. Microsoft says reporting should shift from patches deployed to exposure reduced, detection coverage increased and time to mitigate compressed[1].
2. **Tie each measure to a way in.**
   Exploitation now opens 31% of breaches with a known vector in Verizon's data, more than any other[2]. Pick a few measures for the paths that hurt you; NIST says that initially, less is often more[3].
3. **Count against the whole inventory.**
   Give every share its denominator, including assets found this quarter. A system nobody listed never shows up as uncovered.
4. **Agree targets and tolerances with management.**
   The UK Cyber Governance Code asks boards to require reporting at least quarterly and agree a tolerance for each metric, based on the agreed risk appetite[4].
5. **End every report with a decision.**
   Say whether findings fit the risk appetite and what decision is needed, as NIST suggests[3]. Minute the answer: the BSI recommends decisions as proof of active involvement[6].

Build the set in this order

1. **Which ways in matter most to you?**
   Start from your incidents, near misses and test findings of the last two years, then check the year's M-Trends and DBIR.
2. **What would show each path closing?**
   Write each measure's formula, target, data source, owner and frequency, as NIST's suggested fields do[3]. Prefer ages, times and shares to counts.
3. **What is it counted against?**
   Name the inventory behind each share. List hypervisors, appliances and OT that can't run an agent as gaps, not as out of scope.
4. **What does good look like?**
   After three months of data, propose a target and tolerance per measure, in days, euros or share of critical services, and have management sign them off.
5. **Is each measure still earning its place?**
   Review the set at planned intervals and after significant incidents or changes, as Regulation 2024/2690 requires of digital providers[7]. Drop any measure that changed no decision in a year.

A starter set, tied to how attacks start

Report each as a trend against its target and coverage. The linked sheets define the measures.

- **Internet exposure.** High-risk services open to the internet without an expiring exception, and assets others found first, from the attack surface sheet.
- **Age of exploited vulnerabilities.** Days the oldest known-exploited flaw has been open, and first-tier deadlines met, from the patching sheet. Only 26% of KEV flaws in Verizon's data were fully fixed in 2025, and full fixes took a median of 43 days[2].
- **Phishing-resistant MFA coverage.** Accounts, admins first, that Conditional Access holds to the passkeys sheet's phishing-resistant methods. Entra's passwordless count includes phone sign-in[8], which isn't phishing-resistant[9].
- **Standing privileged accounts.** Tier 0 rights held permanently, not on activation, against the privileged access sheet's limits. Microsoft ranks tiered administration among the best safeguards[1].
- **EDR coverage.** Devices and servers with EDR and tamper protection, as the endpoints sheet sets them up, out of all discovered; Defender's inventory lists devices not onboarded[10]. Count hypervisors apart: virtualization has traditionally sat outside EDR's scope[11].
- **Measured restore time.** Hours to restore each critical service in its last test, against its target, from the backups sheet. A target not met in a test is unmet.
- **Time to detect and contain.** In real incidents and planted tests, with alerts proved monthly from the logging sheet and staff report speed from the awareness sheet. Mandiant's median dwell time rose to 14 days in 2025, from 11[11].

What you can skip

- **Counts of blocked attacks.** They follow attacker volume and filter settings, not your risk.
- **Phishing click rates as a target.** A poorly designed test can show a better rate while saying less, NIST notes[3]. Report reports instead.

Mistakes that cost the most

- **Reports that ask for nothing.** Management can't oversee what it's never asked to decide.
- **Shares without a denominator.** 98% EDR coverage of known devices can hide every hypervisor and appliance that can't run an agent.

- **Colors and maturity levels alone.** NIST doesn't count color scales or rankings as measures[3]. Put a number behind each.
- **Live dashboards for the board.** It needs a quarterly page of trends and decisions, not live data.

What goes on the board page

- **One row per measure.** Value, four quarters of trend, target and tolerance, and why it moved; the NCSC tells boards to expect agreed target ranges[12].
- **Top risks and accepted risks.** The top risks with the status of their measures[6], and each accepted risk with its expiry date.
- **Incidents and near misses.** What happened, what it cost and what changed. A board may need only the main lessons, the NCSC says[12].
- **Decisions needed.** Each with options, cost and a recommendation.
- **The same layout every quarter.** Consistent metrics are what show long-term trends, NIST notes[3].

Keep the numbers honest

- **Reward reporting.** Valuing the absence of reported problems teaches people to keep quiet, the NCSC warns[12]. Count near misses as a success; NIS2 lets entities report them voluntarily[13].
- **Show the worst case.** Put the oldest exploited flaw and the slowest restore next to each median.
- **Separate inventory growth.** Report newly found assets on their own line, so a better inventory doesn't look like decline.
- **Have someone else recompute it.** Once a year, let someone outside the team rebuild two measures from raw data.
- **New definitions every quarter.** Each change breaks the trend. Restate past values when you must.
- **A green report in the quarter of a breach.** The set measured the wrong things. Rework it after each significant incident.

What management must do

- **NIS2.** Management approves the measures, oversees them and can be held liable; the measures include assessing their effectiveness[13].
- **Germany.** Under BSIG § 38, management implements and oversees the § 30 measures, including effectiveness checks, and is liable to the entity[14]. The BSI's example answer adds KPIs, KRIs and a yearly audit[15].
- **Digital providers.** Indicators for the security policy, one person reporting directly to management, and measurement results reported to it[7].
- **DORA.** The management body approves the ICT risk framework and risk tolerance; the strategy sets KPIs and key risk metrics. It hears of major incidents and yearly lessons learned[5]. BSIG § 38 doesn't apply[14].

What changed in 2026

- **The BSI recommends a regular report.** Its October 2026 curriculum lists a resolution on a regular cyber risk report among the decisions to take, ideally within 2 to 6 weeks of management's first training[6].
- **Voice phishing overtook email.** It opened 11% of Mandiant's 2025 intrusions, after exploits; email phishing fell to 6%[11]. Measure how the help desk handles reset calls.
- **Microsoft discounted alert counts.** Its 2026 report says they no longer show SOC maturity; measure detection fidelity and time to contain[1].

What this looks like at your size

Small team, no security staff

- Ask your IT provider for four numbers a quarter: admins on phishing-resistant MFA, EDR coverage, oldest open exploited flaw, last restore time.
- Give the managing directors one page and file their decisions with the training record.

Growing, with IT or security staff

- Pull the numbers from Entra's authentication methods activity (P1 or P2)[8], Defender's device inventory[10] and a scanner matched against KEV.
- Have management sign off targets and tolerances yearly, with the risk appetite.

Enterprise or regulated

- Under DORA, write the KPIs and key risk metrics into the resilience strategy[5].
- Show the gap to the board with CSF 2.0 Current and Target Profiles[16].
- Use one set of definitions in every subsidiary.

Version history

5 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which narrowed 12 statements to what the sources say.

Sources

1. Microsoft Digital Defense Report 2026. Microsoft Threat Intelligence, Oct 2026. cdn-dynmedia-1.microsoft.com
2. 2026 Data Breach Investigations Report. Verizon, 19 May 2026. verizon.com
3. SP 800-55v1, Measurement Guide for Information Security: Identifying and Selecting Measures. NIST, Dec 2024. csrc.nist.gov
4. Cyber Governance Code of Practice. DSIT and NCSC (UK), 8 Apr 2025. gov.uk
5. Regulation (EU) 2022/2554 (DORA), Articles 5, 6, 13 and 17. EUR-Lex, 2022. eur-lex.europa.eu
6. Curriculum für eine Geschäftsleitungsschulung nach NIS-2. BSI, 28 Oct 2026. bsi.bund.de
7. Commission Implementing Regulation (EU) 2024/2690, Article 1 and Annex points 1, 2 and 7. EUR-Lex, 2024. eur-lex.europa.eu
8. Authentication Methods Activity. Microsoft Learn, 22 Oct 2025. learn.microsoft.com
9. Overview of Conditional Access Authentication Strengths. Microsoft Learn, 4 Mar 2025. learn.microsoft.com
10. Microsoft Defender for Endpoint device discovery overview. Microsoft Learn, 8 May 2025. learn.microsoft.com
11. M-Trends 2026 Executive Edition. Google Cloud (Mandiant), Mar 2026. services.google.com
12. Board Toolkit: Questions for the board to ask about cyber security. NCSC (UK), 2025. ncsc.gov.uk
13. Directive (EU) 2022/2555 (NIS2), Articles 6, 20, 21 and 30. EUR-Lex, 2022. eur-lex.europa.eu
14. BSI-Gesetz (BSIG), §§ 28, 30 and 38. BMJV (Germany), checked 5 Nov 2026. gesetze-im-internet.de
15. Schulung für Geschäftsleitungen (Handreichung), version 1.0. BSI, 17 Apr 2026. bsi.bund.de
16. The NIST Cybersecurity Framework (CSF) 2.0. NIST, 26 Feb 2024. nvlpubs.nist.gov