TEMPLATE

Board Cybersecurity Report Template

A structure for reporting cybersecurity to a board that has ten minutes: where the organisation stands, what moved since last time, what is overdue, and the decisions that need the people in the room.

WHO IT IS FOR

Whoever presents security to a board or audit committee — often a CTO, COO or finance lead who is not a security specialist and gets one slot on the agenda.

LAST REVIEWED

14 September 2026

READING TIME

13 minutes

ON THIS PAGE

A board does not need a control list. It needs to know whether the organisation is exposed, whether that is getting better, and whether anything is waiting on a decision from the people in the room. Most security reports answer none of those on the first page, because they are written by the people doing the work, in the language of the work.

This template is built the other way round. Page one answers the board's question. The risk section reports decisions rather than colours. Gaps are named plainly, with an owner and a date. Incidents are reported with a clear line between what belongs in the minutes and what belongs in an appendix. Cost is shown against what it bought. And there is a list of what to leave out, which matters as much as anything that goes in.

Each section lists the fields to complete, with guidance on what a good entry looks like and an example. Every example is written for Fernhill Fabrication Ltd., a fictional 140-person manufacturer invented for this template. Its names, dates and figures are illustrative and do not describe any real organisation.

Use the same structure every time you report. A board can only see movement if this quarter's report has the same shape as last quarter's.

PART 1 OF 8

Page one: the summary

Page one should stand on its own. A director who reads nothing else should know the position, the direction of travel, and what is being asked of them. Keep it to one page, in sentences rather than charts.

Reporting period and source

The period covered, the date the report was prepared, and where the figures come from — the register, system or review behind them. One line.

EXAMPLE

Quarter ending 30 September. Figures taken from the risk register and evidence records as at 25 September.

YOUR ENTRY

Overall position

Two or three sentences on where the organisation stands against the objective the board agreed: a framework readiness target, an insurance requirement, a customer commitment. Words before numbers. If you use a score, say what it is derived from and that it is not a certification or an external rating.

EXAMPLE

We remain on track for the ISO/IEC 27001 readiness review the board approved for next spring. Access control, backups and endpoint protection are in place and evidenced. Supplier security and internal audit are the two areas behind plan.

YOUR ENTRY

Movement since the last report

What improved, what got worse and why — including where a figure worsened because the record became more accurate. Name the change rather than describing a trend.

EXAMPLE

MFA now covers all remote access, closing the gap reported last quarter. Evidence readiness fell because we began tracking expiry dates, and four training and access review records turned out to be out of date. Their renewal is scheduled for October.

YOUR ENTRY

Decisions required

No more than three. For each: the decision, the options, the recommendation, what happens if the board does not decide, and the date a decision is needed by. If nothing needs deciding, say so.

EXAMPLE

Formally accept the risk from the unsupported production scheduling server until its replacement next year, with network isolation in place (recommended); or fund accelerated replacement this quarter. A decision is needed at this meeting because the insurance application is due in six weeks.

YOUR ENTRY

Overdue or at risk

Items past their due date, or likely to miss it, that a director would want to know about. Owner and revised date for each. Keep it short.

EXAMPLE

Security reviews of our three critical suppliers are six weeks overdue. Owner: Head of Procurement. Revised date: 15 November.

YOUR ENTRY

One-line takeaway

The single sentence you would want recorded in the minutes if only one could be.

EXAMPLE

Position improving; one risk acceptance needed today; supplier reviews are the item to watch.

YOUR ENTRY

PART 2 OF 8

Risks: treatment decisions, owners and dates

Report the handful of risks that matter at board level — usually the highest rated, and any that need the board's attention — as decisions rather than as a

heat map. A colour tells a director how worried to feel. A treatment decision with an owner and a date tells them what is being done, and when to ask again.

List accepted risks separately. Accepting a risk is a legitimate management decision, and exactly the kind of decision a board should be able to see.

Risk statement

One sentence describing the event, its cause and its consequence for the business. Avoid category labels such as “ransomware” or “third-party risk” on their own.

EXAMPLE

An attacker who compromises an administrator account could encrypt production systems and their backups together, stopping manufacturing for an extended period.

YOUR ENTRY

Current rating and what it rests on

The rating from your register and, in a few words, the basis for it. A likelihood-and-impact grid is a structured judgement, not a measurement; saying so keeps the discussion honest.

EXAMPLE

High. Based on the August restore test, which recovered systems but took longer than operations can tolerate.

YOUR ENTRY

Treatment decision

Which route was chosen — reduce, transfer, avoid or accept — and who decided. A risk with no recorded decision should be reported as exactly that.

EXAMPLE

Reduce, decided by the executive team in July, with part of the financial impact transferred through the cyber insurance policy.

YOUR ENTRY

Owner

A named person with the authority to deliver the treatment or escalate it. Not a team or a department.

EXAMPLE

IT Manager, with the Operations Director accountable for recovery priorities.

YOUR ENTRY

Actions and target dates

The two or three actions that will change the rating, each with a date and whether it is on track.

EXAMPLE

Immutable backup copy in place (done, August). Separate backup administration credentials (due 31 October, on track). Second restore test to confirm recovery time (due December).

YOUR ENTRY

Change since the last report

What moved and why. If nothing moved, say so and explain why.

EXAMPLE

Rating unchanged. The immutable copy is delivered; recovery time is still to be proven.

YOUR ENTRY

Accepted risks

For each: who accepted it, when, the reason, any compensating measures, and the date it comes back for review. Flag any acceptance that has no review date.

EXAMPLE

Unsupported scheduling server — acceptance proposed today; compensating control is an isolated network segment reachable by two administrators; review date 30 June.

YOUR ENTRY

PART 3 OF 8

Wording for reporting a gap

Gaps are where security reports most often go wrong, in one of two directions: language that alarms a board into a decision it does not need to make, or language that buries the gap so thoroughly nobody asks about it. The pattern that works is plain — what is missing, what it exposes, what limits the exposure now, what will close it, who owns that and by when. The examples below are for the fictional Fernhill Fabrication Ltd.

REPORTING A GAP: ALARMING, BURIED AND PLAIN VERSIONS OF THE SAME NEWS

SITUATION	ALARMING	BURIED	PLAIN
Backups have not been restore-tested	“We have no idea whether we could recover from ransomware.”	“Backup assurance activities are progressing.”	“Backups run and an offline copy exists, but we have not yet proven a full restore. A test is booked for November; until then, our recovery time is unknown.”
Supplier reviews are overdue	“Our suppliers are a major uncontrolled risk.”	“Third-party governance continues to mature.”	“Security reviews of our three critical suppliers are six weeks overdue. Their access is limited and protected by MFA. Reviews will be complete by 15 November, owned by the Head of Procurement.”
An internal check found a control failure	“Access control has failed.”	“Some minor observations were raised.”	“Our access review found two former contractors with active accounts. Both were disabled the same day, the logs we hold show no use of them, and leaver processing now includes a check by IT.”
A readiness measure fell	“Compliance has deteriorated significantly.”	Leaving the measure out of this quarter’s report.	“Evidence readiness fell because we started tracking expiry dates, which showed four records were out of date. The controls still operate; the records proving it will be renewed by the end of October.”

PART 4 OF 8

Incidents and near-misses

Report incidents and near-misses in the same format every period, including the ones where nothing significant happened. A near-miss — a phishing email

reported before anyone acted on it, a supplier compromise that did not reach you — often tells a board more about the programme than an incident does, because it shows a control doing its job.

Where an incident may carry legal, regulatory, contractual or insurance consequences, agree the wording with legal counsel before it goes into board papers. Papers and minutes are records, and they may later be read by people outside the organisation.

Summary for the period

One or two sentences: whether any incident met your threshold for board reporting, and a brief note of lower-level events if you track them. State the threshold, so the board knows what “no incidents” means.

EXAMPLE

One incident met the board reporting threshold this quarter, and two near-misses are summarised below. Our threshold is any event affecting customer data, production, payments or a possible notification obligation.

YOUR ENTRY

What happened

A short, factual account: when it was identified, what was affected and how it was detected. No speculation about causes or attackers.

EXAMPLE

On 12 August the finance team identified a fraudulent request to change a supplier's bank details, sent from a lookalike email domain.

YOUR ENTRY

Impact

Financial, operational, data and customer impact, separating what is known from what is still being established.

EXAMPLE

No payment was made, no systems were compromised, and no personal data was involved.

YOUR ENTRY

Status and obligations considered

Whether the incident is closed, and whether notifying the insurer, customers, regulators or others was considered — by whom, and on whose advice. Record the decision, not a legal analysis.

EXAMPLE

Closed. The insurer's notification requirements were reviewed with our broker and legal counsel, and no notification was required.

YOUR ENTRY

What changed as a result

The actions agreed, with owners, dates and whether each is complete.

EXAMPLE

Call-back verification on the supplier's known number is now required for every bank detail change (Finance Director, complete). Lookalike domain detection is enabled in email filtering (IT Manager, complete).

YOUR ENTRY

Near-misses worth noting

Up to three, one line each, chosen because they show a control working or a weakness found before it was exploited.

EXAMPLE

A member of staff reported a credential phishing email within minutes, and the same message was removed from other mailboxes before anyone else opened it.

YOUR ENTRY

PART 5 OF 8

What belongs in the minutes, and what belongs in the appendix

Minutes record what the board considered and decided. Detail that supports those decisions, or that would help an attacker, belongs in an appendix or in management's own records with appropriate circulation. Your company secretary or legal counsel may have firmer views for your organisation, and theirs should prevail.

WHERE SECURITY AND INCIDENT DETAIL USUALLY SITS IN BOARD PAPERS

ITEM	IN THE MINUTES	IN THE APPENDIX OR MANAGEMENT RECORDS
Decisions, including risk acceptances and funding	The decision, who made it, and any conditions attached.	The supporting analysis and the options considered.
Incident summary	A short factual statement, and any decision the board took.	Timeline, technical detail and investigation notes.

ITEM	IN THE MINUTES	IN THE APPENDIX OR MANAGEMENT RECORDS
Notification decisions	That the question was considered, on advice, and the outcome.	The advice itself, handled as legal counsel directs.
Actions assigned to management	Owner and due date.	The detailed action plan.
System names, vulnerability detail, technical indicators	Not included.	Only where needed, with restricted circulation.
Near-misses	Only if the board discussed or decided something.	One-line summaries.

PART 6 OF 8

Cost and next-period needs

Every security update is followed by a question about money. Answer it before it is asked: what the programme cost, what that bought in terms the board already recognises, what is committed, and what the next period needs and why.

Spend this period against budget

A few categories that match how your finance team reports — people, external services, software, one-off remediation — against the approved budget, with a line on any variance.

EXAMPLE

Spend was within the approved security budget. One-off remediation came in above plan because the backup redesign was brought forward; this was offset by deferring the awareness platform renewal.

YOUR ENTRY

What the spend achieved

Link spend to outcomes the board has already heard about: a risk reduced, a gap closed, a customer or insurance requirement met. Do not list tools bought.

EXAMPLE

The backup redesign closed the offline copy gap disclosed in last year’s insurance application, and is the main reason the ransomware recovery risk is expected to fall from High once the restore test is complete.

YOUR ENTRY

Committed costs for the next period

Renewals and contracts already in place — including the cyber insurance premium once your broker has advised it — so the board sees the baseline before any new request.

EXAMPLE

Endpoint detection and managed monitoring contracts renew in January. The insurance renewal quote is expected from our broker in November.

YOUR ENTRY

Requests for the next period

Each request with the risk or requirement it addresses, the cost, the alternative considered, and what happens if it is declined. Where declining is a genuine option, say so; the board may reasonably choose to accept the risk instead.

EXAMPLE

Replace the unsupported scheduling server next year. This addresses the risk proposed for acceptance today; if the request is declined, the acceptance would need to be extended and revisited at each review date.

YOUR ENTRY

PART 7 OF 8

What to leave out

- Raw vulnerability counts, alert volumes and blocked-attack totals. They are large, they move for reasons unrelated to risk, and a board cannot act on them. Report what they mean instead.
- Tool names and vendor logos. A board needs to know that a control is in place and working, not which product provides it.
- Any figure you cannot trace back to a record. When a director asks where a number came from and the answer is an estimate, the rest of the report loses credibility with it.
- Heat maps without treatment decisions. Colour without a decision invites discussion without an outcome.
- General threat briefings and news about attacks elsewhere, unless they change a decision you are asking for.
- Framework jargon and control reference numbers. Translate them into what the control protects.
- System names, network detail and anything else that would help an attacker if the papers travelled further than intended.
- Promises about outcomes you do not control, such as a certification result, an audit opinion or an insurance premium.

PART 8 OF 8

Before you send it

01	**Every figure traces to a named record.**	Someone will eventually ask where a number came from. The report survives that question only if the answer is immediate.
02	**Every decision request has options, a recommendation and a date.**	Without options, a request for a decision is really a request for approval, and boards notice the difference.
03	**Every risk and action has a named owner, not a team.**	A team cannot be asked for an update at the next meeting. A person can.
04	**The structure matches the previous report.**	Movement is only visible when the same sections appear in the same order each time.
05	**Anything that got worse is stated on page one.**	A decline a director discovers in the appendix costs more trust than the decline itself.
06	**Incident wording has been reviewed by legal counsel where it needs to be.**	Board papers are records. Wording about causes, fault or notification should never be improvised.
07	**Circulation and confidentiality are marked.**	Security detail should reach only the people who need it, and the appendix may warrant tighter circulation than the summary.

CYBERWAVE SENTINEL

Where Sentinel fits

Sentinel's executive and board reporting, part of the Full Platform plan, produces a page from the register your team already maintains: the readiness position, movement since the last snapshot, critical risks with their treatment and owner, decisions outstanding, overdue actions and the evidence position. The Essentials plan includes the Sentinel Score and an executive summary.

The narrative can be drafted with AI assistance, within your plan's monthly allowance, and the person presenting edits and owns it. The report reflects only what is recorded in your workspace, so anything recorded elsewhere — budget figures, for example — comes from your own records, and legal review of incident wording remains your call.

See executive and board reporting →

Limitations

WHAT THIS TEMPLATE IS NOT

This template is a general structure for reporting cybersecurity to a board. It is not legal advice, and it does not set out the duties of directors or the reporting and notification obligations that may apply to your organisation, sector or jurisdiction. Take advice from legal counsel on those, and on the wording of any incident or notification matter.

Fernhill Fabrication Ltd. and every name, date and figure attached to it are fictional. A report built from this template reflects your own records and judgement; CyberWave does not verify its contents, and a readiness position described in it is not a certification, an audit opinion or an insurance outcome.

Related

Executive and board reporting →

Risk management in Sentinel →

Managed vCISO →

Governance and compliance →

All checklists and templates →