ABOUT THIS SAMPLE · A quarterly security briefing in the format I write them and expect them written. Sanitised from real practice: the company is fictionalised, the numbers are illustrative, the structure and standard of candour are exactly what a board should demand. Note what it does: separates knowledge from faith, states what we don't know, and ends with decisions — because a paper with no decisions is a newsletter.

Q2 · BOARD UPDATE · SECURITY OPERATIONS

Where we are, what changed, and the two decisions I need.

Headline

We are in better shape than at the end of Q1. Detection coverage is up materially, the new on-call rota is bedding in, and we closed two of the three Q1 risk items. One item — the third-party identity surface — has got **worse, not better**, and that is where the decisions I need from this board sit.

Where we are

Detection coverage on the production estate is at **94%** of the agreed control set, up from 81% at the Q1 briefing. The remaining 6% is the legacy authentication path we are decommissioning in August; we have chosen not to instrument code we are about to delete, and I would rather spend those engineering hours on the migration.

On-call has run on the new rota for eight weeks. Mean time to acknowledge is **4m 12s**; mean time to first useful action **11m** — both improved from Q1 (8m / 19m). Nobody carries the pager more than one weekend in three.

Fourteen alerts paged a human this quarter. Two were genuine (one minor, one moderate; neither customer-affecting). Twelve were false positives from a single noisy detection rule, tuned mid-June. Post-mortems on both real incidents are appended.

What changed since Q1

- The last shared credential on production was retired in April. All access is now key-only, MFA on the jump host, no exceptions.
- The customer-facing API now sits behind a proxy that drops anything not matching seven known URL shapes. Bot traffic to the origin is down 92%.
- A second incident responder started in May; she has already run two of the last three response exercises.
- We failed a customer's supplier-security questionnaire on a point I disagreed with. It is resolved; the lesson is recorded, not buried.

What I'm watching

- Our federated SSO provider had a 47-minute degraded-mode incident in May. No customer impact — but it surfaced that our manual fallback was documented nowhere. It is drafted now; it has not been drilled.
- New regulatory reporting obligations land in October. We are operationally ready; we are not yet *documentationally* ready, and that gap is mostly mine to close.
- The senior-responder talent market has not slowed. I believe we pay within band; I would like the remuneration committee's sense-check rather than my own assumption.

What we don't know

- Whether the noisy detection rule we tuned was masking real signal. The previous version is running in parallel for thirty days; the answer will be in the next briefing, not this one.
- The blast radius if an attacker phishes our managed-services partner. We asked; their answer was longer than I expected and shorter than I would have liked.
- Whether backup restoration works end-to-end at production scale. Staging-scale: proven. The production drill is scheduled for next month — until it runs, our recovery time is a belief, not a fact.

Risk register — top three

#	RISK	CURRENT TREATMENT	RESIDUAL
1	**Third-party identity dependency.** An SSO degradation over two hours locks customers out of the portal.	Manual fallback documented, *not yet drilled*. Decision requested below.	`moderate`
2	**Senior responder retention.** Losing one of two seniors pushes resolution times from acceptable to uncomfortable.	Market-rate review; rota change reducing burnout.	`moderate`
3	**Regulatory documentation gap.** Operationally compliant ahead of the deadline; evidence trail incomplete.	Focused external-counsel engagement through the summer.	`low, shrinking`

Recommendations

#	RECOMMENDATION	OWNER	OUTCOME
1	Drill the SSO fallback within four weeks.	`head of platform`	A tested runbook and a known answer to "how long does it take".
2	Authorise the responder retention review.	`CEO + RemCo`	Market benchmark for both seniors; the bonus-vs-base question answered for next year.

Decisions I need from this board

- **The SSO fallback drill** (recommendation 1): approve in principle, or push back. I think approve — the cost is a day of engineering across four people.
- **A ring-fenced contingency line** for an emergency third-party incident-response engagement if a major exceeds internal capacity. We have not spent the equivalent in any of the last three years; I would still like to know it is there.

Next briefing

At the next quarterly meeting, in person. If anything material happens before then — a real incident, a regulatory development, a senior departure — an interim update follows by email within two working days.

Document control · SAMPLE — sanitised for publication
Format & standard · Peter Bassill · peterbassill.com/work/non-executive-director
What to notice · knowledge separated from faith · unknowns stated without embarrassment · risks owned, not admired · decisions requested, with the author's own recommendation attached