Good Security

TEMPLATE WATERMARKED PDF

WORKING TEMPLATE

Board Security Reporting Template

A structured quarterly cybersecurity report template for NZ boards and executive leadership — covering security scorecard, key metrics, incidents, compliance status, risk register, roadmap, and budget.

Branded customer-ready document | Shareable with leadership teams | Generated 12 Mar 2026

[ORGANISATION NAME]

Good Security · goodsecurity.co.nz · **hello@goodsecurity.co.nz**

> **How to use this template** Complete the sections marked [IN SQUARE BRACKETS] before each board meeting. This report is designed to be concise — boards need the right information, not all the information. Aim for 2–3 pages maximum when completed. Tailor the RAG (Red/Amber/Green) ratings to your organisation's risk appetite. Remove this instruction box before distributing.

Period: [QUARTER / YEAR — e.g., Q2 2026] **Prepared by:** [NAME, TITLE] **Date:** [DATE]

EXECUTIVE SUMMARY

[Write 2–3 sentences summarising the overall security position this period. What is the headline message the board needs to hear? Be direct.

Example: Our overall security position remains stable. Multi-factor authentication across all staff accounts was completed this quarter, significantly reducing our exposure to account compromise. One medium-severity phishing incident occurred and was contained without data loss.]

Overall security position: 🟢 Strong / 🟡 Improving / 🟠 Requires attention / 🔴 Critical

SECTION 1: SECURITY SCORECARD

Rate each domain as Green (controls in place and effective), Amber (partially addressed or improvement in progress), or Red (significant gap requiring board awareness or action).

DOMAIN	STATUS	KEY POINTS
Identity & access management	🟢 / 🟡 / 🔴	[e.g., MFA enforced for all staff]
Endpoint security	🟢 / 🟡 / 🔴	[e.g., EDR deployed on all managed devices]
Email & phishing protection	🟢 / 🟡 / 🔴	[e.g., DMARC configured; staff training due Q3]
Data protection & backup	🟢 / 🟡 / 🔴	[e.g., Daily backups; last restore test [DATE]]
Vulnerability & patch management	🟢 / 🟡 / 🔴	[e.g., Critical patches applied within 30 days]
Security awareness & training	🟢 / 🟡 / 🔴	[e.g., Annual training completed [DATE]; [X]% staff]
Incident response readiness	🟢 / 🟡 / 🔴	[e.g., Plan documented; not yet tested]
Privacy & compliance	🟢 / 🟡 / 🔴	[e.g., IPP 3A assessment underway; due [DATE]]
Vendor & third-party risk	🟢 / 🟡 / 🔴	[e.g., Top 5 vendors assessed; 2 outstanding]

SECTION 2: KEY METRICS

METRIC	THIS PERIOD	PREVIOUS PERIOD	TREND
Security incidents reported	[NUMBER]	[NUMBER]	↑ / ↓ / →
Phishing simulations sent	[NUMBER]	[NUMBER]	—
Phishing click rate	[%]	[%]	↑ / ↓ / →
Critical vulnerabilities open	[NUMBER]	[NUMBER]	↑ / ↓ / →
Staff completed security training	[%]	[%]	↑ / ↓ / →
Days since last backup restore test	[NUMBER]	[NUMBER]	—
Open high/critical risks on register	[NUMBER]	[NUMBER]	↑ / ↓ / →

Note: An upward trend in incidents reported is often positive — it indicates improved detection and reporting culture, not necessarily increased exposure.

SECTION 3: INCIDENTS & EVENTS THIS PERIOD

Incidents requiring board awareness

[If no significant incidents: "No incidents requiring board-level attention occurred this period."]

[For each significant incident, use the following format:]

Incident [NUMBER]: [BRIEF TITLE]

FIELD	DETAIL
Date	[DATE]
Severity	🔴 Critical / 🟠 High / 🟡 Medium / 🟢 Low
Description	[1–2 sentences: what happened]
Impact	[Data affected? Systems affected? Operational impact?]
Containment	[How was it contained and how quickly?]
Notification obligations	[Was the Privacy Commissioner notified? Were individuals notified?]
Root cause	[Brief description]
Corrective action	[What is being done to prevent recurrence?]
Status	Resolved / Ongoing

Near misses and trends

[Describe notable near misses, patterns in phishing attempts, or threat intelligence relevant to your sector.

Example: We observed a 30% increase in phishing emails targeting finance staff in [MONTH], consistent with a BEC campaign targeting NZ professional services firms reported by CERT NZ.]

SECTION 4: COMPLIANCE STATUS

OBLIGATION	STATUS	NEXT ACTION	DUE DATE
Privacy Act 2020 — IPP 3A	🟢 / 🟡 / 🔴	[Action required]	[DATE]
Cyber insurance renewal	🟢 / 🟡 / 🔴	[Action required]	[DATE]
ISO 27001 / NZISM / other	🟢 / 🟡 / 🔴	[Action required]	[DATE]
Annual staff security training	🟢 / 🟡 / 🔴	[Action required]	[DATE]
Incident response plan review	🟢 / 🟡 / 🔴	[Action required]	[DATE]
Vendor risk reviews	🟢 / 🟡 / 🔴	[Action required]	[DATE]

IPP 3A note: Information Privacy Principle 3A (effective May 2026) requires organisations to notify individuals when personal information is collected indirectly from third parties. [STATE YOUR

ORGANISATION'S CURRENT READINESS.] Note: Cross-border disclosure obligations (IPP 12) are already in force — ensure overseas data flow assessments are current.

SECTION 5: RISK REGISTER SUMMARY

The following are the highest-rated items currently on the security risk register.

RISK	LIKELIHOOD	IMPACT	RATING	TREATMENT STATUS
[e.g., Ransomware attack]	Medium	High	🔴 High	[Controls in place / treatment underway]
[e.g., Business Email Compromise]	High	Medium	🟠 Elevated	[MFA deployed; BEC training scheduled]
[e.g., Data breach via third party]	Low	High	🟡 Medium	[Top vendors reviewed; monitoring ongoing]
[e.g., Staff phishing susceptibility]	Medium	Medium	🟡 Medium	[Annual training; phishing simulations]
[e.g., Outdated software]	Medium	High	🟡 Medium	[Patching schedule implemented]

Rating guide: 🔴 High — immediate action required | 🟠 Elevated — active treatment | 🟡 Medium — monitored | 🟢 Low — accepted or controlled

---

SECTION 6: PROGRESS AGAINST SECURITY ROADMAP

INITIATIVE	STATUS	NOTES
[e.g., MFA rollout]	✅ Complete	Completed [DATE]
[e.g., Staff phishing simulations]	⚠️ In progress	[X] of [Y] campaigns completed
[e.g., Incident response plan testing]	□ Planned	Scheduled for [DATE]
[e.g., IPP 3A data inventory]	⚠️ In progress	Expected completion [DATE]
[e.g., Vendor risk assessment]	□ Planned	Starting [DATE]

SECTION 7: BUDGET & RESOURCES

ITEM	BUDGET	ACTUAL / FORECAST	VARIANCE	NOTES
Security tools & software	$[X]	$[X]	+/- $[X]	[Notes]
Training & awareness	$[X]	$[X]	+/- $[X]	[Notes]
Virtual CISO / advisory	$[X]	$[X]	+/- $[X]	[Notes]
Incident response (if applicable)	$[X]	$[X]	+/- $[X]	[Notes]
Total	**$[X]**	**$[X]**	**+/- $[X]**	

SECTION 8: RECOMMENDATIONS REQUIRING BOARD DECISION

[List items that require board-level decision, approval, or resource allocation. Keep this section short and action-oriented. If no board decisions are required: "No board decisions are required this period."]

Recommendation [NUMBER]: [TITLE]

- **Context:** [Brief background — why this matters]
- **Recommendation:** [Specific action being requested from the board]
- **Cost / resource:** [Estimated cost or resource requirement]
- **Risk if not actioned:** [What is the risk of inaction?]
- **Decision required by:** [DATE]

SECTION 9: NEXT QUARTER PRIORITIES

1. [Priority 1 — e.g., Complete IPP 3A indirect collection source audit and IPP 12 overseas data flow assessment]
2. [Priority 2 — e.g., Conduct incident response tabletop exercise]
3. [Priority 3 — e.g., Complete annual staff security awareness training]
4. [Priority 4 — e.g., Review and update top 3 vendor risk assessments]

APPENDIX: GLOSSARY

BEC (Business Email Compromise): Fraud where attackers impersonate executives or suppliers via email to redirect payments or extract sensitive information.

DDoS (Distributed Denial of Service): An attack that overwhelms a system with traffic to make it unavailable to legitimate users.

EDR (Endpoint Detection and Response): Business-grade security software that monitors and responds to threats on computers and devices, beyond basic antivirus.

IPP 3A: Information Privacy Principle 3A under the NZ Privacy Act 2020, requiring notification when personal information is collected indirectly from third parties. Takes effect May 2026. Cross-border disclosure is covered by IPP 12 (already in force).

MFA (Multi-Factor Authentication): Requiring more than just a password to log in — typically a time-based code from an authenticator app. Eliminates the majority of account compromise attacks.

Phishing: Fraudulent emails designed to trick staff into revealing credentials, making payments, or installing malware.

RAG status: Red / Amber / Green — a traffic light system for indicating risk or progress status.

Ransomware: Malware that encrypts an organisation's files and demands payment for the decryption key.

RTO (Recovery Time Objective): The maximum tolerable time to restore systems after an incident.

SOC 2: A US-based security compliance framework for cloud service providers, used as evidence of security controls during vendor assessment.