

GOOD SECURITY

Board Security Pack

Executive posture, top risks, compliance view, and the decisions leadership needs to take next.

CLIENT Kiwi Manufacturing Ltd	QUARTER Q1 2026	PREPARED 01 March 2026
OVERALL SCORE 74/100	TOP RISKS 3	BOARD ACTIONS 3

LEADERSHIP SUMMARY

Kiwi Manufacturing Ltd's security posture improved to 74/100 in Q1 2026, up 3.5 points from Q4 2025. This reflects strong progress on identity management (MFA rollout) and endpoint protection (EDR deployment). However, two critical weaknesses remain: OT network segmentation and the legacy ERP system. The board should note that the OT segmentation gap represents the highest risk to operations. A successful attack on the SCADA network could halt production. The remediation project is scoped at \$45,000 NZD and should be prioritised for Q2 execution.

Strategic posture / board lens

This board pack is structured to support leadership decisions, not just restate technical posture. It combines the current security score, the most material operational risks, compliance pressure, and the investment requests needed to keep the programme credible under customer and insurer scrutiny.

Domain scorecard

Domain	Score	Status	Trend
Governance	80	Green	Stable
Identity & Access	72	Amber	Up
Endpoint Protection	78	Amber	Up
Network Security	55	Red	Down
Data Protection	65	Amber	Stable
Vendor Risk Mgmt	70	Amber	Up
Incident Response	60	Amber	Stable
Backup & Recovery	75	Amber	Up
Security Awareness	82	Green	Up
Cloud Security	68	Amber	Stable
Email Security	45	Red	Down

Board-ready narrative

- MFA Rollout Complete: IAM domain +14pts
- EDR Deployment: Endpoint domain +8pts
- Security Awareness Training: Awareness domain +12pts

Top risks and business impact

Risk	Severity	Current status	Business impact / treatment
OT Network Segmentation Gap	Critical	SCADA systems share network segment with corporate IT	Network redesign scoped, vendor engaged
Unpatched Legacy ERP	High	SAP R/3 running unsupported version	Migration to S/4HANA approved for Q3
No Offsite Backup	High	All backups on-premises only	Azure Backup POC underway

Incident / resilience update

Area	Resilience update
Operational resilience	No material outage has escalated to the board this quarter, but OT segmentation and legacy ERP risk continue to define the resilience agenda.
Incident readiness	Response workflows exist, but the next exercise cycle is needed to prove leadership decision-making and supplier escalation paths under pressure.

Compliance / assurance view

Framework	Coverage	Assessed	Compliant
NZISM	91%	114	104
ISO 27001:2022	84%	93	78

Investment / resource asks

Investment / resource ask	Why now	Decision needed
Fund OT network segmentation	The OT segmentation gap remains the highest operational and ransomware exposure in the environment.	Approve Q2 capital uplift
Approve privileged-access uplift	Named admin control is still weaker than the standard expected by enterprise customers and insurers.	Approve implementation in current planning cycle

Decisions requested

Decision requested	Reason	Next action
Approve the OT network segmentation project in Q2.	Required to reduce current residual exposure or maintain reporting cadence.	Lock OT segmentation scope and delivery owner
Fund the privileged-access uplift before the next customer audit cycle.	Required to reduce current residual exposure or maintain reporting cadence.	Close privileged-access design and procurement decision
Keep quarterly board reporting on the standing governance agenda.	Required to reduce current residual exposure or maintain reporting cadence.	Keep board-level security review on the standing agenda

Next actions and next-quarter priorities

Next action	Owner	Target quarter
Lock OT segmentation scope and delivery owner	Operations + IT leadership	Q2 2026
Close privileged-access design and procurement decision	Leadership team	Q2 2026
Keep board-level security review on the standing agenda	Executive team	Q3 2026