Case Study:

Cyber Risk Management at Not for Profit (NDIS, Homeless Services)

Offer a wide array of community support services. While their core services include food, housing, clothing, and emergency relief, they also provide key programs for family and parent support as well as mental health and youth programs. These initiatives are designed to help individuals and families stabilize their lives during crises and to strengthen their overall wellbeing, ensuring that every person has the support to thrive

---

Timeframe: 2019–2020
Role: Chief Information Officer (Rodney Ingram)
Focus Area: Cyber Risk Assessment & Governance Uplift

Client

Not for Profit

Challenge

Our Client were operating with fragmented cyber risk governance and legacy IT systems, exposing the organisation to increasing cybersecurity threats. There was no formal cyber risk management framework, and limited visibility into the alignment between technology operations and the broader risk posture. The organisation required strategic leadership to assess and address cyber vulnerabilities and implement an effective governance structure to manage risk long-term.

Our Approach

Under the leadership of CIO Rodney Ingram, the organisation embarked on a structured uplift of its cybersecurity framework and governance model:

- Assessment of Technology Alignment with current and emerging cyber risks, identifying critical areas of exposure.
- Established Governance Structures, including drafting the Terms of Reference for a National Cyber Risk Committee, to unify and streamline oversight.
- Developed a Cyber Risk Management Plan to guide strategic and operational risk decisions.
- Implemented Essential Eight-aligned protocols, including new policies, procedures, and systems to meet ACSC guidelines.
- Initiated Mitigation Plans for identified risks and improved controls across identity, infrastructure, and access management.
- Acted as a liaison with the Australian Cyber Security Centre (ACSC) as a Business Partner, enabling real-time incident response and early warning mechanisms.
- Delivered strategic cyber risk advisory to senior executives and the board, embedding cybersecurity into the organisation's leadership agenda.
- Successfully planned and executed a disaster recovery (DR) strategy, ensuring continuity in the event of a cyber incident or major disruption.

The Outcome

- Introduced national-level governance structures to coordinate cyber risk across their footprint.
- Achieved initial maturity in the Essential Eight framework, significantly enhancing the organisation's security posture.
- Developed a repeatable and scalable Cyber Risk Management Plan tailored for non-profit governance contexts.
- Improved executive and board-level awareness and engagement with cyber and strategic risks.
- Implemented a tested disaster recovery framework, strengthening resilience across IT infrastructure.

Impact Summary

This project marked a fundamental shift in how the Not for Profit (NDIS, Homeless Services) approached cyber risk: from fragmented, reactive measures to a strategic, governance-led model. With a foundation now in place, the organisation is positioned to scale its cybersecurity maturity across other regions and functions, maintaining trust with stakeholders and protecting sensitive community data.

501 Dandenong Road
Armadale, VIC. 3143
+61 3 9507 2052
info@powerdatagroup.com.au