CASE STUDY

How TARDISS Built a Stronger, Safer Cyber Security Foundation

About TARDISS Support Services

TARDISS (Townsville and Regional Disability Individualised Support Service Inc.) is a community-based, NDIS-registered, not-for-profit organisation delivering participant-first disability support across North Queensland (Townsville and Charters Towers). Operating in a high-compliance environment with sensitive medical and personal data, TARDISS needed to uplift its security baseline, reduce people-driven risk, and demonstrate due diligence under NDIS and Privacy Act expectations.

ADITS, which is TARDISS' long-standing technology partner, recommended CyberShield, an all-in-one cyber security program built around SMB1001:2025 Silver controls, continuous monitoring, governance, and staff enablement.

Operating in a high-compliance environment with sensitive medical data, TARDISS needed to uplift its security baseline and demonstrate due diligence.

THE CHALLENGE

Building a Defensible Cyber Security Baseline

Establish a clear, defensible cyber security baseline that:

- Strengthens identity, access, and password practices
- Reduces user-driven risk through continual training and visibility
- Empowers staff to become the first line of defence through ongoing cyber security education and awareness
- Introduces 24/7 monitoring and best-practice controls to mitigate ransomware and phishing; and
- Aligns with SMB1001 Silver to evidence “reasonable steps” and support Privacy Act/NDIS obligations.

THE SOLUTION

Transforming Process & Technology for Cyber Resilience

ADITS' CyberShield solution was implemented as a structured uplift across people, process, and technology.

CyberShield includes mandatory and **regular cyber awareness training** via a Human Risk Management platform to ensure staff are equipped with the knowledge to identify cyber threats.

TECHNOLOGY SAFEGUARDS & MONITORING

Deployment and hardening of core security layers (AV/EDR, firewall), policy-driven patching and updates, and 24/7 threat monitoring & maintenance to detect and respond early, which minimised downtime and exposure.

CYBER SECURITY AWARENESS & TRAINING PROGRAM

A dedicated cyber security awareness and training program was introduced to help staff recognise threats and reduce human-error risk. This was supported by a Human Resources Management (HRM) system for training and compliance tracking.

IDENTITY, ACCESS & PASSWORD MANAGEMENT

Tightened access management and standardised secure password management so staff have strong, unique credentials without admin overhead.

BACKUP, RECOVERY & BREACH READINESS

Reliable backup and recovery practices were reinforced, and OAIC breach notification procedures established so TARDISS can act quickly and compliantly if an incident occurs.

POLICIES, PROCESSES & STAFF CAPABILITY

Clear policies and plans were adopted, while cyber awareness training and HR-linked compliance tracking helped reduce human-error risk and maintain visibility of training completion.

ALIGNED TO SMB1001 SILVER

The uplift followed SMB1001:2025 Silver, which is a practical, multi-tier standard for SMBs that aligns with broader frameworks and is designed for achievable, staged maturity gains.

THE RESULTS

A Safer, Smarter, More Defensible Organisation

A Verified Baseline that Reduces Risk

TARDISS achieved a Silver-level security posture with stronger controls across devices, identities, and data, which significantly lowered exposure to common threats (phishing, ransomware) and improving operational resilience.

Less Friction; More Confidence

Standardised access and password practices reduced admin burden and user frustration, while 24/7 monitoring and documented procedures increased confidence across leadership and frontline teams.

Governance & Defensibility

With SMB1001 Silver alignment and evidence of controls, TARDISS can demonstrate “reasonable steps” to clients, regulators, and insurers. Supporting ongoing NDIS registration and Privacy Act expectations.

Human-Risk Reduction through Training

Ongoing cyber awareness training and compliance tracking improved completion rates and helped build a culture of security, addressing the biggest attack vector: human error.

Proactive Protection that Reduces Risk

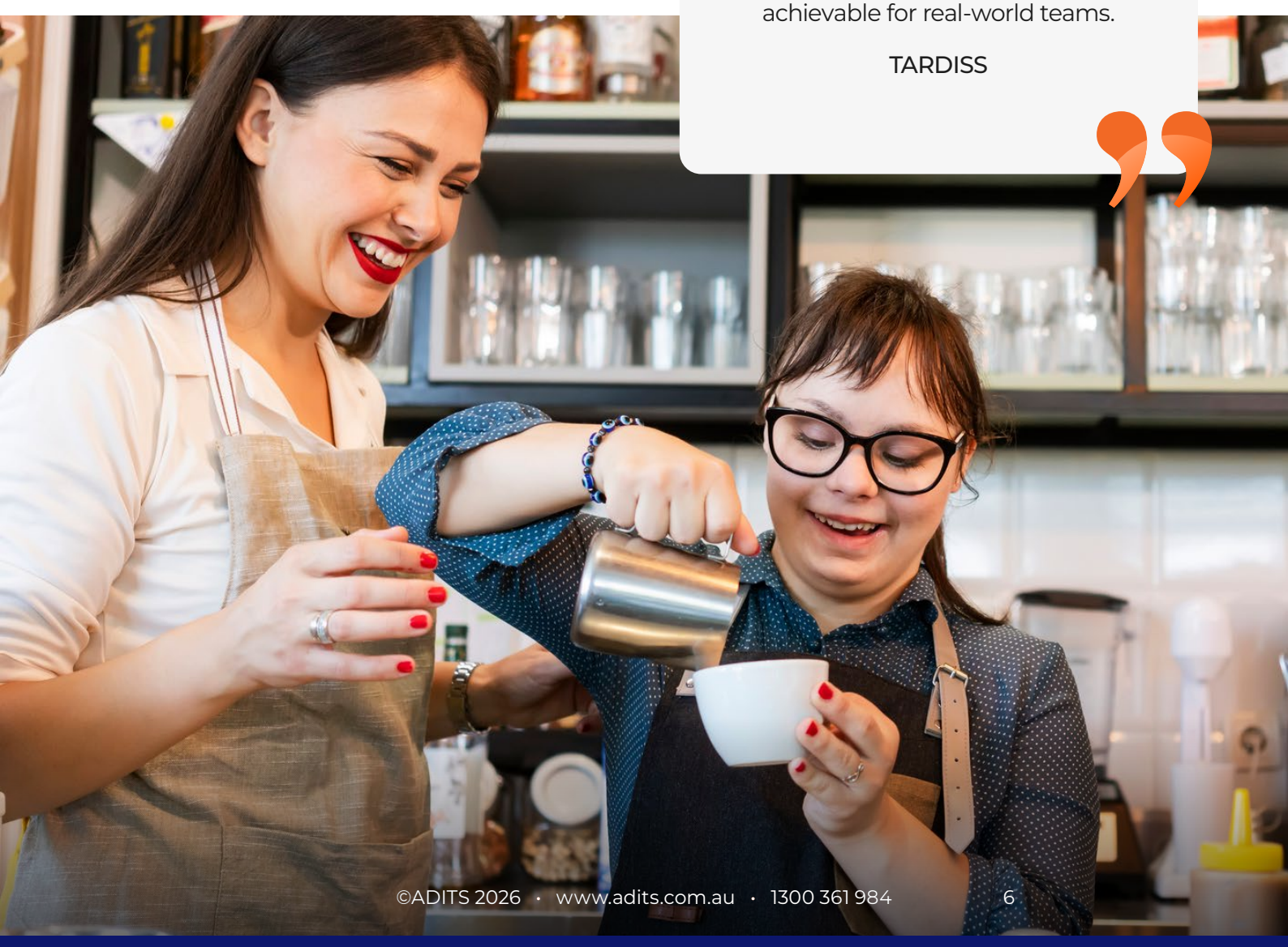
With a Silver-level security posture and strengthened controls across devices, identities, and data, TARDISS now benefits from proactive protection against common threats like phishing and ransomware, improving resilience across the organisation.

LOOKING AHEAD

What's Next in TARDISS' Cyber Maturity Journey?

ADITS will continue supporting TARDISS by embedding a cyber security solution that integrates seamlessly into daily operations. This includes ongoing risk-based reviews, regular staff training, and uplift pathways aligned to the SMB1001 framework as the organisation's needs evolve.

> Don't wait for a breach to validate investment. For organisations handling sensitive data and operating under strict safeguards, start with a structured baseline that blends people, process, and technology, and choose a framework, like SMB1001 Silver, that's practical, certifiable, and achievable for real-world teams.
>
> TARDISS



Protect Sensitive Data with a Framework Built for NFPs

Find out more about CyberShield

Experience all-around protection and transform your business today.

TALK TO OUR FRIENDLY TEAM

1300 361 984
enquiries@adits.com.au
adits.com.au

ADITS