

Borderless CS

CYBER SAFE TOGETHER

CARPENTERS FIJI PTE LIMITED

Vulnerability Assessment and Penetration Testing (VAPT)

Customer success story

CLIENT: CARPENTERS FIJI

CLIENT WEBSITE: <https://www.carpenters.com.fj/>

SERVICE: VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)



Penetration
Testing



Customer Success Story

Carpenters Fiji Pte Limited Strengthens Cyber Resilience with Borderless CS Through Comprehensive Vulnerability Assessment & Penetration Testing (VAPT)

Website: <https://www.carpenters.com.fj/>

Overview

Carpenters Fiji Pte Limited is one of Fiji's largest and most diversified commercial groups, operating across wholesale and retail, hardware and automotive, IT services, finance, logistics, shipping, and industrial engineering.

Given the organisation's scale and reliance on interconnected systems across multiple business units, Carpenters Fiji recognised the need to proactively strengthen its cybersecurity posture against modern cyber threats targeting enterprise networks in the Pacific.

Borderless CS was engaged to deliver a **comprehensive Vulnerability Assessment and Penetration Testing (VAPT)** exercise across Carpenters Fiji's public-facing infrastructure, VPN systems, mail servers, DNS, and associated network services. The engagement was designed to identify vulnerabilities, simulate real-world attacks, and provide an actionable roadmap for reducing security exposure across critical assets.

VAPT Engagement Objectives

Borderless CS was commissioned to:

1. **Identify vulnerabilities across external-facing infrastructure**, including IP ranges, servers, and services.
2. **Simulate real-world cyberattacks** using black-box penetration testing techniques.
3. **Evaluate mail, VPN, and web application security** against industry best practices and OWASP standards.



4. **Provide a risk-prioritised remediation plan** aligned with CVSSv3 scoring and enterprise security benchmarks.
5. **Reduce attack surface and improve resilience** across Carpenters Fiji's distributed business units.

Scope of Work:**1. External Infrastructure Assessment (/29 Subnet)**

Borderless CS assessed the entire **/29 public subnet (6 external IPs)**, including primary and auxiliary services:

Coverage included:

- Port & service enumeration
- Banner analysis & service fingerprinting
- Firewall and exposure testing
- Configuration and patch-level evaluation
- Vulnerability scanning and manual exploitation

2. VPN Portal Security Testing

Testing of one VPN portal included assessment of:

- Protocol weaknesses
- Encryption and certificate issues
- Brute-force protections
- Authentication resilience
- Error-handling and session controls

This validated the security of remote workforce connectivity across Carpenters Fiji's business units.



3. Mail Server Security (2 Servers)

Assessment included:

- Open relay testing
- Spoofing and impersonation resilience
- SPF, DKIM, DMARC policy verification
- Mail service configurations
- TLS and port security

4. Web Application Penetration Testing

Testing aligned with **OWASP Top 10**, including:

- SQL Injection, XSS, CSRF
- Broken authentication and session flaws
- Logic and workflow abuse
- Access control weaknesses
- Server and API misconfigurations

5. TLS/SSL Hardening Assessment

Borderless CS evaluated:

- Certificate validity and chain issues
- Weak cipher suites
- Protocol support (SSLv3/TLS1.0/TLS1.1)
- HSTS, secure renegotiation, forward secrecy

6. DNS & Network-Layer Analysis

Review included:

- DNS configuration integrity
- Exposure of internal records
- Zone transfer validation
- Misconfigurations and stale entries
- Firewall rule baseline analysis



7. OSINT & Dark Web Intelligence Scan

Borderless CS conducted threat intelligence analysis for:

- Credential leaks
- Compromised email accounts
- Exposed server metadata
- Publicly available sensitive information
- External threat actors referencing the organisation

8. Detailed Reporting & Free Retest

Deliverables included:

- Full vulnerability report with **CVSSv3 scoring**
- Reproduction steps and screenshots
- Impact analysis and business risk rating
- Prioritised remediation roadmap
- **One complimentary retest** after patching to confirm fixes

Key Outcomes:

1. Critical Vulnerabilities Identified & Resolved

Borderless CS uncovered exploitable weaknesses, enabling Carpenters Fiji to reduce high-risk exposure across its infrastructure.

2. Strengthened VPN, Mail & Web Security

Improvements were made to authentication, certificate handling, email security policies, and web application controls.

3. Hardened External Attack Surface

Firewall rules, TLS configurations, DNS security, and endpoint exposure were significantly improved.



4. Enhanced Threat Visibility

OSINT and dark web findings allowed Carpenters Fiji to proactively address potential compromises.

5. Improved Cybersecurity Governance & Readiness

Comprehensive documentation and remediation planning supported long-term cyber maturity across the group.

Conclusion:

Partnering with **Borderless CS** enabled **Carpenters Fiji Pte Limited** to significantly uplift its cybersecurity resilience across its public-facing infrastructure and mission-critical services.

The VAPT engagement provided deep visibility into security gaps, strengthened defences against real-world cyber threats, and empowered Carpenters Fiji to protect its diversified business units spanning retail, automotive, marine engineering, IT, and financial services.

Carpenters Fiji is now better positioned to safeguard its customers, employees, and business operations while continuing to deliver trusted services across Fiji.