

# Borderless CS

CYBER SAFE TOGETHER



**FIJI**

Vulnerability Assessment and Penetration Testing (VAPT)

Customer success story

CLIENT: LICI - FIJI

CLIENT WEBSITE: <https://licifiji.com/>

SERVICE: VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)



**Penetration  
Testing**



## Customer Success Story

### LICI Fiji Strengthens Cybersecurity Resilience with Borderless CS Through Comprehensive Vulnerability Assessment & Penetration Testing (VAPT)

**Industry:** Insurance

**Website:** <https://licifiji.com/>

#### Overview

LICI Fiji, one of Fiji's most trusted life insurance providers, delivers critical insurance services to thousands of customers across the nation. With a growing digital footprint and increasing dependency on distributed infrastructure across four locations, LICI Fiji recognised the importance of proactively securing its technology environment to protect sensitive financial and customer data.

To strengthen its security posture, LICI Fiji engaged **Borderless CS** to perform a full **Vulnerability Assessment and Penetration Testing (VAPT)** engagement. This included a deep technical assessment of production systems, disaster recovery infrastructure, and all workstation endpoints across the organisation.

The outcome provided LICI Fiji with clear visibility of its cybersecurity risks, validated real-world attack vectors, and delivered a structured roadmap to uplift security resilience across the business.



## Engagement Objectives

Borderless CS was commissioned to:

1. **Identify vulnerabilities** across servers, endpoints, and supporting infrastructure.
2. **Simulate real-world cyberattacks** to validate exploitability and risk impact.
3. **Assess security posture** across distributed environments and business-critical systems.
4. **Provide an actionable remediation plan** to reduce risk and improve long-term cybersecurity maturity.

## Scope of Work

Two critical virtualised data centre servers were assessed:

- **Production Server (Linux OS, hosted in VM)**
- **Disaster Recovery (DR) Server (Linux OS, hosted in VM)**

## Testing covered:

- Server misconfiguration analysis
- OS hardening and patch levels
- Privilege escalation paths
- Network exposure and service enumeration
- Authentication and access control controls
- File system and configuration security
- Backup and DR environment resilience

## Endpoints Across Four Locations (Total: 44 Workstations)

Borderless CS performed vulnerability scanning and targeted testing of **44 Windows workstations** across four LICI Fiji branches.

### Testing included:

- Missing patches & outdated software
- Endpoint protection effectiveness
- Local privilege escalation
- Password policy validation
- Misconfiguration and insecure services
- Network segmentation and workstation isolation
- User permission hygiene and domain control

### Key Outcomes:

#### 1. Clear Visibility into Critical Vulnerabilities

Multiple server-level and endpoint-level vulnerabilities were identified and categorised by severity, enabling data-driven decision-making.

#### 2. Strengthened Security Across Distributed Workstations

All endpoints were evaluated, revealing configuration gaps and patching inconsistencies that were quickly addressed.

#### 3. Improved Server Hardening & Reduced Attack Surface

Both Production and DR servers underwent deep analysis, resulting in improved controls, reduced exposure, and stronger operational resilience.



#### 4. Validated Real-World Attack Scenarios

Borderless CS exploited selected vulnerabilities under controlled conditions to demonstrate the risk impact and the urgency of remediation.

#### 5. Comprehensive Remediation Roadmap Delivered

A prioritised action plan aligned with best practices (CIS Benchmarks, NIST CSF, and ISO 27001 principles) was provided to guide LICl Fiji's ongoing security uplift.

#### Conclusion

Partnering with Borderless CS enabled LICl Fiji to significantly enhance the cybersecurity resilience of its core infrastructure and distributed workforce.

The VAPT engagement ensured that vulnerabilities were identified early, mitigated effectively, and managed in a structured, compliant manner—protecting LICl Fiji's systems, operations, and customer data against modern cyber threats.

LICl Fiji is now better equipped to maintain a strong security posture while continuing to deliver trusted, reliable financial services across Fiji.