CASE STUDY 2025

CYBERSECURITY SERVICES

COMMUNITY BUSINESS BUREAU

Contact: Peter Moore | Sales and Technical Director

Email: pmoore@logitech.com.au

Contact: Ben Kirk | Business Development Manager

Email: bkirk@logitech.com.au

PARA BELLUM SOLUTIONS

CBB CASE STUDY 2025

About Logi-Tech

Logi-Tech provides comprehensive cybersecurity services designed to help clients understand and strengthen their security posture. In addition to technical solutions, Logi-Tech offers strategic guidance on policy and governance to reduce human error and support compliance with frameworks such as the Payment Card Industry Data Security Standard (PCI DSS), the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the Australian Cyber Security Centre (ACSC) Essential Eight.

Key services include continuous asset validation through automated penetration testing and a full Security Operations Centre (SOC) as a service.
This includes:

- Security Information and Event Management (SIEM)
- Security Orchestration, Automation and Response (SOAR)
- Endpoint Detection and Response (EDR)
- Network Traffic Analysis (NTA)
- User and Entity Behaviour Analytics (UEBA)
- Artificial Intelligence (AI) and Machine Learning (ML)
- Ransomware protection
- Application allow listing
- Email filtering and phishing detection
- Staff education and awareness tools

Logi-Tech also provides expert advice and tools for business continuity and disaster recovery, supported by experienced professionals who can implement and maintain these solutions.
Additional capabilities include:

- Leading the design and management of security strategies
- Incident management and response
- Automating risk profiling, asset inventory, and security operations
- Conducting cybersecurity, regulatory, and risk management reviews
- Delivering phishing simulations and targeted staff training
- Investigating security incidents
- Threat containment and eradication
- Business continuity planning
- Disaster recovery strategy
- Testing operational and executive response plans
- Designing and implementing cybersecurity architectures
- Deploying firewalls and Intrusion Prevention Systems (IPS)
- Endpoint security solutions
- Identity and Access Management (IAM)
- Attack surface management
- Threat detection and prevention
- Intrusion Detection Systems (IDS)
- Vulnerability scanning
- Penetration testing
- SIEM deployment and monitoring

These integrated services provide real-time insights and measurable outcomes, protecting even legacy operating systems and operational technology (OT) environments from modern threats, including zero-day vulnerabilities.

CBB CASE STUDY 2025

Cybersecurity Managed Services for Community Business Bureau (CBB)

Executive Summary

CBB is a socially-driven organisation dedicated to strengthening the not-for-profit sector. Through personalised salary packaging, expert advisory services, and strategic partnerships, CBB helps not-for-profits become more sustainable, capable, and impactful, empowering them to create positive change in more lives.

The PCI DSS defines security requirements to protect environments where credit card account data is stored, processed, or transmitted. PCI DSS provides a baseline of technical and operational requirements designed to protect credit card account data. The PCI Security Standards Council (PCI SSC) is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

The CBB case study stands as a strong example of Logi-Tech's capabilities in full, illustrating how deep engagement, technical innovation, and trust-based collaboration can create lasting cybersecurity outcomes.

Engagement with CBB

CBB engaged Logi-Tech to support their journey toward PCI DSS compliance, seeking both the technology and expertise required to meet rigorous security standards. Logi-Tech developed a strong understanding of the threat landscape and its impact on business operations, then translated complex compliance requirements into practical, achievable actions.

Achieving PCI DSS compliance is a significant undertaking, and CBB approached it with a long-term view. We worked closely and diligently with their team, implementing fit-for-purpose technologies while also advising on forward-looking solutions to support future decision-making.

Recognising the cost and governance implications of security enhancements, we focused on value, ensuring each step was strategic, justifiable, and sustainable. Through proactive monitoring and management of the current toolset, we've prvided CBB wait a clear view of their environment and ensured critical assets, such as firewalls, remain up to date and secure.

This collaborative approach has delivered measurable progress.
Today, CBB benefits from improved visibility, maintained security controls,
and a clear understanding of the remaining capability gaps along with
a roadmap of the technologies that will enable CBB to fully achieve
PCI DSS compliance.

- David Hombsch, Chief Technical Officer, CBB

CBB CASE STUDY 2025

Cybersecurity Managed Services for Community Business Bureau (CBB)

Logi-Tech has delivered a comprehensive Managed Cybersecurity Service to CBB for the past three years. This partnership supports CBB's requirement to meet Payment Card Industry Data Security Standard (PCI DSS) compliance, a necessity due to its role in the financial services sector.

As part of this service, Logi-Tech provides CBB with a suite of advanced cybersecurity tools and advisory support, including:

- Automated Penetration Testing
- Vulnerability and password strength assessments
- Application allow listing
- Phishing and malware detection
- Employee cybersecurity awareness training
- Business continuity planning and testing

A key component is Pentera, a continuous validation platform that conducts weekly automated penetration tests, vulnerability scans, exploit simulations, and password cracking exercises. Each cycle concludes with a detailed report that includes exposure ratings, actionable recommendations, and proposed remediation projects. These insights are used to track progress, inform strategy, and drive ongoing improvements.

Monthly executive-level reports are presented to CBB management to ensure visibility of the current threat landscape and organisational security posture. Any critical issues identified are escalated immediately.

Business Continuity and Disaster Recovery (DR) are maintained through Azure-based backups, with 6-monthly DR testing that includes user acceptance testing by CBB staff. This ensures all on-premises applications can be recovered reliably in the event of a disruption.

Regular patching of software and hardware is conducted via a Remote Monitoring and Management (RMM) tool, with urgent updates, such as firewall patches, addressed immediately where required.

The cybersecurity training program is regularly updated in consultation with CBB to align with PCI DSS requirements and assess staff understanding of emerging threats. Campaigns are tailored to increase organisational awareness and resilience.

All engagements are conducted with full respect for CBB's internal governance and decision-making structures. Scope variations are always quoted and approved in advance, ensuring transparency, auditability, and alignment with business objectives.

All technologies implemented are selected for their relevance to current compliance needs and future-proofing against evolving government regulations and cybersecurity standards. No changes are made without prior approval from the appropriate decision-makers within CBB's management.

Looking ahead, CBB is considering further enhancements to its security infrastructure, this would encompass:

- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)
- Intrusion Prevention and Detection Systems (IPS/IDS)

- Ransomware protection
- Network Traffic Analysis (NTA)
- Endpoint Detection and Response (EDR)
- User and Entity Behaviour Analytics (UEBA)
- Artificial Intelligence (AI) and Machine Learning (ML)
- Data encryption at rest and in transit

Logi-Tech remains a trusted partner to CBB, delivering strategic cybersecurity services that protect its operations today and support its future growth.

Showcasing Logi-Tech's Full Capability Through CBB Partnership

While many clients engage Logi-Tech for select cybersecurity services, our partnership with Community Business Bureau (CBB) offers an opportunity to demonstrate the full breadth of our technical capabilities in action. CBB has leveraged our end-to-end expertise to address a complex challenge: achieving compliance with the Payment Card Industry Data Security Standard (PCI DSS).

In support of this, Logi-Tech expanded its own technical capabilities, adopting new cybersecurity technologies and aligning with relevant frameworks. We assessed risk, translated threats into practical action plans, and delivered tailored, technically sound solutions.

A cornerstone of our work with CBB is the implementation of automated, continuous penetration testing, configured and executed weekly. This includes Black Box and Grey Box testing, vulnerability scanning, and password strength assessments. Each test cycle is reset weekly to ensure a continuous improvement loop, with any identified issues promptly remediated and re-tested.

Additional technologies deployed include:

- Airlock | Application allow listing to prevent unauthorized execution
- Trend Micro XDR | Advanced email filtering and phishing protection
- KnowBe4 | Employee training platform with targeted campaigns focused on PCI DSS awareness
- Azure-based Business Continuity | Cloud backup and quarterly-tested disaster recovery capabilities

These tools, paired with expert configuration and governance support, have transformed CBB's security posture. What was once a gap in compliance is now a well-managed, near-compliant environment, achieved through collaboration, transparency, and trust.

Logi-Tech provides monthly cybersecurity reporting to CBB in executive format, supported by detailed technical reports. This ensures decision-makers remain fully informed, and remediation efforts are tracked and discussed in structured fortnightly meetings.

CBB values our integrity, accuracy, and professionalism. We respect their internal governance processes, never making changes without the appropriate approvals. Our role carries high responsibility, and we approach it with care and accountability.

All solutions are designed with long-term resilience and scalability in mind, typically planned for five years of growth and incorporating hybrid infrastructure for both on-premises reliability and cloud-based flexibility. This enables more predictable budgeting and minimal disruption to business operations.

The result

These strategic implementations have resulted in a well-managed, secure environment. CBB has made significant progress toward PCI DSS compliance, far exceeding their previous position, with consistent visibility and governance in place.

Supported by detailed technical reports to ensure transparency and informed decision-making, regular fortnightly meetings enable proactive discussion of findings and remediation efforts, ensuring alignment and accountability.

Throughout this partnership, Logi-Tech has maintained a high level of trust and responsibility in managing CBB's ICT environment. Our commitment to honesty, integrity, and strategic foresight is recognised and appreciated by the client.

All solutions are designed with long-term growth in mind, typically supporting a five-year lifecycle, and are built to balance on-premise capability with scalable, cloud-based resilience. This forward planning enables predictable budgeting, minimises disruptions, and ensures a secure and sustainable future for CBB.

Contact: Peter Moore | Sales and Technical Director

Email: pmoore@logitech.com.au

Contact: Ben Kirk | Business Development Manager

Email: bkirk@logitech.com.au

Contact us today!

logitech.com.au
sales@logitech.com.au