Pampered Pets: Risk Identification Report

Executive Summary

This report evaluates cybersecurity and business risks for Pampered Pets using the OCTAVE Allegro methodology enhanced with STRIDE threat modelling. Assessment reveals that the digitalisation benefits justify proceeding with managed transformation.

Risk Assessment Methodology

Hybrid Framework Selection: OCTAVE Allegro was chosen for its suitability to small businesses with limited IT resources, focusing on information assets rather than complex technical assessments (Allen-Addy, 2023). STRIDE threat modelling enhances OCTAVE, enabling comprehensive threat identification across six categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (Olmsted, 2024). This hybrid approach combines an organisational risk perspective with systematic threat enumeration.

Current State Risk Assessment (OCTAVE Allegro)

Risk Criteria & Information Assets

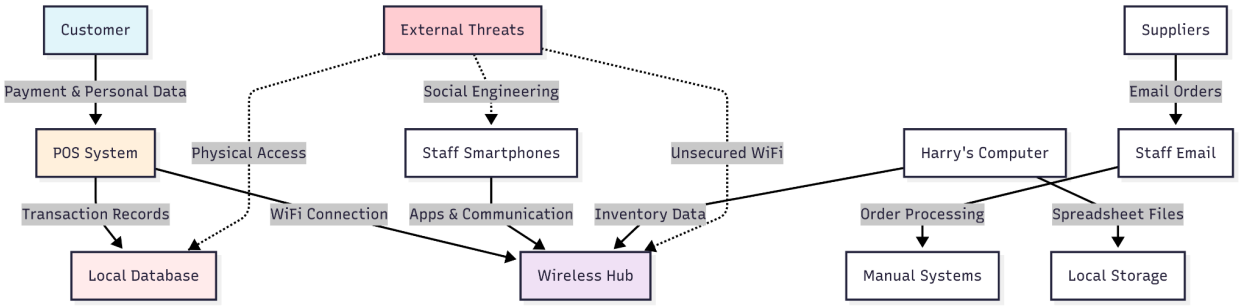
Risk measurement criteria established based on operational impact:

- **High Impact**: Complete business shutdown, inability to process sales, regulatory non-compliance penalties

- **Medium Impact**: Significant operational disruption, customer service degradation
- **Low Impact**: Minor operational inconvenience with quick recovery

Critical Information Assets: Customer transaction data, supplier contact information, employee records, financial documentation, and inventory tracking systems.

Current State Data Flow Diagram



STRIDE Threat Analysis

Current vulnerabilities identified:

- **Spoofing**: Unauthorised WiFi access via an unsecured network
- **Tampering**: Transaction record or inventory data modification
- **Repudiation**: No audit trails for system access or changes
- **Information Disclosure**: Customer data exposure via unsecured wireless
- **Denial of Service**: A single POS system failure halts operations
- **Elevation of Privilege**: Unauthorised staff access to sensitive data

Current Risk Evaluation

- **Data breach incident**: High probability, High impact - unsecured wireless network exposes customer payment data to potential GDPR violations, resulting in regulatory fines and reputation damage.
- **Business continuity failure**: Medium probability, High impact - a single point of failure in the POS system would halt sales operations, given 90% face-to-face dependency.
- **Competitive disadvantage**: High probability, Medium impact - lack of digital presence creates customer retention challenges (Lu & Shaharudin, 2024).

Current Mitigations

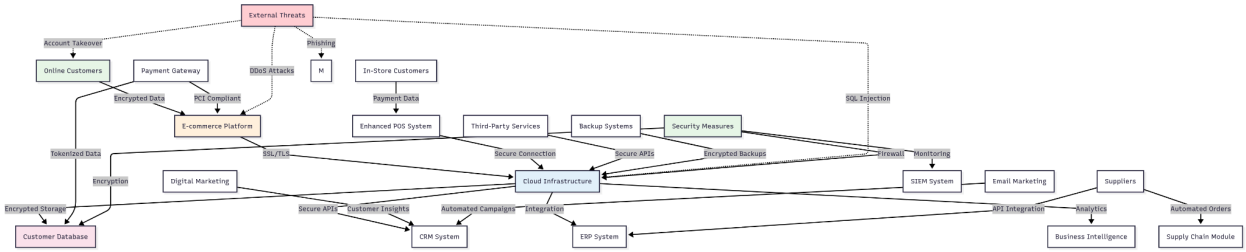
- Implement WPA3 wireless encryption with network segmentation.
- Establish automated daily backup procedures.
- Deploy comprehensive staff cybersecurity training.
- Install an enterprise-grade firewall and endpoint security.
- Develop formal incident response procedures.

Post-Digitalisation Risk Assessment

Proposed Changes

E-commerce platform, CRM system, ERP integration, digital marketing suite, cloud infrastructure.

Post-Digitalisation Data Flow Diagram



Enhanced STRIDE Threats

- **Spoofing**: Customer account compromise via fake accounts
- **Tampering**: SQL injection attacks on databases and web forms
- **Repudiation**: Disputed online transactions without proper logging
- **Information Disclosure**: Payment card data breaches and customer data theft
- **Denial of Service**: DDoS attacks overwhelm web applications
- **Elevation of Privilege**: Admin account compromise, granting full system access

Enhanced Risks

- **PCI compliance violations**: Medium probability, Very High impact - payment card data handling creates regulatory requirements with significant penalty potential.
- **GDPR breaches**: Medium probability, High impact - customer data processing obligations carry substantial regulatory penalties.
- **Cyber attacks**: High probability, Medium impact - small businesses increasingly targeted by cybercriminals (Verizon, 2025).

Digital Mitigations

- Security-by-design implementation with SSL and AES-256 encryption
- PCI-DSS and GDPR compliance frameworks
- Enhanced incident response procedures
- Comprehensive staff digital security training
- Vendor security assessments

Assessment of Key Business Questions

- **50% Online Growth**: Achievable through expanded reach and convenience-driven customers.
- **24% International Supply Cost Reduction**: Not recommended - eliminates local sourcing competitive advantage.
- **33% Customer Loss Without Digital**: High probability given consumer expectations and post-pandemic digital shift (Yu & Jinbo, 2024).

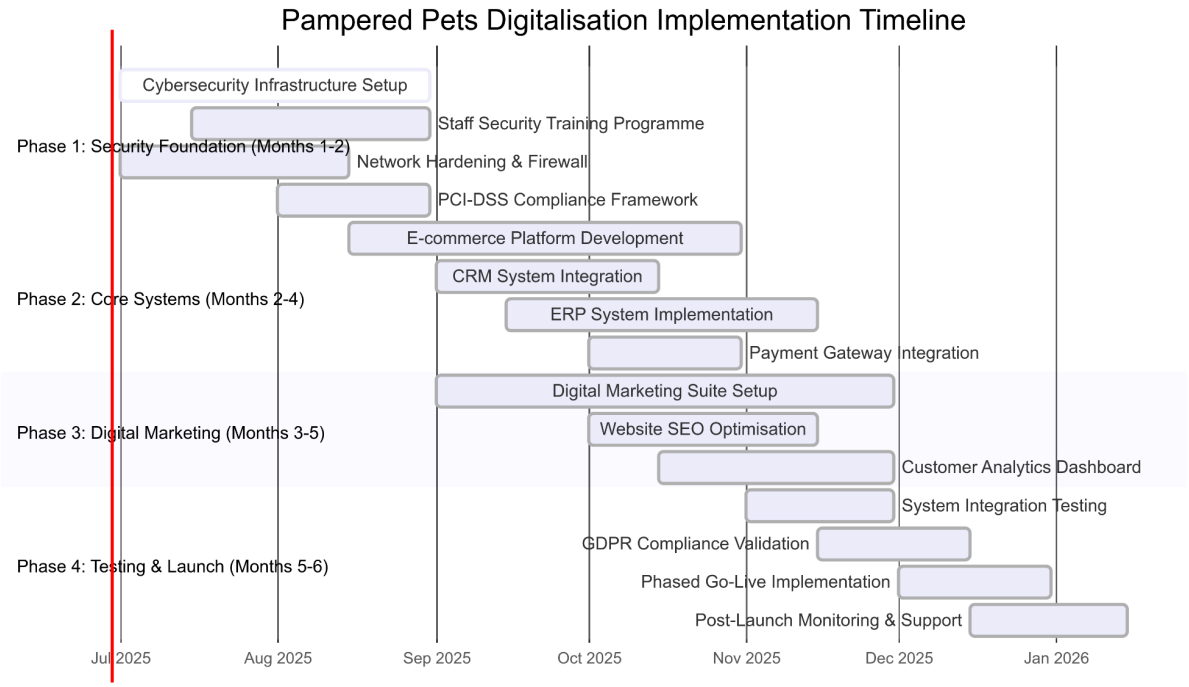
Recommendations

RECOMMENDATION: Proceed with Digitalisation

Rationale:

- Current risks outweigh digitalisation risks with proper mitigations.
- Competitive necessity prevents customer attrition.
- Business resilience against future disruptions

Digitilisation Implementation Timeline:



Critical Success Factors:

- Maintain local supply chain as primary competitive differentiator.
- Invest in a robust cybersecurity infrastructure from inception.
- Implement a phased approach, minimising operational disruption.
- Ensure continuous staff development with comprehensive change management.

References

Allen-Addy, C. (2023) *Threat Modeling Methodology: OCTAVE*. Available at: https://www.iriusrisk.com/resources-blog/octave-threat-modeling-methodologies (Accessed: 26 June 2025).

Lu, H. & Shaharudin, M. S. (2024) ‘Role of digital transformation for sustainable competitive advantage of SMEs: a systematic literature review’, *Cogent Business & Management*, 11(1). Available at: 10.1080/23311975.2024.2419489

Olmsted, A. (2024) *Security-Driven Software Development*. 1st edn. Birmingham, England: Packt Publishing Ltd.

Verizon (2025) *2025 Data Breach Investigations Report*. Available at: https://www.verizon.com/business/resources/reports/dbir/ (Accessed: 28 June 2025).

Yu, C. & Song, J. (2024) ‘After the COVID-19 pandemic: changes and continuities in the food supply chain’, *Food quality and safety*, 2024-01, Vol.8. Available at: https://doi.org/10.1093/fqsafe/fyad066