Summative Assessment 1: Risk Identification Report

Information Security Management June 2024

Word count: 653

Risk Identification Report for Pampered Pets

Introduction

Pampered Pets, a pet food retailer, aims to evaluate the risks of continuing current operations versus transitioning to digital business practices. This report provides a thorough assessment of existing threats and the potential rewards and hazards of digitalisation.

Current Business Risk Assessment

Methodology

The report will employ the NIST SP 800-30 Risk Management Framework (RMF) to evaluate the current risk assessment. NIST SP 800-30 provides a thorough and standardized approach to risk management, especially in cybersecurity, which is critical for protecting digital assets. Its scalability makes it adaptable to the specific needs and resources of small businesses, ensuring comprehensive risk assessment and mitigation（NIST, 2012).

SWOT Analysis

SWOT analysis is simple, accessible, and ideal for businesses with limited strategic planning expertise, examining internal strengths and weaknesses and external

opportunities and threats (Gürel & Tat, 2017; Helms & Nixon, 2010). Table 1 outlines Pampered Pets' SWOT, contrasting its strong reputation and high-quality products with its reliance on in-person sales and outdated technology. It also highlights growth opportunities and threats like cybersecurity and competitive disadvantages if the company does not modernize.

Table 1. Current business SWOT analysis.

Strengths:	**Weaknesses:**
• High-quality, locally sourced pet food. • Strong local reputation. • Direct control over supply chain.	• Heavy reliance on face-to-face sales (90%). • Limited online presence. • Manual and outdated IT systems (e.g., old computer for warehouse management).
Opportunities:	**Threats:**
• Potential growth through digitalization. • Expanding market reach via online sales. • Enhancing customer convenience with online features.	• Cybersecurity risks: The current wireless network and outdated systems are vulnerable to attacks. • Competitive disadvantage: Competitors with online presences might attract tech-savvy customers. • Operational inefficiencies: Manual processes are prone to errors and inefficiencies.

Figure 1 illustrates Pampered Pets' current IT setup, showing data exchange among customers, employees, and systems. It highlights the reliance on in-person interactions, manual procedures, outdated devices, and a basic wireless network.

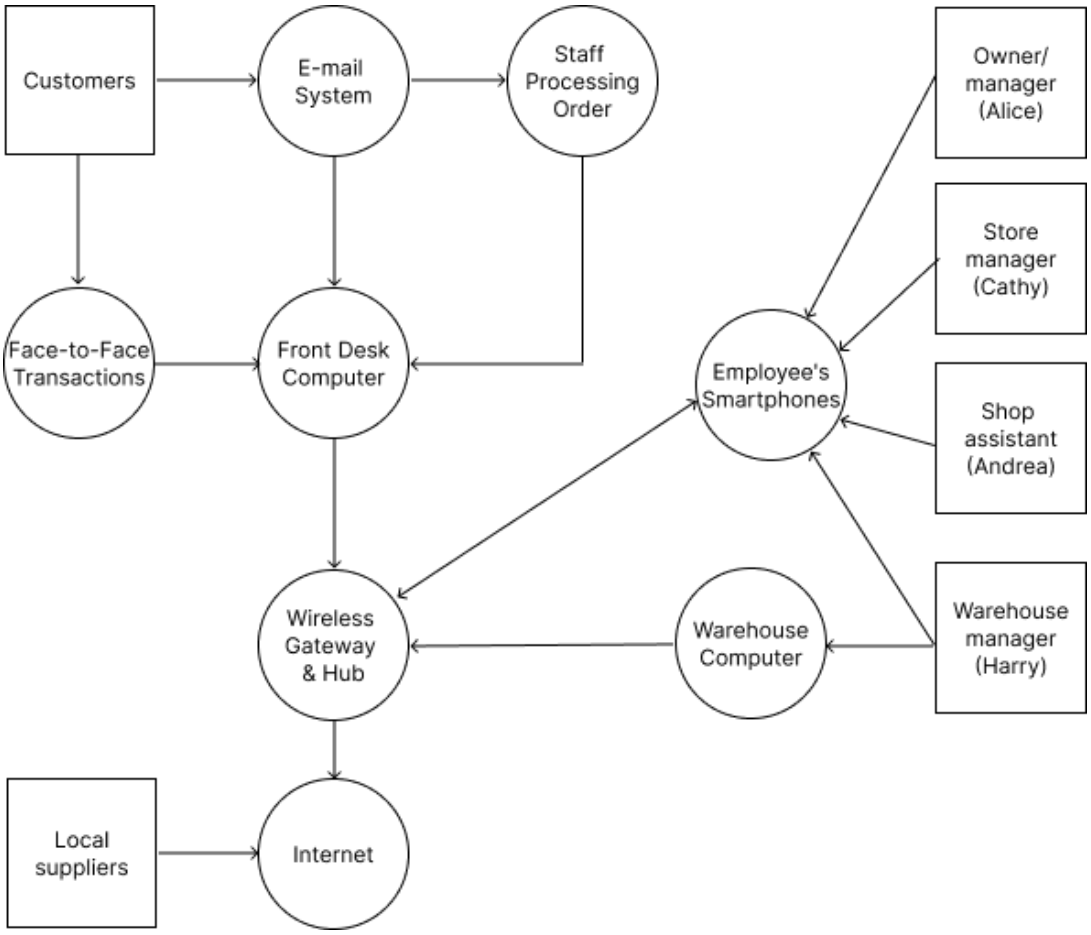

Figure 1. Current Business IT Infrastructure.

Threat Modelling and Risk Enumeration

Using the STRIDE model, we can systematically identify and categorize potential threats to Pampered Pets' operations. Table 2 details these specific threats (Shostack, 2014).

Table 2. Current business STRIDE Threat model identification.

Threat Type	Description	CAPEC ID	Impact	Risk Level
Spoofing	Unauthorized access to wireless network	162	Data breaches, unauthorized transactions	High
	Fake emails from customers placing orders	163	Financial losses, fraudulent orders	Medium
Tampering	Manipulation of digital sales records	59	Financial discrepancies, tax issues	High

	Alteration of warehouse inventory data	56	Stock management issues	Medium
Repudiation	Denial of transaction by customers	179	Revenue loss, disputes	Medium
	Employees denying actions performed on the system	280	Internal fraud, operational issues	Medium
Information Disclosure	Data breaches exposing customer information	212	Legal consequences, loss of trust	High
	Leakage of proprietary recipes and supplier information	206	Competitive disadvantage	High
Denial of Service	Wireless network outages impacting sales and warehouse operations	227	Business disruption, revenue loss	High
Elevation of Privilege	Unauthorized escalation of access privileges by an employee	233	Data breaches, misuse of information	High

Current Risks and Mitigations

Based on the identified threats, it is crucial to outline the corresponding risks and propose mitigations to manage these risks effectively, presented on table 3.

Table 3. Current Risks and Mitigations.

Risk Type	Risks	Mitigations
Technical	Outdated hardware	Upgrade hardware, regular maintenance schedules
	Lack of encryption on wireless network	Encrypt wireless networks, implement strong password policies
	Insufficient backup processes	Establish automated backup systems
Operational	Dependency on physical store operations	Enhance online presence with a basic informational website
	Limited online presence	Automate order processing and inventory management

	Manual handling of orders and inventory	
Human	Staff lacking cybersecurity training	Conduct regular cybersecurity training for all staff
	Potential for internal fraud or negligence	Implement strict access control measures and logging

The table 4 provides a detailed plan to mitigate each identified threat under current business operations using the STRIDE model.

Table 4. Current business STRIDE Threat model Risk mitigation.

Threat Type	Description	Mitigations	Priority	Action Needed
Spoofing	Unauthorized access to wireless network	Implement WPA3 encryption, use strong password policies	High	Upgrade wireless security settings, enforce strong password policies
	Fake emails from customers placing orders	Use email authentication and filtering	Medium	Implement SPF, DKIM, and DMARC; train staff on phishing email recognition
Tampering	Manipulation of digital sales records	Use tamper-evident logs, implement integrity checks	High	Deploy logging mechanisms and integrity monitoring tools
	Alteration of warehouse inventory data	Implement access controls, regularly audit inventory records	Medium	Set up role-based access controls, conduct regular audits
Repudiation	Denial of transaction by customers	Implement digital signatures and non-repudiation mechanisms	Medium	Adopt digital signature tools for transaction validation
	Employees denying actions performed on the system	Use detailed logging and monitoring	Medium	Implement detailed activity logs and regular monitoring
Information Disclosure	Data breaches exposing customer information	Use encryption for stored data,	High	Encrypt sensitive data at rest, enforce strict

		implement access controls		access control policies
	Leakage of proprietary recipes and supplier information	Apply data loss prevention (DLP) tools, use NDA agreements	High	Deploy DLP solutions, have employees sign NDAs
Denial of Service	Wireless network outages impacting sales and warehouse operations	Use network redundancy, implement DDoS protection measures	High	Set up backup internet connections, deploy DDoS mitigation solutions
Elevation of Privilege	Unauthorized escalation of access privileges by an employee	Use least privilege principle, regularly review access rights	High	Apply least privilege policies, conduct regular access reviews

Digitalisation Risk Assessment

Methodology

The report will use the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) methodology for the digitalisation risk assessment, ideal for small businesses as it:

- Identifies critical assets, threats, and vulnerabilities.
- Engages employees, promoting a security-conscious culture.
- Focuses on protecting essential assets with thorough risk analysis and effective mitigation plans (Alberts & Dorofee, 2001).

Proposed Digitalisation Changes

The digitalisation involves several key changes aimed at enhancing business operations and expanding market reach. The table 4 outlines the proposed changes for digitalisation. Implementing an e-commerce portal, ERP system, online marketing strategies, and a CRM system are key steps to modernize and expand the business.

Table 5. Proposed Digitalization Changes.

Proposed Change	Description
E-commerce portal	Development of an online platform for sales, expanding market reach
Enterprise Resource Planning (ERP) System	Implementation for integrated business management, improving efficiency and data insights
Online marketing strategies	Adoption of SEO, social media to increase visibility and attract new customers
CRM system	Introduction to enhance customer engagement and improve service quality

Below, Figure 2 depicts projected data flow and integration improvements for Pampered Pets, showcasing how digitalisation enhances operations, customer service, and business expansion. It emphasizes system interdependence for operational effectiveness and precise data management across the organization.

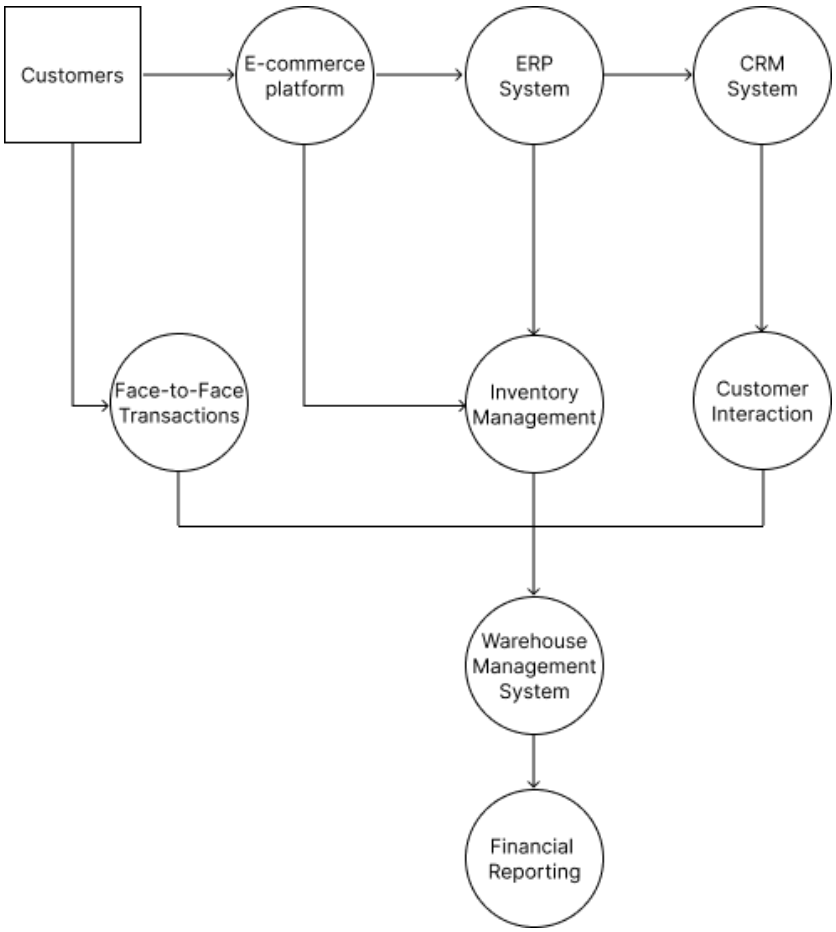

Figure 2. Digitalized Business IT Infrastructure.

Threat Modelling and Risk Enumeration

Table 6 details specific digitalisation threats using the STRIDE model, offering insights into potential risks and their impacts to aid comprehensive threat management planning.

Table 6. STRIDE model for Digitalisation.

Threat Type	Description	CAPEC ID	Impact	Risk Level
Spoofing	Unauthorized access to the e-commerce platform	162	Manipulation of transactions, data breaches	High
Tampering	Alteration of online orders and inventory data	56	Financial losses, operational disruptions	High
Repudiation	Customers denying online transactions	179	Revenue loss, disputes	Medium
Information Disclosure	Data breaches exposing customer and business data	212	Legal issues, reputational damage	High
Denial of Service	DDoS attacks on the e-commerce website	227	Sales disruption, customer dissatisfaction	High
Elevation of Privilege	Unauthorized access to ERP and CRM systems	233	Data breaches, business operation disruptions	High

Potential Risks and Mitigations

Identifying and mitigating risks associated with digitalisation is crucial for a smooth transition. Bellow identified risks with suggested mitigations for the digitalisation process.

Table 7. Digitalisation Risks and Mitigations.

Risk Type	Risks	Mitigations
Technical	Increased attack surface with online presence	Implement robust cybersecurity measures (firewalls, anti-malware), ensure secure coding practices, regular audits
	Integration challenges with existing systems	Gradual and planned integration, regular testing and validation
	Dependency on third-party service providers	Select reputable vendors, establish SLAs, continuous monitoring
Operational	Transition period impacting business continuity	Develop phased implementation plan, maintain parallel systems during transition
	Increased complexity in managing digital platforms	Establish dedicated IT support team, ongoing training and support
	Need for continuous monitoring and maintenance	Implement monitoring systems, schedule regular maintenance
Human	Requirement for staff training on new systems	Provide comprehensive training programs, foster culture of continuous learning
	Potential for resistance to change from employees	Communicate benefits, involve staff in planning, provide support during transition

Table 8 presents a prioritized approach to mitigate digitalisation risks using the STRIDE model, detailing specific actions to address the most critical threats first.

Table 8. STRIDE Threat model for Digitalisation Risk mitigation.

Threat Type	Description	Mitigations	Priority	Action Needed
Spoofing	Unauthorized access to the e-commerce platform	Implement multi-factor authentication (MFA), use HTTPS	High	Deploy MFA for all user accounts, ensure all web traffic is encrypted with HTTPS
Tampering	Alteration of online orders and inventory data	Implement end-to-end encryption, use tamper-evident logs	High	Encrypt data in transit and at rest, deploy logging mechanisms for tracking changes
Repudiation	Customers denying online transactions	Use transaction verification methods, implement digital signatures	Medium	Integrate transaction verification steps, adopt digital signature solutions
Information Disclosure	Data breaches exposing customer and business data	Use comprehensive encryption, implement strong access controls	High	Encrypt all sensitive data, enforce stringent access control measures
Denial of Service	DDoS attacks on the e-commerce website	Implement DDoS protection, use content delivery networks (CDN)	High	Deploy DDoS mitigation services, leverage CDNs to distribute traffic and reduce impact
Elevation of Privilege	Unauthorized access to ERP and CRM systems	Use role-based access control (RBAC), regularly review and audit access	High	Implement RBAC policies, perform regular access audits and reviews

Recommendations

Digitalisation Recommendation

Based on the risk assessments, it is recommended that Pampered Pets proceed with digitalisation. The potential benefits, including increased market reach, improved operational efficiency, and enhanced customer engagement, outweigh the associated risks. According to a study by Gartner (2020), digital transformation can significantly

enhance business agility and customer satisfaction, which are critical for long-term success.

Implementation Approach and Timeline

Table below outlines a timeline for implementing digitalisation at Pampered Pets, covering phases for planning, implementation, testing, optimization, and continuous improvement.

Table 9| Timeline.

Phase	Duration	Activities
Planning and Preparation	3 months	Conduct detailed requirement analysis, select vendors and solutions, develop comprehensive project plan
Implementation	6 months	Set up e-commerce platform, integrate with existing systems, implement ERP and CRM systems, train staff
Testing and Optimization	3 months	Conduct thorough testing, optimize processes based on feedback, launch marketing campaigns
Go-Live and Improvement	Ongoing	Officially launch digital platforms, monitor performance and security, regularly update systems, train staff

Conclusion

Digitalisation presents a significant opportunity for Pampered Pets to grow its business and improve operational efficiency. By addressing the identified risks through robust mitigations and adopting a structured implementation approach, the business can successfully transition to a digital model and achieve sustainable growth.

Reference list

Blos, M. F., Wee, H.-M., & Yang, J. (2010). Analysing the external supply chain risk driver competitiveness: a risk mitigation framework and business continuity plan. International Journal of Production Research, 48(11), 3391-3408.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Software Engineering Institute, Carnegie Mellon University.

Gai, K., Qiu, M., & Sun, X. (2018). A survey on FinTech. Journal of Network and Computer Applications, 103, 262-273.

Gallagher, P. (2009). Recommended Security Controls for Federal Information Systems and Organizations. NIST.

Gürel, E., & Tat, M. (2017). SWOT Analysis: A Theoretical Review. The Journal of International Social Research, 10(51).

Helms, M. M., & Nixon, J. (2010). Exploring SWOT analysis – where are we now? A review of academic research from the last decade. Journal of Strategy and Management, 3(3), 215-251.

Martin, N., & Rice, J. L. (2010). Emergency preparedness for small businesses. International Journal of Business Continuity and Risk Management, 1(3), 278-292.

National Institute of Standards and Technology (NIST). (2012). NIST SP 800-30: Guide for Conducting Risk Assessments.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. NIST.

The OCTAVE Method. CERT Division, Software Engineering Institute, Carnegie Mellon University.