By Louis Dodge, James Edney, Fiqki Azizah and Milad Chowdhury

Risk Identification Report- Pampered Pets

# Risk Assessment Report for Pampered Pets

## Introduction

Pampered Pets is a local pet supply business in Hashington-on-the-Water, primarily conducting face-to-face transactions with occasional email orders. This report assesses the current risks of their operations and evaluates the potential risks and benefits of implementing an e-commerce platform and changing to an international supply chain. Recommendations are provided to guide Pampered Pets in enhancing business processes and achieving growth objectives.

## Risk Assessment of Current Business

### 2.1 Methodology Selection

The NIST SP 800-30 framework is selected for its structured approach suitable for small businesses requiring qualitative analysis (Stoneburner et al., 2002). The STRIDE model is chosen for threat modeling due to its effectiveness in identifying security threats in straightforward systems (Shostack, 2014).

### 2.2 Risk and Threat Modeling

Applying STRIDE reveals the following threats to the current business operations:

|  |  |  |  |
| --- | --- | --- | --- |
| Threat Type | Description | Impact | Mitigation |
| Spoofing | Unauthorized access to unsecured Wi-Fi network | Data breaches, unauthorized access to sensitive information | 1. Implement WPA3 encryption. 2. Use strong, unique passwords for network access. 3. Enable MAC address filtering to restrict access to authorized devices. |
| Tampering | Manipulation of inventory spreadsheets | Inaccurate inventory data, financial discrepancies | 1. Establish role-based access controls (RBAC) to limit who can modify data. 2. Implement version control to track and audit changes in spreadsheets. |
| Repudiation | Lack of transaction logs allows denial of actions | Difficulty in auditing, resolving disputes | 1. Implement secure, tamper-evident transaction logging (Kent & Souppaya, 2006). 2. Use digital signatures to verify the integrity of transactions. |
| Information Disclosure | Unencrypted emails expose customer data | Loss of customer trust, potential legal liabilities | 1. Use end-to-end encrypted email services. 2. Establish a data classification policy to ensure sensitive information is always protected. |
| Denial of Service | System failures due to outdated hardware | Operational downtime, loss of sales | 1. Upgrade outdated systems to meet current performance standards (Microsoft, 2018). 2. Implement redundancy in hardware to minimize the impact of failures. |
| Elevation of Privilege | Staff access sensitive data without controls | Unauthorized changes, potential insider threats | 1. Implement multi-factor authentication (MFA) for sensitive data access. 2. Enforce principle of least privilege (POLP) to minimize unnecessary access rights. |

## Risk Assessment of Digitalization Process

### 3.1 Methodology Selection

Continuing with NIST SP 800-30 and STRIDE ensures consistency in assessing digitalization risks (Stoneburner et al., 2002; Shostack, 2014).

### 3.2 Proposed Changes

* **E-commerce Platform:** Enable online sales to expand market reach. The proposed e-commerce platform will streamline operations by integrating features such as real-time inventory tracking, customer support tools, and a centralised transaction database. (Adobe, 2021)
* **International Supply Chain:** Source supplies internationally to reduce costs.

### 3.3 Risk and Threat Modeling

#### 3.3.1 E-commerce Platform

|  |  |  |  |
| --- | --- | --- | --- |
| Threat Type | Description | Impact | Mitigation |
| Spoofing | Attackers create fake websites | Financial loss, reputational damage | 1. Register variations of the business domain to prevent phishing. 2. Implement SSL certificates to help customers verify legitimate websites. |
| Tampering | Unauthorized modification of website content | Loss of customer trust, financial inaccuracies | 1. Use a Web Application Firewall (WAF) to detect and block suspicious modifications. 2. Implement Content Security Policy (CSP) to mitigate cross-site scripting attacks. |
| Repudiation | Customers deny transactions | Revenue loss due to chargebacks resolving disputes | 1. Implement secure, tamper-evident transaction logging (Kent & Souppaya, 2006). |
| Information Disclosure | Data breaches expose customer information | Legal penalties, loss of confidence | 1. Encrypt sensitive customer data both in transit and at rest (NIST, 2015). 2. Conduct regular security audits to identify vulnerabilities. |
| Denial of Service | DDoS attacks make website unavailable | Loss of sales, customer dissatisfaction | 1. Use a DDoS protection service (Cloudflare, 2020). 2. Establish traffic rate limiting to minimize the impact of attacks. |
| Elevation of Privilege | Exploitation of vulnerabilities | System compromise, operational disruption | 1. Perform regular vulnerability scanning and patching. 2. Use role-based access controls to limit administrative privileges. |

#### 3.3.2 International Supply Chain

|  |  |  |  |
| --- | --- | --- | --- |
| Risk Area | Description | Impact | Mitigation |
| Supply Chain Disruption | Political instability causes delays | Stock shortages, loss of sales | 1. Develop contingency plans with multiple alternative suppliers. 2. Use local warehousing to maintain a safety stock of critical items. |
| Quality Control Issues | Variations in product quality | Customer dissatisfaction | 1. Implement regular quality checks and audits for suppliers. 2. Establish contractual quality standards and penalties for non-compliance. |
| Regulatory Compliance | Non-compliance with trade laws | Legal penalties | 1. Hire compliance experts to monitor international trade laws. 2. Establish a compliance management system to track legal requirements. |

## Addressing Key Business Questions

### 4.1 Could an Online Presence Grow the Business by up to 50%?

Yes, e-commerce could increase sales by up to 50%. An American Express survey from 2023 reports that 53% of companies saw the most sales from e-commerce, a 49% increase from 2022 (Morell, 2024). Online presence expands market reach, tapping into consumer preferences for online shopping.

### 4.2 Could Changing to an International Supply Chain Reduce Costs by up to 24%?

Yes, sourcing internationally can reduce costs due to lower production expenses (Ellram, 2013). However, risks must be managed to realize savings without compromising quality.

### 4.3 Could the Business Lose up to 33% of Customers Without Online Features?

Yes, lacking online features could lead to losing customers. A PwC survey found 35% of consumers would stop doing business with companies lacking user-friendly digital platforms (PwC, 2018).

## Summary of Recommendations

### 5.1 Implement an E-commerce Platform

1. Increase Sales: Potential growth up to 50% (eMarketer, 2020).  
2. Retain Customers: Meet expectations to prevent loss (PwC, 2018).  
3. Enhance Competitiveness: Stay relevant in the digital market

### 5.2 Evaluate International Supply Chain Options

1. Assess Suppliers: Ensure reliability and compliance.  
2. Risk Management: Mitigate supply chain risks (Christopher & Holweg, 2017).  
3. Hybrid Approach: Consider combining local and international suppliers.

### 5.3 Implementation Considerations

1. Trusted Providers: Use reputable platforms.  
2. Security Measures: Implement recommended mitigations.  
3. Staff Training: Train employees on new systems (SANS Institute, 2018).

## Timeline

To enforce these mitigations, it is recommended to share responsibility with a “cloud broker” or Managed Service Provider (MSP). This shared responsibility transfers most of the risk to the MSP, with just configuration and access control the responsibility of the business (NCSC, 2021). The following Gantt chart outlines the estimated timeline for Pampered Pets to implement this recommendation:

A screenshot of a computer

Description automatically generated

Concurrently, Pampered Pets should ensure they facilitate a CSAT (Cyber security awareness training) program, as people are consistently the weakest link in the security chain (Zhang, 2021).

## Conclusion

Implementing an e-commerce platform and carefully transitioning to an international supply chain can significantly grow Pampered Pets by expanding market reach, reducing costs, and meeting customer demands. Risks associated with digitalization can be effectively mitigated through recommended measures. Proceeding with digitalization is recommended for business growth and sustainability.

## References

Adobe (2021) *E-Commerce Platforms*. Available at: https://business.adobe.com/blog/basics/ecommerce-platforms (Accessed: 08 November 2024).

AIRMIC (2010) *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000*. Available at: https://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf (Accessed: 3 November 2024).

Christopher, M. and Holweg, M. (2017) 'Supply Chain 2.0 revisited', *International Journal of Physical Distribution & Logistics Management*, 47(1), pp. 2-17.

Cloudflare (2020) *DDoS Attack Trends*. Available at: https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q2-2020 (Accessed: 01 December 2024).

eMarketer (2020) *Global Ecommerce Update 2020*. Available at: https://www.emarketer.com/content/global-ecommerce-2020 (Accessed: 01 December 2024).

Ellram, L. M. (2013) 'Offshoring, reshoring and the manufacturing location decision', *Journal of Supply Chain Management*, 49(2), pp. 3-5.

Federation of European Risk Management Associations (FERMA) (2010) *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000*. Available at: https://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf (Accessed: [Date]).

Hiremath, O. (N.D.) 'Comparison of STRIDE, DREAD and PASTA'. Available at: https://www.softwaresecured.com/post/comparison-of-stride-dread-pasta (Accessed: 06 November 2024).

Kent, K. and Souppaya, M. (2006) *Guide to Computer Security Log Management*. NIST SP 800-92. Available at: [URL] (Accessed: [Date]).

Microsoft (2020) *What is: Multifactor Authentication (MFA)*. Available at: <https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661> (Accessed 01 December 2024)

Morell, K. (2024) 'Report: Online Commerce, Pricing Among Top 2024 Priorities For Small Retailers'. Available at: https://www.americanexpress.com/en-us/business/trends-and-insights/articles/report-online-commerce-pricing-among-top-2024-priorities-for-small-retailers/ (Accessed: 03 November 2024).

NCSC (2021) *Cloud security guidance*. Available at: https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model (Accessed: 09 November 2024).

NIST (2015) *Guide to Data-Centric System Threat Modeling*. SP 800-154. Available at: [URL] (Accessed: [Date]).

PwC (2018) Available at: ttps://www.pwc.com/us/en/industries/consumer-markets/library/attract-retain-customers.html (Accessed: 01 December 2024

SANS Institute (2018) *Security Awareness Planning Kit*. Available at: https://www.sans.org/tools/security-awareness-planning-toolkit/ (Accessed: 01 December 2024)

Shevchenko, N. *et al.* (2018) *Threat Modelling: A Summary of Available Methods*. Software Engineering Institute, Carnegie Mellon University. Available at: https://insights.sei.cmu.edu/documents/569/2018\_019\_001\_524597.pdf (Accessed: 3 November 2024).

Shostack, A. (2014) *Threat Modelling: Designing for Security*.

Shostack *et al.* (2020) *Threat Modelling Manifesto*. Available at: https://www.threatmodelingmanifesto.org/ (Accessed: 06 November 2024).

Statista (2024) *E-Commerce in the United Kingdom (UK) - statistics and facts*. Available at: https://www.statista.com/topics/2333/e-commerce-in-the-united-kingdom/#dossierKeyfigures (Accessed: 06 November 2024).

Stoneburner, G., Goguen, A. and Feringa, A. (2002) *Risk Management Guide for Information Technology Systems*. NIST Special Publication 800-30. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://dl.acm.org/doi/book/10.5555/2206240 (Accessed: 3 November 2024).

Zhang, Z. *et al.* (2021) 'Cybersecurity awareness training programs: a cost–benefit analysis framework', *Industrial Management & Data Systems*. DOI: 10.1108/IMDS-08-2020-0462.