|  |
| --- |
|  |
| **RISK IDENTIFICATION REPORT – PAMPERED PETS** |
| Prepared by Group A: James Edney/ Fiqki Azizah/Louis Dodge/ Milad Chowdhury  **Contents**  [1. Introduction 3](#_Toc529482123)  [2. Risk Assessment Approach 3](#_Toc302348270)  [3. Current Risk Assessment 3](#_Toc1463648670)  [I. Current Risks 3](#_Toc306648449)  [II. STRIDE Modelling 4](#_Toc366586315)  [4. Digitalisation Risk Assessment 5](#_Toc60021512)  [I. Objectives 5](#_Toc758836666)  [II. Benefits 6](#_Toc1413581156)  [III. STRIDE Modelling for Digitalisation 6](#_Toc878493125)  [IV. Mitigations 7](#_Toc1076163238)  [5. Summary of Recommendations 8](#_Toc1279636400)  [6. Conclusion 8](#_Toc933690843)  [References 10](#_Toc642026097) |

# **1. Introduction**

Pampered Pets is a local pet supply business operating primarily through face-to-face transactions and a small number of orders taken by email. Inventory management is carried out with a spreadsheet package. This report evaluates the current risks with this approach and those associated with a potential digital transformation.

# **2. Risk Assessment Approach**

For this analysis, NIST SP 800-30 will be used as a framework, with a qualitative approach to identify risks and areas of improvement (Stoneburner, 2002). For threat modelling, STRIDE was chosen due to its simplicity and suitability for smaller businesses with linear workflows (Shevchenko, 2018). It is the more appropriate threat model for a small business of this type compared to other models such as PASTA (Hiremath, N.D.).

# **3. Current Risk Assessment**

## **I. Current Risks**

Pampered Pets’ existing operations present several vulnerabilities, including:

* **Physical Security:** The absence of advanced security measures such as CCTV or controlled access systems leaves the premises exposed to theft and unauthorised access.
* **Data Handling:** Inventory and customer data are managed using manual spreadsheets without digital backups, increasing the risk of data loss through accidental deletion or hardware failure.
* **Operational Disruption:** Dependency on staff availability poses a significant risk. Unforeseen absences could result in delayed service or inventory errors, affecting customer satisfaction.
* **Insider Threat:** Employees with unrestricted access to critical systems may unintentionally or maliciously compromise sensitive data

## **II. STRIDE Modelling**

To improve the security of the system and provide value to the stakeholders (Shostack, 2020), it is vital to analyse these areas of risk, and the inherent threats they bring to the business. Using STRIDE modelling, the inherent threats to these identified risks are as follows:

|  |  |  |
| --- | --- | --- |
| **STRIDE Category** | **Example Threat** | **Impact** |
| Spoofing | Disgruntled staff impersonating the business owner to modify inventory records. | Loss of trust and operational disruption. |
| Tampering | Unrestricted access enables modification of inventory or customer records. | Data integrity compromised. |
| Repudiation | Lack of activity logging allows denial of unauthorised data changes. | Reduced accountability and increased risk. |
| Information Disclosure | Emailing unencrypted customer orders risks exposing sensitive information. | Customer privacy was violated, breaching GDPR. |
| Denial of Service | Outdated systems are susceptible to technical failures or overloads. | Service interruptions and lost revenue. |
| Elevation of Privileges | Lack of user role segregation allows unauthorised critical actions. | System misuse leads to financial losses. |

These findings indicate that a digital transformation strategy is essential to mitigate current risks and enhance operational efficiency.

# **4. Digitalisation Risk Assessment**

## **I. Objectives**

Pampered Pets aims to achieve the following objectives through digitalisation:

1. **Business Growth:** Increase sales by 50% through an enhanced online presence.
2. **Cost Efficiency:** Reduce supply chain costs by 24% using international suppliers and automated inventory management.
3. **Customer Retention:** Prevent the loss of existing customers by offering a seamless, modernised experience.

The proposed e-commerce platform will not only streamline operations but also integrate features such as real-time inventory tracking, customer support tools, and a centralised transaction database (Adobe, 2021).

## **II. Benefits**

The benefits of an e-commerce platform include:

* **An increase in sales:** 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).
* **Reduced supply chain costs:** Accurate inventory management negates the “bullwhip effect”. This allows reduced inventory investment, greater customer service levels and more efficient transportation (Wiley, N.D.)
* **Larger customer base:** Non-digital buyers are the minority of the population (Statista, 2024), leaving a currently untouched customer base for Pampered Pets.

## **III. STRIDE Modelling for Digitalisation**

The proposed e-commerce platform introduces its own set of risks, which have been analysed using the STRIDE model:

|  |  |  |
| --- | --- | --- |
| **STRIDE Category** | **Example Threat** | **Impact** |
| Spoofing | Attackers impersonating the business via phishing scams. | Damage to reputation and loss of customer trust. |
| Tampering | SQL injection attacks altering product prices or customer orders. | Financial loss and customer dissatisfaction. |
| Repudiation | Customers disputing unauthorised purchases. | Increased administrative burden and legal risks. |
| Information Disclosure | Platform vulnerabilities expose sensitive customer data. | GDPR violations and reputational harm. |
| Denial of Service | DDoS attacks render the platform inaccessible during peak hours. | Loss of revenue and customer frustration. |
| Elevation of Privileges | Exploitation of vulnerabilities to gain administrator access. | System control is compromised, risking major outages. |

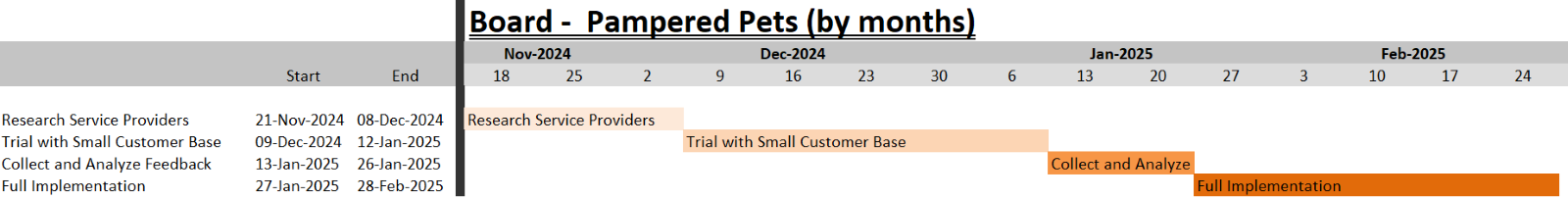
## **IV. Mitigations**

A qualitative approach will describe each threat’s impact as high; however, using a risk mitigation strategy, these threats can be tolerated, treated, transferred, or terminated (AIRMIC, 2010). Suggested risk mitigation is given below:

|  |  |
| --- | --- |
| **S**poofing | Multifactor authentication and complex passwords must be implemented. |
| **T**ampering | HTTPS is vital for secure communication. Input validation is also recommended to prevent SQLi. |
| **R**epudiation | Multifactor authentication can be used, and the system must be regularly audited. |
| **I**nformation Disclosure | Sensitive data must be encrypted; financial transactions can be outsourced to a third party. |
| **D**enial of Service | A web application firewall or content delivery network can be used which offers denial of service capabilities. |
| **E**levation of Privilege | Auditing user permissions and ensuring secure coding will prevent an elevation of privilege. |

# **5. Summary of Recommendations**

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, 2023). The following Gantt chart outlines the estimated timeline for Pampered Pets to implement this recommendation:

Concurrently, Pampered Pets should ensure they facilitate a CSAT (Cyber security awareness training) program, with the users being the weakest link in the security chain (Zhang, 2021).

# **6. Conclusion**

To achieve their aims of growing the business by 50%, reducing supply chain costs, and maintaining their existing customer base, it is recommended Pampered Pets adopts a digital transformation strategy. To do this, they will create an online presence, using a cloud broker. This will be trialled by an initial customer base, before then being fully rolled out. Staff training will be performed, concurrently. This approach enables Pampered Pets to address current vulnerabilities and achieve sustainable growth with a secure digital foundation, positioning the business for future expansion.

# **References**

* Adobe. (2021) E-Commerce Platforms. Available from: <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 from: <https://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf> [Accessed 3 November 2024].
* 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>
* Hiremath, O. (N.D.) Comparison of STRIDE, DREAD and PASTA. Available from: <https://www.softwaresecured.com/post/comparison-of-stride-dread-pasta> [Accessed 06 November 2024].
* Morell, K. (2024) Report: Online Commerce, Pricing Among Top 2024 Priorities For Small Retailers. Available from: <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 from: <https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model> [Accessed 09 November 2024].
* Shevchenko, N., et al. (2018) *Threat Modeling: A Summary of Available Methods*. Software Engineering Institute, Carnegie Mellon University. Available from: <https://insights.sei.cmu.edu/documents/569/2018_019_001_524597.pdf> [Accessed 3 November 2024].
* Shostack et al. (2020) Threat Modelling Manifesto. Available from: <https://www.threatmodelingmanifesto.org/> [Accessed 06 November 2024].
* Statista. (2024) E-Commerce in the United Kingdom (UK) - statistics and facts. Available from: <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 from: <https://dl.acm.org/doi/book/10.5555/2206240> [Accessed 3 November 2024].
* Wiley. (N.D.) E-Commerce and Supply Chain Management. Available from: <https://catalogimages.wiley.com/images/db/pdf/0471347248-ch04.pdf> [Accessed 09 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