**Risk Identification Report**

**1. Introduction**

This report addresses all credible threats to the Pampered Pets business based in the UK. It consists of two parts:

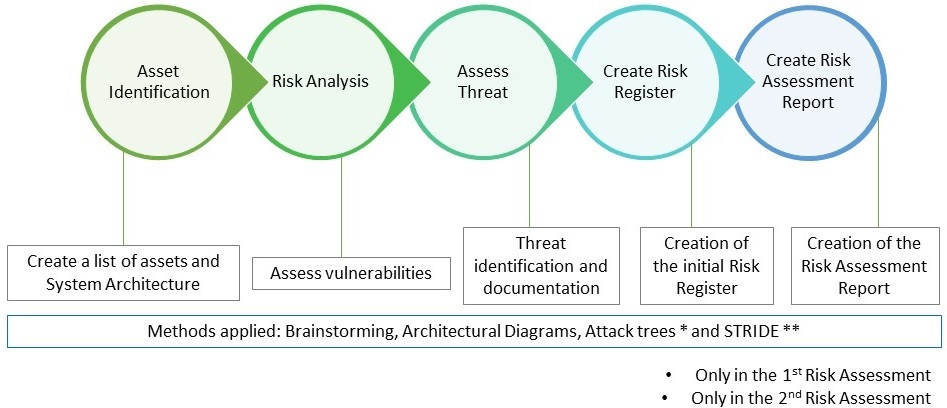
1. Risk Assessment of the business 'as is'
2. Risk Assessment around the potential digitalisation process of the business.

Methodology and justifications for each part are provided, along with the risk and threat modelling exercise and the potential mitigations to the identified risks and threats. Furthermore, a list of the proposed changes to the digitalisation transformation is also provided, along with a summary of recommendations for the digitalisation process.

**2. Methodology**

**2.1 Risk Assessment Methodology**

The same five-step risk assessment methodology presented in Figure 1 was applied to both risk assessments. These steps represent a holistic approach to risk assessment (Nordlayer, 2022). The additional detail added to these steps was the creation of the mitigations for the threats identified (Wolfman, 2023) once the Risk Register was created. Such a structured approach provided a good understanding of the system.



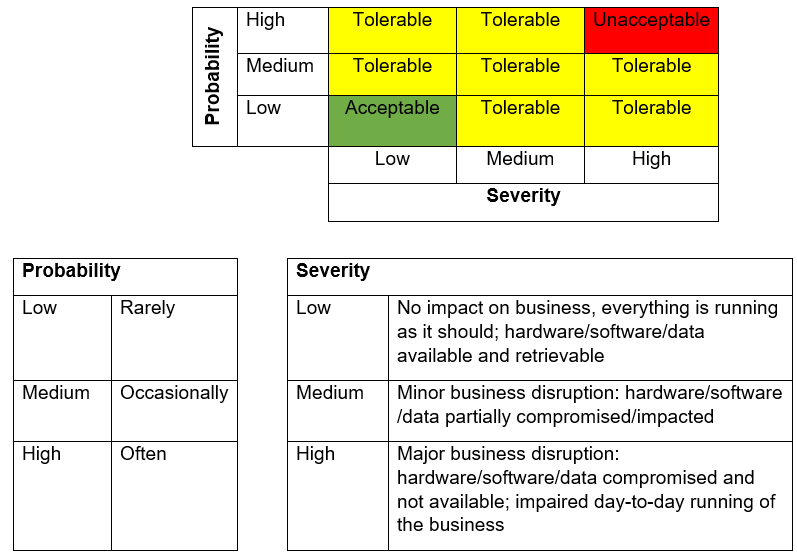
**Figure 1: Risk Assessment Methodology**

**2.2 Assessing Threat Probability**

The risk assessment's core part was applying the threat probability. It was applied using the 3x3 Risk Matrix presented in Figure 2 to assets in Table 4. The risk was either:

* Acceptable: The risk is acceptable ‘as is’ with no additional mitigations required
* Tolerable: The risk is acceptable, with some mitigations required
* Unacceptable: The risk needs further analysis and re-assessment of mitigations

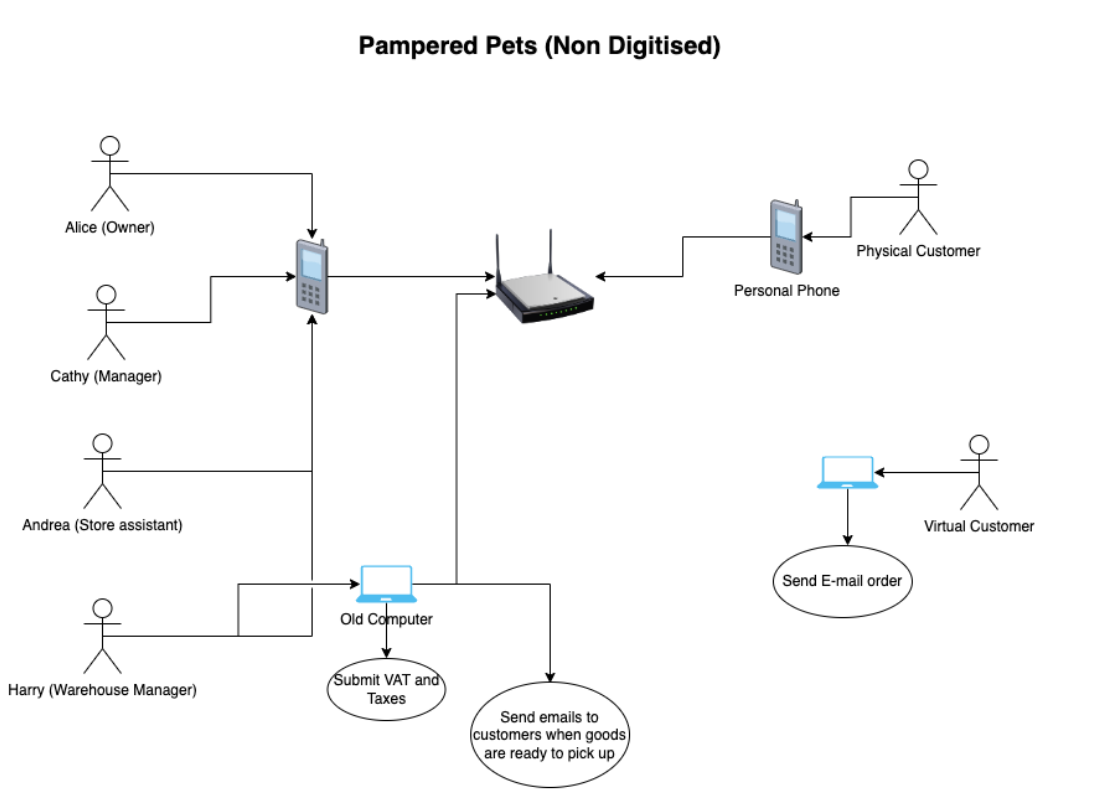
Figure 2 also contains the definitions for qualitative probability and severity.



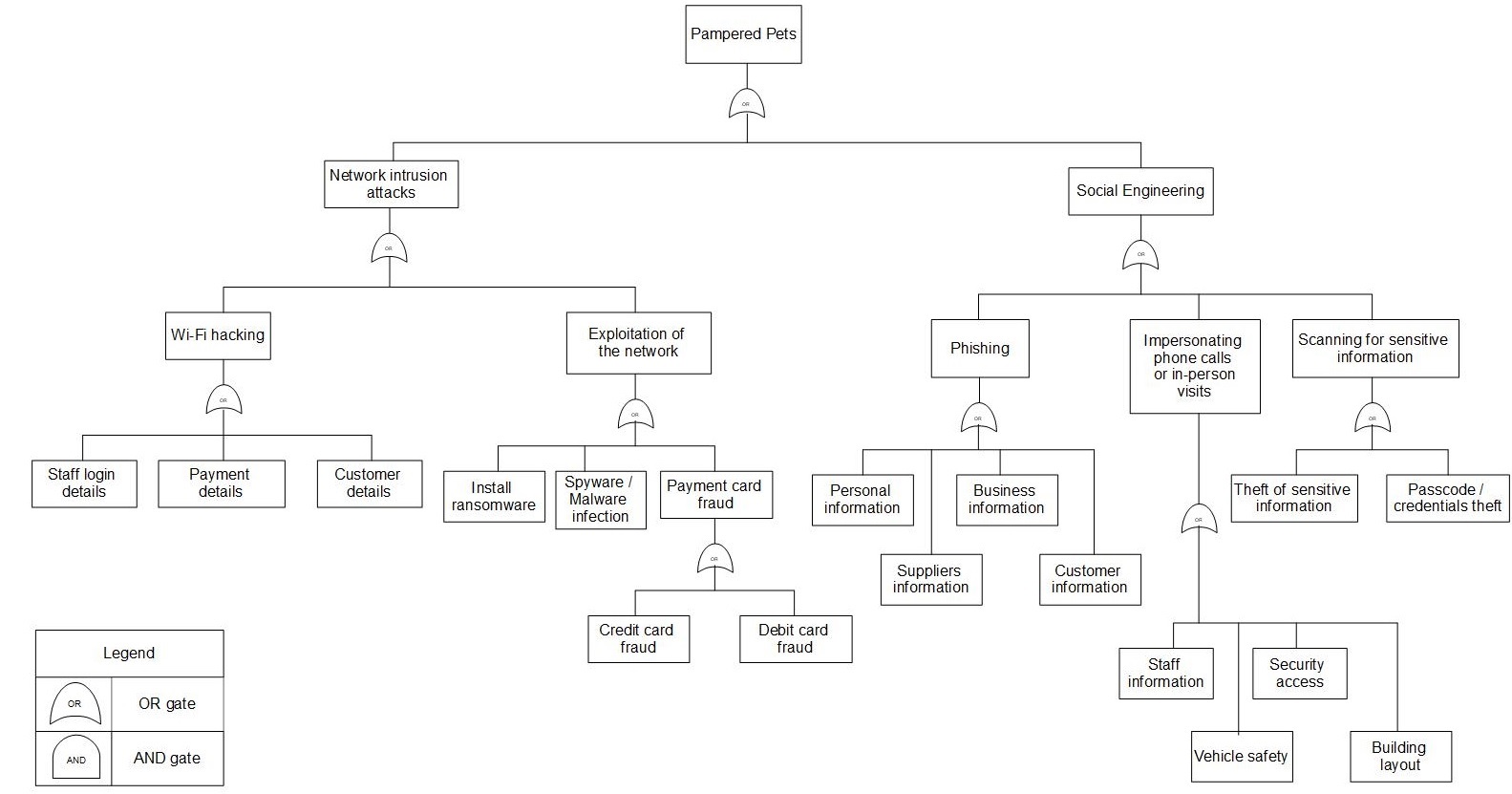
**Figure 2: Risk Matrix**

**3. Risk Assessment #1**

After brainstorming, a system diagram was developed to understand the current architecture (Figure 3). Attack Tree (Figure 4) scenarios were applied for the best results. The output is presented in Table 1, which also contains proposed mitigations to the existing threats.



**Figure 3: Current Architecture**

**Figure 4: Attack Tree**

| **Asset** | **Vulnerability** | **Threat** | **Mitigations** |
| --- | --- | --- | --- |
| Wi-Fi hub | Weak password protection  Network disruptions | Compromised Wi-Fi access point  Network attacks | Separate Wi-Fi network (one for staff, one for customers)  Firewalls on hubs/devices |
| Desktop computers | Weak password protection  Outdated software  Malware/spyware/phishing/ransomware  Unauthorised  modifications | Compromised access to hardware/software | Anti-virus software  Updated/patched software  Multi-Factor Authentication (MFA)  Company cyber security policies: BYOD and removable storage devices [1] |
| Card payment system | Outdated software  Unencrypted data | Credentials theft  Data leakage | Secure payment systems (online and physical) |
| Mobile phones | Weak password protection  Outdated software  Malware/spyware/phishing/ransomware | Identification theft  Phishing attacks | Updated/patched software  MFA  Strong password protection  The same as [1] |
| VAT payment software | Outdated software  Transaction/ order disputes | Unsafe encryption/decryption | Updated/patched software |
| Product database | Outdated software  Unauthorised access | SQL injection  XSS attacks | Firewalls  IDS/IPS  Data back-up and recovery plan |
| Staff | Shared login credentials  Intentional or unintentional insider threat  Lack of skill, knowledge, and training | Social Engineering  Front/back-office security | Separate Wi-Fi network (staff)  Staff training (malware/spyware/phishing/ransomware and password management)  The same as [1] |
| Customers | Theft/damage of computers and other devices  Staff disputes | Violence to staff | Separate Wi-Fi network (customers) |
| Building | Open/insecure doors/windows/gateways/locks | Damage to the goods/inventory/building  Adverse weather effects  Natural disaster | Back/front of the house CCTV  Protected entry |

**Table 1 – Risk Assessment #1**

**4. Risk Assessment #2**

Brainstorming led to the creation of the proposed system architecture (Figure 5) and asset identification (Appendix I), with assigned access classification (Appendix I). STRIDE was the main input for Table 4, which also includes mitigations.

| **STRIDE** | **Asset** | **Threat** | **Likelihood** | **Severity** | **Mitigation** |
| --- | --- | --- | --- | --- | --- |
| **S**poofing | Cloud infrastructure  Wi-Fi hub | DNS/IP spoofing | Medium | Medium | Implement DNSSec to protect DNS integrity  Use Ingress and Egress filtering (Kaspersky, 2022) |
| **T**ampering | E-commerce website  Inventory management | Upload malicious files | Medium | High | Auto-scan file upload integrity check.  Website should include CSRF tokens, and CSP headers (Jin et al., 2014) |
| **R**epudiation | Payment system  E-commerce website  Cloud infrastructure  Real-time analytics | System and data manipulation  Unauthorised actions, transfers, and creating admin users | Medium | High | System implementation of access logs, transaction logs, audit data and use SIEM to detect anomalies |
| **I**nformation Disclosure | User data  Payment data  Digital backup  Real-time analytics | SQL Injections  Disclosure of user and payment data | Medium | High | Access controls with the least privilege.  Data encryption, I.e., AES, RSA |
| Staff | Human error  Intentional theft | Low | High | Continuous training  Access controls |
| **D**enial of Service | E-commerce website  Cloud infrastructure  Physical stores | Botnet DDoS attacks  Natural disasters | Medium | Medium | Throttle requests from users  User WAF for application layers  Incident response planning |
| **E**levation of Privilege | Staff  Physical store | Unauthorized access to resources | Low | High | Apply the least privilege to access internal resources  Authentication and authorisation controls to handle resources |

**Table 2 – STRIDE for Risk Assessment #2**

Diagram

Description automatically generated

**Figure 5: Proposed Architecture**

**4.1 Proposed changes**

Proposed changes for implementing the digitalised store:

* Create an e-commerce website with a responsive web design which aligns with the company's reputation (Joyce, 2001).
* Use a cloud-based provider to improve the scalability, accessibility, and security whilst reducing the cost of self-hosting of web infrastructure (Al-Jaberi et al., 2015).
* Use Real-time analytics software for website traffic and customer behaviours (Simchi-Levi et al., 2018).
* Inventory management system to manage demand fluctuation (Patil & Divekar, 2014).
* Set up a back-office/ERP that allows the business to have a portal with an overview of its backend systems (Luttighuis and Biemans, 2000).
* Integrate a payment system from third-party services, i.e., PayPal, to allow secure handling of online purchases.
* Develop and execute an online marketing strategy to reach a wider audience and generate leads.

**4.2 Timeline for digital transformation**

Chart, timeline

Description automatically generated

**Figure 6 – Timeline**

**5. Summary of recommendations**

It is strongly recommended that digitalisation is carried out as part of the business expansion and for increased security, in particular:

1. Business recommendations:
2. Upgrading software and hardware architecture with network access segregation will keep the risks tolerable with improved mitigations.
3. Well-designed cloud-based e-commence website will improve the company's reputation and increase security.
4. Adding online marketing as an asset will widen the customer base and strengthen its online presence.
5. Also, conduct quantitative risk assessments to determine different losses the business can face and apply suitable mitigations.
6. Security recommendations:
7. Patched and updated systems with the latest security patches and updates will address vulnerabilities and reduce the risk of cyber-attacks.
8. Implement regular data backups for critical data and disaster recovery procedures to ensure business continuity in case of data loss or system failures.
9. Perform regular internal and external audits to ensure system compliance with GDPR (data protection) and PCI-DSS (secure payments).

**6. Conclusion**

Based on the research by Statista (2015) and recent surveys by Hyder (2021), it is expected that the application of digitalisation of Pampered Pets business could grow between 10% and 44%.

Furthermore, a digital transformation would support the data by Eurostat (2021), which says 72% of EU citizens are transitioning towards online shopping, vital to growing businesses and retaining customers. Therefore, digital transformation is strongly recommended.

However, certain risks and threats are tied to the change, and the mitigations and recommendations mentioned in this report must be carefully implemented before rolling out the whole business online to make it successful.

**References**

Al-Jaberi, M., Mohamed, N. and Al-Jaroodi, J. (2015) E-commerce cloud: Opportunities and challenges. In 2015 international conference on industrial engineering and operations management (IEOM) (pp. 1-6). IEEE.

Eurostat (2021) Online shopping ever more popular in 2020 - Products Eurostat News - Eurostat. Available at: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20210217-1#:~:text=In%20the%2012%20months%20prior,compared%20with%202015%20(62%25). [Accessed 04 April 2023].

Hall, H. (2023) Evaluating risks using quantitative risk analysis. Project Risk Coach. Available from: <https://projectriskcoach.com/evaluating-risks-using-quantitative-risk-analysis/> [Accessed: 31 March 2023].

Hyder, S. (2021). Available at: <https://www.inc.com/shama-hyder/how-brick-mortar-businesses-can-adjust-to-a-digital-landscape.html> [Accessed 12 April 2023].

Jin, X., Hu, X., Ying, K., Du, W., Yin, H. & Peri, G. N. (2014) Code injection attacks on html5-based mobile apps: Characterization, detection and mitigation, in ‘Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security’, pp. 66–77.

Joyce, R. (2001) Digitization, the internet, and electronic commerce. Futurics, 25(3/4), p.95.

Kaspersky (2022) IP spoofing: How it works and how to prevent it. Available from: <https://www.kaspersky.com/resource-center/threats/ip-spoofing> [Accessed 04 April 2023].

Luttighuis, P.O. and Biemans, F. (2000) ERP in the E-Commerce Era. Netherlands: Telematic Institute.

Nordlayer (2022) Cybersecurity Risk Assessment in 5 Steps. Available from: https://nordlayer.com/blog/cyber-security-risk-assessment/. [Accessed 05 April 2023].

Patil, H. and Divekar, B.R. (2014) Inventory management challenges for B2C e-commerce retailers. Procedia Economics and Finance, 11, pp.561-571.

Simchi-Levi, D. and Wu, M.X. (2018) Powering retailers’ digitization through analytics and automation. International Journal of Production Research, 56(1-2), pp.809-816.

Statista (2017) Technology & Telecommunications: Turnover growth of digital businesses compared to non-digital businesses from 2011 to 2015 in the United Kingdom (UK). Available from: https://www.statista.com/statistics/693219/digital-business-growth-compared-to-non-digital-business-in-the-uk/ [Accessed 04 April 2023].

Wolfman, S. (2023) Risk assessment methodology, Version 4. Available from: <https://coralogix.com/wp-content/uploads/2020/09/Risk-Assessment-Methodology.pdf> [Accessed 04 April 2023].

**Appendix I**

|  |  |  |
| --- | --- | --- |
| Asset | Asset Type | Classification |
| Wi-Fi access point (Wi-Fi hub) | Hardware | Public/Internal |
| Company computer (Workstation) | Internal |
| Personal phone | Personal |
| Back-office system | Service/application | Restricted |
| Payment system |
| Inventory management |
| Real-time analytics | Internal |
| E-commerce website | Public |
| Cloud infrastructure | Public/Restricted |
| User data | Data | Confidential |
| Digital backup |
| Staff | Human | Internal |
| Physical store | Building | Public |
| Online marketing | External service (external dependency) |

**Table 3 – Asset Identification**

|  |  |  |  |
| --- | --- | --- | --- |
| **Classifications** | |  | **Asset Types** |
| Confidential | Only senior management have access |  | Hardware |
| Restricted | Designated employees have access |  | Service/Application |
| Internal | All employees have access |  | Data |
| Public information | Everyone has access |  | Human |
| Personal |  |  | Building |

**Table 4 – Asset Classification**