RISK ASSESSMENT REPORT FOR PAMPERED PETS

The consulting firm conducted this exploratory risk assessment research to weigh the benefits and drawbacks of transferring the pampered dogs' daily activities to digital platforms. It is projected that global retail e-commerce sales will reach over 4.1 trillion dollars in 2024 and will continue to grow to previously unheard-of heights in the years to follow (Gelder, 2024). Since the advent of the internet in recent years, online shopping has become a crucial part of worldwide purchasing. Like many other industries, the buying and selling of commodities has undergone significant change (Cai and Cude, 2016). This report identifies medium-to-severe risks in areas including compliance, data and information security, and operational continuity. Questions from pampered pets will be addressed in this report, along with suggestions that may be implemented to mitigate the dangers that have been highlighted.

1. Risk Assessment Methodology Selected Methodology: NIST Cybersecurity Framework (CSF) Risk Management Approach

Justification for Selection

1. **Systematic Approach: The NIST CSF provides a structured method for identifying, analysing, and managing risks across five core functions: identify, protect, detect, respond, and recover *(Alraddadi, 2023)*.**
2. **Scalability: It is suitable for businesses of all sizes, making it an excellent choice for pampered pets *(Heiber & Farrow, 2024)*.**
3. **Industry Standard: recognised and widely accepted, ensuring adherence to best practices and regulatory compliance *(Walters et al., 2021)*.**

2. Proposed Changes in the Digitalisation Process

To modernise its operations and remain competitive, Pampered Pets could adopt the following digital tools and systems:

1. **E-commerce Portal: A platform to sell pet products and services online, offering customers a convenient shopping experience.**
2. **Enterprise Resource Planning (ERP) System: Integration of core business processes such as inventory management, customer relationship management (CRM), and accounting.**
3. **Online Marketing: Utilisation of SEO, social media campaigns, and email marketing to expand customer reach.**
4. **Pet-Care Blog: A dedicated space for sharing tips, updates, and engaging content with the pet owner community.**
5. **Mobile App Development: A user-friendly application for booking grooming services, purchasing products, or receiving pet updates.**
6. **Data Analytics Tools: Tools to analyse customer behaviour, preferences, and improve decision-making processes.**
7. **Cloud Storage Solutions: Secure and scalable storage for digital operations, customer data, and backups *(Relao & Santos, 2024)*.**

3. <u>Risk and Threat Modelling Exercise</u>

Risk Identification and Categorisation

Risk/Threat	Description	Likelihood	Impact	Mitigation Strategy
Cybersecurity Breach	Unauthorised access to customer data or financial records through the e-commerce portal.	High	High	Implement multi-factor authentication (MFA), encryption, and regular vulnerability assessments.
Downtime/Service Outages	Disruptions in the ERP system or e-commerce portal affecting business operations.	Medium	High	Use cloud-based systems with redundancy and maintain a service level agreement (SLA) with the provider.
Data Privacy Violations	Mishandling of customer data leading to non-compliance with GDPR or similar regulations.	High	High	Develop a robust data privacy policy, train employees, and implement data anonymisation techniques.
Resistance to Change	Staff reluctance to adopt new digital tools or systems, slowing down transformation.	Medium	Medium	Provide change management workshops, comprehensive training, and involve employees throughout the process.
Phishing/Social Engineering	Employees or customers falling victim to scams targeting login credentials or sensitive information.	High	Medium	Conduct regular cybersecurity awareness training and implement email filtering systems.
Overbudget Implementation	Costs exceeding estimates due to unforeseen challenges or scope creep.	Medium	High	Define clear project goals, regularly monitor progress, and allocate a contingency budget.
Loss of Customer Trust	Poorly implemented e-commerce portal causing dissatisfaction or security concerns.	Medium	High	Test platforms rigorously, ensure ease of use, and provide responsive customer support.
Third-Party Vendor Risks	Vulnerabilities in software or services provided by external vendors.	High	High	Vet vendors thoroughly, include robust security clauses in contracts, and monitor vendor compliance.

4. Threat Evaluation

Internal Threats

- **Insufficient employee training leads to unintended data breaches.**
- **Insider threats, including deliberate misuse of systems by staff *(Canham et al., 2020)*.**

External Threats

- **Cyberattacks ultimately target customer and financial data.**
- **Malware and ransomware attacks compromising IT infrastructure *(Bhadouria, 2022)*.**

Environmental/Operational Threats

- **Natural disasters or technical failures disrupt cloud services.**
- **Power outages affecting on-site operations *(Mohanty et al., 2024)*.**

5. **<u>Next Steps</u>**

1. **Develop a detailed risk mitigation plan: Address identified risks with actionable measures.**
2. **Test Digital Systems: Conduct penetration testing and usability trials to ensure system robustness.**
3. **Implement Continuous Monitoring: Use advanced tools to monitor anomalies and manage risks dynamically.**
4. **Engage stakeholders: Involve employees, customers, and partners in the digital transformation process to ensure alignment and trust.**

<u>Risk Assessment and Identification Report for the current state of Pampered Pets</u>

1. Risk Assessment Methodology

- **Selected Methodology:** Failure Modes and Effects Analysis (FMEA) (Subriadi, and Najwa, 2020)

Justification:

1. **Scalability:** FMEA is effective for small businesses with limited resources.
2. **Risk Prioritization:** Helps focus on high impact risks by scoring severity, likelihood, and detectability.

3. **Action-Oriented:** Provides actionable insights for mitigation, critical for Pampered Pets given its small size and limited technical infrastructure.

2. Risk and Threat Modelling Framework and Process

Framework: STRIDE Threat Modeling

Justification: STRIDE identifies diverse threats systematically (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) and is simple enough for a small business context (Landuyt, and Joosen, 2022).

Identified Threats and Potential Mitigations

Identified Threats and Potential Mitigations

STRIDE Category	Identified Threats	Likelihood	impact	Priority	Potential Mitigations
Spoofing	Unauthorized access to the wireless network	**high**	Moderate	**high**	Secure Wi-Fi with WPA3 encryption and restrict access to authorized devices only.
Tampering	Alteration of warehouse inventory spreadsheets or transaction	**medium**	**high**	**high**	Use password-protected files and regular backups to prevent unauthorized changes
Repudiation	Lack of logs to track user actions, leading to disputes over errors	**medium**	**moderate**	**medium**	**Implement basic logging systems on computers to track user activity and changes**
Information Disclosure	Unencrypted emails exposing sensitive business or customer information	**high**	**high**	**high**	Enable encryption for all emails and sensitive data transmitted over the network.
Denial of Service (DoS)	Wireless network disruptions due to overuse or external attacks	**low**	**high**	**medium**	Set up network monitoring tools to detect and address abnormal traffic patterns.

Recommendations

Pampered pets as a small business that is known to be crucial to the local community would greatly benefit from shifting their day-to-day activities online to increase sales and bring the business closer to the locals than ever before;

however, this concept is known to have its cons, which would be conveyed to the executive members of the team (Jones, 2014). According to statistics, global retail e-commerce sales are predicted to surpass 4.1 trillion dollars in 2024, and this amount is anticipated to rise to unprecedented levels in years to come (Gelder, 2024). As highlighted at the beginning of this report, staying put with the old technology in the business could also pose risks as there are outdated computers, which could expose the business to attackers. Secondly, it is a known fact that the use of spreadsheets can be categorised as being outdated and might not be able to keep up with growing corporate needs, which could cause operational problems in the long run.

Having answered significant concerns from the business in the report, the consulting firm would make the following recommendations to Pampered Pets on appropriate and positive roadmaps to achieving the goals of the business. Bearing in mind these suggestions are in line with the objectives of the company and its present capabilities:

- **It would be beneficial to the business to create a website with simple navigation that allows users to explore merchandise, place orders, and pay. It would be an immense difference as well if features such as subscription options for recurring delivery of pet food were incorporated.**

- **Reviews seen online are digital word-of-mouth; they improve your brand's visibility and attract more potential clients. (The, 2021). It would be advantageous to the firm to capitalise on customer reviews to increase trust, draw in new clients, and encourage current clients to post reviews online.**

- **Pampered pets would benefit from training its employees to detect vulnerabilities and basic security practices, as bad actors capitalise on this concept before systems are attacked.**

- **Pampered pets would benefit from investing in modernised IT infrastructure for real-time tracking.**

References

Aashi SINGH Bhadouria (2022). Study of: Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few... *ResearchGate*. [online] Available at: https://doi.org/10.29322/IJSRP.X.2022.p091095.

Alraddadi, A.S. (2023). Developing an Abstraction Framework for Managing and Controlling Saudi Banks' Cybersecurity Threats Based on the NIST Cybersecurity Framework and ISO/IEC 27001. *Journal of Software Engineering and Applications*, [online] 16(12), pp.695–713. Available at https://doi.org/10.4236/jsea.2023.1612036.

Cai, Y. and Cude, B.J. (2016). Online Shopping. *Handbook of Consumer Finance Research*, pp.339–355. Available at https://doi.org/10.1007/978-3-319-28887-1_28.

Canham, M., Posey, C., & Bockelman, P.S. (2020). *Confronting Information Security's Elephant, the Unintentional Insider Threat.* HCII 2020 Proceedings. Springer International Publishing.

Gelder, K. van (2024). *E-commerce Worldwide - Statistics & Facts*. [online] Statista. Available at: https://www.statista.com/topics/871/online-shopping/#topicOverview.

Jones, G. (2014). *Click.ology : what works in online shopping and how your business can use consumer psychology to succeed*. London: Nicholas Brealey Publishing.

Mohanty, A., Ramasamy, A.K., Renuga Verayiah, Satabdi Bastia, Sarthak Swaroop Dash, Cuce, E., T.M. Yunus Khan and Elahi, M. (2024). Power system resilience and strategies for a sustainable infrastructure: A review. *Alexandria Engineering Journal*, 105, pp.261–279. Available at https://doi.org/10.1016/j.aej.2024.06.092.

Ronnel Relao and Sharmaine, P. (2024). Paws and Reflect: Assessing the Impact of User Reviews and Ratings on Pet Food E-commerce Purchase Decisions. *SEISENSE Business Review*, 4(1), pp.118–131. Available at https://doi.org/10.33215/02vbn632.

Schmidt, A. and Wallace, K. (2024). *The Digital Transformation of Product Formulation*. *CRC Press eBooks*. Informa. Available at https://doi.org/10.1201/9781003385974.

Subriadi, A.P. and Najwa, N.F., (2020). The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment. *Heliyon*, *6*(1).

The, F. (2021). *How to manage your customer reviews*. [online] Fsb.org.uk. Available at: https://www.fsb.org.uk/resources-page/how-to-manage-your-customer-reviews.html [Accessed 25 Nov. 2024].

Van Landuyt, D. and Joosen, W., (2022). A descriptive study of assumptions in STRIDE security threat modeling. *Software and Systems Modeling*, pp.1-18.

Walters, D., Johnstone, R., Bluff, E., Limborg, H.J. and Ulrik Gensby (2021). Improving Compliance with Occupational Safety and Health regulations: an Overarching review: Literature Review.