**Risk Assessment Report for Pampered Pets**

Pampered Pets, a bricks-and-mortar business known best for their premium pet food. Pampered Pets are considering growth of their company through digitalization. This includes consideration for having an online presence for potential business growth, changing to an international supply chain for cost savings and providing online features to prevent potential loss of existing customers. Within this report, the options of digitalization of the company and maintaining the status quo will be weighed through the use of risk assessment and threat modeling.

**Part 1: Current Business Risk Assessment**

For the risk assessment of pampered pets as it currently stands, the National Institute of Standards and Technology’s (NIST) Special Publication 800-30 Revision 1” Guide for Conducting Risk Assessments” was chosen. This is due to NIST SP 800-30 being a structured and well documented risk assessment approach that allows for flexibility in the scope and analysis of risk. This assessment will be qualitative due to lack of numerical information. This assessment will make assumptions and statements based on information provided.

1) Identifying Assets:

**Technical Assets:**

* POS Computer
* Old Networked warehouse Computer with spreadsheet of warehouse deliveries and item locations.
* Wireless Hub and Gateway used by both computers and employees mobile devices
* Company Email for orders

**Information Assets:** Customer Data, Financial Records and Supplier Information.

**Intangible Assets:** Brand reputation for high quality pet food

2) Identifying Threat Sources:

* **Hackers**
* **Trusted Insider**
* **Competitors**
* **Environmental**

3) Identifying Potential Threats:

**Cyber Threats:**

* **Phishing attacks** to company email
* **Unauthorized Access** to customer and financial data
* **Wireless attacks**(Sniffing, Session Hijacking, Denial of Service, etc..)
* **Unauthorized Access of Web Gateway**(Default Credentials)
* **Exploits** on old, likely unpatched computers.
* **Insider Attack(Accidental or Intentional)**

**Operational Threats:**

* **Disruption to the supply chain**
* **Employee Errors** when entering data into spreadsheet

4) Identifying and predisposing conditions:

The following will contain assumptions of potential vulnerabilities based on information provided. In order to have a more comprehensive and accurate vulnerability list it is recommended to perform vulnerability scanning, penetration testing and review of configurations.

Technical Vulnerabilities:

* **Legacy Systems:** The old networked computer in the warehouse is likely to have an outdated operating system, unpatched software and outdated security measures making it vulnerable to attack.
* **Wireless Network:** Using the same wireless network for business operations and personal use by employees increases the attack surface and vulnerability to network attacks.
* **Default Credentials:** If the wireless hub and gateway are using default credentials, this poses a significant risk of unauthorized access.
* **Unpatched Systems:** Both the POS computer and the warehouse computer may have unpatched software vulnerabilities.

**Operational Vulnerabilities:**

* **Manual Processes:** Reliance on manual data entry for tracking warehouse deliveries can lead to errors and inefficiencies.
* **Supply Chain Dependency:** The business's dependence on local suppliers and employee vehicles for transporting ingredients is a vulnerability. Any disruption (e.g., vehicle breakdown, supplier issues) can significantly impact operations.

.

5) Threat Modeling (Overall risk based on assumed likelihood and impact)

|  | | SEVERITY | | --- | |  |  |
| --- | --- | --- | --- | --- |
| | LIKELIHOOD | | --- | | **1** | **2** | **3** |
|  | **LOW** | **LOW** | **MEDIUM** |
| **1** | **– 1 –** | **– 2 –** | **– 3 –** |
|  | **LOW** | **MEDIUM** | **HIGH** |
| **2** | **– 2 –** | **– 4 –**  **-Employee Errors**  **-Supply Chain Disruptions** | **– 6–**  **Unauthorized Access of Web Gateway**  **- Unauthorized Access to Data**  **- Wireless Attacks** |
|  | **MEDIUM** | **HIGH** | **HIGH** |
| **3** | **– 3 –** | **– 6 –** | **– 9 –**  **-Phishing**  **-Exploits on unpatched computers** |

6) Proposed Mitgations:

* Enforcing encryption of data at rest, while processing and in transit
* Enforcing Access Control Policies
* Implementing Antivirus, Firewall and Switched Network
* Patching All software
* Purchasing new pc’s
* User security training
* Performing Vulnerability Assessments and Scanning
* Adhering to PCI DSS
* Implementing an Incident Response Plan
* Implementing strong Password Policies
* Implementing MFA
* Obtaining a work vehicle

**Part 2: Risk Assessment of Digitalisation Process**

**Introduction:**

Pampered Pets, a small pet store, is considering digital transformation to enhance operations and expand market reach. This section outlines the risk assessment for digitalization, evaluating potential threats and risks and suggesting mitigation strategies.

**Selection of Risk Assessment Methodology**

**- Methodology:** NIST Risk Management Framework (RMF)

**- Justification:** The NIST RMF provides a structured approach to managing risks associated with digitalization, ensuring information security and regulatory compliance.

**Proposed changes for Digitalization: -**

**1-** **E-commerce portal**

**- Purpose:** Facilitate online sales and expand the customer base.

**- Benefits:** Increased sales and broader market reach.

**2-** **ERP System**

**- Purpose:** Integrate business processes.

**- Benefits:** Improved operational efficiency.

**3-** **Online Marketing**

**- Purpose:** Increase visibility through digital channels.

**- Benefits:** Enhanced brand presence.

**4-** **Cloud Computing**

**- Purpose:** Store data remotely.

**- Benefits:** Scalability and cost saving.

**5-** **Mobile App**

**- Purpose:** Provide a platform for orders and information.

**- Benefits:** Improved customer experience.

**Risk and Threat Modelling for Digitalization**

**1-** **Cyber Attacks**

**- Threat:** Haking, Phishing, ransomware.

**- Risks:** Financial losses and data breaches.

**- Mitigations:** Firewalls, anti-malware, security audits.

**2-** **Data privacy Issues**

**- Threat:** Unauthorized access to data.

**- Risks:** Legal consequences, loss of trust.

**- Mitigations:** GDPR compliance, encryption, multi-factor authentication.

**3-** **System Integration Challenges**

**- Threat:** Compatibility issues.

**- Risks:** operational disruptions.

**- Mitigations:** Thorough planning and testing, IT consultants.

**4-** **Technology Dependence**

**- Threat:** Over-reliance on digital systems.

**- Risks:** Continuity issues.

**- Mitigations:** Backup systems, disaster recovery plans.

**5-** **Reputation Risks**

**- Threat:** Negative Customer experiences.

**- Risks:** Loss of customers.

**- Mitigations:** Service monitoring, rapid response strategies.

**6-** **Supplier Dependence**

**- Threat:** Dependence on international suppliers.

**- Risks:** Supply chain disruptions.

**- Mitigations:** Diversify suppliers and quality checks.

**7-** **Regulatory compliance**

**- Threat:** Non-compliance with laws.

**- Risks:** Legal penalties.

**- Mitigations:** Legal consultation, compliance management systems.

**Recommendations**

Digitalization is recommended for pampered pets due to its potential to enhance business growth and efficiency. Implementing an e-commerce platform, ERP system, online marketing, cloud computing, and a mobile app can significantly benefit the business. Comprehensive risk management is crucial to mitigating associated risks.

**Involved changes**

**- E-commerce platform:** Extend Market reach.

**- ERP system:** Improve efficiency.

**- Online marketing:** Increase visibility.

**- Cloud computing:** Ensure data management.

**- Mobil app:** Enhance customer experience.

**Conclusion**

Digitalization, supported by robust risk management, offers significant opportunities for Pampered Pets. Ensuring staff training, effective communication, and continuous improvement will help the company navigate this transformation successfully, positioning It as a competitive player in the pet care industry.

References:

Django Stars, Jan 25, 2024. Measuring the impact: Risk Assessment in Digital Transformation. Linkedin.

Gina M. Raimondo, January 2023. Artificial intelligence Risk Management Framework (AI RMF 1.0). U.S. , nvipubs.

Lisbeth Karltorp, 22 May, 20217. Digital Transformation Strategies in Small Businesses. Sweden, Jonkoping University.

Leaman Crews, May 14, 2024. A Complete Guide to the NIST Risk Management Framework. EC-Coincil, Cybersecurity exchange.

National Institute of Standards and Technology (2012). Guide for Conducting Risk Assessments NIST Special Publication 800-30 Revision 1 JOINT TASK FORCE TRANSFORMATION INITIATIVE. [online] Available at: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>.

What is Information Security (InfoSec)?, hackerone.

Nazanin Ghodsian, May19, 2024. 5 Strategies of change Management Resulted by Digitalization. Neuroject.

Ychong Li, Qinghui Liu, November 2021. A Comprehensive review study of cyber-attacks and Cyber Security; Emerging trends and recent development. China, ScienceDirect.

‌