Pampered Pets Risk Assessment

Introduction

Pampered pets is a customer-centric business focussed on the quality of their products, specialists in face-to-face service. We begin by outlining the current technological risks involved in the business model and recommended mitigation strategies. We will suggest further technology implementation, and consider the associated risks of doing so.

Asset Identification

Category	Description	Use	Remarks
Hardware			
	PoS System	Sales transactions.	Adequate.
	Warehouse Computer	Inventory tracking.	Older model.
	Wireless Gateway/Hub	Network connectivity for computers/mobiles.	Functional.
	Cameras	Physical monitoring.	May be non-existent.
Software			

	Spreadsheet	Warehouse inventory management.	Outdated for expanded needs.
	Sales Recording	PoS transaction recording.	Meets current needs.
	Antivirus Software	Protecting computers from malware.	Needs updating.
Network Devices			
	Wi-Fi Routers/Extenders	Internet distribution.	Adequate, security concerns
	Firewalls	Network traffic protection.	May be non-existent/outdated.
Mobile Devices			
	Smartphones	Used by staff.	Connected to store Wi-Fi.

1. Current Operational Risk Assessment

Risk Assessment Methodology: Qualitative Risk Assessment.

Justification:

- Suitable for small businesses like Pampered Pets;

- limited availability of financial and operational data (Haneef, Riaz, Ramzan, Riaz, & Kausar, 2013);
- qualitative results are based on a person's judgement rather than a numerical scale (Altenbach, 1995);
- main stakeholders are non-technical, so will likely benefit from qualitative description of technical risks (Rot, 2008).

Risk and Threat Modelling:

The following evaluation uses part of OCTAVE-S approach which is a variant of OCTAVE: Manual by Alberts et al. (2005). It is

- asset-based;
- suitable for organisations looking to implement the security strategy themselves;
- specifically for smaller teams of 3-5 people.

(Lambrinoudakis et al., 2022).

Evaluation of Organisational Security Practices

Considering the assets identified in the previous section:

Operational Practice Area	**Spotlight Status**	**Justification**
Physical Access Control	Red	No key card/pad, security guard, alarms.
Monitoring and Auditing Physical Security	Red	No access logs, visitor records.
System and Network Management	Red	No firewall, IDS, segmentation, scanning.
Monitoring and Auditing IT Security	Red	No system logs, pen-tests.
Authentication and Authorisation	Yellow	Likely shared password without role-based-access-control (RBAC).
Vulnerability Management	Red	Out-of-date equipment, no patch/update schedule.
Encryption	Red	Spreadsheet data/customer emails unencrypted.

Security Architecture and Design	Red	Existing devices added ad-hoc without integration tests.
Incident Management	Red	No problem/incident management or disaster recovery.

STRIDE Analysis of Critical Assets

STRIDE used as it is a concise but effective model to discover major threats. It is used by Microsoft, and is endorsed by the UK National Cyber Security Centre (DSIT, 2023).

Threat Category	**POS Computer**	**Warehouse Computer**	**Wireless Gateway/Hub**
Spoofing Identity	Impersonation to gain unauthorised access and perform malicious actions.		Spoof MAC addresses or

			impersonate legitimate devices to gain unauthorised network access.
Tampering with Data	Modify transaction data to manipulate records or conduct fraudulent transactions.	Alter inventory records or cover up stock theft.	Intercept and manipulate wireless communications, altering network traffic.
Repudiation	Deny involvement, leading to disputes or financial losses.		
Information Disclosure	Sensitive payment information stored on the computer.	Critical inventory data stored on the computer.	Sensitive network traffic or credentials.
(DoS)	Disruption to POS operations and transactions.	Disruption to warehouse operations.	Disruption to wireless connectivity.
Elevation of Privilege	Exploiting software vulnerabilities allows unauthorised users to gain elevated system privileges.		

Mitigations:

- Keypads/cards, have system profiles (RBAC);
- CCTV cameras, alarm systems to deter theft/vandalism;
- Implement and configure firewall, IDS, and vulnerability scanning;
- Segment network for business, staff personal, and guest use;
- Employ regular patching, updates, penetration tests;
- Protect stored spreadsheet data and encrypt customer emails;

2. Digitalisation Process Risk Assessment

Methodology: Quantitative Risk Assessment.

This method quantifies the potential financial impact of risks, which is essential for calculating the return on investment in digital infrastructure (Aven, 2016).

Proposed Changes for Digitalisation:

- **E-commerce Portal:** To facilitate online sales and widen market reach.
- **ERP System:** For integrated inventory, sales, customer relationship management.
- **Online Marketing and Blogs:** enhance brand visibility and engage with a broader audience.

Risk and Threat Modelling:

Assumption:

Current Annual Revenue: $500,000

Assets and Their Financial Value:

- **Point of Sale System**: Estimated Value: $5,000
- **Warehouse Computer**: Estimated Value: $1,000
- **Wireless Gateway and Hub**: Estimated Value: $500
- **Security Cameras**: Estimated Value: $2,000

Analysis of the potential financial impact of risks identified:

1. **Data Breach (Financial Data and Customer Information)**:
    - **Probability**: Moderate (10% per year, outdated antivirus and security)
    - **Impact**: High ($25,000, potential fines, loss of customer trust, and remediation costs)
    - **Annual Loss Expectancy (ALE)**: Probability x Impact = 0.10 x $25,000 = $2,500
2. **Physical Security Breach (Theft/Vandalism)**:
    - **Probability**: Low (5% per year, physical breaches are less likely)
    - **Impact**: Moderate ($10,000, asset damage and replacement)
    - **ALE**: 0.05 x $10,000 = $500
3. **System Downtime (Due to Hardware Failure)**:
    - **Probability**: High (20% per year, older model of the warehouse computer)
    - **Impact**: Moderate ($5,000, lost sales/productivity)
    - **ALE**: 0.20 x $5,000 = $1,000

Using an attack tree threat modelling process. The main goal of the attack is "Compromise POS System." This goal can be achieved through various paths:

1. **Physical Access to POS**
    - **Steal POS Terminal**: Cost to attacker = $500, Success rate = 5%
    - **Install Hardware Keylogger**: Cost to attacker = $150, Success rate = 10%
2. **Remote Access to POS**
    - **Phishing Attack to Obtain Credentials**
        - **Send Phishing Emails**: Cost to attacker = $100, Success rate = 25%
        - **Employee Falls for Phishing**: Success rate = 30%

From the analysis, “installing hardware keylogger” and “phishing attack to obtain credentials” emerge as the most potentially successful attacks due to their higher risk rewards for attackers.

Mitigations should therefore prioritise:

- **Physical Security**: Enhance physical security measures at POS terminals.
- **Phishing Training**: Conduct regular employee training on recognizing and responding to phishing attempts.
- **Network Security**: Strengthen network security to detect and thwart unauthorised access attempts.
- **Update and Patch Management**: Regularly update POS software to rectify vulnerabilities.

Digitalization conclusion

- Establishing online presence might increase sales from existing base of $1,000,000 annually by as much as 50%.
- Using an ERP system to increase supply chain efficiency, supply costs could be reduced by up to 24% (Ferraiolo & Kuhn, 1992).
- Without these, Pampered Pets could lose a significant portion of its market to rivals who do (Chapple & Stewart, 2019).

3. Recommendations

Pampered Pets should pursue digitalization. This strategic move is supported by:

- The potential to significantly expand the customer base and sales through an e-commerce platform.
- Improved operational efficiencies and reduced long-term costs through an integrated ERP system.
- Enhanced market presence and customer engagement through sustained online marketing efforts.

Conclusion: The digitalization of Pampered Pets holds substantial promise for revenue growth and operational improvement, outweighing the manageable risks associated with the transition. With careful planning and execution, the store can successfully transition into a more resilient and profitable business model.

References

Alberts, C., Dorofee, A., Stevens, J. & Woody, C. (2005) Octave-s implementation guide, version 1.0. *Manuel electronique.* Pittsburg, PA: Software Engineering Institute, Carbegie Mellon University.

Altenbach, T. J. (1995) 'A comparison of risk assessment techniques from qualitative to quantitative', *ASME Pressure Vessels and Piping Conference.* Honolulu, Hawaii, 23-27 July. Livermore: Lawrence Livermore National Laboratory. 1-14.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research, 253*(1), 1-13.

Chapple, M., & Stewart, J. (2019). *CISSP Study Guide*. Sybex.

Coleman, M. E. & Marks, H. M. (1999) Qualitative and quantitative risk assessment. *Food Control* 10(4-5): 289-297.

DSIT (Department for Science, Innovation & Technology) (2023) Conducting a STRIDE-based threat analysis. Available from: https://assets.publishing.service.gov.uk/media/645bb8142226ee00130ae612/Conducting_a_STRIDE-based_threat_analysis.pdf [Accessed on 20 April 2024].

Ferraiolo, D., & Kuhn, R. (1992). Role-Based Access Controls. *15th National Computer Security Conference*.

Goodin, D. (2017). The essential guide to protecting your business against distributed denial of service attacks. *Ars Technica*.

Haneef, F., Riaz, Z., Ramzan, M., Riaz, S., & Kausar, R. (2013). Risk Management in SMEs: a systematic literature review and future directions. *European Journal of Business and Social Sciences, 2*(6), 76-88.

Lambrinoudakis et al. (2022) COMPENDIUM OF RISK MANAGEMENT FRAMEWORKS WITH POTENTIAL INTEROPERABILITY. Available from: https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks doi:10.2824/75906 [Accessed 17 April 2024].

Rot, A (2008) 'IT Risk Assessment: Quantitative and Qualitative Approach', World Congress on Engineering and Computer Science. San Francisco, USA, 22-24 October. Newswood Limited.

Shema, M. (2014). *Hacking Web Apps: Detecting and Preventing Web Application Security Problems*. Syngress.