A Digital Risk Assessment of Pampered Pets

Table of Contents

1. Introduction....3

2. Pampered Pets - Current....3

2.1 Current Digital Network....3

2.2 Current System Threats....5

2.3 Threat Mitigation....6

3. Pampered Pets Digitized....6

3.1 Expanded Network....7

3.2 Cloud Computing....10

3.3 Cloud System Threats....11

3.4 Cloud Threat Mitigation....11

4. Final Summary....12

5. Appendix I: Expansion Timeline....14

6. References....15

1. Introduction

This report aims to present a digital risk assessment of the business Pampered Pets to facilitate the identification and mitigation of digital risks that are unique to Industry 4.0 (Ghernaouti-Helie et al, 2011; Kuhn et al., 2009; Nikolic & Ruzic-Dimitrijevic, 2009). The assessment utilizes the OCTAVE-S model to outline critical assets and networking components, as these are essential for small enterprise success (Alberts et al., 2005), as well as the CAPEC-ATT&CK and STRIDE taxonomies, which provide a robust profile of network vulnerabilities (Chick et al., 2018; Bezerra et al., 2020). A final summary is provided recommending future digitization and security measures.

2. Pampered Pets - Current

2.1 Current Digital Network

Though Pampered Pets has a localized business model there exists a digital attack surface for potential security breaches (Figure 1):

- A wifi network for multiple devices
- A storefront PC with an email server and 3rd party transaction software
- A warehouse PC with an email server and Excel software

The network has five critical assets (Figure 2) in need of fortification against digital attack. Each asset contains sensitive information which could be disclosed, modified, or lost.

Strengths include:

- A localized supply chain
- Guaranteed product quality
- A loyal customer base

Weaknesses include:

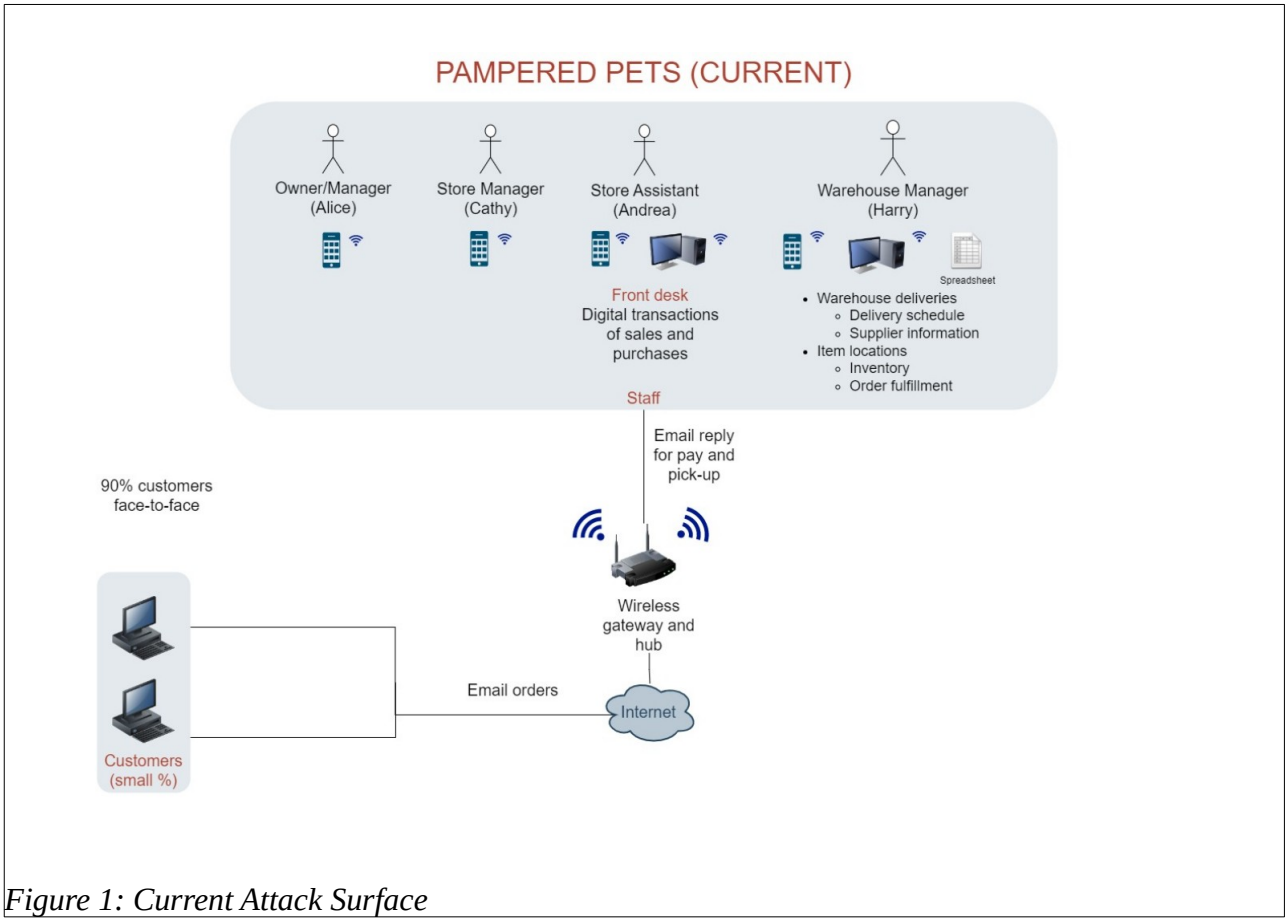

Figure 1: Current Attack Surface

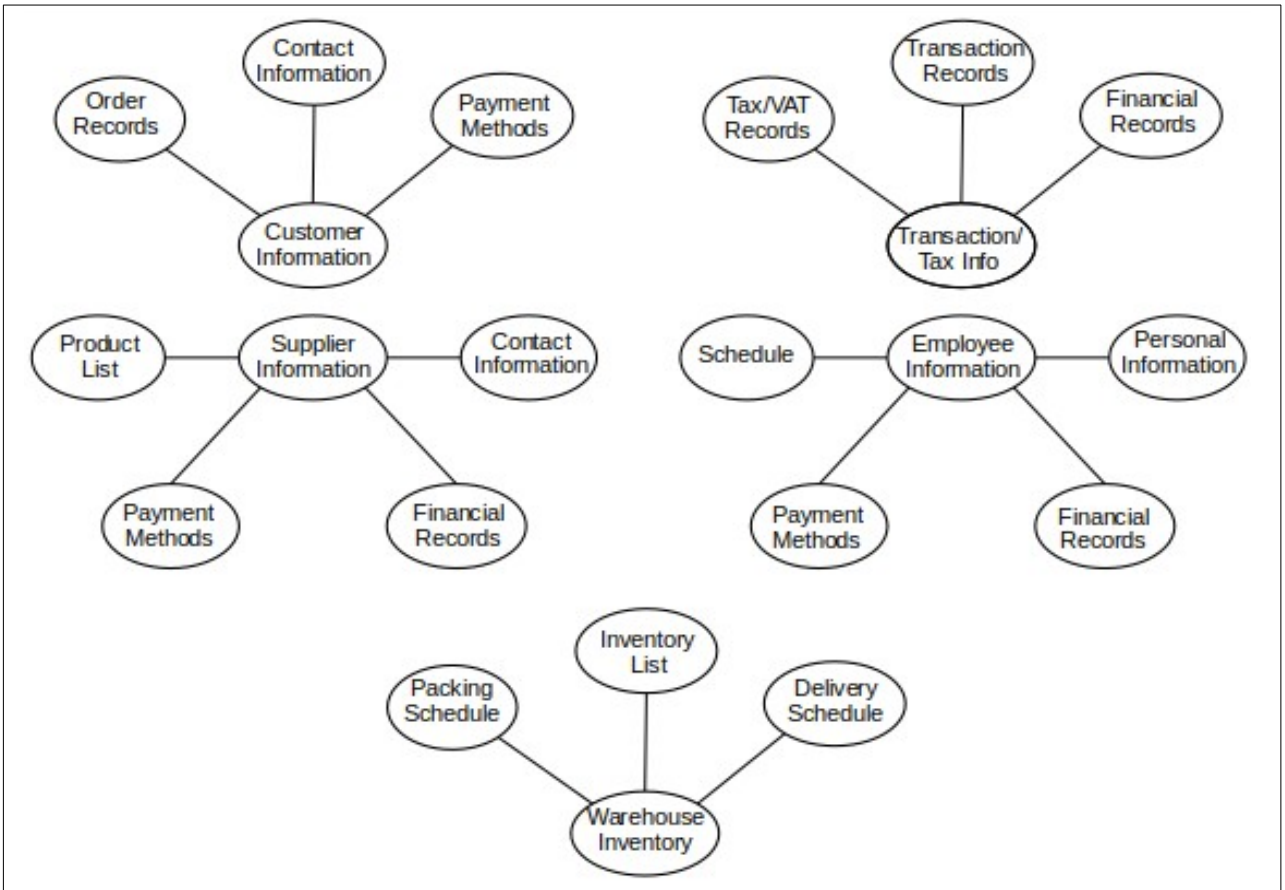

Figure 2: Current Critical Assets and Information

- No current network security controls
- Unpatched/old enterprise hardware/devices
- Personal devices can be connected to the main wifi network

2.2 Current System Threats

CAPEC-ATT&CK has a library of 177 possible attack vulnerabilities (Mitre, 2021); of these the current system is vulnerable to 128 attacks, or 72%. Five applicable attacks are listed below (Table 1):

Table 1: STRIDE Threat Profile - Current

Attack Name	Likelihood of Attack	Typical Severity	Required Skill Level	STRIDE Attack Type
Using Malicious Files	High	Very High	Low	System Tampering
Phishing	High	Very High	Medium	Personnel Spoofing
Privilege Abuse	High	Medium	Low	Elevation of Privilege
Footprinting	High	Very Low	Low	Information Disclosure
Flooding	High	Medium	n/a	Denial of Service

2.3 Threat Mitigation

The following (Table 2) should be implemented to prevent a catastrophic network breach (Alberts et al., 2005):

Table 2: OCTAVE Mitigation List - Current

Mitigation	Example
Employee Training	Phishing prevention, GDPR compliance

Security Strategy	Least Privilege Necessary
Security Management	Clear implementation of security regulations
Security Policy and Regulations	Access controls, authentication, session management, employee expectations
Collective Security Management	Employee input in security regulations
Continued Planning	Continued risk assessment
Authentication and Authorization	Username/password, employee ID
System & Network Management	Enforcement of updated network protocols
Encryption	Hash-256

3. Pampered Pets Digitized

3.1 Expanded Network

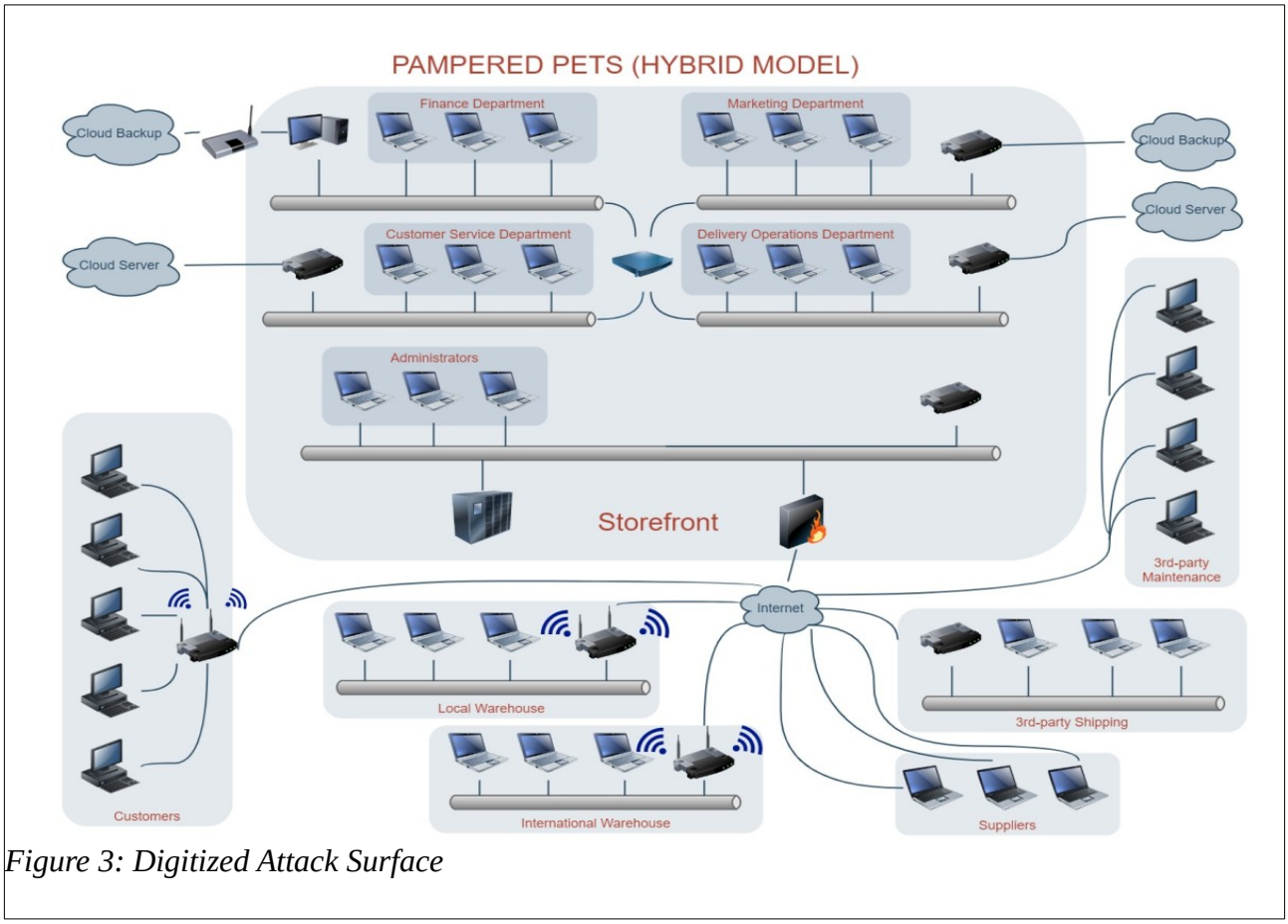

Figure 3: Digitized Attack Surface

If the Pampered Pets network were to expand, a hybrid model would allow the current local model to exist alongside an international supply chain (Figure 3):

- Cloud servers would connect operations and departments
- Departmental servers/back up would log and protect business data
- Third party operations would include suppliers, shipping, and server maintenance

The international supply chain would mirror the current local-supply model to ensure product quality (Alibaba, 2018; Donaldson, 2018; Grabler, 2019):

- International location hubs would be sourced for optimal shipping logistics
- Local farms would be sourced for high-quality products
- Products would continue to be packaged in nearby warehouses

Figure 4 provides a possible timeline in which this infrastructure expansion could be implemented (see Appendix I).

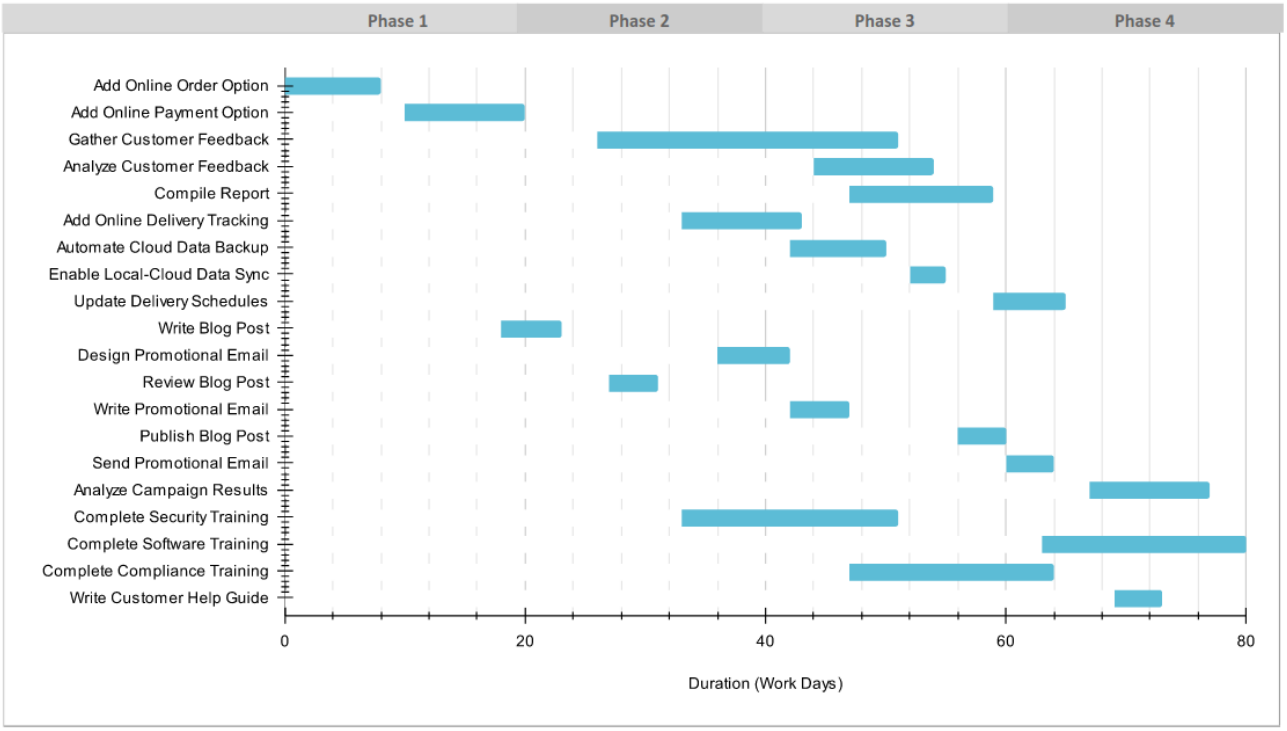

Figure 4: Digitization Timeline

It should be noted that implementation would result in:

- An increase in critical assets (Figure 5)
- Web application portal vulnerabilities (Figure 6)
- A need for compliance with online payment regulations (PCI, 2022)

Though this would expand the enterprise attack surface, previous qualitative assessments have shown that digitization can provide a:

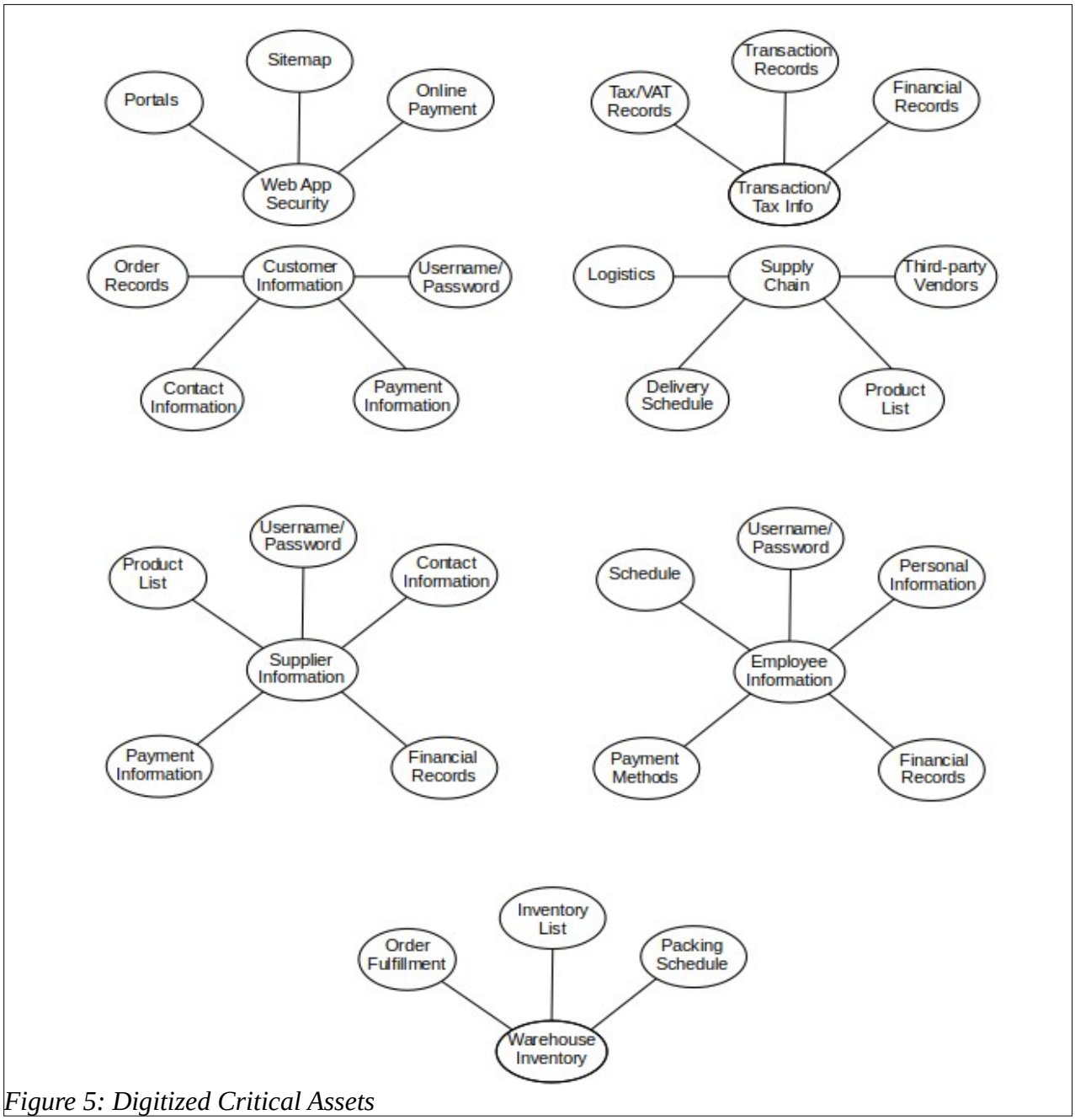

Figure 5: Digitized Critical Assets

- 40% higher online customer base (Gill & VanBoskirk, 2016)
- 24% reduction of local supply chain costs (Saini, 2020)
- 27% reduction of international supply chain costs (Giusti et al., 2019)

Additionally, digitization can help retain customers:

- 56% of clientele do not trust a business without a website (Businesswire, 2013)
- Trust is a key factor in customer retention (Listyawati et al, 2014).

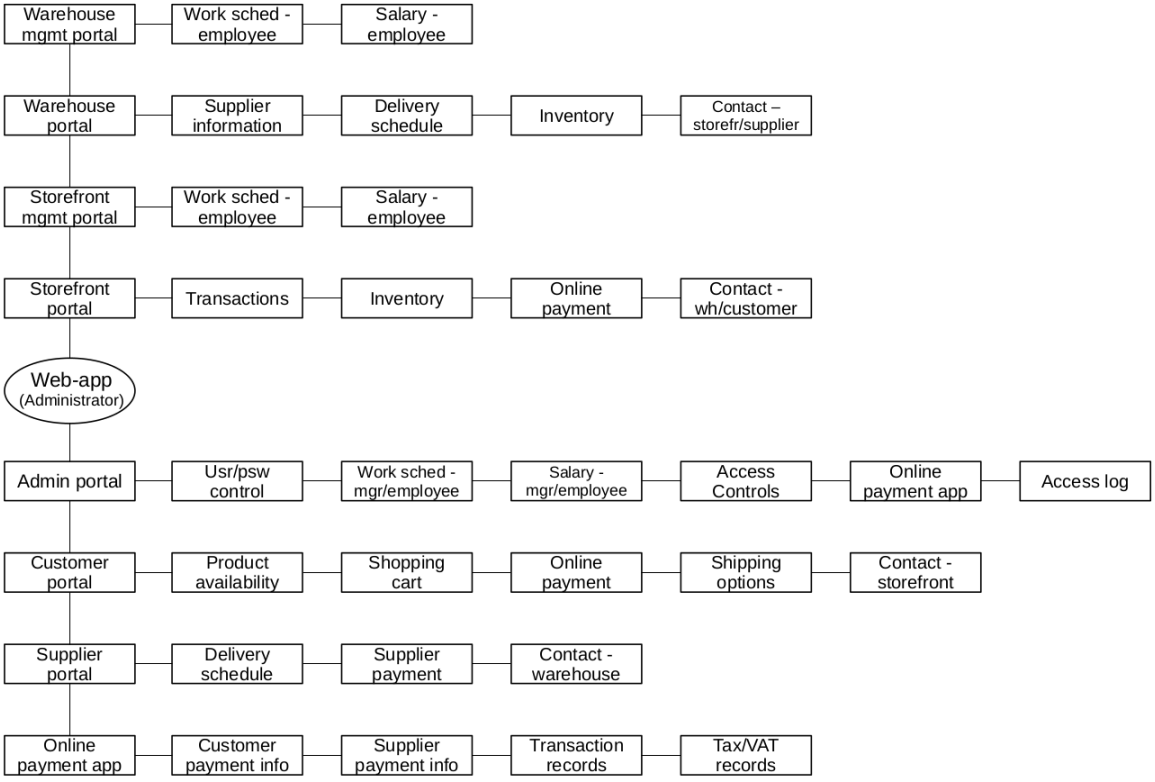

Figure 6: Web Application Attack Surface

3.2 Cloud Computing

The proposed utilization of cloud computing offers several digitized services of particular interest to small enterprises (Reckmann, 2022; Tharkal, 2022):

- Offsite data storage
- Data synchronization and restoration
- Database and web application hosting

- SaaS software delivery
- IaaS pay-as-you-go IT infrastructure

Strengths include:

- Remote data access
- Cost-efficiency
- Scalability
- No technical expertise required

Weaknesses include:

- Reliance on the Internet
- Compliance challenges in line with GDPR (Bygrave et al., 2020)
- Lack of control over data integrity
- Personnel training

3.3 Cloud System Threats

As Cloud computing would result in a public web application, all of the 177 vulnerabilities listed in CAPEC-ATT&CK are possible to execute (Mitre, 2021). Five applicable attacks are listed below (Table 1):

Table 3: STRIDE Threat Profile - Cloud

Attack Name	Likelihood of Attack	Typical Severity	Required Skill Level	Attack Type
Session Hijacking	High	Very High	Low	Tampering
Adversary in the Middle	High	Very High	Medium	Spoofing
Embedding Scripts within Scripts	High	High	Low	Tampering
Cache Poisoning	High	High	Medium	Information Disclosure

Repo Jacking	Medium	High	Low	Elevation of Privilege

3.4 Cloud Threat Mitigation

The following (Table 4) should be implemented to prevent a catastrophic network breach (Alberts et al., 2005):

Table 4: OCTAVE Mitigation List – Cloud

Mitigation		Example
In-House		
	Employee Training	Phishing prevention, GDPR compliance
	Security Strategy	Least Privilege Necessary
	Security Management	Clear implementation of security regulations
	Security Policy and Regulations	Access controls, authentication, session management, employee expectations
	Collective Security Management	Employee input in security regulations
	Continued Planning	Continued risk assessment
	Authentication and Authorization	Username/password, employee ID
	System & Network Management	Enforcement of updated network protocols
	Encryption	Hash-256
Cloud Computing		
	Monitor IT Security	Pen-testing
	Authentication and Authorization	Access controls, two factor authentication
	Vulnerability Management	Software patching, pen-testing
	Encryption	Hash-256
	Secure Architecture and Design	Have detailed explanation of system
	Incident Management	Have a security team to intercept/mitigate security breach

These mitigations in tandem appear to increase enterprise resiliency against vulnerabilities at both local and international levels (Alberts et al., 2005; Chu, 2015; Shoer, 2021).

4. Final Summary

While Pampered Pets' current business model has a number of benefits, the total vulnerability of the digital network prompts a recommendation to implement a hybrid model that will:

- Retain the current local storefront and warehouse
- Implement a similar supply-chain model internationally to ensure product quality
- Maintain the personalized ambiance of the current business model

While at the same time executing:

- Network diversification to expand exponentially
- Cloud computing for data security and web hosting
- Online payment methods for an increased customer base
- Enterprise security regulations in line with GDPR

Implementation of this model would allow customer growth, cost reduction, and product quality preservation. The company would be able to realize an international commerce and security potential without sacrificing local quality.

5. Appendix I: Expansion Timeline

Pampered Pets Digitalisation 2022-2023

Website e-commerce portal + brick & mortar = Hybrid model

* = an automatically calculated cell

	TASK NAME	START DATE	END DATE	START ON DAY*	DURATION* (WORK DAYS)	TEAM MEMBER
Sales: Online Order + Payment System						
Digital transactions, VAT, tax	Add Online Order Option	12/1	12/8	0	8	Andrea
	Add Online Payment Option	12/11	12/20	10	10	Harry
	Gather Customer Feedback	12/27	1/20	26	25	Alice
	Analyze Customer Feedback	1/14	1/23	44	10	Andrea
	Compile Report	1/17	1/28	47	12	Cathy
Logistics (Supply Chain)						
Warehouse deliveries, item locations	Add Online Delivery Tracking	1/3	1/12	33	10	Andrea
	Automate Cloud Data Backup	1/12	1/19	42	8	Harry
	Enable Local-Cloud Data Sync	1/22	1/24	52	3	Harry
	Update Delivery Schedules	1/29	2/3	59	6	Cathy
Marketing						
Social media, blogs	Write Blog Post	12/19	12/23	18	5	Alice
	Design Promotional Email	1/6	1/11	36	6	Andrea
	Review Blog Post	12/28	12/31	27	4	Harry
	Write Promotional Email	1/12	1/16	42	5	Cathy
	Publish Blog Post	1/26	1/29	56	4	Andrea
	Send Promotional Email	1/30	2/2	60	4	Harry
	Analyze Campaign Results	2/6	2/15	67	10	Cathy
Training						
Upskill staff, enable customers	Complete Security Training	1/3	1/20	33	18	All
	Complete Software Training	2/2	2/18	63	17	All
	Complete Compliance Training	1/17	2/2	47	17	All
	Write Customer Help Guide	2/8	2/11	69	4	Andrea

6. References

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005) OCTAVE-S implementation guide, version 1.0 (No. CMU/SEI-2003-HB-003). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Alibaba (2020) Local vs global sourcing: The pros and cons.Available from: https://seller.alibaba.com/businessblogs/pxxf9hls-local-vs-global-sourcing-the-pros-and-cons [Accessed 30 October 2022].

Bezerra, J., César, C., de Souza, N., & Hirata, C. (2020) Extending STPA with STRIDE to identify cybersecurity loss scenarios. *Journal of Information Security and Applications*, 55: 1-13.

BusinessWire (2013) "Weebly Empowers Millions to Start Something and Unveils All New Service for Creating Unique Sites," 2 May.

Bygrave, L., Dreschler L., Docksey, C., & Kuner C. (2020) *Commentary on the EU general data protection regulation (GDPR). A commentary*. Kettering: Oxford University Press.

Chick, T. A., O'Riordan, P., Scanlon, T. P., Shevchenko, N., & Woody, C. (2018) *Threat modeling: a summary of available methods.* Carnegie Mellon University Software Engineering Institute Pittsburgh United States.

Chu, W. (2015) 5 Ways to Mitigate Cloud Computing RisksAvailable from:https://www.neweggbusiness.com/smartbuyer/over-easy/5-ways-mitigate-cloud-computing-risks/ [Accessed 30 October 2022].

Donaldson, D.(2018) Why local pet food ingredient sourcing can pay off.Available from: https://www.petfoodindustry.com/blogs/7-adventures-in-pet-food/post/7377-why-local-pet-food-ingredient-sourcing-can-pay-off [Accessed 30 October 2022].

Ghernaouti-Helie, S., Tashi, I., & Simms, D. (2011) Optimizing security efficiency through effective risk management. In: *International Conference on Advanced Information Networking and Applications Workshops*, Biopolis, Singapore: 51-59.

Gill, M. and VanBoskirk, S. (2016) *The Digital Maturity Model 4.0 Measure: Your Maturity And Develop A Digital Transformation Plan*. rep. Forrester: 1–16.

Grabler, T.(2019) How to Reduce Supply Chain Cost and Avoid the Cost of Poor Quality. Available from: https://topo.cc/how-to-reduce-supply-chain-cost-and-avoid-cost-of-poor-quality/ [Accessed 30 October 2022].

Giusti, R. *et al*. (2019) "Sustainable and de-stressed international supply-chains through the Synchro-Net Approach," *Sustainability*, 11(4), p. 1083. Available at: https://doi.org/10.3390/su11041083

Kuhn, R., Liu, S., & Rossman, H. (2009). Understanding insecure IT: Practical risk assessment. IT Professional, 11(3): 57-59.

Listyawati, D., Rizan, M. and Warokka, A. (2014) “Relationship marketing and customer loyalty: Do customer satisfaction and customer trust really serve as intervening variables?,” *Journal of Marketing Research and Case Studies*, pp. 1–12. Available at: https://doi.org/10.5171/2014.724178.

Mitre. *Common attack pattern enumeration and classification* (2021) *CAPEC*. Available at: https://capec.mitre.org/data/definitions/658.html (Accessed: October 31, 2022).

PCI (2022) *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 4.0.* tech. PCI DSS.

Nikolic, B. & Ruzic-Dimitrijevic, L. (2010) Information System and Risk Reassessment. Issues in Informing Science and Information Technology (7): 191-207.

Reckmann, N. (2022) Cloud Computing: A Small Business Guide. Available from: https://www.businessnewsdaily.com/4427-cloud-computing-small-business.html [Accessed 30 October 2022].

Saini, N. (2020) How SMEs are reducing their business costs and increasing efficiency with technology. Available at:https://yourstory.com/smbstory/sme-msme-business-cost-technology/amp [Accessed 8 October 2022].

Shoer, M. J. (2021) How to mitigate cloud security threats. Available from: https://www.industrialcybersecuritypulse.com/iiot-cloud/how-to-mitigate-cloud-security-threats/ [Accessed 30 October 2022].

Tharkal, A. (2022) 5 reasons why SMEs should use Cloud-Based services. Available from: https://targetintegration.com/5-reasons-why-smes-should-use-cloud-based-services/ [Accessed 30 October 2022].