This document consists of a risk identification report for Pampered Pets who are a company that provides quality pet food to its clientele. This report shall include various risks that the company have in their current business setup with the IT infrastructure and the potential risks considered they digitalise their business.

Risk Assessment of Pampered Pets Current Setup

The table below summarizes the risks and solutions to mitigate the risks that Pampered Pets currently have with their current IT infrastructure. Appendix 1 shows a detailed table on how the asset risk value is derived along with the likelihood and rationale.

Asset	**Vulnerability Description**	**Mitigations**	**Risk Value**
Customer Data	Customer records not backed up, records incorrectly entered to the current spreadsheet	• Ensure data is backed up on a regular basis on an external drive	High
Company Emails	Losing emails by accidently deleting the email with other irrelevant emails and potentially missing important order emails from customers	• Plan for email backup	Low

Collection of ingredients from suppliers	Loss of valuable time to build on the business	• Provide a list of ingredients to the supplier and arrange for delivery of goods	Low
Network Security	High risk of compromising the network	• install a firewall, end point security	High
Trademark Registration for recipes	High risk of losing business	• Register the Trademark for the food formula / recipe • Register with Government agencies (www.uspto.gov, https://www.gov.uk/register-an-animal-feed-business)	Low

Risk and threat modelling exercise that enumerates and evaluates the current threats and risks to the business

Threat modelling is the process of using concepts to help think through risks (Shostack, 2014). Microsoft Security Development Lifecycle defined it as the technique that can use to aid identifying threats, attacks, vulnerabilities, and countermeasures that could potentially affect a system or an application Microsoft (2018). Threat modelling consist in five major steps that should enable to refine the threat model and reduce risks. These include.

- Define
- Diagram
- Identify
- Mitigate
- Validate

The chosen threat model for Pampered Pets is STRIDE, which is the most mature modelling method and was used by Microsoft in 2002 (Shevchenko et al, 2018).

Threat Type	Threats	Risks
Spoofing	Phishing and other Social Engineering Attacks	Spam emails to download a virus or malware onto the company computer to access sensitive data
Tampering	SQL Injection, Ransomware	Company data modified and unsecure network

Repudiation	DoS attack	Use of port-scanning utilities and carry out repudiation attack to change deliveries and item locations
Information disclosure	Integrity of Data	Company data being exposed to unauthorsied personnel
Denial of service	Receiving a lot of traffic and services are slow in processing	Applications taking long to respond causing delays in process (Take Your SSDLC Forward With STRIDE Threat Modelling, 2022)
Elevation of privilege	Granting access to unauthorsied personnel	Risk of a ransomware attack (The Dangers of Privilege Escalation | WALLIX Cybersecurity Simplified, 2022)

Risk Assessment of Pampered Pets Digitalised

The table below summarizes the risks and mitigations that Pampered Pets may have while digitalizing their business. Appendix 2 shows a detailed table on how the asset risk value is derived along with the likelihood and rationale.

Asset	**Vulnerability Description**	**Mitigations**	**Risk Value**
GDPR compliance	Customer Data breach	• Choose the e-commerce software which are GDPR compliant	High

PCI compliance	Loss of customer payment details	• E-commerce software must be PCI-DSS compliant • Use secure communication (https-SSL) during the payment processing	High
Supplier Background check	Due to vulnerable supplier, there may be a delay in production	• Regular background check • Quality of the products Financial Stability	Low
Distribution contracts and SLA	Due to vulnerable distributor shipping and handling may impact the quality of the product	• Negotiate and update the required shipment handling requirements during contract • Include SLA of delivery	Medium

Proposed Changes

Digitalising the organisation to increase the business growth and clientele is an important factor of consideration. As part of the digital transformation for Pampered Pets, its vital for the organisation to understand the four pillars. These include the following. (Marotta, 2022)

- Customer Engagement – businesses depend on a satisfied customer base

- Employee Empowerment - providing employees confidence by equipping them with knowledge and skills
- Optimise Operations- in order for Pampered Pets to provide customer experience the clients expect, it is important there is operational consistency
- Reimagine Products – for Pampered Pets to keep up with the innovation it's important to understand the market and improve on what Pampered Pets can offer to its customers

With the four pillars in consideration, we propose Pampered Pets to consider the following to help in the digitalisation process

- E-commerce website
- ERP- Enterprise Resource Planning
- CRM- Customer Relationship Management

STRIDE approach for Digitalization Business Risk

This is derived from the attackers' use of techniques that exploit commonly known vulnerabilities that may potentially have risks to the business. The following figure illustrates the potential risks.

Threat Type	Risk/Threat
Spoofing	Use of brute force attack to access customer session
Tampering	Tamper with the price or customer data
Repudiation	Access to the system logs and manipulating the logs
Information Disclosure	Extract customer sensitive information from the webserver
Denial of Service	Cause slowness, or crash by using all the server resources
Elevation of Privilege	Access at admin level of the network of the business

The below image shows the various methods on how the risks can be exploited

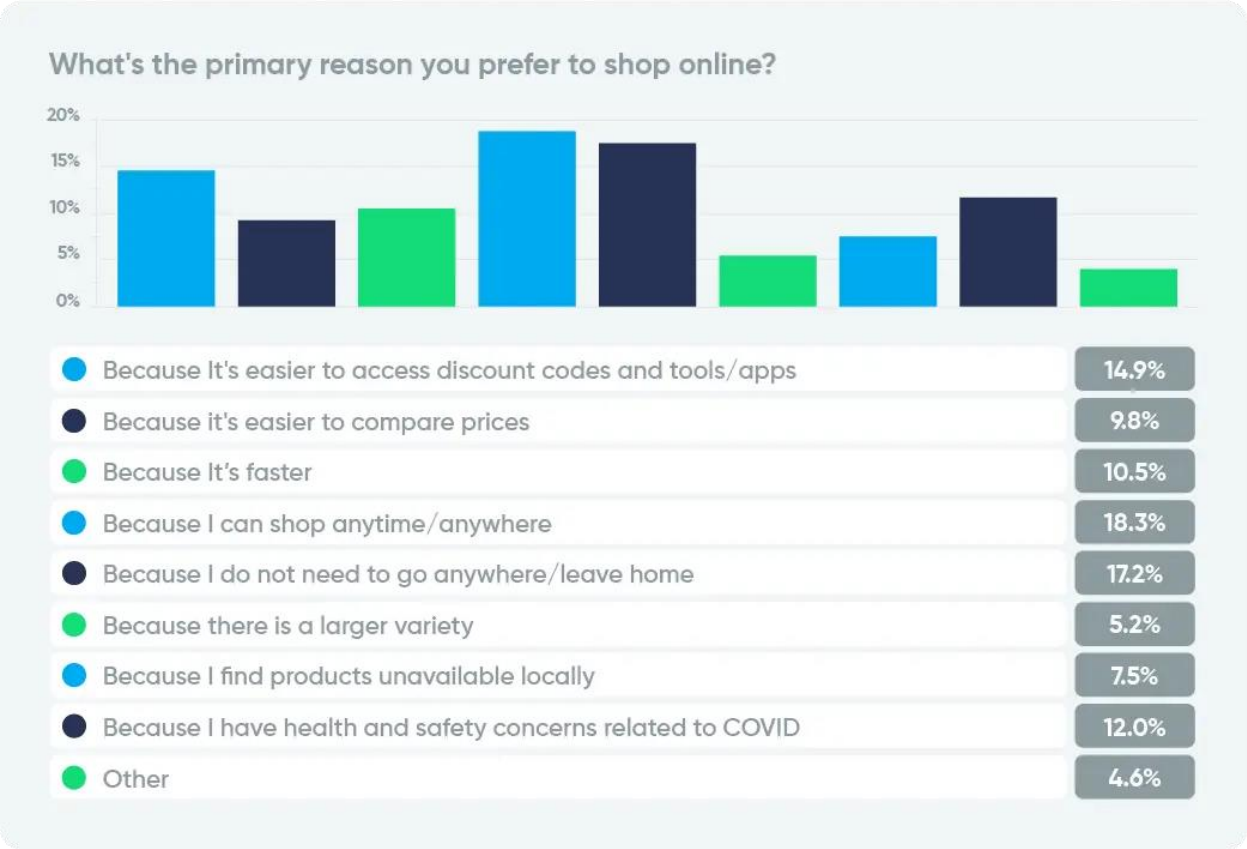
Threat Type	Threat type example	Digitalization business risk scenario
Spoofing	Attackers can brute force attack to access customer session	**Threat Agent**: Attackers use various methods to access a valid customer session **Attack Method**: 1. Login to e-commerce system 2. Attackers may steel the customer data or place orders without customer knowledge
	Attackers may set up cross site scripting and link to alternative sites and miss lead customers	**Threat Agent:** Attacker setup CSRF on e-commerce infected links and links to other sites **Attack Method:** 1. Attackers may redirect customer to a fake site or install malicious code
Tampering	Attackers may use vulnerable API on the webserver to tamper price or customer data	**Threat Agent**: Attackers tamper the project price by injecting malware **Attack Method:** 1. Attackers scan the webserver for week API programs 2. Discover un-patched vulnerabilities of the system to get access to the database

Repudiation	Attackers may gain access to the system logs and manipulating the logs to show the actions executed by malicious users in order to log wrong data to log files	**Threat Agent:** Attackers add the entries to server logs **Attack Method:** 1. Inject malicious data by controlling the user's session-id 2. Use server malicious codes and modify the logs RCE (Remote code execution) for eg. Log4J vulnerabilities
Information Discloser	Attackers extract customer sensitive information from the webserver	**Threat Agent:** Attackers use SQL injection technique to extract customer sensitive information **Attack Method:** 1. Vulnerable webserver code which allows attackers to execute code remotely 2. Insecure direct object reference (IDOR)
Denial of service	Attackers would cause slowness, or crash by using all the server resources	**Threat Agent:** Attackers use Distributed denial of service method and IDOR. Attackers use all the server resources and make the webserver not available for customers **Attack Method:** 1. By using IDOR references attackers run large SQL query 2. Brute-force login attack and lock the users accounts
Elevation of Privilege	Attacker gain admin level access	**Threat Agent:** Attackers use gain admin access of the webservers **Attack Method:** 1. Attackers may try with the default username and password of the servers 2. Access admin console 3. Gather customer credentials

(Abasi-amefon, N.D)

The growth of the business can have a growth with an online presence due to the following.

Marhamat (2022)



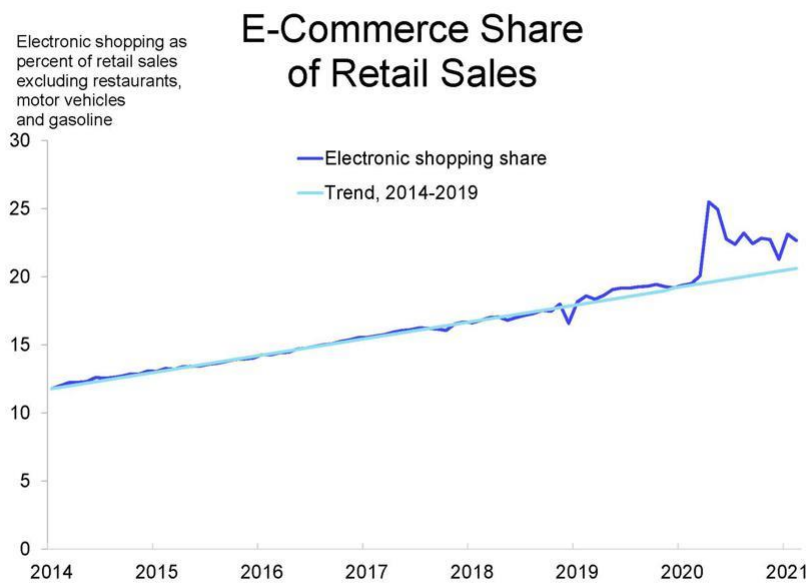
- Based on the survey by Raydient.com(C.Marhamat), 55.6% is preferring online vs in-store, so the online presence is critical to the business growth

- Customer can place order even after business hours and holidays

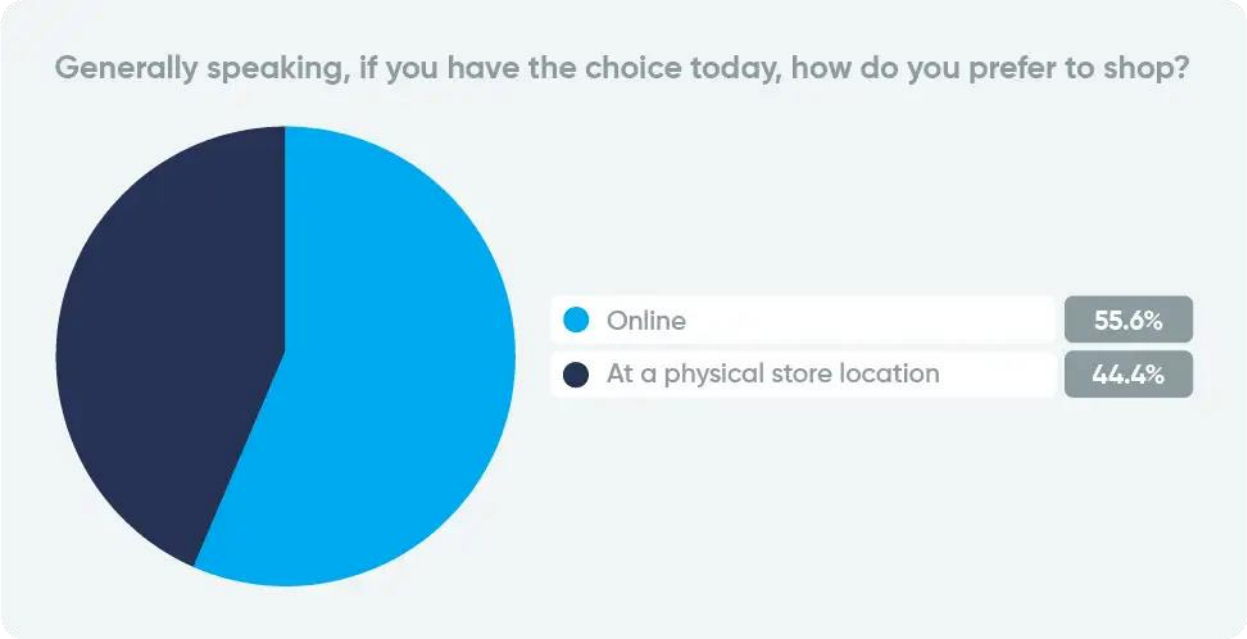
Additionally, by changing to an international supply chain, this can reduce the costs by up to 24% ensuring that the product distribution is beyond the local market. This can be done by the following. (James. N.D)

- Boosting domestic capabilities by increasing local sourcing can cut down the souring cost
- Global contracts with Shipping company reduces the shipping cost
- Strategically build the manufacturing site where the all the transport mode facilities (Road, Train, Cargo-Ship, Air)
- Optimize Distribution centers

Despite the business can potentially grow by 50% or reduce costs by changing to an international supply, the business may lose 33% of its customers by not integrating features.



Schnuer (2021)



(Marhamat, 2022)

- Based on the research by Suchner, Fobers.com the online business has grown 15-25%, and Based on the survey by Raydient.com(C.Marhamat) 56.6% of the customer prefer online.
- User friendly portal
- Secured payment gateway
- Multi factor authentication
- Loyalty services
- Product availability

Recommendation

We recommend that Pampered Pets should consider digitalizing their business and for the business to be digitalized, we recommend the following.

- A secure e-commerce website that increases online shopping
- A secure 3rd party payment gateway to be connected to the e-commerce platform (Anon. N.D)
- Secure network and wireless with Firewall, Web-application-firewall (WAF)
- Ensuring business practice and application meet the regulation standards of GDPR and PCI Security Standards
- Secure local government body regulatory approval for products if market goes beyond the current geographical boundary

Appendix

Appendix 1

Asset description		Asset value	Rationale for assigning the asset value	Vulnerability description	Likelihood of vulnerability being realised	Rationale for likelihood	Mitigations	Risk value
1	Customer Data	100	Without customer data, pampered pets would be unable to fulfil purchases to their regular customers	Customer records not encrypted, backed up, Customer records incorrectly entered to the current spreadsheet	0.8	Customer records not currently backed up is high as the organisation does not have the current recourses to back up customer data	1.Ensure customer data is backed up on a regular basis on an external drive	**80**

2	Company Emails	100	Provides a formal communication to the clients	Losing emails by deleting the email with other irrelevant emails and potentially missing important order emails from customers	0.1	The user of the account will be careful on deleting emails and has access to his/her emails	1. Plan for email backup	**10**
3	Collection of ingredients from suppliers	50	The management using their valuable time to collect supplies.	The management of Pampered Pets are to lose valuable time to build on the business	0.7	The management to waste valuable time is high as the management currently requires going to the supplier to collect the ingredients	Provide a list of ingredients to the supplier and arrange for delivery of goods	**35**

4	Network Security	100	The network security is important for the current daily tasks to take place	High risk of compromising the network	0.8	The likelihood of the network security is high as the current wireless gateway is unsecure	install a firewall, end point security (patching of OS, Anti-virus, antimalware protection)	**80**
5	Trademark Registration for recipes	100	Any animal feed products have to be registered and certified by government	High risk of losing business	0.1	The likelihood of competitor copying the product, Gov compliance issue	1. Register the Trademark for the food formula / recipe 2. Register with Government agencies (www.uspto.gov, https://www.gov.uk/register-an-animal-feedbusiness)	**10**

Asset Value Key	
1	Low
50	Medium
100	High

Risk Value Key	
0-49	Low
50-75	Medium
76-100	High

Appendix 2

Asset description		Asset value	Rationale for assigning the asset value	Vulnerability description	Likelihood of vulnerability being realised	Rationale for likelihood	Mitigations	Risk value
1	GDPR compliance	100	Without customer data, pampered pets would be unable to fulfil purchases to their regular customers	Customer data breach	0.9	Customer data may breach due to the application vulnerability	1. Choose the ecommerce software which are GDPR complient	**90**

2	PCI compliance	100	PCI-DSS compliance would allow the customers to purchase online	Customer Credit card information leak	0.9	Customer credit card data my breach due to the application vulnerability	1. E-commerce software must be PCI-DSS complient 2. Use secure communication (https-SSL) during the payment processing	**90**
3	Supplier Background check	50	Poor quality may result in customer satisfaction, Supplier finicial background etc	Due to vulnerable Supplier, there may be a delay in production	0.3	Supply chain is critical for the business	1. Regular background check 2. Quality of the products 3. Financial Stability	**15**

4	Distribution contracts and SLA	100	Distributor contracts and SLA are critical for on-time delivery	Due to vulnerable Distributor shipping and handling may impact the quality of the product	0.5	Chances of product mishandling are high, on time delivery tracking is essential	1. Negotiate and update the required shipment handling requirements during contract 2. Include SLA of delivery	**50**

Asset Value Key		**Risk Value Key**	
1	Low	0-49	Low
50	Medium	50-75	Medium
100	High	76-100	High

References:

- Marotta, D., 2022. *Digital Transformation in Retail: Why It's Important & How to Achieve It – Hitachi Solutions*. [online] Hitachi Solutions. Available at: <https://global.hitachi-solutions.com/blog/digital-transformation-retail-is-important-now/> [Accessed 9 September 2022].
- Anon, (N.D) Repudiation Attack Available from https://owasp.org/www-community/attacks/Repudiation_Attack [Accessed Sep 09 2022]
- Jinson, V (2022) Ecommerce Security Available from : https://www.getastra.com/blog/knowledge-base/ecommerce-security/ [Accessed Sep 11 2022]
- Nsrav, et.al (N.D) Denail of service Available from https://owasp.org/www-community/attacks/Denial_of_Service [Accessed Sep 11 2022]
- Affia A (N.D) Security Risk Management of E-commerce Systems Available from https://core.ac.uk/download/pdf/237084476.pdf [Accessed Sep 08 2022]
- Microsoft (2018). Microsoft Security Development Lifecycle Threat Modelling. [online] Microsoft.com. Available at: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling.
- Shostack, A. (2014). Threat modeling: designing for security. Wiley.
- Shevchenko, Nataliya, et al. Threat modeling: a summary of available methods. Carnegie Mellon University Software Engineering Institute Pittsburgh United States, 2018.

- Cynance. 2022. *Take Your SSDLC Forward With STRIDE Threat Modelling*. [online] Available at: <https://www.cynance.co/stride-threat-modelling-6-steps-to-secure-apps/> [Accessed 14 September 2022].
- WALLIX. 2022. The Dangers of Privilege Escalation | WALLIX Cybersecurity Simplified. [online] Available at: <https://www.wallix.com/blog/the-dangers-of-privilege-escalation/> [Accessed 16 September 2022].
- Anon, (N.D), PCI Compliance guide [online] Available from: https://www.pcicomplianceguide.org/faq/ [Accessed Sep 10 2022]
- Calvin,S (2021) Brick-And-Mortar Retail Is Bouncing Back Available from: https://www.forbes.com/sites/calvinschnure/2021/03/18/brick-and-mortar-retail-is-bouncing-back/?sh=6a8c560bd0f4
- Bobby, M (2022) State of Consumer Behavior 2022. Available from https://www.raydiant.com/blog/state-of-consumer-behavior-2022 [Accessed Sep 16 2022]
- Margot, J (N.D), Supply Chain Resilience (SCR) during pre-Brexit and Covid-10 Available from : https://warwick.ac.uk/fac/sci/wmg/business/supply_chain_resilience_hub_report_-_final.pdf [Accessed on: 16 Sep 2022]