University of Essex Online

Subject Name: Security and Risk Management August 2022

Assignment: Development Team Project: Risk Identification Report

Description: Pampered pets sell pet food to local users, Using ingredients from local suppliers. Employs four members of Staff and has a small digital footprint.

Team Name: Cyber Masters

Tutor: Douglas Millward

Students: Deepak Sidhar

Demian Berisford-Maynard

Gokul Kurunthasalam

Jonathan Ajodo

Table of Contents

Introduction

Risk assessment entails procedure for locating dangers, assessing any risks they may pose, and then emplacing feasible control measures to get rid of or minimize them. It is a key function of any enterprise as it helps in creating an awareness of risk. the Team adopted the STRIDE and OWASP methodology for risk identification.

Question 1 - Risk Assessment of Existing Business

A comprehensive, hybrid methodology consisting of both OWASP, and STRIDE was selected. These frameworks when utilized in unison, provide a holistic and symbiotic formula that form a quintessential basis for any modern risk assessment.

All entry and exit points of the existing business model, as well as their associated vulnerabilities or threats were assessed and addressed in detail. Suitable mitigative countermeasures are indicated and consequently explained.

1. A. I). - STRIDE Analysis

STRIDE an acronym which stands for 6 security risk categories, which are:

- Spoofing - This identifies risk with authorisation and determines if login credentials of users are being used by someone else to log into the system.
- Tampering - This prevents unauthorised modification of data.
- Repudiation - This ensures if a security breach occurs this can be proven and traced.

• Information Disclosure - This ensures that sensitive data is not exposed to individuals who are not authorised to access the data.

• Denial of Service - This attack stops users from being able to use the system.

• Elevation of Privileges - This threat identifies if someone has been able to access something or perform something that they should not have the authority/ permission to do.

[Peeple, K, 2015]

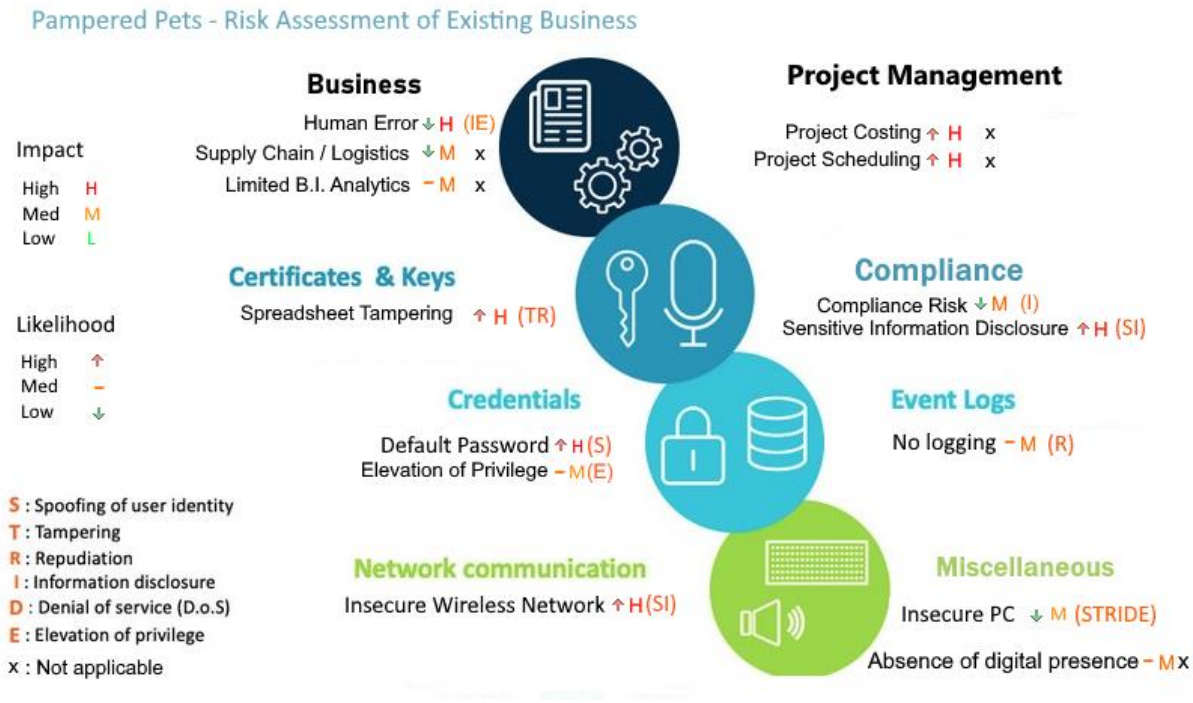

Fig 1 - STRIDE diagram of Pampered Pets

1. A. II). - OWASP Analysis

The following is an OWASP orientated analysis of all factors (both internal and external) that may influence the impacted risk of the current business model. These

will later be utilized in determining the proposal for a defensive solution. The model is broken down into three categories, The first is to gather information about the system. The second stage is to determine the risks and to rank them in order of importance and the final stage is to mitigate the risks using a framework [OWASP, 2022]

External Dependencies: Components that are not part of the application's code but could endanger it.

ID	Description
1	Availability of E-mail services
2	Dependency on local suppliers for raw material
3	Spreadsheet vulnerability
4	Internet Service Provider faulty

Entry Points: Entry points specify the interfaces that allow potential attackers to communicate with or provide data to the program.

ID	Name	Description	Trust Levels
1	Wifi Access	Wifi needs to be secure	Anonymous user
2	SMTP Port 25	All mailing will be carried out on port 25	User with Invalid Login Credentials

3	Spreadsheet	Anyone can access the Spreadsheet and modify	Read and write privileges and access for users and staff.
4	Physical Entry	Able to access the shop floor	Allowing anyone access.

Exit Points: When attacking the client, exit points may be helpful.

ID	Name	Description
1	Email Service	Ensure Access control is granted to staff members
2	Wifi Access	Ensuring only privileged access is possible
3	Exposing vulnerabilities if any of the spreadsheet	Data Breach GDPR (Breach of Data Protection)

Assets: The system must contain objects or areas of interest to the attacker; these things are referred to as assets.

ID	Name	Description	Trust Levels
1	Customer Details	Details of customers purchase -	Staff

2	Valid Login	Valid user login credentials for the spreadsheet	Staff
3	Wi-Fi	Access for staff and maintaining network	Staff

Fig 2 - Data Flow Diagram of Existing Business

1. C). - Risk and Corresponding Mitigations of Existing Business

Risk	Mitigative Solution
Spoofing (↑H)	Introduce firewalls (↓ L)
Ensure Wireless Security Policies (↑H)	Ensure Wireless Security Policies (↓ L)
Spreadsheet Tampering (↑H)	Convert to Secure Database (↓ L)
Repudiation/Logging absent (⁻ M)	Utilize Industry Standard Logging API's (↓ L)
Sensitive Information Disclosure (⁻ M)	Encrypt and Hash data (↓ L)
Elevation of Privilege(⁻ M)	Ensure Least privilege authorization (↓ L)
Project Costing(↑H)	Use BI Analytics to determine Costs (⁻ L)
Project Scheduling (↑H)	Use AI to assist in Project Scheduling (↓ L)
Supply Chain/Logistics/Manual Process (⁻ M)	Automate and validate Logistics (↓ L)
Absence of Digital Presence (⁻ M)	Have secure public facing website (↓ L)
Compliance Risk (↓M)	Periodically Audit system (↓ L)
Human Error (↓H)	Automate with BPM Controls (↓ L)
Limited Business Intelligence/Analytics (⁻ M)	Apply a Secure Solution (↓ L)

Question 2 - Risk Assessment of Proposed Digital Business

2. A) - Risk Methodology

Cybersecurity solutions are best designed with industry Best Practices in mind. After much thought, the OWASP Risk Methodology was adopted, due to its Peer-Reviewed nature, and comprehensive framework.

OWASP promotes the foundations for accountability, and as a Cyber Security firm, we wish to be accountable in our risk assessment of the proposed solution for Pampered Pets.

2. B). - List of Proposed Changes for Digital Transformation

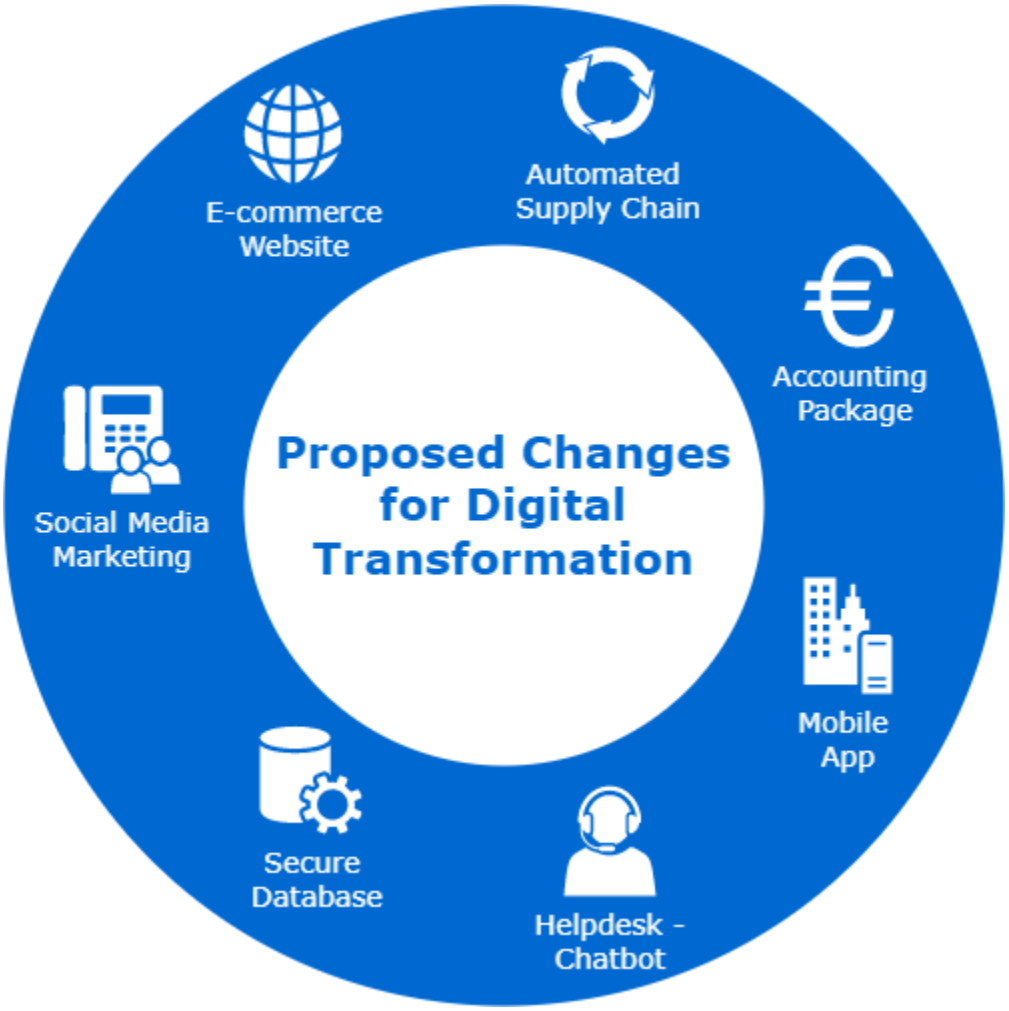

Fig 3 - Digital Solution to Current Business

2. C. I). - Risk and Threat Modelling

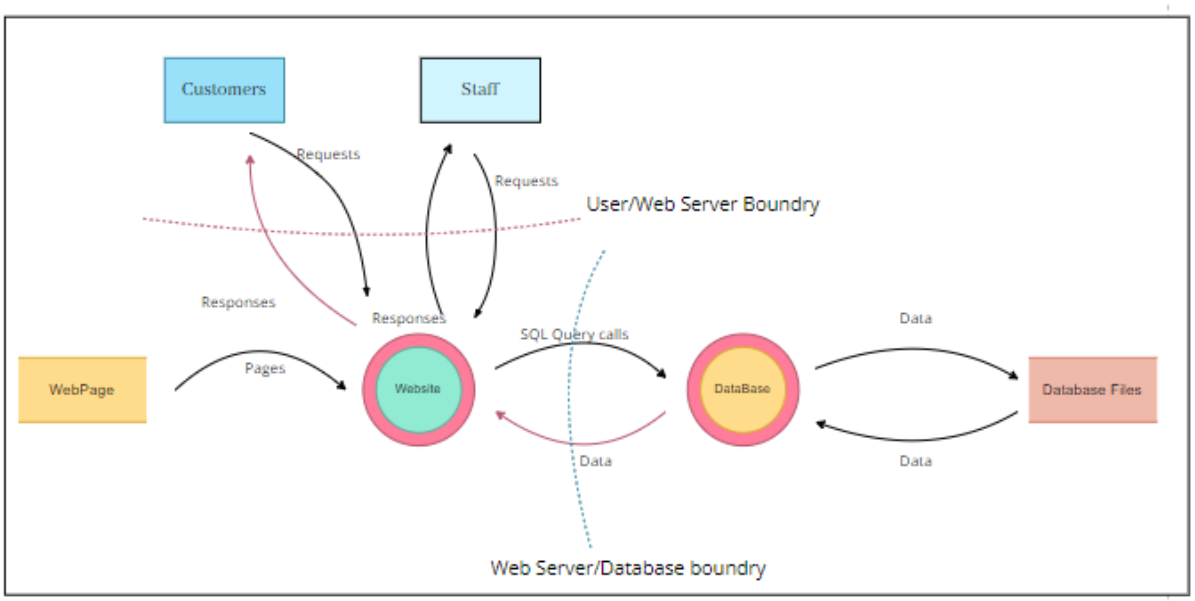

Fig 4 - Proposed Architecture without Security recommendations

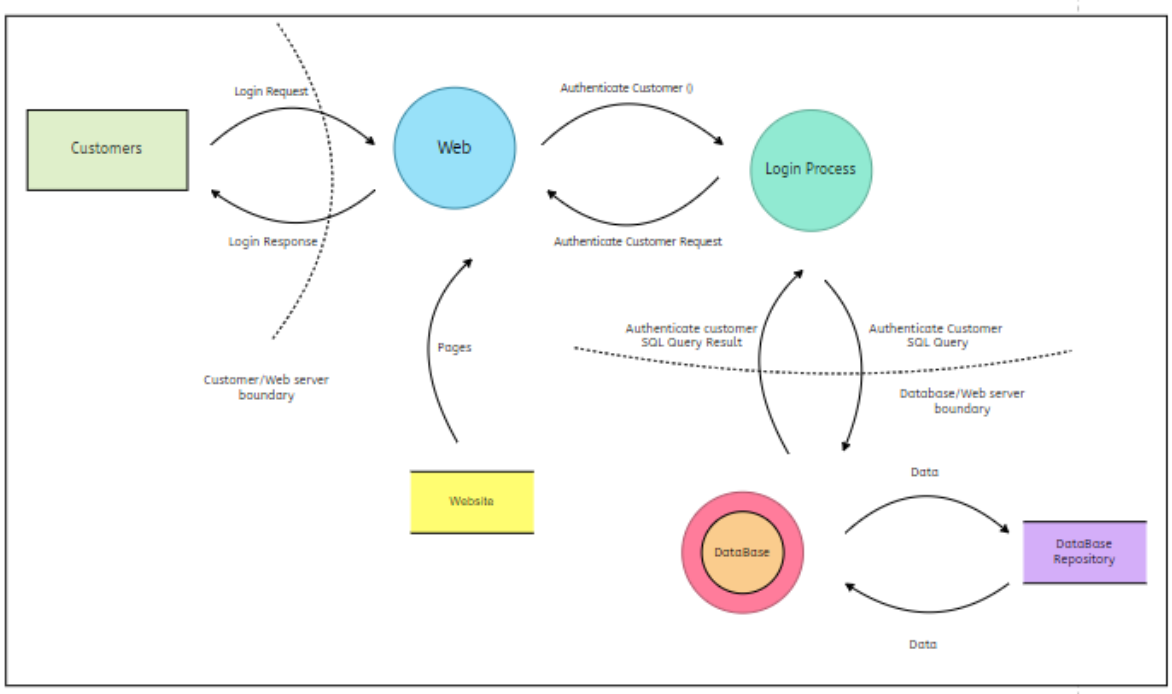

Fig 5 - Proposed Authentication Solution

2. C. II) - Examples of 3 Prominent Risks

Risk Information sheet			
Risk ID: Q2_R_CRM01	Date: 3 Sep 2022	Prob: 80%	Impact: High
Description:	CRM has little to no Authentication (by default)		
Context:	Newly implemented Customer Relationship Mangement system		
Mitigation techniques:	Enable Authentication, strong logging and best practices		
Contingencies:			
Current status	In development / Under review		
Originator:	Cathy	Assigned:	Cyber Security Team

Risk Information sheet			
Risk ID: Q2_R_GDPR01	Date: 10 Sep 2022	Prob: 60%	Impact: High
Description:	GDPR Compliance - leaking of personal information		
Context:	Database has clear text of all customer details, providing a legal risk		
Mitigation techniques:	Database Encryption of sensitive fields, stronger Web App security		
Contingencies:			
Current status	In development / Under review		
Originator:	Cathy	Assigned:	Cyber Security Team

Risk Information sheet			
Risk ID: Q2_R_FIN01	Date: 3 Sep 2022	Prob: 80%	Impact: High
Description: PCI DSS / Payment Gateway compliance			
Context: A secure payment portal must be used to mitigate online fraud and theft			
Mitigation techniques: Utilize a standard 3rd party payment portal, with a valid certificate			
Contingencies: Utilize an Electronic Funds Transfer, and retain manual accounting reconciliations			
Current status: In development / Under review			
Originator: Finance Department		Assigned: Cyber Security Team	

2. D). - Mitigative Solution

Risk	Mitigative Solution
Open Network (↑ H)	Firewall (↓ L)
Exposed Network Endpoints (↑ H)	Strict Whitelisting Firewall Rules (↓ L)
No Network Monitoring (↑ H)	Intrusion Detection/Prevention Systems (↓ L)
No Packet Filtering (¯ M)	Reverse Proxy Web Server (scrubbing/filtering packets) (↓ L)
Sensitive Information Disclosure (¯ M)	Secure Logging (↓ L)
Default Authentication/Elevation of Privilege (↑ H)	Remove Default Accounts (↓ L)
Clear Text Information / GDPR Leak (¯ H)	Comprehensive Encryption Standards (¯ L)
Outdated System (¯ M)	Periodic Revisioning (↓ L)
Total System Failure (¯ M)	Segregated/Secure VM Hosting with Backups (↓ L)
Payment Theft and Fraud(↑ H)	Secure Banking Gateway (↓ L)

Question 3 - Benefits of an Online Business

If Cathy markets her website on social media, she could potentially see exponential growth far exceeding 50%. This is dependent on a few factors, such as couriering the products outside of her vicinity, as well as adequate branding (Brown, 2012; Brynjolfsson & Smith, 2000).

Import duties can potentially increase costs, so utilizing an international supply chain must be approached with caution (Cappariello et al, 2018).

During the COVID lockdown, many consumers migrated to e-commerce platforms that could deliver directly to their doorsteps. Having an online presence will significantly reduce any risk of losing customers in similar adverse situations (Li et al, 2022).

Conclusion

Online presence and digitalization are critical to the growth of Pampered pet, and it is beyond having just a website. It also entails digital transformation of the business, having social media accounts and blog, which enhance social engagement. In the modern world, failure to connect with others could result in isolation and stunted growth. Furthermore, online presence provides 24 hours accessibility unlike a store; hence, customers can buy products after normal working hours. The opportunity for growth through online presence and digitalisation could be well illustrated by Amazon's growth. The contemporary businesses involve complex interactions between clients, suppliers, and organisations across international borders. For Pampered pet to succeed in this ecosystem, the business would require connectivity along not only roads, rail, and sea, but in telecommunications, financial markets and information-processing to enhance its supply chain management. In summary, every potential facet of risk has been assessed and addressed. Although nothing can ever be 100% risk free, every effort has been taken to mitigate these risks, in an effective and responsible manner.

References

Brown, E. (2012) *Working the crowd: Social media marketing for business*. BCS, The Chartered Institute.

Brynjolfsson, E. & Smith, M.D. (2000) Frictionless commerce? A comparison of Internet and conventional retailers. *Management science*, *46*(4) : 563-585.

Cappariello, R., Damjanovic, M., Mancini, M. & Vergara Caffarelli, F. (2018) EU-UK global value chain trade and the indirect costs of Brexit. *Bank of Italy Occasional Paper.*

Li, S., Liu, Y., Su, J., Luo, X. & Yang, X., (2022) Can e-commerce platforms build the resilience of brick-and-mortar businesses to the COVID-19 shock? An empirical analysis in the Chinese retail industry. *Electronic Commerce Research* : 1-31.

OWASP. (2022) *Threat Modelling Process*. Available from: https://owasp.org/www-community/Threat_Modeling_Process

[Accessed 08 September 2022]

Peeple, K. (2015) *STRIDE Threat Model*. Available from: https://dzone.com/articles/stride-threat-model#:~:text=Repudiation%20threats%20are%20associated%20with,to%20trace%20the%20prohibited%20operations

[Accessed 07 September 2022]