GROUP – 03

Development Team Project: Executive Summary

Module Name - Security and Risk Management March 2023

Word Count - 1024

Risk assessment before digitalization

A. Selection of a risk assessment methodology

'Pampered pets' is a Micro enterprise under the European SME category, which has less than 10 employees and an annual turnover under EUR 2 million (Pačaiová et al., 2013). Since we (consultant team) are uninformed of the company asset's value and loss in dollar value for each asset, the most appropriate methodology for a risk assessment is '*qualitative risk assessment'*. The qualitative method is used for risk analysis for several reasons, including simplicity of understanding and application across all areas and levels of the business, and the lack of proper numerical data or resources to undertake a quantitative study (Crotty and Daniel, 2022).

B. Risks and threat modelling exercises

A standard list of possible risks to the current business

- Unauthorized data or system access
- Unauthorized access to data or a system
- Unauthorized data disclosure
- Unauthorized data or system modification
- Unauthorized data or system destruction/loss

Attack Trees is the best option since it gives a formal and methodical means of explaining how a system can be threatened or attacked and represents various attack vectors against a system. The root node reflects the attacker's aim, while child nodes represent various paths to that goal. Each child node indicates a condition that validates the parent node (Matt, 2022).

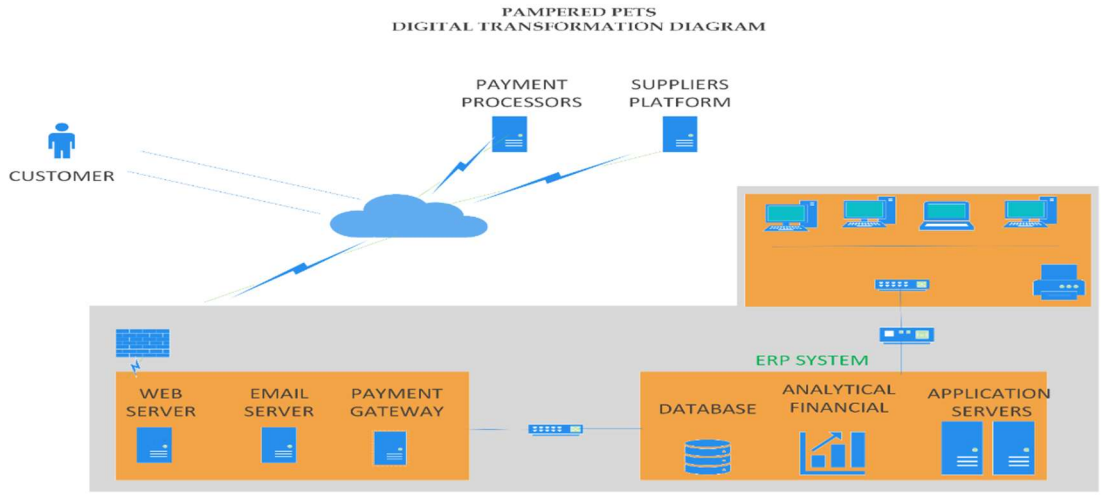
C. List of potential mitigations to the identified risks and threats.

A priority list should be developed to rank each risk based on the probability of occurrence and the severity of its impact on the business. Then, to mitigate the risks and vulnerabilities, a strategy and action plan should be developed. These include initiatives such as data protection policies and technology disaster recovery strategies. Using cloud storage so that the data is physically distinct from the business location, using antivirus software and ensuring all IT equipment are on the latest version (Hardware and software). Most popular operating systems now include a firewall, so it is only a matter of turning them on (National Cyber Security Centre, 2020).

Risk assessment after digitalization

A. The proposed Digital transformation for Pampered Pets business

The following diagram shows the proposed change to perform the required digital transformation.



The digitalization process of Pampered Pets business will include.

- Fully functional and response website that provide items description, prices, account creation for customers, ordering and order tracking.
- Online payment functionality that accepts most payment cards.
- ERP system that includes HR, financial applications, stock management and sales
- Applications to orders items from suppliers.
- Local networks separated from the two other networks where employees can perform their daily tasks and connect to other functionality.

B. Selection of a risk assessment methodology

Qualitative risk assessment methodology will be used, since we do not have the value of assets, associated risk history, and loss for each asset in dollar value. Risk matrix can be created by using the guidelines outlined in NIST SP 800-30 (Guide for Conducting Risk Assessments, 2012).

C. Threats and Mitigations

This initial risk assessment was conducted using the guidelines outlined in the NIST SP 800-30, Guide for Conducting Risk Assessments1. A QUALITATIVE approach will be utilized for this assessment. Risk will be determined based on a threat event, the likelihood of that threat event occurring, known system vulnerabilities, mitigating factors, and consequences/impact to mission.

Identification of threats

	Threat	Description	Denial of Service	Destruction	Unauthorized Modification	Unauthorized Disclosure
	Natural Threats					
1	Fire/Smoke in Pampered Pets daya center.	An accidental or intentional fire could damage system equipment or facility.	√	√		
2	Acts of Nature	Hurricanes, tornadoes, flood according to the location of Pampered Pets business	√	√		√
	Human Threats					
3	Espionage/Sabotage	Espionage is the intentional act of or attempt to obtain confidential information stored in Pampered Pets data storage. Sabotage is premeditated destruction or malicious modification of Pampered Pets' assets or data.	√	√	√	√
4	Theft/Pilferage	Theft is the unauthorized removal of computer equipment or media. Pilferage is theft of property by personnel granted physical access to the property.	√			√

Threat		Description	Denial of Service	Destruction	Unauthorized Modification	Unauthorized Disclosure
5	Hacking/Social Engineering	Software may be modified intentionally to bypass system security controls, manipulate data, or cause denial of service. Social engineering is the human-to-human interaction in which a hacker gathers data for use in modifying or manipulating the system.	√		√	√
6	Malicious Code	Malicious software such as viruses or worms may be introduced to Pampered Pets' system, causing damage to the data or software.	√	√	√	√
7	User Errors/Omissions	Pampered Pets's application and support system components may be inappropriately modified or destroyed due to unintentional administrator or user error.	√	√	√	√
8	Eavesdropping/interception	Intentional unauthorized access to confidential information through technical means (sniffing/interception) or by personnel having some level of system access but not having a need to know (eavesdropping)				√
9	Data Integrity Loss	Attacks on the integrity of Pampered Pets' system data by intentional alteration. For example changing the order / price / customer information in Pampered Pets systems.			√	
10	Misuse/Abuse	Individuals may employ system resources for unauthorized purposes.	√	√	√	√

- Natural threats such as Fire/smoke, Hurricanes, tornadoes, and flood according to the location of Pampered Pets business can cause damage to equipment.
- Human threats such as theft, misuse of the systems by employees and cyber threats such as espionage, hacking, malicious code, or user error/omissions which can cause data loss and control of the system.
- Environmental and physical threats such as power disruptions and hardware (equipment's) failures which can shut down the entire system.

Potential mitigations

Threat Event		Mitigation
1	Fire/Smoke in Pampered Pets daya center.	*Install and Maintain Fire Control and Suppression Systems* - **Install a sprinkler, foam system, or other fire control and suppression system** - **Install fire alarms and smoke detectors** - **Establish and promote a fire safety plan and an evacuation plan**
2	Acts of Nature	**Mitigate hurricane: boarding up windows and doors, placing sandbags outside building openings, and installing a backup power system to keep all critical assets working.** Mitigate flood: use **floodplain protection** **The second option will be to buy inssurance**
3	Espionage/Sabotage	*Implement encryption system*
4	Theft/Pilferage	*Implement strict access control system* *Use system auditing and log* *Physical access control system*
5	Hacking/Social Engineering	*Install firewall / IPS / IDS* *Employee training and awerness*
6	Malicious Code	*Install antivuris and antimalware*
7	User Errors/Omissions	*Implement data verification and validation system* *Use auditing and journals* *User education and training*
8	Eavesdropping/interception	*Encryption* Using packet filtering configure routers and firewalls to reject any packets
9	Data Integrity Loss	*Implement Data loss prevention (DLP)* *Buy Software as a servuce (SAAS) cloud*
10	Misuse/Abuse	*Implement Need to know access*

Installing fire alarms and smoke detectors with a fire safety plan can minimize the damage to equipment, business must be insured by an insurance company. In case of cyber threats, keeping all data secured by using encryption, authentication, firewalls and updating all software to the latest versions. Keeping backup power plans (uninterruptible *power* supply) and cloud can keep the system working.

Summary of Recommendations

Based on our analysis and considering the rapidly changing market environment, we strongly recommend that Pampered Pets undergo a digital transformation to expand its business, improve internal processes, and adapt to customers' evolving needs. The adoption of digital and mobile technology will ensure business growth and resilience by following the steps:

1. Pampered Pets must develop an online presence by establishing a user-friendly website, engaging social media presence, and an e-commerce platform to reach a more extensive customer base, facilitate online orders, and attract new customers.
2. Optimize internal processes by implementing integrated inventory management systems, customer relationship management (CRM) software, and other digital tools to streamline operations. Furthermore, to improve customer service and enhance staff communication.
3. Assess international supply chain options: Explore international suppliers for potential cost reduction while considering the trade-offs between cost savings, product quality, and sustainability.

4. Enhance customer experience with online features by offering online ordering and appointment scheduling, personalized customer accounts, and other digital features to prevent losing existing customers.
5. Investing in staff training is critical to provide necessary training and support to help staff adapt to modern technologies and processes the transitions to a more digital model.
6. Implement digital and mobile strategies: Embrace digital tools and mobile technology, collaborative technology, fixed wireless technology, mobile hotspots, buy online pickup in-store (BOPIS) options, home delivery, and subscription boxes.
7. Monitor and evaluate progress: Regularly assess the impact of digital transformation on sales growth, cost savings, and customer retention and, if needed, adjust and improvements to ensure Pampered Pets' continued success.

Technology can amplify the growth of small businesses both horizontally and vertically, offering tangible and intangible benefits that yield the desired results. These technological endeavours will enable businesses to operate more swiftly and efficiently.

Furthermore, by embracing digitalization and leveraging Orla O'Dour's financial support, Pampered Pets can strengthen its position in the market, enhance customer satisfaction, and achieve sustainable growth. Therefore, we highly recommend the digitalization process to ensure the business remains competitive and adapts to the ever-changing landscape.

References:

- Pačaiová H, Nagyová A, Kotianová Z, Bernatík A (2013) Risk Assessment Methodology in SME. Acta Mechanika Slovaka, 17, 30-5.
- Crotty J, Daniel E (2022) Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. Applied Computing and Informatics(ahead-of-print).
- Gonzalez, C. (2022). Top 8 Threat Modelling Methodologies and Techniques. InfoSec Trends. Available at: https://www.exabeam.com/information-security/threat-modeling/ [Accessed 5 Apr. 2023].
- Matt (2022). Cybersecurity Threat Modelling for Small Business. Totem Tech. Available at: https://www.totem.tech/small-business-cybersecurity-threat-modeling/ [Accessed 5 Apr. 2023].
- National Cyber Security Centre (2020). Cyber Security Small Business Guide. Small Business Guide Collection ed. [online] United Kingdom: National Cyber Security Centre, pp.4–9. Available at: https://www.ncsc.gov.uk/files/NCSC_A5_Small_Business_Guide_v4_OCT20.pdf [Accessed 5 Apr. 2023].
- National School of Standards and Technology (2012). Guide for Conducting Risk Assessments. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf