Risk Assessment OF Pampered Pet Current Business Review

The risk assessment and evaluation of current business model will be assessed using Qualitative Risk Assessment Methodology to identify potential opportunities and threats in the business environment. This assessment method focuses on different elements of the business rather than only on financial or technical factor (Juma.A,2022) and the method will be complemented with STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of privilege) threat modelling and Risk Assessment Matrix (RAM) to evaluate the business risk. STRIDE assist in creation of measures for future threat occurrence while RAM assist to prioritise risk impact.

Risk identification and Mitigation

S/N	Asset	Threats	Impact	Mitigation
1	Wireless Gateway &Hub	1. Data Snooping. 2. Eavesdropping/Rogue Access Point. 3. Denial of Service (DOS). 4. MAC Address spoofing. 5. Lack of Segmentation	1.Network traffic flooding denials genuine customers from accessing the enterprise web. 2.Unauthorised access to wireless gateway 3. Competitors can divert mails for purpose of accessing list of enterprise's products and pricing. 4.Sensitivity information disclosure (Log-in credential).	1.Implementation of firewall (e.g network firewall/end-point firewall). 2.Authentication message policy (e,g. SPF & DMARC). 3.Use Encrypted and Authenticated protocols on the network. 4. Antivirus/anti-malware software scans and Host based intrusion detection and prevention (HID & HIP). 5. Regular monitoring of the network.

2	Hardware (Old Computer) & Software Application	1.Malware & Virus. 2.Data Breaches. 3. Exploitable vulnerabilities (OS, Excel spreadsheet & word)	1.System crash leading to data loss (inadequate financial/sale data can lead to higher Government Tax & VAT assessment figure). 2. Inability to support modern software (Compatibility issues). 3.High risk of software and hardware leading to data breach & exposure of Personal Identifiable Information (PII) including data of the pets. 4.System accessibility to unauthorised user.	1.Change the old computer to newer version. 2.Installation of updated antivirus & anti-malware. 3.Data back-up in hardware or software and recovery mechanism. 4.Deprovision of old applications. 5. Use of strong password.
3	Employees	1.Phishing/Vishing. 2. Insider threats & errors (weak password). 3. Elevation of privilege.	1.The employee can fall to social Engineering threat which can affect the survive of the business. 2.Employee can open the same business with	1.Email security and Access control policies. 2, Security Awareness Training. 3. Implement employees’ monitoring and behaviour analytics solution to

			access to both suppliers and buyers. 3. Theft of raw material as the employee act as the logistic provider at times. 4. Delivering of Payload (e.gTrojan backdoor) as a result of phishing	detect unusual/ suspicious activities. 4, Limit access to the supplier and other business trade secrets. 5.Change of business model to digitalisation

Implementing the required guidelines of ISO270001(ISMS) will assist by providing further mitigation to current challenges faced by Pampered Pets.

Risk Assessment Matrix of Pampered Pets &Threat Impact

Assessment Area	Low	Medium	High
Network Connectivity (Wireless gateway &Hub)	-	-	High
Hardware (Old Computer) & Software Application	-	-	High
Employees (Accidental /Deliberate interference)	-	-	High
Data Process	-	Medium	-
Business Continuity	-	-	High

Reference

1. Shotstack. A,(2014). Threat Modeling : Designing for Security.Available from: https://ebookcentral.proquest.com/lib/universityofessex-ebooks/reader.action?docID=1629177[Accessed September 9 2023].

2. Spears, J. & Barki, H. (2010). User Participation in Information Systems Security Risk Management. MIS Quarterly 34(3): 503. Available from: https://www-jstor-org.uniessexlib.idm.oclc.org/stable/25750689 [Accessed August 21 2023]

3. Sphera (N.D.). Digital Transformation Across the Complete Asset Lifecycle. Available from: https://sphera.com/digital-transformation-across-the-complete-asset-lifecycle. [Accessed September 14 2023].
4. University of Essex Online Lecture-cast 3 (2023). Threat Management and Modelling. Available from: https://www.my-course.co.uk/Computing/Cyber%20Security/SRM/SRM%20Lecturecast%202/content/index.html#/lessons/ieO_uo7-67lmlblEhYZpQttFUJjRJ6C8 [Accessed August 29 2023].