Risk Identification Report

Introduction

This report provides two risk assessments that analyze the company in its current state as a brick-and-mortar store and a predicted state for a digitalisation transition. The analysis provides risk methodologies, threat modeling and mitigation approaches. It Identifies risks, provides qualitative and quantitative risk analysis, then classifies the risks into four categories for a suggested mitigation approach. It also answers three questions about growth and savings within the summary from a qualitative aspect.

Risk Assessment - status quo

Connecting employees' mobile phones to the business wireless for personal use comes with magnified risk to the shop digital system. To illustrate the point, an attacker can get his/her way to the system through a vulnerability in employees personal Apps. Consequently, the business needs a detailed risk assessment to address the risks associated with both digital and non digital critical assets.There are different risk assessment methodologies these methodologies come in two types; Qualitative and Quantitative (Meir, 2020). According to Munteanu (2006), small businesses are better to be assessed using qualitative assessment techniques as there is not much data to be calculated and studied.

After looking into several different threat modeling techniques, Octave would be the most suitable one for our scenario. While techniques such as OpenFAIR focus heavily on large enterprises and are therefore more complex to implement, Octave was specifically designed with small and medium businesses in mind, meaning that they can also be implemented by a small team of IT professionals (enisa, 2005).

Octave was developed in 2001 and consists of three stages:

1. Build Asset-Based Threat Profiles

As Pamper Pets stands today the assets are considered to be the following:

1. The email used to collect orders from different clients
2. Old Networked Computer
3. Spreadsheet that includes warehouse deliveries and item location
4. Front desk computer
5. Wireless gateway and hub

2. Identify Infrastructure Vulnerabilities

1. Employees using the Wireless for personal use makes the environment prone to malware.

2. Communication and ordering process exposes the business to Social Engineering Attacks

3. An old computer is currently used to keep track of deliveries and item locations which includes Outdated or unpatched software that would expose the assets to cyber security threats.

4. No firewall is installed which makes the environment vulnerable.

3. Develop Security Strategy and Plans

While all three phases are equally important, it is the final phase that allows us to create specific plans for individual threats. Mitigations are divided into three categories to ensure securing most aspects of the environment. In the below table (Table 1) mitigations are classified and mapped to the risk. As shown in Table 1, accessing the network would comprise the whole system as it is currently a small environment consists of two computers, and old network and wireless, consequently the risks associated with the Network and Wireless had to be eliminated to bring the risk to acceptable level.

Risk Category / Classification	Eliminate Risk	Tolerate Risk	Reduce Risk	Transfer Risk	Description for mitigation
Email Security			X		• Multi-Factor authentication shall be deployed to ensure integrity. Moreover, installing spam and phishing protection tools along with password policy to enhance password security (Nwabueze et al. 2017)
Network Security	X				• SIEM solution shall be used for monitoring to detect suspicious behaviours (Podzins & Romanovs, 2019). • Network access control solution shall be used with policy that follows best practices (Singh & Kumar, 2009) • Antivirus and anti-spyware softwares shall be installed to protect the environment. Moreover, network segregation shall be used (Devi et al. 2017)
Wireless Security	X				• To prevent users from connecting to the wireless, SSID shall be disabled. Default passwords shall be changed with strong passwords that complies with password policy (Devi et al. 2017)

Table 1: Risk category classification

2 - Risk Assessment - Potential digitalisation

The activities of the pet company are insecure. The pet industry is unique in that it caters to pets rather than people. As a result, we must combine the attributes of the industry and take into account industry-specific hazards in addition to generic risks. Some hazards cannot be accounted for monetarily (for example, the loss of confidentiality of customer data) The pet grooming sector is susceptible to changes in many adjacent businesses, such as beauty tools, pet supplies, and pet food. The operating standards are challenging to standardize, and they run the danger of losing clients due to poor management.

Proposed changes for digitisation transformation

The PCI DSS standard puts forward many security baseline requirements in terms of information security management system, network security, physical security, and data encryption. Although there is no information security standard or security construction that can guarantee 100% protection against security risks, according to the accumulation of the industry, PCI DSS can be implemented and the security protection for cardholder data environment and security incidents can be implemented in strict accordance with the requirements of PCI DSS. The probability of occurrence will be greatly reduced.

Risk and threat modelling

As Shevchenko et al. stated (2018), “STRIDE, OCTAVE, PASTA and LINDDUN are some available threat models that are used” after being implemented to discover threats to an environment. In the case of Pamper Pets after digitalization the STRIDE model is used as it is known to be the most mature threat model available as it evaluates the system in detail. The first part of STRIDE is implementing a data flow diagram as below:

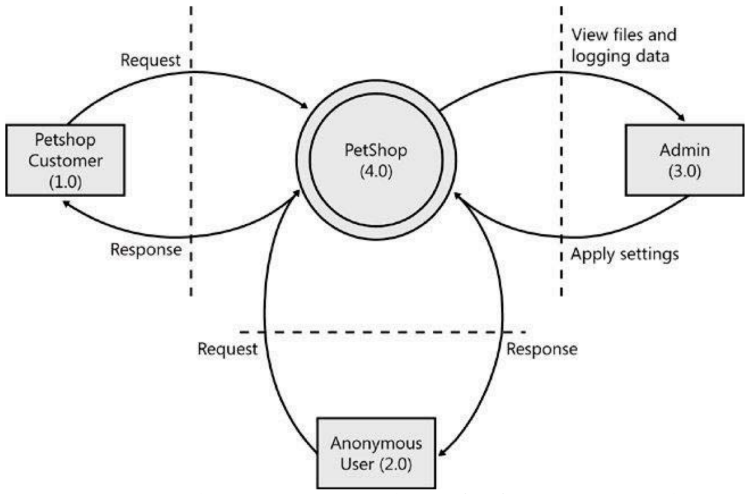

Figure 1: Data Flow Diagram of Pamper Pets Digitized (Johnstone, 2010).

To optimize business continuity and services, we recommend STRIDE for system hardening and LINDDUN for privacy of the client and data

Potential mitigations

Based on the risk and threat modeling analysis, we can implement three mitigation mechanisms (Figures 2,3,4,) to provide Preventative, directive, detective and corrective controls. Table 2 provides risk classification and mitigation for digitization.

Procedural Controls to help minimize the possibility of a breach to the systems, data and processes.

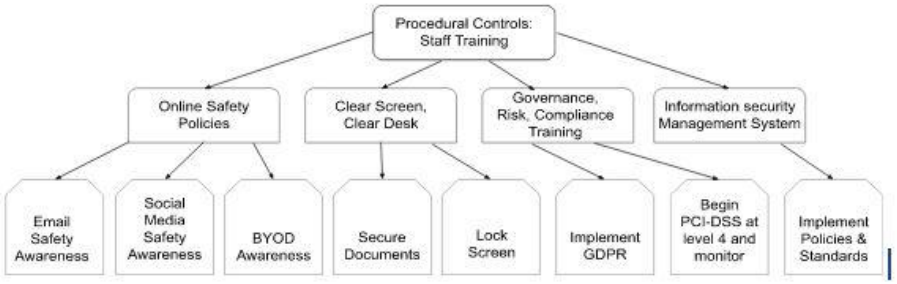

Figure 2: Four Procedural Controls and there Mitigation approach

Technical Controls can be implemented to improve System security and mitigate risks to the C.I.A. of data.

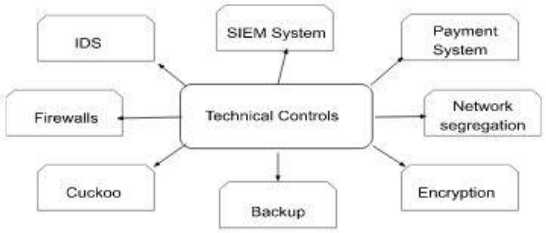

Figure 3: Technical controls for mitigation

Physical Controls to improve the location security and mitigate risks

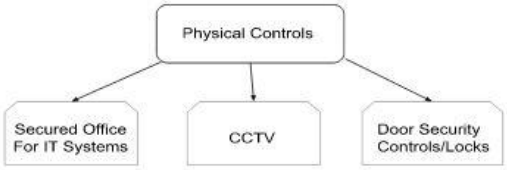

Figure 4: Physical controls

Current Status	Eliminate Risk	Tolerate Risk	Reduce Risk	Transfer Risk	Mitigation approach to reduce risk for digitalization
4 Staff members		x			Train staff in security awareness and apply access controls. Consider more specialized staff.
Customers in the store			x		Block off all ports and system access points, ensure network is password protected,
Receive email orders			x		Secure data, encrypt, install AV and malware detection, Train staff about social engineering and security good practice.
Staff email customers			x		Ensure compliance, GDPR and data encryption, train staff in compliance/privacy law and security good practice.
Old networked computers	x				Install new systems, patch and harden. Apply controls and passwords
Front desk computer system	x				Re-locate the computer system in a secure area, apply passwords and lock screen, install a till system on the front desk. PCI-DSS
Staff use wifi with BYOD	x				Deploy access controls, endpoint detection, MAC address ID, Network zoning, Firewalls.

Table 2: Risk classification and Mitigation for digitization

3 - Recommendation

To address the three questions, previous research found that an online presence has a positive impact on SMEs (Lanyi et al. 2020 :477) and findings by Yigi & Jewoo (2021) showed that a 1% increase of positive online reviews had lead to an 0.18% increase in profitability which helps growth. A quantitative analysis would provide better accuracy but requires more data.

Our assessment indicates that the business requires new hardware, software and staff training prior to digitalization. GDPR compliance is required and PCI-DSS compliance can be monitored and planned for.

Group 2 - Word count 997

References

Abomhara, M., Koien, G. & Gerdes, M. (2015) A STRIDE Based Threat Model for Telehealth Systems. Available from: https://www.researchgate.net/profile/Mohamed-Abomhara/publication/291766457_A_STRIDE-Based_Threat_Model_for_Telehealth_Systems/links/56a5de3208ae1b6511345e4a/A-STRIDE-Based-Threat-Model-for-Telehealth-Systems.pdf [Accessed 23 October 2022].

Aswal, M.S., Rawat, P. and Kumar, T. (2009) Threats and vulnerabilities in wireless mesh networks. *International Journal of Recent Trends in Engineering*, *2*(4): 155. Available from: https://www.researchgate.net/profile/Mahendra-Singh-4/publication/229003862_Threats_and_Vulnerabilities_in_Wireless_Mesh_Networks/links/5732dc2a08ae9f741b23639c/Threats-and-Vulnerabilities-in-Wireless-Mesh-Networks.pdf [Accessed 13 October 2022]

Enisa. (2005) *OCTAVE v2.0.* Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html. [Accessed 30 October 2022].

Johnstone, M. (2010) Threat Modelling with STRIDE and UML. Available from: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1087&context=ism [Accessed 23 October 2022].

Lányi, B., Hornyák, M. and Kruzslicz, F. (2021) The effect of online activity on SMEs' competitiveness. *Competitiveness Review: An International Business Journal*. Available from: https://www.emerald.com/insight/1059-5422.htm

Meir, M. (2020) The 2 Types of Risk Assessment Methodology. Available from: https://securityscorecard.com/blog/types-of-risk-assessment-methodology [Accessed 10 October 2022].

Munteanu, A., 2006, June. Information security risk assessment: The qualitative versus quantitative dilemma. *In Managing Information in the Digital Economy: Issues & Solutions-Proceedings of the 6th International Business Information Management Association (IBIMA) Conference* 227-232. Available from: https://www.researchgate.net/profile/Adrian-Munteanu/publication/228319538_Information_Security_Risk_Assessment_The_Qualitative_Versus_Quantitative_Dilemma/links/541aa46d0cf203f155ae4290/Information-Security-Risk-Assessment-The-Qualitative-Versus-Quantitative-Dilemma.pdf [Accessed 10 October 2022].

Mohan, A.K. & Sethumadhavan, M., (2017) Wireless security auditing: attack vectors and mitigation strategies. *Procedia computer science* 115: 674-682. DOI: https://doi.org/10.1016/j.procs.2017.09.153 [Accessed 15 October 2022]

Nwabueze, E.E., Obioha, I. and Onuoha, O., (2017) Enhancing multi-factor authentication in modern computing. *Communications and Network 6*(3): 172. DOI: 10.4236/cn.2017.93012. [Accessed on 13 october 2022]

Podzins, O. and Romanovs, A., (2019) April. Why siem is irreplaceable in a secure it environment?. In *2019 Open Conference of Electrical, Electronic and Information Sciences (eStream)* 1-5. IEEE. Available from: https://www.researchgate.net/profile/Andrejs-Romanovs-2/publication/345426832_Why_SIEM_is_Irreplaceable_in_a_Secure_IT_Environment/links/600c45fb92851c13fe31f23a/Why-SIEM-is-Irreplaceable-in-a-Secure-IT-Environment.pdf [Accessed 13 October 2022].

Shevchenko, (2018) Threat Modeling: A Summary of Available Methods. Available from: https://apps.dtic.mil/sti/pdfs/AD1084024.pdf [Accessed 23 October 2022].

Wang, Y. and Kim, J. (2021) Interconnectedness between online review valence, brand, and restaurant performance. *Journal of Hospitality and Tourism Management* 48: 138-145. DOI: https://doi.org/10.1016/j.jhtm.2021.05.016) [Accessed 25 October 2022]