2022

RISK IDENTIFICATION REPORT

GROUP 5
PATRICIA LAPIERRE, IASON RIGAS, YASH ROONGTA

Table of contents

Risk Identification Report

This report was compiled and sent to Pampered pets. This paper identifies risks and is separated into four sections: risk assessment, offline business threats, possible digitization, and mitigations.

1. Risk Assessment

Our security risk evaluation is qualitative since we do not have access to historical data at this time. Moreover, a qualitative risk assessment offers a helpful screening to develop a priority system and identify the most essential issues in order to swiftly evaluate the enterprise's risk aversion. (Olson & Desheng, 2020).

a. Threat Modeling Method DREAD

Every qualitative risk assessment is based on opinion, but it is never unjustified. It employs rating values to assess the risk associated with each recognized danger. In this evaluation, qualitative risk analysis was performed using the DREAD model.

DREAD poses the following key questions to assign risks to potential threats:

- Damage – How much damage can be caused if a threat exploit occurs?
- Reproducibility – How easy is it to reproduce the threat exploit?
- Exploitability – What is needed to exploit this threat?
- Affected Users – How many users are affected?
- Discoverability – How easy is it to discover the threat?

(EC-Council, 2022)

2. Threats of Offline business with internal networks and employees

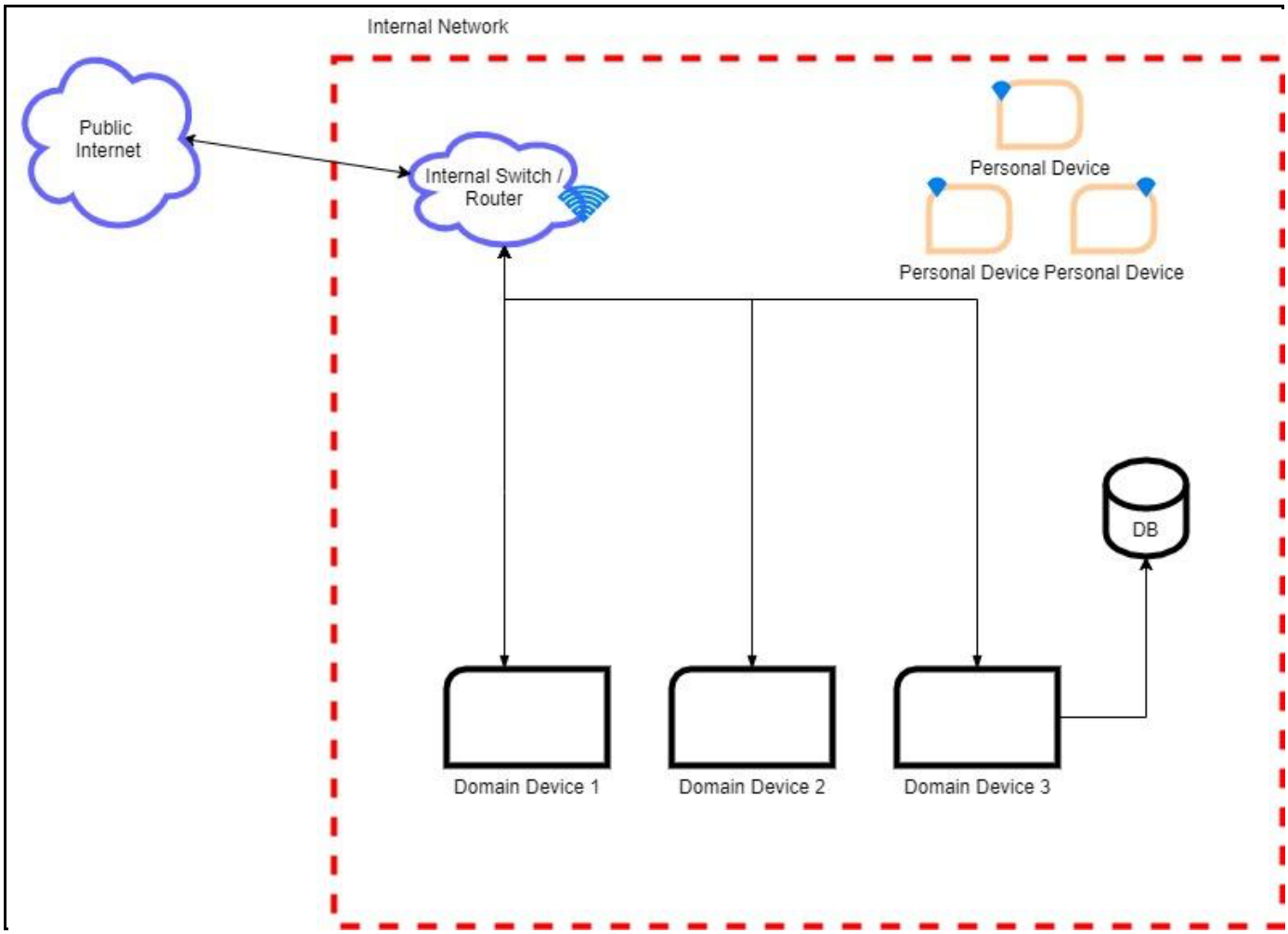

Figure 1: Highlighting an Overall Structure of Existing Offline Business

a. Cyber risks:

i) **Phishing:** Social-engineering-based cyber-attacks that tend to steal victims' information. 90% of organizations faced targeted phishing attacks in 2019 (Proofpoint, 2020).

ii) **Ransomware:** Attacks where malicious individuals encrypt victims' critical data and ask for payment in order to provide the decryption keys (Barker *et al.*, 2021). Ransomware was named the top threat type in 2021 according to IBM (2022).

iii) **Insider Threat:** Individuals in organizations that are tempted to leak sensitive organizational data in return for financial compensations (Jeong & Zo, 2021). 68% of organizations feel vulnerable to insider attacks, and 52% of all respondents find it more challenging to cope with insider threats than external cyberattacks (Gurucal, 2019).

b. Operational risks:

i) **Inventory management issues**: loss orders, duplication of orders, inconsistent or impossibility of tracking, increased costs, inventory imbalance, time-consuming, ineffective decision making (Tally Solutions Private Limited, 2021; Clear Spider, 2014).

3. Potential digitalization

After a thorough examination of the advantages and scope of digitization, it is recommended that Pampered Pets undertake their "online" expansion in phases. We have thoroughly assessed the following business processes and transformations to determine their suitability:

a. E-Commerce Portal (Online Shop) online with a payment gateway

Almost 1.8 billion people used online platforms (Walmart, Amazon, daraz.pk, and flipkart.com) in 2018 to do their purchases, with a volume of $US 2.8 trillion in transactions. (Clement, 2019;

cited in Qalati *et al.*, 2021: 2). Some of the main reasons for online shopping are “time-saving, discounted pricing, convenience, competitive pricing, expert advice, and greater access to information” (*Ibid*). That is why the e-commerce portal would include an online payment gateway following the compliance requirements of the Payment Card Industry Data Security Standard (PCI-DSS) (Chapple *et al.*, 2021).

b. Inventory Management (IM)

Effective inventory management is one of the cornerstones of a successful company. The advantages include improved inventory accuracy, cost savings, avoiding stockouts and surplus inventory, as well as a decreased risk of overselling and the ability to overcome demand changes. (Müller,2003).

c. Content Management System (CMS)

A CMS system permits the rapid and efficient generation of content without the need for technical knowledge in constructing web pages. A CMS may be used for the internet presence, content generation, and blogging of pampered pets (Jones & Farrington, 2013).

We employed the DREAD risk model to conduct a risk assessment on the possible digitalization since our risk assessment is based on a qualitative technique for the reasons outlined above.

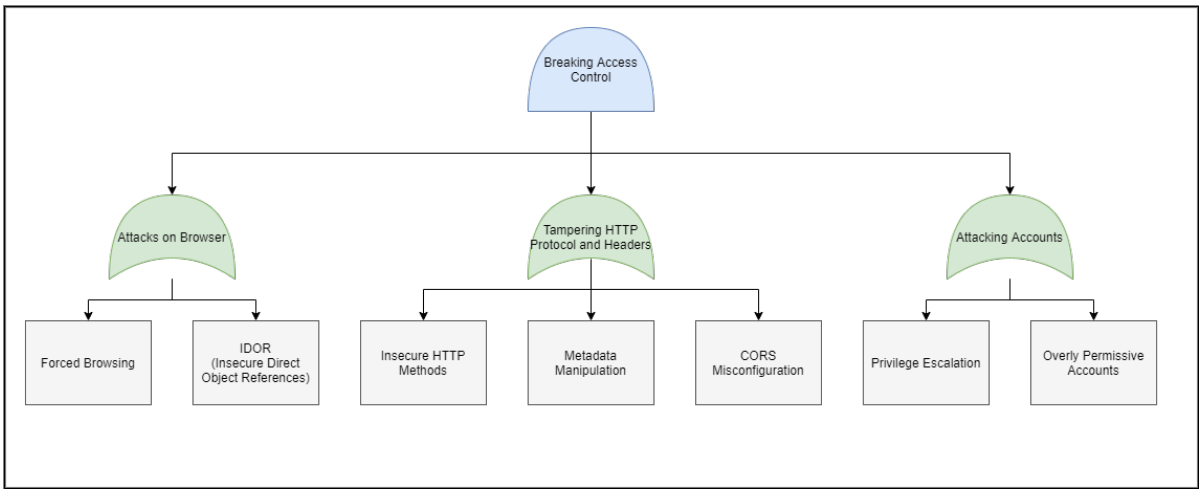

Figure 2: Attack-Tree for Breaking Access Controls on Websites

Based on the DREAD threat modeling technique, Pampered Pets' online presence is vulnerable to the following threats, with Broken Access Control as a probable scenario:

Risk	**D**	**R**	**E**	**A**	**D**	**Score**	**Rating**
Overly Permissive Accounts	10	5	5	10	0	30	**High**
Forced Browsing	5	10	10	2.5	10	37.5	**High**
Insecure direct object references (IDOR)	5	10	10	2.5	10	37.5	**High**
Insecure HTTP Methods (PUT/DELETE)	10	10	9	10	5	44	**Critical**

Privilege Escalation	9	5	2.5	8	0	27.5	**High**
Metadata manipulation	5	0	2.5	2.5	0	10	**Low**
CORS misconfiguration	8	5	5	6	0	24	**Medium**

Due to the size and scope of the web application's attack surface, only the most significant attacks have been listed.

- The following are possible countermeasures for defective access control:
- Model access restrictions should enforce record ownership rather than allowing that the user may add, read, alter, or remove any record. Disable directory listing on the web server and check that file metadata (e.g., git) and backup files do not exist inside web root directories.
- Implement access control measures once and repurpose them across the program, including limiting the usage of Cross-Origin Resource Sharing (CORS).
- Except for public resources, by default decline.
- Stateful session IDs should be invalidated on the server upon logout.

4. Recommendations

- Could an online presence grow the business by up to 50%?

- Could the business lose up to 33% of its existing customers if the business doesn't provide some online features?

With online presence digitalization and e-commerce being some of the buzzwords of our times an informed decision regarding the adoption of online presence by small and medium enterprises is essential.

Despite claims regarding the benefits of ecommerce there are very few studies conducted to measure tangible benefits. Some of the benefits of online presence and e-commerce reported are reduced operating costs, increased sales, and efficiency improvements (MacGregor and Vrazalic, 2007) as well as market expansion (Daniel and Wilson, 2002). In Johnston, Wade and McClean (2007) an increase in revenue of up to 10% and a reduction in costs of goods sold (COGS) of up to 8% was measured for SMEs employing under 100 employees. In other studies, such as in Rahayu and Day (2016) benefits to SMEs such as increased sales, reduced operation costs and extending market reach are confirmed.

- Could changing to an international supply chain reduce costs by up to 24%?

Changing to an international supply chain has the potential for cost reductions as much of the cost of products is not confined to the cost of production itself but needs to consider costs incurred until the product reaches the end customer. A global supply chain can lead to lower unit costs through better logistics and more efficient supply chain management. Such costs can be significant as for example in the USA the total cost of logistics is estimated to be close to 10% as a percentage of GDP (Christopher,2016). Without detailed knowledge of Pampered Pet's cost structure, it is not possible to estimate the precise impact of moving to an international supply chain.

References

Barker *et al.* (2021) Cybersecurity Framework Profile for Ransomware Risk Management. *National Institute of Standards and Technology. Preliminary Draft NISTIR*, *8374*. Available from: https://csrc.nist.rip/external/nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8374-draft.pdf [Accessed 3 September 2022].

Chapple *et al.* (2021) *(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide*, 9th Edition, 1248 pages.

Christopher, M (2016) *Logistics and Supply Chain Management: Logistics and Supply Chain Management*, Pearson Education, Limited, Harlow.

Clear Spider (2014) Top Ten Consequences of Not Having Inventory Management. Available from: https://clearspider.net/blog/consequences-inventory-management/ [Accessed on the 5th August, 2022].

Daniel, E., Wilson, H. & Myers, A. (2003) Adoption of e-commerce by SMEs in the UK. *International Small Business Journal* 20(3): 253-270.

EC-Council (2022) DREAD Threat Modeling: An Introduction to Qualitative Risk Analysis. Available from: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/ [Accessed 30 August 2022].

Gurucul (2019) 2020 Insider Threat Survey Report. Available from: https://gurucul.com/2020-insider-threat-survey-report [Accessed 27 August 2022].

Jeong, M., & Zo, H. (2021) Preventing insider threats to enhance organizational security: the role of opportunity-reducing techniques. *Telematics and Informatics*, *63*, 101670.

Johnston, D., Wade , M. & Mcclean, R. (2007) Does e-Business Matter to SMEs? A Comparison of the Financial Impacts of Internet Business Solutions on European and North American SMEs, *Journal of Small Business Management*, 45(3): 354-361.

Jones, K. M. L. & Farrington, P.-A. (2013) *Learning from libraries that use WordPress content-management system best practices and case studies*. Chicago, Ill: American Library Association.

IBM (2022) Combating new threats in a time of constant change. Available from: https://www.ibm.com/security/data-breach/threat-intelligence/ [Accessed 3rd September 2022].

MacGregor, R. & Vrazalic, L. (2007) *E-commerce in Regional Small to Medium Enterprises*. London: IGI Publishing.

Müller, M. (2003) *Essentials of inventory management*. New York: American Management Association.

Olson, D.L. & Desheng D.W (2020) *Enterprise risk management models*. Berlin, Germany: Springer.

Proofpoint (2020) 2020 state of the phish. Available from: https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf [Accessed 3rd September 2022].

Qalati *et al.* (2021) Effects of perceived service quality, website quality, and reputation on purchase intention: The mediating and moderating roles of trust and perceived risk in online shopping. *Cogent Business & Management*, 8: 1869363.

Rahayu, R. & Day, J. (2016) E-commerce adoption by SMEs in developing countries: evidence from Indonesia. *Eurasian business review*, 7 (1): 25–41.

Tally Solutions Private Limited (2021) Common Inventory Management Problems, Challenges, And Solutions. Available from: https://tallysolutions.com/business-guides/common-inventory-management-problems-challenges-solutions/ [Accessed 5 September 2022].