Julius Cloos
Module: Security and Risk Management
Tutor: Dr. Siddiqui

Risk Identification Report

Before carrying out a risk assessment, it is important to choose a suitable methodology. For this project, the OCTAVE-S process was picked in favor of other alternatives like OCTAVE Forte given it is designed for smaller organizations like Pampered Pets and small risk assessment teams (Alberts et. al., 2005). The OCTAVE-S process consists of the following steps:

Phase 1a: Identifying important assets

According to Alberts et. al (2005), 3-5 critical assets are selected for analysis:

- Physical structures (storage spaces etc.)
- Inventory (pet food, toys etc.)
- Critical technical infrastructure (servers holding confidential data according to GDPR etc.)
- Sensitive customer/employee data

Phase 1b: Threats to important assets

Now, threats to these important assets are described (Alberts et. al., 2005):

- Fires, natural disasters
- Vandalism, theft
- Cyber-attacks (both from outside hackers as well as insiders)
- Unintentional losses (employee losing their business laptop)

Phase 2: Infrastructure vulnerabilities

In Phase 2, vulnerabilities in the infrastructure are analyzed (Alberts et. al., 2005):

- Weak password policy
- Unsecured wired network allows attackers with physical access unauthorized network access
- Physical structures are not monitored

Phase 3: Mitigations

In the final phase, mitigations to the detected risks are listed (Alberts et. al., 2005):

- Use LAN with authentication
- Install surveillance cameras

STRIDE/DREAD Risk Assessment for Cyber Security

This report will model the threats to the new warehouse's management system according to the methodology proposed by Dykstra et. al. (2023):

1. Identification of different threats using STRIDE methodology (qualitative risk assessment).
2. The risks from the different threats are rated according to DREAD (quantitative risk assessment).

Advantages of this methodology include that risks are not only identified systematically using the STRIDE-methodology, but also rated to allow Pampered Pets' management to address the high-priority risks first.

	Threat
Spoofing	T1: Attackers could assume the role of a warehouse employee T2: Warehouse employees could sign in using other employee’s credentials
Tampering	T3: Malicious actors (both rogue employees and outside attackers) could manipulate inventory and/or user data
Repudiation	T4: Users can deny they carried out actions when their password is so weak it could have been guessed by anyone
Information Disclosure	T5: Attackers could gain access to sensitive customer information by gaining access to the customer database via the webserver
Denial of Service	T6: Cyber attackers can overload the warehouse management software, disrupting the warehouse’s operations. T7: Physical vandalism against the servers of the management system
Elevation of Privilege	T8: Attackers could escalate their privileges to Administrator, causing widespread disruptions.

The risks identified will now be weighted and ordered according to DREAD (Dykstra et. al., 2023):

Threat	Damage			Reproducability	Exploitability	Affected Users	Discoverability	Score
	Legal	Reputation	Productivity					
T1	0	3	7	7	7	5	5	27,33
T2	0	3	7	8	8	5	9	33,33
T3	9	5	6	6	5	7	8	32,67
T4	9	6	5	9	9	7	9	40,67
T5	10	6	2	2	6	6	6	26,00
T6	0	5	10	8	9	8	9	39,00
T7	5	4	9	7	4	8	7	32,00
T8	0	6	10	4	5	10	5	29,33

To reduce the subjectivity of scoring the threats (a weakness of the DREAD-methodology), this report orients itself on the scoring of Dykstra et. al. (2023). However, despite these efforts, the exact score remains subjective.

It's especially important to consider the implications of data protection regulations, such as GDPR. Especially the disclosure of user data can be problematic according to GDPR-regulations (Wolford, 2024). This can be very costly for the business, with penalties up to 20 million euros or 4% of the business' global turnover for the most severe cases (Wolford, 2024). Even minor infringements carry fines up to half of the penalties for severe violations (Wolford, 2024).

Recommended Location for the business

This report uses the SMART-method to rank the different proposed locations. This technique is well-suited for ranking choices based on different factors, each with different weight (Olson & Desheng, 2020).

Using the SMART-method and given the example data cited by Pampered Pets, this report recommends using Alabama or Vietnam, leaning slightly towards Alabama.

The SMART-method can be summed up as follows (Olson & Desheng, 2020):

1. Identify the choices and the relevant factors (i.e. tax and labor cost)
2. Transform all values into numerical values (i.e. very good becomes 1)
3. Identify the rating of the different issues (i.e. cost per unit produced is more important than insurance structures) and calculate the weight ($\frac{Rating}{Sum\ of\ Ratings}$)
4. Assign each value a number between 0 and 1, with 1 being the best (i.e. the cheapest insurance cost of 300$ is the best with a value of 1, and insurance twice as expensive is assigned a value of 0.5).
5. Calculate the score for each choice by summing the products of weight and factor.

According to these calculations, we get the following ranking (Olson & Desheng, 2020):

Rank	Site	Score
1	Vietnam	0.762
2	Alabama	0.754
3	India	0.721
4	China #2	0.710
5	Oregon	0.706
6	China #1	0.679
7	Utah	0.674
8	Mexico	0.626
9	Indonesia	0.557
10	Crete	0.394

Given the small difference between the ranking of Vietnam and Alabama, this report advises to take current political events in Vietnam into account. There is currently some political in Vietnam, after several high-ranking members of government have stepped down or been arrested, including the former national assembly chairman Vuong Dinh Hue and the arrest of former Cabinet Secretary Mai Tien Dung (Tomiyama, 2024). As of now, there has been no economic impact (Tomiyama, 2024). Due to the Politburo's significant influence on Vietnam politics, it is however still recommended to at least consider the latest developments which may not be included in the sample data provided by Pampered Pets.

Conclusions

According to this report, the new facility should be placed in Alabama or Vietnam. First and foremost, the weak password policy and the lack of DoS protection need to be addressed. Also, despite the low ranking according to DREAD, Pampered Pets should immediately take precautions against the leaking or unauthorized modifying of customer data, as the fines can be crippling for a SME. Once these risks are mitigated, others should be addressed, such as preventing physical vandalism against the servers and DoS-attacks against the warehouse's IT infrastructure.

Mitigations include:

- A stronger password policy
- Web application firewalls can help mitigate many injection-based vulnerabilities, protecting data from being read by attacks such as SQL-Injection (Wagenseil, 2023)
- Increasing physical security, such as installing surveillance cameras.
- Regular penetration tests to identify security issues. This is also required by GDPR (Weismann, 2023).

Julius Cloos
Module: Security and Risk Management
Tutor: Dr. Siddiqui

References

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005) OCTAVE® -S Implementation Guide, Version 1.0. Available from: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=32a2f97e58cbc7efc0f07f98e005230a20c6e526 [Accessed 26 July 2024]

Dykstra, J., Lander, T. E., Mittal, S., Rastogi, N., Reece, M., Sampson, A. & Stoffolano, M. (2023) Systemic Risk and Vulnerability Analysis of Multi-cloud Environments. Available from: https://arxiv.org/pdf/2306.01862 [Accessed 01 August 2024]

Olson, D.L. & Desheng D.W. (2020) *Enterprise Risk Management Models*. 3rd ed. Berlin: Springer. Available via the Vitalsource Bookshelf. [Accessed 24 July 2024]

Tomiyama, A. (2024) Vietnam rocked by political upheaval: 5 things to know. Available from: https://asia.nikkei.com/Politics/Vietnam-rocked-by-political-upheaval-5-things-to-know [Accessed 25 July 2024].

Wagenseil, P. (2023) How the latest SQL injection attacks threaten web application firewalls. Available from: https://www.scmagazine.com/resource/how-the-latest-sql-injection-attacks-threaten-web-application-firewalls [Accessed 27 July 2024].

Wolford, B. (2024) What is GDPR, the EU's new data protection law?. Available from: https://gdpr.eu/what-is-gdpr/ [Accessed 26 July 2024].

Weismann, A. (2023) Why Do Penetration Testing for GDPR? Article 32 & Much More. Available from: https://networkassured.com/compliance/penetration-testing-for-gdpr/ [Accessed 27 July 2024].