Pampered Pets, a bricks-and-mortar pet store, is considering digitalizing its operations to enhance processes and expand internationally. To assess the risks involved, the business can employ various methodologies such as quantitative, qualitative, or hybrid risk analysis.

Quantitative analysis assigns numerical values to risks and calculates their probability and potential impact. Qualitative analysis assesses risks subjectively based on likelihood and impact. Hybrid analysis combines elements of both approaches. To carry out a risk and threat modeling exercise for Pampered Pets, follow these steps: (*owasp-summit-2017/Working-Sessions/Threat-Model/Threat-Modeling-Cheat-Sheet.md at master · OWASP/owasp-summit-2017*, no date)

1. Identify Assets: Determine critical assets like customer data, payment information, inventory, and website infrastructure.
2. Identify Threats: Enumerate potential threats, such as data breaches, DDoS attacks, system failures, unauthorized access, and malware.
3. Assess Vulnerabilities: Identify vulnerabilities in systems, processes, and infrastructure, like outdated software, weak passwords, lack of encryption, or inadequate security measures.
4. Evaluate Impact: Determine the potential impact of each threat on operations, reputation, and finances, considering likelihood and severity.
5. Mitigation Strategies: Implement mitigations such as a disaster recovery plan, robust security measures, regular software updates, backups, secure payment gateways, vetting third-party vendors, and website performance optimization.

1. Website Downtime: (Initiative, 2012)
    1. Likelihood: Moderate to High
    2. Impact: High
    3. Mitigation: Regularly monitor the website's uptime using reliable monitoring tools. Implement redundancy measures, such as backup servers and load balancing, to minimize downtime. Have a disaster recovery plan in place to quickly restore the website in case of an outage.
2. Cybersecurity Breaches:
    1. Likelihood: High
    2. Impact: High
    3. Mitigation: Implement robust security measures such as firewalls, intrusion detection systems, and encryption protocols. Regularly update software and plugins to address vulnerabilities. Conduct regular security audits and penetration testing to identify and fix any weaknesses.
3. Compatibility Issues:

1. Likelihood: Moderate
2. Impact: Moderate
3. Mitigation: Conduct thorough testing on multiple devices and browsers to ensure compatibility. Keep software and plugins up to date to address compatibility issues. Provide clear instructions to customers on system requirements and recommended settings.

4. Payment Processing Risks:
   1. Likelihood: Moderate to High
   2. Impact: High
   3. Mitigation: Use secure payment gateways that comply with industry standards and regulations. Regularly update and patch payment processing software. Monitor transactions for any suspicious activity and implement strong authentication measures.
5. Third-Party Service Provider Risks:
   1. Likelihood: Low to Moderate
   2. Impact: Moderate to High
   3. Mitigation: Thoroughly vet and select reliable and reputable service providers. Review their security protocols and data handling practices. Implement contractual agreements that clearly define the responsibilities and liabilities of both parties.

Qualitative Risk Assessment Methodology: (Zastite, 2013)

Type	**Details**	**likelihood**	**Impact**
Mark competition	Competition from other pet pampering businesses can impact market share and pricing.	**high**	**high**
Staff training	Insufficiently trained staff may provide inadequate services or cause harm to pets.	**Moderate**	**Moderate**
Pet health/safety	Accidents, allergies, or illnesses of pets under care can result in legal liabilities.	**High**	**High**
Supply chain disruptions	Delays or shortages in pet grooming products and supplies can affect operations.	**Low**	**low**
Reputation damage	Negative reviews or incidents of poor service	**Moderate**	**Moderate**

Qualitative Risk Assessment Justifications: (Rut,2008)

1. **Simplicity and Accessibility:** it's relatively easy to understand/ implement, making it suitable for small businesses where complex quantitative data may not be readily available.
2. **Subjective Insights:** It allows for the inclusion of subjective judgments and insights from experts and stakeholders, which can be valuable in identifying and understanding risks specific to the business.
3. **Quick Identification:** risks are quickly identified and categorized based on their importance, helping managers/owners focus on the most important issues.
4. **Risk Communication:** It facilitates communication about risks within the organization, ensuring that all relevant parties are aware of potential threats.

A list of proposed changes for the digitalization process:

1. Allows pet owners to schedule grooming, boarding, and other services conveniently through a website/mobile app.
2. Create a digital system for storing and managing pet records, including medical history, vaccinations, and grooming preferences.
3. Develop a mobile app that offers on-demand pet grooming services.
4. Launch an e-commerce platform to sell pet products.
5. Introduce a digital loyalty program that rewards repeat customers with discounts / special offers.
6. Enhance social media presence to showcase grooming results, share pet care tips, and engage with customers.
7. Offer various digital payment options, including mobile payments and online invoicing.
8. Install pet cams in grooming areas/boarding facilities, allowing pet owners to check in on their pets.
9. Send automated reminders to customers.

STRIDE: (Krishnan, no date)

Type	Threat	Vulnerability	Countermeasures
1- Spoofing identity	Unauthorized individuals /entities pretending to be legitimate customers, employees, or service providers.	• Lack of strong authentication measures for customers or employees. • Weak password policies. • Inadequate verification of pet ownership.	• Implement strong authentication methods. • Educate employees about identifying fake IDs. • Verify pet ownership through proper documentation.

2- **Tampering with Data:**	Unauthorized modification/alteration of pet and customer data, appointment schedules, or payment records.	• Inadequate data encryption. • Insufficient access controls. • Lack of data integrity checks.	• Use encryption to protect sensitive data. • Implement access controls and restrict data access to authorized personnel. • Implement data validation and integrity checks.
3- Repudiation	Denial of actions or transactions by customers/employees.	• Inadequate logging of customer interactions. • Weak record-keeping practices	• Implement comprehensive logging of customer interactions. • Maintain detailed records of services provided and transactions.
4- Information disclosure	Unauthorized access to sensitive customer information.	• Insufficient data access controls. • Weak encryption for customer and business data.	• Implement strict access controls to limit access to sensitive data. • Use encryption to protect customer and business data.
5- Denial of service	Deliberate actions/events that disrupt operations	• Over-reliance on a single service provider.	• Diversify service providers and

		- Lack of redundancy in critical systems. - Absence of a disaster recovery plan.	implement redundancy. - Develop a disaster recovery plan to ensure business continuity.
6- **Elevation of Privilege**	Unauthorized individuals gain elevated access to systems/resources.	- Weak access controls. - Poorly configured user privileges.	- Implement strong access controls. - Regularly review/adjust user privileges to the principle of least privilege.

In summary, digitization in pet pampering businesses modernizes operations, from online booking and payments to customer profiles and scheduling. Digital marketing drives promotions, while online reviews and loyalty programs boost engagement. Video monitoring offers pet owners' remote access and transparency. Digital health records streamline pet care management, and data analytics inform business decisions. Remote consultations and online training resources expand services, fostering convenience. Cybersecurity safeguards sensitive data, and eco-friendly practices reduce environmental impact. These digital strategies enhance customer experiences and operational efficiency, positioning pet-pampering businesses for success in the modern marketplace.

References:

Initiative, J.T.F.T. (2012) *Guide for Conducting Risk Assessments*. NIST Special Publication (SP) 800-30 Rev. 1. National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-30r1.

Krishnan, S. (no date) ‘A Hybrid Approach to Threat Modelling’.

owasp-summit-2017/Working-Sessions/Threat-Model/Threat-Modeling-Cheat-Sheet.md at master · OWASP/owasp-summit-2017 (no date) *GitHub*. Available at: https://github.com/OWASP/owasp-summit-2017/blob/master/Working-Sessions/Threat-Model/Threat-Modeling-Cheat-Sheet.md (Accessed: 18 September 2023).

(2008)’IT Risk Assessment: Quantitative and Qualitative Approach’, Paper ICSEEM_60, Available at:https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=11fe25b459871f9beac7ec3a35c21955025abfe4

(2013) ‘Safety Engineering’, Safety of Technical systems, Vol 3, available at: https://www.znrfak.ni.ac.rs/SE-Journal/Archive/SE-WEB%20Journal%20-%20Vol3-3/Safety%20Engineering%20Vol03No3.pdf#page=21