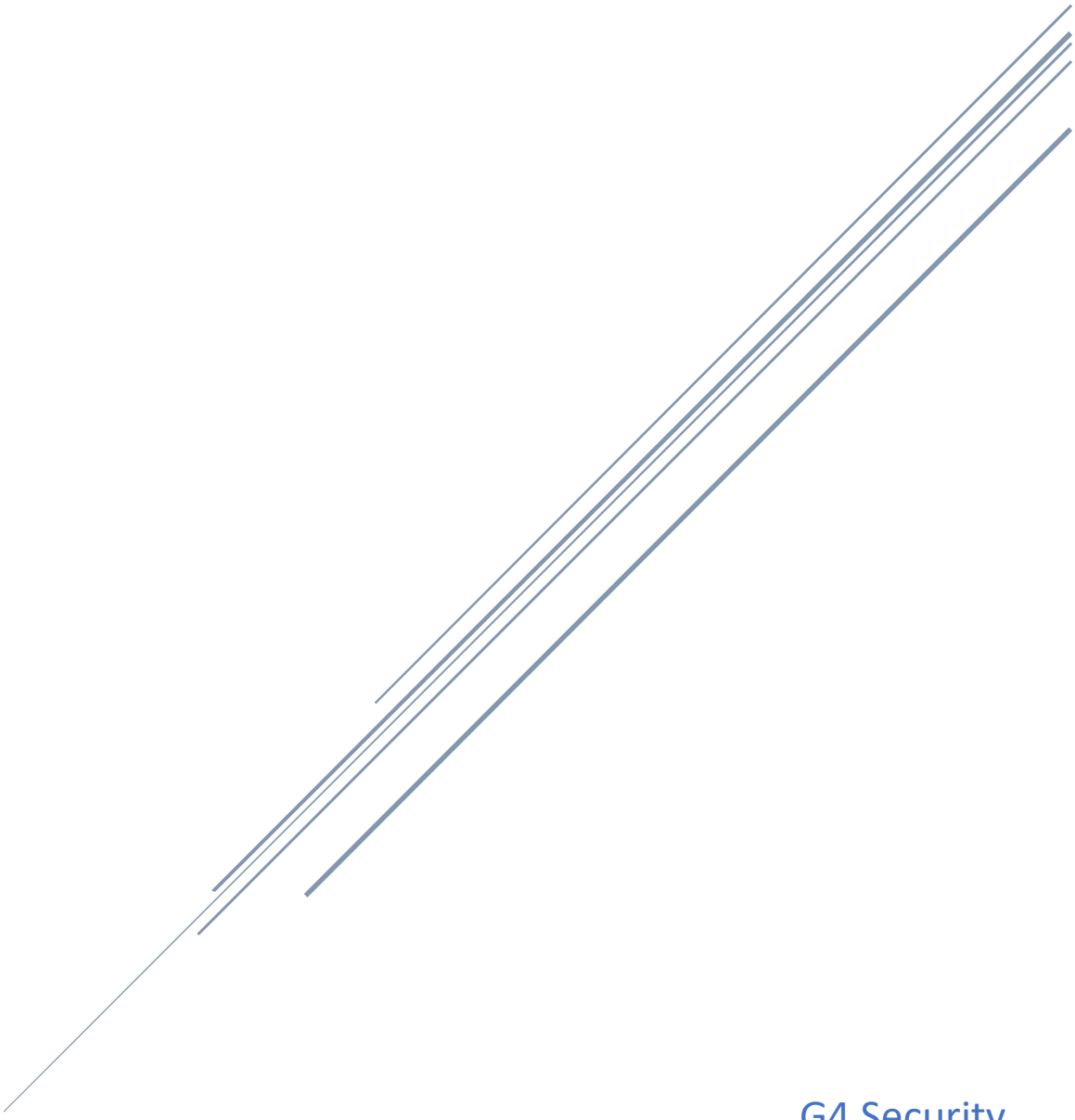
CYBERSECURITY RISK MANAGEMENT ASSESSMENT REPORT

Pampered Pets



G4 Security

12th April 2023

Table of Contents

Executive Summary

Pampered Pets is a brick-and-mortar enterprise transitioning to digital solutions in order to improve its operations, develop growth potential, and establish a strong online presence. This report provides a risk assessment for the Pampered Pets bricks-and-mortar business, with a focus on evaluating the current and potential risks and threats facing the business. The report is divided into two sections: the first section evaluates the current status of the business's operations. The second section assesses the risks and threats associated with the potential digitalisation of the business. The company's security team will conduct a baseline analysis using ISO 31000:2018 risk management framework, (ISO, 2018) identify and prioritize information security risks, and apply mitigation strategies based on NIST 800-53 guidelines (**Appendix A**). The digital transformation initiatives will be implemented and monitored, with STRIDE (**Appendix B**) analysis and OCTAVE-Allegro (**Appendix C**) evaluation conducted after the transformation to reassess the risks.

Current Status

The risk assessment methodology selected for this report is the ISO 31000:2018 (ISO, 2018). This methodology is widely recognized and provides a structured approach to risk assessment. It is based on a thorough analysis of the business environment, including internal and external factors that may impact the business.

Risk, Threat Modelling Exercise and Mitigation: (**APPENDIX D**)

Evaluation of Risks and Threats:

The following table provides an assessment of the potential impact of the identified risks and threats on the business:

Risk/Threat	**Likelihood**	**Impact**
Fire	Low	Moderate
Theft	Moderate	Moderate
Cyber-attacks	High	High
Supply chain disruptions	Moderate	High
Staff turnover	Low	Low
Reputation damage	Low	High

Overview – Digitalisation Process

The risk assessment methodology selected for this section is the NIST Cybersecurity Framework and NIST 800-53 guidelines, (NIST, 2014) which provides a comprehensive, risk-based approach to managing cybersecurity risk. This framework is well-suited to the digitalisation process, as it takes a holistic view of risk and can identify potential threats and vulnerabilities. Additionally, it is recognised globally and aligns with other risk assessment methodologies, making it a sound choice for this assessment.

Proposed Changes for Digitalisation:

The proposed changes for digitalisation include the implementation of an online presence, changing to an international supply chain, and adding online features to the business.

1. **International Supply Chain**: The first proposed change is the adoption of an international supply chain. The current supply chain is mostly local, with employees driving to local farms to pick up ingredients. Changing to an international supply chain will provide access to a wider range of suppliers and reduce costs. However, it may increase the risk of supply chain disruptions due to transportation and customs issues.
2. **Implement an E-commerce Online Platform:** The second proposed change in addition to a website presence, the business should implement an e-commerce platform that enables customers to make purchases online. This will increase convenience for customers and expand the business's reach beyond its physical

location. The platform should be secure and user-friendly, and include features such as product reviews and ratings.

Risk and Threat Modelling Exercise:

The following is a risk and threat modelling exercise that identifies potential risks and threats to the business of the proposed changes. (**Appendix E**)

Evaluation of Risks and Threats

Risk/Threat	**Risk Rating**	**Likelihood**	**Impact**
Cyber-attacks	High	High	High
Data breaches	Medium	Medium	High
Financial Loss	Medium	Medium	High
Supply chain disruptions	High	High	High
Staff turnover	Low	Low	Low
Reputation damage	Low	Low	High

Mitigations Strategies:

The following is a list of potential mitigations to minimize the impact of the identified risks and threats. (**Appendix E**)

Investigation of Growth

The following section will investigate the three key questions posed in the assignment:

- An online presence has the potential to significantly grow the business by expanding its reach beyond its physical location. According to a study by Retail Insider, online sales in the UK increased by 36% in 2020, with e-commerce accounting for 30% of total retail sales (Jahshan, 2021). By implementing an e-commerce platform, Pampered Pets can tap into this growing market and attract new customers who prefer to shop online (Science Direct, 2005). Additionally, an online presence can provide valuable marketing opportunities, such as email campaigns and social media promotions, which can further increase revenue.
- Changing to an international supply chain has the potential to reduce costs, but also poses certain risks. By sourcing ingredients from international suppliers, the business may be able to reduce its costs by taking advantage of lower labour and material costs. However, international sourcing also poses risks such as increased shipping costs, longer lead times, and the potential for quality issues. Additionally, Pampered Pets prides itself on using high-quality, local ingredients, which may be difficult to replicate with international sourcing.
- If the business does not provide online features, it may lose up to 33% of its existing customers who prefer the convenience of ordering products online.

Recommendations:

It is recommended that Pampered Pets undergoes a digitalisation process. Digitalisation has numerous benefits, including increased efficiency, streamlined operations, improved customer service, and access to new markets. Digitalisation will enable the business to expand its customer base, automate many of its processes, and reduce the risk of errors and fraud. To successfully implement digitalisation, the business must ensure that the process is managed and overseen by skilled and experienced IT professionals and implement the various mitigations and recommendations of this report.

Conclusion

The digitalisation of Pampered Pets is necessary for the growth and sustainability of the business. The risks associated with digitalisation can be mitigated through the implementation of cybersecurity measures, data privacy measures, and comprehensive employee training. Digitalisation will enable the business to expand its customer base, streamline its operations, and improve its efficiency. To ensure a successful digitalisation process, the business should hire an experienced IT professional to assess the business's current IT infrastructure, make recommendations for improvements, and oversee the digitalisation process.

Appendices

Appendix A

Baseline Analysis Plan

Step 1: Establish context - Define scope and objectives for Pampered Pets' digital transformation.

Step 2: Risk identification - Perform a baseline analysis with NIST 800-30 to identify assets and risks.

 Step 3: Risk analysis - Assess likelihood and impact of risks on business operations.

 Step 4: Risk evaluation - Prioritize risks to inform decision-making.

 Step 5: Risk treatment - Apply NIST 800-53 mitigation strategies and ensure ISO 27001 compliance.

 Step 6: Digital transformation - Implement the transformation and execute recommended solutions.

 Step 7: Monitoring, review, and evaluation - Continuously monitor risk management processes, update as needed, and reassess risks using STRIDE analysis and OCTAVE Allegro post-transformation.

 Step 8: Communication and consultation - Involve stakeholders throughout the risk

Appendix B

STRIDE Risk Analysis

The following is a risk assessment conducted after recommendations have been implemented; the STRIDE method classifies attacks, allowing us to rate them qualitatively after the strategy has been implemented.

STRIDE Risk Analysis Table where Pampered Pets digital transformation is active:

Category	Attack	Likelihood	Impact	Risk Level	Mitigation Strategy
Spoofing	Fake login pages	Medium	High	High	Two-factor authentication (ERP System)
	Email phishing attacks	High	High	High	Email security solutions (FAaS)
Tampering	Modification of sales data	Low	High	Medium	Data access control (ERP System)
	Alteration of customer/financial data	Low	High	Medium	Data access control (ERP System)
Repudiation	Unauthorized transactions	Low	High	Medium	Transaction monitoring (ERP System)
	Denial of unauthorized data access	Low	Medium	Low	Logging and auditing (SIEM Solution)
Information Disclosure	Unauthorized access to customer data	Medium	High	High	Encryption & access control (ERP System, FAaS)
	Leakage of financial data	Low	High	Medium	Encryption & access control (ERP System, FAaS)
Denial of Service	DDoS attacks	Medium	High	High	DDoS protection service (FAaS)
	Ransomware attacks	Medium	High	High	Antivirus & cloud-based backup (Endpoint Security, Disaster Recovery)
Elevation of Privilege	Exploiting vulnerabilities in devices	Low	High	Medium	Patch management (Endpoint Security)
	Gaining administrative access	Low	High	Medium	Strong access control (FAaS, ERP System, Admin accounts, Endpoint agents)

Appendix C

8-Step Process Octave Allegro

OCTAVE Allegro (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a risk management approach that helps organizations identify and prioritize information security risks (Caralli et al., 2007). The security team will use the OCTAVE Allegro methodology to conduct a baseline assessment of Pampered Pets' current setup and re-apply after mitigations for digital transformation recommendations. The process typically involves the following steps (Caralli et al., 2007):

8-Step Process OCTAVE Allegro

Steps	Description
1.Establish Context	Gather information about Pampered Pets' operations, objectives, and environment (Caralli et al., 2007, p. 15).
2. Identify Key Assets	Determine critical assets for Pampered Pets, e.g., customer info, financial data, inventory, IT infrastructure, and intellectual property (Caralli et al., 2007, pp. 16-17).
3. Identify Threats	Recognize potential threats to Pampered Pets' assets, such as cyberattacks, theft, natural disasters, or human error (Caralli et al., 2007, pp. 18-20)
4. Identify Vulnerabilities	Assess vulnerabilities in Pampered Pets' assets, including weak security measures and outdated systems (Caralli et al., 2007, pp. 21-23).
5. Evaluate Risk	Determine the likelihood and impact of threats exploiting vulnerabilities, prioritize risks for Pampered Pets (Caralli et al., 2007, pp. 24-26).
6. Develop Risk Mitigation Plan	Create a plan for Pampered Pets to address significant risks, including stronger security measures and employee training (Caralli et al., 2007, pp. 27-29).
7. Monitor and Review	Continuously monitor the effectiveness of implemented measures and adjust as needed for Pampered Pets (Caralli et al., 2007, pp. 30-31).
8. Implement Risk Mitigation Plan	Execute the risk mitigation plan, ensuring that measures are effectively integrated into Pampered Pets' operations.

Appendix D

Risk & Threat Modelling Exercise with Potential Mitigations

Risk/Threat	Threat Modelling Exercise	Mitigation Strategies
Fire:	A fire in the store could result in damage to the inventory and the building. This could disrupt the business and result in financial losses.	Install smoke detectors, fire alarms, and fire extinguishers in the store. Conduct regular fire drills to ensure that staff members are familiar with the evacuation procedures.
Theft:	Theft of inventory or cash could result in financial losses for the business.	Implement security measures, such as CCTV cameras and alarm systems. Conduct background checks on new staff members before hiring them.
Cyber-attacks:	The business uses a networked computer and wireless connections for various apps. This makes it vulnerable to cyber-attacks, which could result in loss of data or financial theft.	Implement cybersecurity measures, such as firewalls, anti-virus software, and regular software updates. Train staff members on cybersecurity best practices, such as using strong passwords and avoiding phishing emails.

Supply chain disruptions:	Pampered Pets uses local suppliers for its pet foods. Any disruptions to the supply chain could result in a shortage of inventory, which could impact the business.	Maintain a diversified supplier base and build relationships with multiple suppliers. Conduct regular reviews of the suppliers' operations and have contingency plans in place to manage any disruptions.
Staff turnover:	The business employs four staff members. Any sudden loss of staff could disrupt business operations.	Implement a succession plan that identifies key roles and responsibilities and potential replacements. Provide training and development opportunities for staff members to ensure that they are motivated and engaged.
Reputation damage:	Pampered Pets has built a reputation for quality pet foods. Any incidents that could damage this reputation could result in financial losses.	Monitor social media and online reviews to identify any negative comments or reviews. Respond promptly to any complaints and take steps to address any issues raised by customers.

Appendix E

Risk & Threat Modelling Exercise with Potential Mitigations

Risk/Threat	Threat Modeling Exercise	Mitigation
Cybersecurity Risks	With the implementation of an online presence and the addition of online features, the business may become vulnerable to cybersecurity risks, such as hacking, phishing, and malware attacks. These attacks can lead to data breaches, loss of revenue, and reputational damage.	Implementing cybersecurity measures such as firewalls, antivirus software, and multi-factor authentication can help protect the business from cyber-attacks. In addition, regular training for employees on cybersecurity awareness can help reduce the risk of human error.
Supply Chain Disruptions	Changing to an international supply chain may increase the risk of supply chain disruptions due to transportation and customs issues. This can lead to delays in deliveries and a shortage of inventory, which	If the business changes to an international supply chain, it should conduct a thorough risk assessment of its suppliers and implement appropriate measures to mitigate any identified risks. The business should also diversify its supply chain to

	can lead to loss of revenue and customer dissatisfaction.	reduce the impact of any single supplier failure.
Operational Risks	The implementation of digital processes may increase operational risks such as system failures, power outages, and equipment malfunctions. These risks can lead to a loss of revenue and customer dissatisfaction.	The business should upgrade its computer systems and network infrastructure to ensure they are robust enough to handle the additional load of a digitalization process. Pampered Pets should also implement a disaster recovery plan and conduct regular backups of its data.
Legal and Regulatory Risks	The implementation of digital processes may increase legal and regulatory risks such as compliance with data protection laws, tax regulations, and online transaction regulations. Non-compliance can result in fines and reputational damage.	The business should keep up-to-date with changes in laws and regulations, conduct regular risk assessments, Develop policies and procedures that align with legal and regulatory requirements. Regular monitor the business to ensure it is complying. Have a plan to manage legal and regulatory crises. Seek legal advice if unsure about legal or regulatory

		advice. These steps can help mitigate legal and regulatory risk.
Customer Loss	If the business does not provide online features, it may lose up to 33% of its existing customers who prefer the convenience of ordering products online.	The business should provide training and development opportunities for its staff to enable them to manage the additional workload associated with digitalization. Pampered Pets should also consider outsourcing some of its digitalization tasks to a third-party service provider.

References

ISO, 2018. *ISO 31000:2018(en) Risk Management - Guidelines.* [Online]
Available at: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
[Accessed 12 April 2023].

Jahshan, E., 2021. *Online retail sales growth hit 13-year high in 2020.* [Online]
Available at: https://www.retailgazette.co.uk/blog/2021/01/online-retail-sales-growth-hit-13-year-high-in-2020/

NIST, 2014. *Cybersecurity Framework.* [Online]
Available at: https://www.nist.gov/cyberframework/framework
[Accessed 12 April 2023].

Science Direct, 2005. *eCommerce adoption in developing countries: a model and instrument.* [Online]
Available at: https://www.sciencedirect.com/science/article/abs/pii/S0378720604001314
[Accessed 12 April 2023].

Caralli, R. A. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Software Engineering Institute, Carnegie Mellon University. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8370

Alberts, C., & Dorofee, A. (2003). Managing Information Security Risks: The OCTAVE Approach. Addison-Wesley.

Chen, Y. (2017). The Importance of NIST Compliance for Organizations. Retrieved from https://www.tripwire.com/state-of-security/regulatory-compliance/the-importance-of-nist-compliance-for-organizations/

NIST (2012). Guide for Conducting Risk Assessments (NIST Special Publication 800-30 Rev. 1). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Kumar, V., & Reinartz, W. (2016). Creating enduring customer value. Journal of Marketing, 80(6), 36-68. https://doi.org/10.1509/jm.15.0416

Molla, A., & Licker, P. S. (2005). eCommerce adoption in developing countries: a model and instrument. Information & Management, 42(6), 877-899. https://doi.org/10.1016/j.im.2004.09.002

ISO. (2013). ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements. https://www.iso.org/standard/54534.html

Microsoft. (2021). Threat modeling: Designing for security. https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-guide