**Risk Identification Report – Digitising the Pampered Pets Business**

**Introduction**

Digitisation changes the behavioural pattern of people and businesses due to the incorporation of technological drivers such as big data, artificial intelligence, sensors, cloud computing, robotics, and so on (Kovaitė and Stankevičienė, 2019). A qualitative risk assessment method describing the characteristics and potential impact, in addition to categorising risk as high, medium, or low is used (Hubbard, 2020). The digitisation of the business will require the PASTA (The Process for Attack Simulation and Threat Analysis) threat modelling methodology. This is a risk centric framework with seven stages aiming to merge business objectives and technical requirements together (Shevchenko et al., 2018).

**Risk and Threat Modelling - PASTA**

1. Objectives: Digitisation of the business to improve internal business processes, and to expand its reach internationally.
2. Technical Scope: The digital migration opens up technical changes/innovations to the business outlook. These innovations will include Online ordering system (e-commerce), website and social media, payment gateways, shipping services, management information systems (ERP and CRM), digital marketing, data analytics tools, cyber security tools, collaborative tools, and physical security systems.
3. Application Decomposition: User interface, server, database, roles, assets, services, data storage, data flow, and logging.
4. Threat Analysis: External and insider attack analysis. Hacking, data breaches unauthorised access, espionage, disgruntled employee sabotage, user error, trade wars, cultural differences, social engineering, cyber-attack and network compromise.
5. Vulnerability Analysis: Use of manual and automation vulnerability scanners to identify vulnerabilities such as weak authentication, zero-day vulnerabilities, unpatched software, misconfigurations, inadequate encryption, and weak data security.
6. Attack Modelling: Attack surface analysis, attack tree development and analysis.
7. Risk and Impact Analysis: This is contained in the risk analysis matrix and risk mitigation in table 1.0 and table 2.0 respectively.

**Table 1.0 - Risk Analysis Matrix**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Risk Category** | **Likelihood** | **Impact** | **Risk Level** |
| **Supply Chain Risks** | Supplier failure | Medium | High | High |
|  | Ingredient quality issues | Low | Critical | High |
|  | Delivery delays | Medium | Medium | Medium |
|  | Price fluctuations | High | Medium | High |
| **Operational Risks** | Staff absence | Medium | High | High |
|  | Quality control issues | Medium | High | High |
|  | Equipment failure | Medium | High | High |
| **Technology Risks** | System Integration Issues | High | High | High |
|  | Data Security | Medium | Critical | High |
|  | Security Breach | High | High | High |
|  | Inadequate know-how | High | High | High |
| **Market Risk** | Trade wars between countries | Low | High | High |
|  | Customer Resistance | Low | Medium | Medium |
|  | Competition and Market Saturation | Medium | High | High |
| **Legal and Compliance Risk** | Privacy Issues | Low | Medium | Medium |
|  | Intellectual Property | Low | Medium | Medium |
|  | Regulatory Compliance | Low | High | High |
| **Reputation Risk** | Brand Image | Medium | High | High |
|  | Negative Customer Perception and Feedback | Low | High | High |
| **Finance Risk** | No Return on Investment | Medium | High | High |
|  | Ongoing Cost | High | Medium | High |

**Table 2.0 – Risk Mitigation/Recommendation**

|  |  |  |
| --- | --- | --- |
| **Technology Security** | **Operations** | **Market and Finance** |
| Implement Regular Data Backups | Document Standard Operating Procedures | Constant Customer Engagement |
| Secure Endpoints | Business Continuity Planning | Improved Product Quality |
| Document IT Processes | Implement Quality Assurance and Management | Strategic Alliance and Partnership |
| Train Staff on Security Basics | Establish Regular Supplier Reviews | Monitor Financial Performance |
| Carryout Updates and Patches to Software and Applications Frequently | Create Quality Control Metrics | Create Loyalty Program |
| Monitor and Analyse Security Threats | Implement Staff Backup Plans | Establish Communication Protocols |
| Develop IT Disaster Recovery Plan | Create Training Documentation | Hedge Financial Risk |
|  | Establish Supplier Agreements | Regular Financial Audit |
|  | Outsource Non-Critical Activities | Maintain Quality Relationship with Financial Institutions |
|  | Conduct Regular Audits and Reviews | Maintain Fiscal Discipline |

**Digitisation**  
The process is a holistic transformation with a tendency to open up the business for growth and efficiency.

|  |  |  |
| --- | --- | --- |
| **Item** | **Digitisation** | **Risk** |
| **Digital Presence** | Website and Social Media Set-up | Reduced Credibility, Reduced Competitive Edge, Limited Reach, Poor Customer Engagement |
| Digital Marketing | Limited Market Reach, Reduced Competitive Edge, Poor Data Insight, High Costs, Reduced Customer Engagement |
| E-commerce platform | Increased Operational Cost, Limited Reach, High Foot Traffic to Physical Store |
| **Management Information Systems** | Supply Chain and Inventory Management ERP Systems | Poor Decision Making, Increased Operational Cost, Reduced Customer Satisfaction, Regulatory Non-Compliance |
| Customer Relationship Management Systems | Reduction in Customer Satisfaction, Reduced Competitive Advantage, Poor Customer Data Management |
| Data Analytics tools | Poor Customer Insights, Inefficient Operations, Reduced Competitive Edge |
| **Digital Communication** | Collaborative Tools | Poor Communication, Delay in Service Delivery, Decreased Productivity |
| Chabots and Online Support | Decreased Customer Satisfaction, Missed Sales Opportunities, Loss of Competitive Edge, Increase in Operational Cost |
| **Cyber Security** | Anti-Virus Software, Intrusion Detection Systems, Vulnerability Scanners, Firewalls | Data Breaches, Theft, Operational Disruption, Increased Vulnerability, Reputational Damage, Regulatory Penalties and Fines. |
| **Physical Security** | Access Control Systems | Unauthorised Access, Safety Risks, Operational Disruption, Data Breaches, Loss of Trust |
| Alarm and Surveillance Systems | Fire and Safety Hazards, Operational Disruption, Repudiation, Higher Liability and Insurance Premium |
| Power Backup Systems | Power Outages and Operational Interruptions |
| **Training and Development** | Staff Training and Re-Training | Incompetence |

**Reference**

Hubbard, D.W., 2020. *The failure of risk management: Why it's broken and how to fix it*. John Wiley & Sons.

Kovaitė, K. and Stankevičienė, J., 2019, May. Risks of digitalisation of business models. In *Proceedings of 6th International Scientific Conference Contemporary Issues in Business, Management and Economics Engineering ‘2019*.

Shevchenko, N., Chick, T.A., O’Riordan, P., Scanlon, T.P. and Woody, C., 2018. Threat modeling: a summary of available methods. *Software Engineering Institute| Carnegie Mellon University*, pp.1-24.