JPD

Risk Assessment Report For Jessa's Pickled Delights

Name: Jessa Fayer

Date: 05/15/2024

INST464-102

Table of Contents

Table of Contents

About This Document

Introduction: Jessa's Pickled Delights, a family owned business. A generational Ukrainian family pickle recipe . originally made and produced in Odessa Ukraine reestablished in Clarksburg, Maryland. Jessa's Pickled Delights embodies family, orientated, high-quality, simple ingredients, ethically produced and extraordinary flavors. Since restoring this family passion in 2000, we've grown our business locally, sharing our heritage at Maryland farmers' markets. only starting in a small kitchen, we were able to expand. Today using the digital world we have been able to share our product worldwide. generating online sales, and digital customer engagement, the necessity to safeguard our cyber infrastructure is more pressing than ever. In this risk assessment cyber security report, aims to share the digital paths our pickles travel, ensuring that every mason jar we sell, embodies what we stand for heartfelt tradition. an addition. A statistical report on How the business To protects its growing online sales and consumer engagement platforms against cyber attacks.

Objective: Our objective is to identify and evaluate potential cybersecurity vulnerabilities that could potentially cause disturbances to our business or negatively impact our financial standing. This analysis will assist us to develop suitable plans for safeguarding our vital digital and informational resources, thus ensuring the security and resilience of our organization in the case of cyber attacks.

Goals:Assessing by, identifying vulnerabilities, detecting security gaps that has a risk of being exploited. then evaluating the risks determining appropriate within our current IT systems operational, reputational, and the financial impacts of the potential cyber security threats may cause. Based on the findings from our research, we were able to create a cyber security protocol tailored to these challenges. Finally, our goal is to strengthen our company's ability to respond and recover and based on the findings from our research, we were able to create a cyber security protocol tailored to these challenges. Finally, our goal is to strengthen our company's ability to respond and recover and prevent. from any cyber incidents,

Scope:A walk-through of several key areas of our cybersecurity posture. starting with an examination of the security measures for the website and online payment systems. Data management to ensure protection of the business data and customers information. compliance of regular protocol.as PCI-DSS and local data protection laws enhancing our staff's cybersecurity practices to reduce the risks associated with human factors.

Methodology: Assessing identifications of both digital and physical assets, then organizing Using the FAIR model, assessing identifications of both digital and physical assets, then organizing proceed to threat modeling to analyze potential threats and their impacts followed by a vulnerability analysis, where we review any identifications of weaknesses in our system, using the findings from our research, apply qualitative and quantitative methods to conduct a detailed risk analysis, assessing the severity of the identified risks. develop a mitigation strategy that addresses the vulnerabilities.

Innovation: With the use of Advanced AI tools. Kat, hyper analyze analytics to predict and prepare potential breach scenarios interrogating these tools will enhance the overall I risk management approaches. to not only react to current security challenges but also proactively prepare for potential future threats.

Data Collected: Includes examination of network architecture, software usage, transaction logs and history, access controls, and cybersecurity awareness surveys.

Limitations: the availability of historical data on past incidents limits our prediction accuracy and hinders breach prediction. The cybersecurity landscape resource constraints within our organization, particularly in terms of budget and cybersecurity expertise, limit our ability to implement the most advanced security measures, potentially leaving some areas less protected than others.

Analytical Confidence: Comprehensive use of established methodologies and detailed data analysis, rating of medium high

Key Terms

FAIR: Factor Analysis of Information Risk
In our cybersecurity strategy at Jessa's Pickled Delights, we leverage the FAIR model as a fundamental tool for risk assessment. Unlike traditional qualitative methods, which often provide only broad estimations, FAIR introduces a quantitative approach. It helps us gauge the probability and potential financial impact of various cybersecurity threats, enabling us to allocate resources more effectively and ensure our digital storefront and customer data are robustly protected against potential cyber threats.

PCI-DSS: Payment Card Industry Data Security StandardAdhering to PCI-DSS is critical for us at Jessa's Pickled Delights, where we handle numerous online transactions daily. This set of security standards, developed by the Payment Card Industry Security Standards Council, is designed to secure credit card transactions and protect cardholder data. Compliance is not merely about following regulations—it is crucial for preventing data breaches and maintaining trust with our customers by ensuring their payment information remains secure.

DDoS: Distributed Denial of Service A Distributed Denial of Service (DDoS) attack poses a significant threat to our online presence by overwhelming our website with traffic, effectively blocking legitimate customers from accessing our products. These attacks typically employ a network of compromised computers to inundate the site with traffic. Recognizing the critical nature of website availability for our sales, we prioritize robust DDoS protection measures to maintain uninterrupted service, ensuring that our customers can consistently access and purchase their favorite pickles.

Limitations

Our risk assessment aims to comprehensively identify and mitigate potential cybersecurity threats to Jessa's Pickled Delights. However, it's important to recognize certain limitations that could influence the accuracy and reliability of our findings:

Limited Historical Data: As a small, family-operated business specializing in gourmet pickles, Jessa's Pickled Delights has fortunately not faced significant cybersecurity incidents to date. This lack of previous incidents, while positive, means we have limited empirical data to inform our risk predictions. This could affect our ability to forecast and prepare for potential future threats accurately.

Dynamic Threat Landscape: The nature of cybersecurity threats is rapidly evolving, with new challenges emerging more quickly than many organizations can adapt. For a boutique company like ours, staying ahead of the latest threats without the same resources as larger corporations can be particularly challenging.

Internal Resource Constraints: Our operations, while efficient, do not include extensive monitoring and reporting systems often found in larger organizations. This limitation might impact the depth and accuracy of our cybersecurity analysis, as our capacity to track and manage cyber threats in real-time is less developed.

Third-Party Dependencies: We rely on external partners for critical services, including payment processing and web hosting. While these relationships are essential for our business operations, they also expose us to risks that are not entirely within our control, as these third parties could potentially be sources of vulnerabilities

Subjectivity in Risk Valuation: Although we utilize quantitative methods like the FAIR model for a structured approach to risk assessment, certain aspects still require subjective judgment. Estimating the likelihood of specific threats and their potential impacts can vary depending on the individual analyst's perspective and experience, introducing a level of subjectivity to our assessments

Analytical Confidence

Analytical Confidence: Medium

The confidence in this cybersecurity risk assessment is rated as Medium, supported by our rigorous approach and professional insights, yet mindful of certain constraints:

- Industry-Standard Methodologies: We've utilized well-established frameworks like FAIR and adhered to PCI-DSS guidelines, ensuring our methods are aligned with recognized standards in risk assessment and data security.
- Integrated Data Analysis: Our assessment combines qualitative insights with quantitative data, offering a well-rounded analysis through detailed scenario evaluations and projections.
- Expert Input: Conducted by professionals with deep expertise in cybersecurity, our analysis is rooted in the latest best practices, ensuring reliable interpretations and recommendations.
- Data Limitations: This rating reflects the constraints posed by limited historical data, affecting our ability to predict certain cybersecurity events with greater precision.
- Proactive Strategy: Despite these data limitations, our report proactively addresses both current and emerging threats, underscoring our commitment to enhancing the company's resilience.

Executive Summary

Company Profile: Jessa's Pickled Delights

Introduction: This report provides an overview of Jessa's Pickled Delights, a family-owned business specializing in gourmet pickles, operating within the food and beverage industry.

Company Overview:

Jessa's Pickled Delights is celebrated for producing a variety of artisanal pickles, each crafted with traditional methods blended with unique, modern flavors. originally established in Odessa Ukraine has newly renovated in Clarksburg, Maryland, the company has since prioritized local, high-quality ingredients sourced directly from regional farmers.

Industry Overview:

The company is classified under the foodservice industry. Specializing in gourmet preserved foods market. This sector is known for its level of quality, artisanal products, and being sold directly to consumers through local markets and online platforms. The product has a short shelf time due to no added preservatives. The industry has seen a surge in demand, particularly with the freshness of our products, locally sourced and organic products.In Addition increasing consumer interest on social media platforms and a high demand in unique pickle products from tik tok trends.

Company Size:

Jessa's Pickled Delights is a small-scale operation with fewer than 25 employees, generating an estimated annual revenue of approximately $200,000. This size allows for a hands-on approach to product quality and customer service but presents challenges in scaling operations without compromising the artisanal quality.

Security Concerns in the Industry:

The food and beverage industry, particularly small organizations with online sales platforms, confronts a number of cybersecurity vulnerabilities. These include data breaches involving consumer personal and payment information, as well as company disruptions caused by DDoS attacks. The reliance on digital platforms for sales and consumer connection has made organizations more vulnerable to cyberattacks.

Known Attacks:

Historically, the industry has witnessed several high-profile cybersecurity incidents:

- Small businesses, including boutique food shops, have been targets for phishing attacks aiming to steal financial data.
- DDoS attacks have disrupted online sales during peak shopping seasons, causing significant financial losses.
- Ransomware attacks have targeted larger entities within the industry, leading to substantial ransom demands and operational downtime.

Company Overview

Establishment and Operations

The business was established originally in the early 2000s in Ukraine, using a pass down family recipe in 2024 the business reopened in Clarksburg, Maryland. Jessa's Pickled Delights has carved it's status in niche food and beverage industry with its focus on high-quality, ethically made, gourmet pickles.The company uses traditional techniques in creating strong, captivating flavors for a unique pickle varieties such as pineapple jalapeño, and cinnamon.   This combination of old and new encapsulates the company's ethos of blending tradition with modernity. A flavor the customer has never experienced before, complete originality.

Products and Customers

The primary offerings of Jessa's Pickled Delights include a range of artisanal pickles, each made using fresh, locally-sourced ingredients without preservatives. The company caters to health-conscious consumers looking for premium, flavorful options. customers will able to count the number of ingredients with their fingers, and no exactly what they're putting in their consuming . Customers range from local gourmet food enthusiasts, local visitors at farmers, social media fans from all around the United States.

Financial Overview and Staffing

With an annual revenue of approximately $200,000 and operating costs around $150,000, Jessa's Pickled Delights operates on a modest scale with fewer than 25 employees, mostly being friends and family. This small team allows the company to maintain a hands-on approach to quality for top notch customer service.

IT and Cybersecurity Infrastructure

The IT infrastructure data includes essential systems that support business operations:

- **Business Productivity**: The company utilizes Google Suite to manage emails, documents, and spreadsheets, facilitating efficient organizational management.
- **Website and Online Presence**: The website is custom-coded by the creator of the company using C++, Java, and Python, hosted on visual code studios, and integrates tools like Google Analytics for tracking website traffic, Mailchimp for marketing campaigns, and Zendesk for customer support.

- **Payment Processing Systems**: Transactions are processed through various platforms including credit cards, PayPal, Venmo, Apple Pay, and cash. The online payment system adheres to PCI-DSS standards, ensuring secure data handling.
- **Customer Relationship Management**: Salesforce Essentials is used to manage customer interactions, chosen for its suitability for small businesses.

Security Measures

While Jessa's Pickled Delights does not currently have an IT team, it dose prioritize security and privacy. Security measures such as encrypted storage and restricted access to protect the business and customer data. Regular audits and employee training sessions are conducted to enhance cybersecurity awareness and mitigate human-factor risks.

Regulatory Compliance and Risks

The company complies with FDA regulations of food safety and adheres to privacy regulations to protect customer data. Potential risks include data breaches from online sales and payment processing, and system interruptions that could impact production. Steps are taken to assess and fortify against these vulnerabilities continually.

Summary

Inspired by family owned secret recipes and morels. The company wants to share the joy and heritage by giving the public delicious pickles. Jessa's Pickled Delights not only offers distinctive pickle products but also engages deeply with the local community. The company's focus on quality, coupled with a robust approach to business operations and cybersecurity, positions it well within the competitive landscape of the food and beverage industry.

[1]

[1]

Qualitative Risk Analysis

Assets and Their Value to the Company:

1. **Recipes and Production Methods:** The core of Jessa’s unique offerings lies in its secret family recipes and specialized production methods, which differentiate its products in the competitive market.
2. **Customer Data:** Includes users payment, and shipping information that is needed for online sales.Production equipment and inventory, needed for operations.
3. **Website and Online Sales Platform:** The primary interface for engaging with customers and processing sales, integral to revenue generation.
4. **Brand Reputation:** Built on family values, promising top quality products, customer trust, pivotal for long-term business sustainability.

Threat Vectors:

- **Cyberattacks on IT Infrastructure:** Threats such as hacking, which can compromise the website and payment systems.
- **Physical Damage or Theft:** Affecting production capability and inventory.
- **Data Breaches:** Leading to the loss of sensitive customer information.
- **Intellectual Property Theft:** Potentially exposing company recipes and techniques to competitors.

Threat Actors:

- **Cybercriminals:** Targeting the company for financial gain through data theft.
- **Disgruntled Employees:** Who might misuse their access to sensitive information.
- **Competitors:** Interested in gaining insights into proprietary production processes.
- **Natural Events:** Such as fires or floods that could damage physical assets.

Potential Losses:

- **Primary Losses:**
  - **Financial Losses from Cyberattacks:** Including the cost of rectifying security breaches and potential fines for data breaches.
  - **Loss of Intellectual Property:** loss of competitive edge if production methods are leaked, loses its originality
- **Secondary Losses:**
  - **Reputation Damage:** Resulting from customer distrust if personal data is compromised or product quality is affected by theft of recipes.
  - **Operational Disruption:** From physical damage to production facilities or IT systems.
  - **Legal and Compliance Costs:** Arising from failure to protect customer data or adhere to follow food safety regulations.

Scenarios and Assumptions:

1. **Scenario - Data Breach via Hacking:**
   - **Assumption:** Cybercriminals target the company's payment system, exploiting a vulnerability in the website.
   - **Probability:** Medium (20-30%), given the increasing sophistication of cyberattacks and current reliance on standard cybersecurity measures.
   - **Impact:** High, considering the potential financial losses and damage to customer trust.
2. **Scenario - Theft of Intellectual Property:**
   - **Assumption:** Competitors or disgruntled employees steal proprietary recipes or production techniques.
   - **Probability:** Low (10-15%), due to limited access to these assets and existing non-disclosure agreements.
   - **Impact:** Severe, as it could erode the unique market position and future product development.

3. **Scenario - Physical Asset Damage from Natural Disaster:**
    - **Assumption:** A significant natural event damages the production facility.
    - **Probability:** Low (5-10%), based on geographic and climatic conditions.
    - **Impact:** High, due to the direct impact on production capability and associated recovery costs.

Scenario Chart

Asset	Threat Methods	Threat Actors	Loss Types	Loss Scale
Server	DDOS, Ransomware, Virus, Misconfiguration, Physical Damage	Script Kiddies, Criminal Groups, Disgruntled Staff, Natural Events	Loss of revenue, Cost to restore services, Cost to move to cloud, Legal fees & settlement	Minimum loss $5K/day offline, Rebuild: $30K, Cloud: $150K/year, Estimated direct loss of $1.5M, Legal fees & settlement: $1M
Payment Info	Direct Hack, Phishing, Admin Theft	Criminal Groups, Individual Criminals	Loss of payments, Secondary loss from lawsuit	Direct loss: ~$500K, Legal fees & settlement: ~$3M
Account Info	Direct Hack, Phishing, Admin Theft	Script Kiddies, Criminal Groups, Individual Criminals	Loss of personally identifiable information (PII), Possible payment loss, Lawsuit	Direct loss: ~$500K, Legal fees & settlement: ~$3M

Scenarios and Assumptions:

Server:

- **Scenario:** The server of Jessa's Pickled Delights is susceptible to multiple threats ranging from cyberattacks like DDOS and ransomware. In the case of nature disasters risk of physical damage.

- **Assumption:** Regarding digital sales, any significant downtime from the business can impact the sales, revenue and necessitate costly moves to more secure cloud environments.

Payment Information:

- **Scenario:** The payment system is vulnerable to direct hacking and phishing attempts, leading to significant financial data breaches.
- **Assumption:** The high-value nature of financial data makes this system a prime target, with potential lawsuits stemming from breaches.

Account Information:

- **Scenario:** Customer account databases, risk of cyber threats including, hacking, leading to loss of personal information.
- **Assumption:** These databases contain sensitive PII, making them attractive targets for data theft, which can lead to substantial legal repercussions and potential payment losses.

Table 2: Heat Map

Certain	🟨	Scenario: Loss of Server/Website	🟥	🟥
Very Likely	🟨	Scenario: Loss of Customer Payment Info	🟧	Scenario: Compromise of Payments System

Likely	🟨	Scenario: Loss of User Account Logins	🟧	🟧
Unlikely	🟩	🟨	🟨	🟧
Possible	🟩	🟩	🟨	🟨
Probability vs. Severity	Low	Medium	High	Severe

Scenario Chart Detailing

Asset: Server

- **Threat Methods:** DDOS, Ransomware, Virus, Misconfiguration, Physical Damage
- **Threat Actors:** Script Kiddies, Criminal Groups, Individuals, Staff, Natural Events
- **Loss Types:** Loss of revenue, Cost to restore, Cost to move to cloud, Legal fees & settlement
- **Loss Scale:** Minimum $10K/day offline, Rebuild: $50K, Cloud: $200K/year, Estimated direct loss of $2M, Legal fees & settlement: $2M

Asset: Payment Info

- **Threat Methods:** Direct Hack, Phishing, Admin Theft
- **Threat Actors:** Criminal Groups, Individual Criminals, Staff
- **Loss Types:** Loss of payments, Secondary loss from lawsuit
- **Loss Scale:** Direct loss: ~$1M, Legal fees & settlement: ~$5M

Asset: Account Info

- **Threat Methods:** Direct Hack, Phishing, Admin Theft
- **Threat Actors:** Script Kiddies, Criminal Groups, Individuals
- **Loss Types:** Loss of PII for users, Possible payment loss, Lawsuit?
- **Loss Scale:** Direct loss: ~$500K, Legal fees & settlement: ~$2M

Placement: Severe Reasoning: Risky sensitive information needs constant maintaining online operations. The high costs of recovery and significant revenue loss due to downtime place it in the high risk category.

Scenario: Loss of Customer Payment Info

Placement: High Reasoning: The potential risk of customer payment information being tampered and leaked. Massive financial and reputational damage, requiring extensive recovery efforts including legal settlements and potential legal issues.

Scenario: Compromise of Payments System

Placement: High Reasoning: A compromise in the payments system directly impacts the business's ability to run, pause operations, potentially leading to significant direct financial loss and secondary losses such as legal fees.

Scenario: Loss of User Account Logins

Placement: Likely

Reasoning: The loss of user account logins is likely given potential vulnerabilities in user authentication systems. While not as severe as other scenarios, it requires preventive measures due to the risk of unauthorized access to customer accounts.

Quantitative Risk Analysis

Quantitative Risk Analysis for Jessa's Pickled Delights

In this section, we explore the quantitative components of our cybersecurity probability assessment for Jessa's Pickled Delights . using the equitable system, we carried out simulations for each identified likelihood scenario, reduce specifically on the financial affects preferably the broader CIA triad of confidentiality, integrity, and availability .Methodology and Data Inputs

The input numerical for our simulations were derived based on a combination of historical data, industry benchmarks, and projections based on observed trends within the food and beverage industry. For each scenario—server disruption, payment information breach, and account information compromise—we estimated the probability of occurrence as follows:

- Minimum Probability: This figure represents the lowest probability under optimal security conditions.
- Most Likely Probability: This value is the expected likelihood under typical daily operations.
- Maximum Probability: This rate reflects the probability during peak vulnerability, such as during high traffic seasons or immediately following significant changes to the IT infrastructure.

These probabilities were informed by insights gained from the qualitative analysis where specific cybersecurity weaknesses were identified. For instance, our analysis highlighted vulnerabilities in server security and payment information systems which influenced our probability estimations.

Simulation Results and Loss Exceedance Curves (LEC)

We generated Loss Exceedance Curves for each scenario to visualize the potential financial impact over a range of probable loss scenarios. The LECs provided three critical data points:

- Minimum Loss: Represents the guaranteed minimum financial loss due to an incident, observable with near certainty (100% probability).
- Maximum Loss: Corresponds to the catastrophic potential loss, albeit at a very low probability (.0001%).
- Average Loss: Typically aligns with the median financial impact, around the 40% probability mark.

From these points, we further calculated the discounted losses for more refined probabilities:

- 95% Likelihood: Typically smaller operational impacts, such as short-term service disruption.
- 50% Likelihood: Represents significant but manageable financial impacts, possibly involving moderate data breaches.
- 5% Likelihood: Encompasses extreme scenarios such as full-scale data breaches with severe financial and reputational damage.

Interpretation of Results

The LEC illustrates not just potential losses but also aids in decision-making regarding cybersecurity investments. The curve's intersection with the company's risk appetite indicates whether the current security measures are sufficient or if additional investments are necessary. For instance, if the curve's higher loss ranges fall below the company's risk threshold, it suggests an over-investment in risk mitigation which could be scaled back to optimize resource allocation.

Risk Mitigation and ROI

The analysis of the LECs assists in identifying effective mitigation strategies and calculating their return on investment (ROI). For example, enhancing server security might involve an upfront cost but if it significantly reduces the probability of high-impact scenarios, the investment can be justified through a lower expected annual loss.

Conclusion

This quantitative analysis reaffirms the necessity of targeted cybersecurity improvements at Jessa's Pickled Delights. By understanding the financial implications through the FAIR model and LECs, we can better manage cybersecurity risks, ensuring the protection of our digital assets and the long-term viability of the company.

Recommendations for Cyber Risk Management at Jessa's Pickled Delights

Actionable Plan Overview:

Based on the comprehensive qualitative and quantitative analysis conducted, we recommend a set of strategic actions tailored to enhance the cybersecurity posture of Jessa's Pickled Delights. These recommendations are designed to align with industry norms and address identified vulnerabilities effectively.

Industry Norms:

In the food and beverage sector, especially among small to medium-sized enterprises (SMEs), there is a growing emphasis on safeguarding digital transactions and customer data. Compliance with standards like PCI-DSS and GDPR is critical for protecting against data breaches and ensuring consumer trust.

Risk Trade-Offs and Mitigation Strategies:

1. Avoiding Risks:
   - Activity Elimination: Discontinue use of legacy systems that cannot be securely updated. This prevents potential security breaches from outdated technology.
2. Mitigating Risks:
   - Employee Training: Implement targeted training programs focusing on phishing detection, safe internet practices, and secure handling of customer data. Specific, role-based training can enhance the effectiveness of these programs.
   - Security Enhancements: Deploy advanced security solutions such as encryption for stored and transmitted data, and multi-factor authentication for system access. Regular security audits and updates to these measures are crucial.
   - Social Controls: Establish a security-aware culture through ongoing educational initiatives and visible management support for cybersecurity practices.
3. Transferring Risks:
   - Cybersecurity Insurance: Obtain insurance that covers data breaches and cybersecurity incidents. For a business like Jessa's Pickled Delights, annual premiums could range from $1,500 to $3,000, depending on coverage levels.
   - Outsourcing Security Management: Consider contracting with a cybersecurity firm for advanced security management, which could cost $2,000 to $10,000 monthly depending on the services provided.
4. Accepting Risks:
   - Cost-Benefit Analysis: If the cost of implementing cutting-edge security measures significantly outweighs the potential loss reduction spending $500K annually to reduce losses by only $50K, it may be more economical to accept and budget for these risks, particularly where the probability of occurrence is low.

Updating Loss Exceedance Curves (LECs):

After implementing the recommended security measures, it is important to maintain updates of the LECs to reflect the reduced risk levels. This demonstrates how effective risk management can lead to substantial financial savings.

Loss Comparison Chart:

- Before Mitigation: Potential loss from a server breach reach $200K.

After Mitigation: With improved security protocols, potential losses could be reduced to $10K.

- This visual comparison highlights the return on investment from the implemented security measures.

Conclusion:
These recommendations strive to improve Jessa's Pickled Delights' overall defense's against potential cybersecurity threats in addition to reducing the specific risks that have been identified. By implementing these tactics, the business may preserve its competitive advantage in the market, safeguard its client connections, and guarantee ongoing adherence to industry norms.

Appendix 1: FAIR Results

Insert your spreadsheet of FAIR results
This is where you can show the details of the inputs to the FAIR App

Appendix 1: FAIR Results

The following spreadsheet provides a detailed view of the inputs and results from the FAIR (Factor Analysis of Information Risk) model utilized in the quantitative risk analysis of Jessa's Pickled Delights. These results outline the threat frequency, probable loss magnitudes, and the associated financial impacts calculated for each identified risk scenario.

FAIR Model Spreadsheet Overview:

Risk Scenario	Annual Rate of Occurrence	Probable Loss Magnitude	Minimum Loss	Most Likely Loss	Maximum Loss	Calculated Annual Loss Exposure
Loss of Server/Website	0.05 (5%)	$50K to $2M	$10K	$500K	$2M	$250K
Loss of Customer Payment Info	0.02 (2%)	$100K to $5M	$1M	$3M	$5M	$600K
Compromise of Payments System	0.01 (1%)	$500K to $5M	$500K	$2.5M	$5M	$250K

Notes on FAIR Analysis:

- **Annual Rate of Occurrence**: Estimated based on industry data and previous incident reports.
- **Probable Loss Magnitude**: Derived from potential financial impacts including direct costs, fines, and reputational damage.
- **Calculated Annual Loss Exposure (ALE)**: Product of the probable loss magnitude and the annual rate of occurrence, giving a rough estimate of the expected yearly financial impact.

These inputs were selected based on historical data, professional opinion, and industry standards. The range in the 'Most Likely Loss' column highlights the uncertainty in the level of damage caused by each scenario, emphasizing the crucial necessity for effective risk management measures.

Appendix 2: c

Grillo’s Pickles. (n.d.). Our story. Retrieved from https://www.grillospickles.com/our-story/

Institute of Risk Management. (n.d.). Homepage. Retrieved from https://www.theirm.org/

Common Good. (n.d.). Food & beverage. Retrieved from https://www.commongood.co/food-beverage/?keyword=food%20marketing%20agency&matchtype=p&campaign=19689708450&adgroup=146147268157&device=c&utm_term=food%20marketing%20agency&utm_campaign=CPG+%7C+GFF&utm_source=adwords&utm_medium=ppc&hsa_acc=6393051773&hsa_cam=19689708450&hsa_grp=146147268157&hsa_ad=648462871631&hsa_src=g&hsa_tgt=kwd-332554439263&hsa_kw=food%20marketing%20agency&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=Cj0KCQjwgJyyBhCGARIsAK8LVLORTa0JFhZ2wFSUekUEYpxVilYMRt5LzJ1rLtZBO4nQuibdXjKOfQUaAq92EALw_wcB

National Institute of Standards and Technology. (n.d.). Glossary: Risk assessment report. Retrieved from https://csrc.nist.gov/glossary/term/risk_assessment_report#:~:text=Definitions%3A,the%20process%20of%20assessing%20risk.

IPKeys Technologies. (n.d.). NIST risk assessment report. Retrieved from https://ipkeys.com/blog/nist-risk-assessment-report/

Health and Safety Executive. (n.d.). Risk assessment: Template and examples. Retrieved from https://www.hse.gov.uk/simple-health-safety/risk/risk-assessment-template-and-examples.htm