Risk Assessment:

Incident No.	0001 (Conti Lab)
Date of Incident:	8th September 2021
Client Name:	Joes Fishshop
Type of Incident:	Data Breach, Ransomware, Phishing Attack

Data Confidentiality:
Impact: High
Likelihood: Moderate/High
Description: The potential compromise of sensitive data during the incident, coupled with the sophisticated attack methodology, poses a significant risk to data confidentiality. This could lead to unauthorized access to sensitive information, including customer data, intellectual property, or financial records.

System Availability:
Impact: High
Likelihood: High
Description: The attack's potential impact on system availability is substantial. The deployment of ransomware or other malicious activities could lead to system failure, disrupting critical business operations. The business may face downtime, which in this case it did as systems were encrypted and access blocked, therefore impacting productivity and potentially resulting in significant financial losses.

Operational Integrity:
Impact: High
Likelihood: High
Description: The attacker's ability to execute malicious code, create unauthorized user accounts, manipulate system processes and disable vital software such as windows defender, indicates a risk to the organization's ability to maintain control over its IT system and infrastructure. This can result in unauthorized access, data manipulation, data exfiltration or even system shut down

Financial Loss:
Impact: High
Likelihood: High
Description: The incident poses a huge risk of financial loss to the organization. Financial loss can come from various factors in relation to this type of incident, see the list as follows;

Data Confidentiality – regulatory fines and reputation.
System Availability – business continuity.
Operational Integrity – business continuity and reputation.
System Restoration – The most obvious as businesses are usually required to pay huge sums for restoring their systems.
Legal Consequences – The business could be taken to court of data loss, confidential payment information via banks.

Reputation Damage:

Impact: High
Likelihood: High
Description: The potential loss of sensitive data and potential disruption of services can lead to severe damage to the organization's reputation. Customers, partners, and stakeholders may lose trust in the organization's ability to protect their information and fulfil their needs, ultimately impacting the company’s image. Depending on the size of the company and coverage of this incident the consequences could be even more severe.

Regulatory Compliance:
Impact: High
Likelihood: High
Description: The incident poses a high risk of non-compliance in relation with data protection regulations and national/international industry standards. There are many factors here to consider that could influence the outcome such as the nature of the compromised data, the organization may face legal consequences, regulatory fines, and the need for extensive remediation efforts to meet compliance requirements.

Overall Risk Level:

High

Recommendations:

1. 34% of Conti Ransomware attacks are via Phishing Emails. Therefore conduct thorough security awareness and phishing email training for employees. Extremely important as this was initial port of entry.
2. Strengthen network segmentation and access controls.
3. Implement a robust backup and recovery strategy. Look into cold storage backup options
4. Enhance monitoring and detection capabilities with intrusion prevention systems.
5. Regularly update and patch systems and software. 36% of Conti attacks are initiated via software vulnerabilities.
6. Conduct thorough security awareness and phishing scam training for employees.
7. Establish clear policies and guidelines for remote desktop use, ensuring that all users are aware of and comply with security measures. Implement MFA authentication to add extra levels of security. 30% of Conti attacks are initiated via RDP
8. Collaborate with regulatory authorities to ensure compliance with data protection regulations.