#NextGen Solutions:Risk Assessment Report

1. **Scope of Assessment**

Focus Areas

- Data Security
- Employee cyber Awareness
- Network Infrastructure

Assets to be protected: Customers data, Severs, NextGen's Infrastructure, Applications.

2. **Identified Risks**

External Risk

A. Phishing Attacks

- Likelihood: High
- Impact: Severe (comprising employee credentials leading to data breaches), If the software development team, Security Operations Center, Customer support and Admin team is to fall for a phishing attack, it will be very severe.

B. Malware Attacks

- Likelihood:Medium
- Impact: Severe (data breaches can damage company reputation leading to loss of revenue and customers making it very severe).

C. DDoS Attacks

- Likelihood: Low
- Impact: Moderate (disrupting of hosted services affecting client operations), API targeting payment gateway can be very serious but not severe.

Insider Threat

A. Insider threat

- Likelihood: Medium
- Impact: High (unauthorized access to sensitive employee data through breach from the customers support will be very serious but not severe).

B. Data misconfiguration

- Likelihood: Medium
- Impact: High (unintended exposure of cloud resources from the software development team can be very high).

Physical Threat

A. Device Theft

- Likelihood: Medium
- Impact: High (loss of company laptops containing sensitive information can have high damages to the company.

B. Unauthorized Physical Access

- Likelihood: Medium
- Impact: Moderate (tampering with network devices in the IT room)

3. **Risk Analysis and Risk Prioritization (Matrix)**

**Likelihood **	**Minimal**	**Moderate**	**High**	**Severe**

Impact				
Low		DDoS Attacks		
Medium		Unauthorized Physical Access	Insider Threats, Data Misconfiguration , Device Theft	Malware Attacks
High				Phishing Attacks

4. **Mitigation Strategies**

For External Threats:

A. Phishing Attacks:

- Conduct wide phishing awareness training for employees according to Payment Card Industry Data Security Standard (PCI DSS) and GDPR.
- Implement robust email filtration solutions in laptops and gadgets used to detect malicious emails in NextGen Solutions.

B. Malware Attacks:

- Deploy endpoint protection tools with anti-malware features in all the systems in NextGen solution.

C. DDoS Attacks:

- Use a cloud based DDoS protection service to filter malicious traffic in NextGen Solution.

For Internal Threats:

A. Insider Threats:

- Enforce role-based access controls (RBAC) to limit data access in NextGen Solution.
- Implement employee activity monitoring tools for all staff in NextGen solution.

B. Data Misconfiguration:

- Regular audit cloud storage configurations to all systems in NextGen Solution.
- Use automated tools to detect and alert on misconfiguration.

For Physical Threats:

A. Device Theft:

- Use full-disk encryption on all laptops in NextGen Solution.
- Mandate the use of cable locks for devices in NextGen Solution offices

B. Unauthorized Physical Access:

- Install access control system for secure areas in NextGen Solutions.
- Use surveillance cameras to monitor physical spaces in and around NextGen solutions.

5. **Risk Registry**

Risk	Likelihood	Impact	Severity Rating Based on Impact and likelihood	Mitigation Strategy
Phishing Attacks	High	Severe	Severe	Conduct wide phishing awareness training for employees according to Payment Card Industry Data Security Standard (PCI DSS) and GDPR. Implement robust email filtration solutions in laptops and gadgets used to detect malicious emails in NextGen Solutions.
Malware Attacks	Medium	Severe	Severe	Deploy endpoint protection tools with anti-malware features in all the systems in NextGen solution.
DDoS Attacks	Low	Moderate	Moderate	Use a cloud based DDoS protection service to filter malicious traffic in NextGen Solution
Insider Threats	Medium	High	High	Enforce role-based access controls (RBAC) to limit data access in NextGen Solution. Implement employee activity monitoring tools for all staff in NextGen solution.
Data Misconfiguration	Medium	High	High	Regular audit cloud storage configurations to all systems in NextGen Solution. Use automated tools to detect and alert on misconfiguration.
Device Theft	Medium	High	High	Use full-disk encryption on all laptops in NextGen Solution. Mandate the use of cable locks for devices in NextGen Solution offices
Unauthorized Physical Access	Medium	Moderate	Moderate	Install access control system for secure areas in NextGen Solutions. Use surveillance cameras to monitor physical spaces in and around NextGen solutions.

6. **Recommendation**

   I recommend that the Company should conduct wide phishing awareness training for employees and implement robust email filtration solutions to detect malicious emails.