**Risk Assessment Report: NextGen Solutions**

**1. Summary of Identified Risks**

Because of its dependence on cloud-based services, financial apps, and sensitive consumer data, NextGen Solutions, a prominent fintech company, is vulnerable to a number of cybersecurity risks. The following are the main dangers that have been identified:   
• Phishing Attacks: Operations and customer service representatives may be tricked by phony emails, which could result in credential theft and illegal access.   
• Malware and ransomware: Malware has the ability to infiltrate cloud environments and endpoint devices.   
• Insider Threats: Workers with special access rights may abuse private financial information.   
• API Exploits: Attackers may target payment gateway APIs in order to influence transactions.   
Unauthorized attempts to gain access to client accounts are known as brute force attacks.   
• Physical security breaches include equipment theft and unauthorized access to restricted areas.   
• Misconfigured Cloud Resources: Negligently set up GitLab or AWS repositories may reveal important financial information.

**2. Risk Matrix (Likelihood vs. Impact)**

| **Risk** | **Likelihood** | **Impact** | **Priority** |
| --- | --- | --- | --- |
| Phishing Attacks | High | Severe | Critical |
| Malware/Ransomware | Medium | Severe | High |
| Insider Threats | Medium | High | High |
| API Exploits | High | Severe | Critical |
| Brute Force Attacks | Medium | Moderate | Medium |
| Physical Security Breach | Low | High | Medium |
| Misconfigured Cloud | High | Severe | Critical |

**3. Key Recommendations**

1. Boost Phishing Awareness & Email Security   
• Provide personnel the required security awareness training.   
• Implement multi-factor authentication (MFA) and email filtering programs.

2. Strengthen Network and Endpoint Security   
Advanced endpoint detection and response (EDR) tools should be installed and maintained.   
• Strict access control guidelines should be implemented for all internal systems.

3. Cloud Infrastructure & Secure API   
• Put API gateways and Web Application Firewalls (WAF) into place.   
Perform frequent security audits and penetration tests.   
Configure role-based access control (RBAC) and other AWS security best practices.

4. Boost Insider Threat Monitoring & Access Controls   
• For privileged access management (PAM), use CyberArk.   
• Put in place stringent user activity tracking and anomaly identification.

5. Strengthen Physical Security Protocols   
• Implement security audits and biometric access controls for restricted locations.   
• Set up asset tracking for devices that are provided by the company.