Risk Treatment Plan for NexSoft

Introduction: In this plan, I'll address how NexSoft, a company with a moderate risk appetite, can handle cybersecurity threats. I'll consider which risks they can accept, and which need to be avoided, reduced, or transferred. The goal is to balance innovation and security based on their business model.

Identifying threats

NexSoft operates with sensitive data, so they face several potential threats:

- Data breaches from unauthorized access.
- Phishing and social engineering attacks targeting employees.
- Cloud infrastructure vulnerabilities that could expose their system.
- Insider threats, where employees misuse their access.
- Malware or ransomware attacks that can disrupt operations.

Threats and Preventions

Since NexSoft has a moderate risk appetite, they're willing to take on some risk but still need to focus on reducing major threats.

Threat	Risk Level	Details
Data Breaches (Unauthorized Access)	High	Use stronger encryption and implement multi-factor authentication (MFA). Regular security audits.
Phishing Attacks	Moderate	Keep up employee training to recognize phishing. Some risk may be accepted as unavoidable.
Cloud Vulnerabilities	High	Regular updates, strong access controls, and monitoring tools. Prioritize cloud security patches.

Insider Threats (Employee Misuse)	Low	Use stricter access controls and monitor for suspicious activity. Consider cyber insurance.
Malware/Ransom ware	High	Advanced malware detection, regular backups, and security patches to reduce attack likelihood.

Security Measures:

NexSoft should focus most of their resources on high-risk threats, like data breaches and malware, because these could cause the most damage. For moderate risks like phishing, they can reduce the chance of attacks through training, but they should accept that some attempts will get through. Low-risk threats, like insider misuse, can be handled with basic precautions and possibly transferring the risk through insurance.

Conclusion

NexSoft's risk treatment plan focuses on reducing high-priority risks like data breaches and cloud vulnerabilities while accepting or transferring lower-level risks. This balanced approach lets them stay secure without stifling their ability to grow and innovate.