Risk Treatment Plan for NexSoft

Introduction: In this plan, I will address how NexSoft, a company with a moderate risk appetite, can handle cybersecurity threats. I will consider which risks they can accept, and which need to beavoided, 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 are willing to take on some risk but still need to focus on reducing major threats.

Threat	STRIDE type	Priority	Score	Details
Data Breaches (Unauthorized Access)	Information disclosure	High	10	- Implement multi-factor authentication (MFA) for all users. - Use role-based access control (RBAC). - Encrypt sensitive data at rest and in transit.
Phishing Attacks	Spoofing	High	8	- Regular employee training on phishing awareness. - Implement email filtering and anti-phishing tools. - Set up a quick reporting mechanism for

				suspicious emails.
Cloud Vulnerabilities	Information disclosure/Tempering	Medium	7	- Conduct regular vulnerability assessments and audits of cloud resources. - Enable network segmentation for critical assets. - Deploy Web Application Firewalls (WAFs).

Insider Threats (Employee Misuse)	Elevation of Privilege/Repudiation	Medium	6	- Implement strict access control policies with RBAC. - Monitor and log user activities, especially for privileged accounts. - Conduct background checks for high-risk roles.
Malware/Ransomware	Denial of Service/Tempering	Low	5	- Install anti-malware and endpoint protection on all systems. - Regularly back up data to a secure, isolated location. - Implement network segmentation to contain potential infections.

Security Measures:

Unauthorized access leads to data breaches.

To avoid data breaches, NexSoft should focus on implementing robust access control measures and encryption. Introducing MFA on all user accounts enhances security by adding an extra verification step, diminishing the chances of unauthorized entry. Role-Based Access Control (RBAC) is crucial in restricting users' access to only the resources required for their specific job roles, reducing the risk of exposing sensitive data. Furthermore, data encryption must be applied while data is stored and while it is being transmitted, guaranteeing that unauthorized individuals cannot read intercepted data. Collectively, these actions improve data protection and minimize the chance of expensive breaches.

Cybercriminals utilize phishing and social engineering tactics to carry out their attacks.

Phishing and social engineering attacks are still one of the most prevalent and effective forms of attack, focusing on exploiting the human factor in companies. NexSoft should regularly train employees to recognize phishing attempts and other social engineering tactics in order to combat the threat. These training sessions will assist employees in identifying suspicious communications and prevent accidentally revealing credentials. Moreover, it is important to implement email filtering and anti-phishing tools to obstruct identified phishing sources and highlight potentially harmful messages. Having a rapid reporting system enables employees to quickly report suspicious phishing emails, which helps the IT security team take fast action to address threats.

Weaknesses in Cloud Infrastructure.

It is crucial to protect the cloud infrastructure that supports NexFlow from external risks and weaknesses to ensure the security of data processing and storage. NexSoft needs to regularly assess the vulnerabilities in its cloud resources to detect and fix security weaknesses before they are taken advantage of. Segmenting the network is crucial as it helps prevent threats from spreading to other parts of NexSoft's infrastructure by isolating important cloud resources. Web Application Firewalls (WAFs) provide an additional level of security by screening and overseeing HTTP traffic, preventing harmful requests, and minimizing vulnerabilities from attacks at the application layer. These collective actions guarantee a strong, layered protection for the cloud setting.

Threats from within, specifically by individuals with access to sensitive information or systems.

It is important to closely monitor and have strict access controls for insider threats, such as employees abusing their access privileges. Enforcing rigorous access control policies, particularly with RBAC, guarantees that employees can only access information relevant to their specific roles. Tracking and recording user actions, especially those of privileged users, enables immediate identification of abnormal behavior and maintains responsibility. Background checks in high-risk positions help provide extra security by decreasing the possibility of fraudulent behaviors from insiders. These actions as a whole protect NexSoft from intentional or accidental misuse of sensitive information.

Attacks involving Malware and Ransomware

To defend against malware and ransomware, NexSoft needs to install anti-malware and endpoint protection software on all devices, ensuring they are consistently updated to detect and combat new threats. Backing up data to a safe and separate location serves as a protection against data loss, guaranteeing uninterrupted business operations in case of a ransomware incident. Network segmentation helps prevent malware from spreading by isolating infections to certain areas of the network. Working together, these measures reduce the chance of operational disturbances caused by malware and ransomware.

Conclusion

In summary, NexSoft's security plan tackles key risks by using a layered method that involves access controls, employee education, infrastructure reinforcement, and surveillance. Through the implementation of these specific security measures, NexSoft can enhance the protection of sensitive data, thwart unauthorized access, and promptly address possible threats. Taking proactive measures not only boosts NexSoft's cybersecurity stance but also builds trust with clients and stakeholders, reinforcing the company's dedication to providing secure, high-performance solutions.