Risk Treatment Plan for SSAS Inc.

Introduction: SSAS Inc. is a company with a high cybersecurity risk appetite, meaning they are willing to accept more risks compared to typical organizations in exchange for business gains or innovation. This plan outlines how SSAS Inc. can address potential cyber threats while balancing risks against their business strategy.

Identifying Threats

- Based on their operations, SSAS Inc. faces several cybersecurity threats:
- Data breaches due to unauthorized access or vulnerabilities in the platform.
- Phishing or social engineering attacks targeting employees.
- Cloud infrastructure vulnerabilities, which could expose customer or internal data.
- Insider threats, where employees misuse their access to sensitive information.
- Malware or ransomware attacks that could disrupt operations and affect business continuity.

Threats and Preventions

Since SSAS Inc. has a very high-risk appetite, they may choose to accept certain risks, especially those that would otherwise stifle innovation. However, they still need to mitigate critical risks that could cause major harm to the business.

Threat	STRIDE type	Priority	Score	Details
Data Breaches (Unauthorized Access)	Information Disclosure	High	9	Use advanced encryption (AES, RSA), multi-factor authentication (MFA), and regular security updates to

				reduce the risk of unauthorized access.
Phishing Attacks	Spoofing	Medium	7	Given their high-risk appetite, SSAS may accept some risk but should continue regular cybersecurity training to reduce the chances of phishing success.
Cloud Vulnerabilities	information Disclosure	High	8	Ensure strong access controls, regular security patches, and constant monitoring of cloud systems to minimize vulnerabilities.
Insider Threats (Employee Misuse)	Elevation of Interest	Medium	6	Accept some level of risk while implementing monitoring tools to track user activities. Regular audits can reduce the risk of misuse.
Malware/Ransomware	Denial of Service	High	9	Use robust endpoint security, regular backups, and software updates.

				Implement intrusion detection systems to detect and respond quickly.

Security Measures

Data breaches are caused by unauthorized access or vulnerabilities in platforms.

In order to prevent data breaches, it is important to enable multi-factor authentication (MFA) for all user accounts, particularly those with privileged access. MFA enhances security by requesting various forms of verification, like passwords and temporary codes sent to a mobile device. Stringent access controls must be implemented to guarantee that every user is granted solely the essential permissions for their designated role (principle of least privilege). Regular evaluations of vulnerabilities and penetration tests aid in discovering and addressing possible system weaknesses before they are exploited. Moreover, implementing encryption for sensitive data, whether it is stored or transmitted, enhances security by guaranteeing that the data stays safeguarded even in the event of interception or unauthorized access.

Phishing or Social Engineering Attacks Directed at Staff Members

Phishing and social engineering are frequently utilized tactics to trick employees into disclosing sensitive information. Continuous security awareness training is crucial in dealing with these threats. Staff members need to undergo training to identify phishing emails and other forms of social engineering, like questionable links, personal information requests, and unsolicited messages from unfamiliar contacts. Anti-phishing software can assist in detecting phishing attempts by marking harmful emails. MFA is also necessary for all employee accounts; even if a hacker gets login credentials, extra verification steps can stop unauthorized access.

Customer or Internal Data is being exposed by vulnerabilities in cloud infrastructure.

Because cloud services are frequently at risk from hackers, it is important to regularly perform security audits of cloud setups to guarantee compliance with recommended procedures. These audits detect and correct misconfigurations that can make the system susceptible to attacks.

Utilizing the security features offered by cloud providers (like AWS Security Hub or Azure Security Center) to monitor, log, and automatically alert can also aid in identifying suspicious actions. Partitioning the cloud infrastructure into separate segments creates more obstacles, making it more difficult for attackers to reach sensitive information or systems in case one segment is breached. Moreover, restricting access rights to important systems decreases the potential for attacks by granting sensitive data access only to authorized personnel.

Insider Threats arise when employees misuse their access to sensitive information.

In order to prevent insider threats, it is important to enforce role-based access control (RBAC), which restricts user access to the systems and data required for their particular role. Access rights should adhere to the concept of least privilege, whereby staff are granted only the necessary level of access for their job duties. Introducing logging and monitoring systems to monitor access to sensitive information aids in promptly identifying unauthorized or suspicious actions. Regular access reviews guarantee that authorizations are kept current, particularly when staff transitions between positions, reducing internal threats.

Conclusion

To protect against malware and ransomware, it is necessary to install endpoint protection software on every device used by employees. This program needs to have features for detecting and preventing malicious software, including anti-malware and anti-ransomware functions, to stop them from running. In addition to that, it is crucial to regularly backup all important data and keep these backups in a secure cloud environment or offsite location to guarantee data recovery in the event of an attack. Creating a thorough plan for disaster recovery and incident response is crucial to guarantee the organization's ability to swiftly bounce back from interruptions. This strategy must outline specific measures for containing, eliminating, and recovering from a ransomware attack or other major security breaches, along with ongoing testing to validate the readiness of the organization.