Risk Register Report

Executive Summary

Total Risks	23
Critical	8
High	4
Medium	8
Low	3
Generated	2025-12-06 18:36:07

Detailed Risk Register

ID	Risk Name	Likelihood	Impact	Score	Severity	Controls
1	Ransomware Attack	4	5	20	Critical	None
2	Insider Threat	3	5	15	High	CC6.1, CC6.6
3	DDoS Attack	3	4	12	Medium	CC6.6
4	Unpatched Systems	4	4	16	High	CC7.1, CC6.1
5	API Security Breach	3	5	15	High	CC6.1
6	Third-Party Vendor Risk	3	3	9	Low	CC6.1
7	Data Loss	2	4	8	Low	None
8	Social Engineering	4	3	12	Medium	None
9	SQL Injection	3	4	12	Medium	None
10	Data Breach via Phishing	5	5	25	Critical	None
11	SQL Injection Vulnerability	4	5	20	Critical	CC7.1
12	Ransomware Attack	4	5	20	Critical	None
13	Insider Threat	3	4	12	Medium	CC6.6
14	DDoS Attack	4	3	12	Medium	CC6.6
15	Third-Party Vendor Breach	3	4	12	Medium	None
16	Weak Password Policy	4	3	12	Medium	None
17	Unpatched Systems	5	4	20	Critical	A.8.8
18	Cloud Misconfiguration	3	5	15	High	CC6.1
19	Physical Security Breach	2	4	8	Low	A.5.15
20	Unencrypted Patient Records	5	5	25	Critical	164.312(c)(1)
21	Credit Card Data in Logs	5	5	25	Critical	164.312(b), 164.312(c)(1)
22	No Data Subject Access Request	3	4	12	Medium	GDPR-34, GDPR-5
23	Lack of Incident Response Plan	4	5	20	Critical	RS.RP, PR.AT

Risk Details

Risk 1: Ransomware Attack
Potential ransomware infection through phishing emails or malicious downloads

Risk 2: Insider Threat
Malicious or negligent employees accessing sensitive data without authorization

Risk 3: DDoS Attack
Distributed denial of service attack disrupting online services and availability

Risk 4: Unpatched Systems
Critical security vulnerabilities due to outdated software and missing patches

Risk 5: API Security Breach
Insecure API endpoints exposing sensitive customer and business data

Risk 6: Third-Party Vendor Risk
Security vulnerabilities introduced through third-party vendors and suppliers

Risk 7: Data Loss
Accidental deletion or loss of critical business data due to inadequate backups

Risk 8: Social Engineering
Attackers manipulating employees to divulge confidential information

Risk 9: SQL Injection
Web application vulnerable to SQL injection attacks

Risk 10: Data Breach via Phishing
Employee credentials compromised through phishing emails

Risk 11: SQL Injection Vulnerability
Web application vulnerable to SQL injection attacks

Risk 12: Ransomware Attack
Critical systems could be encrypted by ransomware

Risk 13: Insider Threat
Malicious or negligent employee actions

Risk 14: DDoS Attack
Distributed denial of service attack on web services

Risk 15: Third-Party Vendor Breach
Data exposure through compromised vendor

Risk 16: Weak Password Policy
Users using easily guessable passwords

Risk 17: Unpatched Systems
Servers running outdated software with known vulnerabilities

Risk 18: Cloud Misconfiguration
AWS S3 buckets publicly accessible

Risk 19: Physical Security Breach
Unauthorized access to server room

Risk 20: Unencrypted Patient Records
ePHI stored in plain text on database

Risk 21: Credit Card Data in Logs
PAN data visible in application logs

Risk 22: No Data Subject Access Request Process
Lack of procedure for handling GDPR DSARs

Risk 23: Lack of Incident Response Plan
No formal plan for cybersecurity incidents