GRC ZHS CASE STUDY

Auditors:
Scott Seburn
Merrick Wilensky

12/7/23

Introduction:

Risk management is a crucial organizational process that involves identifying, assessing, prioritizing, and mitigating potential risks. It encompasses evaluating risks from various sources, prioritizing them based on severity, and implementing strategies for risk mitigation, such as avoidance, reduction, transfer, or acceptance. Ongoing monitoring and control ensure adaptability to changes, and effective communication disseminates risk information across the organization. This process adds significant value by supporting strategic decision-making, optimizing resource allocation, maintaining regulatory compliance, enhancing resilience. Ultimately, risk management contributes to organizational sustainability and long-term growth by safeguarding assets and reputation.

GRC Team Introduction:

The Governance, Risk, and Compliance (GRC) team plays a critical role in ensuring that an organization operates effectively, ethically, and in compliance with relevant regulations and standards. The GRC team is responsible for establishing and maintaining governance structures, risk management processes, and compliance protocols. By closely monitoring regulatory changes, industry standards, and internal policies, the GRC team helps the organization proactively identify and address potential risks, ensuring alignment with legal requirements.

Risk Register (Findings and Analysis)

Priorities and Risks labeled: LOW, MODERATE, SIGNIFICANT

Ref. No.	Priority	Risk Name	Risk Description	Cause	Dependent Systems	Risk Owner	Cost	Risk Treatment	Control	Residual Risk	Accepted (Y/N)
1	SIGNIFICANT	Ransomware attacks aimed at sensitive patient and employee data.	Ongoing ransomware attacks aimed at the ZHS. Company has suffered a history of data breaches in the past.	Spear phishing techniques used on employees and possible data leaks from disgruntled employees	-Company Databases -Patient Records -employee records -Insecure PHI	Mr. Hacker CISO (Cyber Security)	Upwards of $4.5 Million in ransom + $100 to $50,000 for each violation dependent on the culpability.	-Educate employees on avoiding ransomware infections -Keep systems fully patched -Employ zero trust principles in all networked systems -Allow installation and execution of authorized apps only -Continuously monitor -Block access to untrusted web sources (server names, IP addresses, ports, etc.) **NISTIR-8374**	Contingency Training/ Simulated Events **NIST-SP800-53 CP-3(1)**	MOD	NO
2	SIGNIFICANT	Insider Threats	Disgruntled employees leak sensitive personal or company data.	Various motivations: Financial, disgruntled employee, negligence, espionage.	-Company Database and records -Company Servers	Mr. Clicker CLO	$4.61 million **SOURCE: "COST OF A DATA BREACH REPORT (2021)" PG.20**	-Access Controls (Principle of least privilege) -Audit and Accountability(Establishing proper monitoring and auditing capabilities) -Personal Security and proper Incident Response	Implement an incident handling capability for incidents involving insider threats. **NIST- SP800-53 IR-4(6)**	MOD	NO

3	MOD	Phishing and Social Engineering	Social Engineering: An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. Phishing: The practice of sending emails or other messages claiming to be from a reputable source to induce individuals to reveal personal information	Lack of proper employee training and education has led some employees to be phished into revealing sensitive company data.	-Employee passwords and credentials -Sensitive patient and employee information -Patient financial information	Mr. Clicker (CLO)	Upwards of: $10.93 million. https://medcitynews.com/2023/07/healthcare-data-breach-cybersecurity-ransomware/#.	Provide practical exercises in literacy training that simulate events and incidents Employ independent assessors or assessment teams to conduct control assessments **NIST-800-53 AT-2(1) CA-2(1)**	Control Assessments Independent Assessors Literacy Training and Awareness Practical Exercises **NIST-800-53 AT-2(1) CA-2(1)**	LOW	NO
4	MOD	Weak and outdated firewall	The IT department has failed to comply with **NIST-800-41 (guidelines on Firewalls and Firewall Policy)** by not updating and consistently reconfiguring firewalls. Allowing possibly malicious internet traffic through the ZHS website.	Firewall rules have failed to be reviewed and updated on a consistent schedule (Every 6 Months recommended)	-The ZHS web site and web server	Ms. Digger (CIO) + IT Team Mr.Hacker (CISO) + Cyber Security Team	Fines for neglected firewalls range from: $100 - $877 million according to past reports. https://www.csoonline.com/article/	Review firewall rules every 6 months. Keep updated on ongoing cyber threats to reconfigure firewall appropriately. Plan, configure, and test in accordance with: **NIST-800-41**	Review and reconfigure schedules for IT team Updated list of needed firewall rules	**LOW**	NO

Conclusion:

In conclusion, the risk management process plays a pivotal role in organizational resilience and sustainability. By systematically identifying, assessing, and mitigating potential risks, organizations can safeguard their assets and reputation. The specific findings from the risk assessment for the organization include a significant risk of ransomware attacks targeting sensitive patient and employee data, insider threats arising from disgruntled employees, phishing and social engineering attacks due to a lack of proper employee training, and a moderate risk associated with weak and outdated firewalls. The recommended risk treatments involve a combination of employee education, access controls, incident response capabilities, and regular review and updating of firewall rules in alignment with NIST standards. Overall, the risk management process provides a proactive framework for addressing vulnerabilities and enhancing the organization's overall security posture.

Source List:

1. NISTIR-8374
2. NIST- SP800-53 CP-3(1)
3. “COST OF A DATA BREACH REPORT (2021)” PG.20
4. NIST- SP800-53 IR-4(6)
5. https://medcitynews.com/2023/07/healthcare-data-breach-cybersecurity-ransomware/#:~:text=It%20revealed%20that%20the%20average,2020%2C%20it%20was%20%247.13%20million
6. NIST-800-53 AT-2(1) CA-2(1)
7. NIST-800-41
8. https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html
9. NIST-800-41