Cyber Risk Assessment and Mitigation Strategy for NorthBridge Healthcare

Name of Student

Course Code

Instructor's Name

Institutional Affiliation

Cyber Risk Assessment and Mitigation Strategy for NorthBridge Healthcare

Organizational Context and Risk Framing

Organizational Overview

NorthBridge Regional Healthcare Network is a medium-sized healthcare organization consisting of two hospitals and seven clinics, employing 4,500 workers. It offers important services such as Electronic Health Records (EHR), imaging, and patient scheduling. The hybrid technology design at NorthBridge consists of a high-performance, task-based clinical system on-premises, and a cloud-based system, such as Microsoft Azure, to provide identity management and administrative services.

Critical Services and Digital Assets

The EHR system, the medical imaging infrastructure, and the patient portal are the most critical digital resources. The systems are important in the smooth running of patient care and efficiency.

Threat Landscape

NorthBridge is at risk of ransomware and credential theft. The ransomware attacks are also increasing, particularly towards healthcare organizations, because attackers want to control how patients receive treatment and access sensitive data (Dart, 2024; Mohammed et al., 2025). Phishing-related credential theft is also a serious threat, as it will grant access to valuable systems.

Relevant Threat Actors

NorthBridge is of particular concern with ransomware groups such as LockBit. Often, the perpetrators attack healthcare organizations and employ tricks like phishing and stealing credentials to hack into systems (Cybersecurity and Infrastructure Security Agency, 2023) Moreover, there are also internal threats like malicious or careless insiders.

Time Horizon for the Analysis

The 12-18 months period will be analyzed, as the tactics of ransomware and new vulnerabilities are constantly changing (Khan, 2024). The main assumptions are a rise in targeted attacks on healthcare organizations and the risk of third-party services.

Top 2-3 Cyber Risk Statements

Risk 1: Ransomware Attack on EHR System

- **Risk Statement**: There is a risk that ransomware can be used to take advantage of the vulnerabilities of the EHR system and impact patient data storage, health care services, and regulatory fines.
- **Key Assets**: EHR and patient data storage are central to operations and patient care.
- **Primary Threats and Vulnerabilities**: Ransomware attacks take advantage of vulnerable systems and weak access control to attack health systems in order to obtain financial benefits (Mohammed et al., 2025).
- **Impact**: The losses are estimated to be between $5M-$10M because of the operational downtime, recovery costs, and regulatory fines through HIPAA (Dart, 2024).
- **Likelihood**: High, based on the fact that the healthcare industry has experienced a trend of increasing ransomware-targeted attacks.

Risk 2: Data Breach from Third-Party Vendor

- **Risk Statement**: There is a risk of third-party vendor credentials being stolen to exploit cloud storage of sensitive patient data, resulting in a loss of data and reputation.

- **Key Assets**: Cloud storage of sensitive patient information is under threat, and so is the integrity of outsourced systems.
- **Primary Threats and Vulnerabilities**: Credential theft as a result of phishing or a lack of proper access control protocols by third-party vendors (Oluwatosin Ilori et al., 2024).
- **Impact**: Legal cost, reputational losses, breach notification may be about $2M-$5M.
- **Likelihood**: Medium, because third-party vendor hacking has increased in healthcare.

The risks highlight the importance of effective cybersecurity controls and vendor risk management as a remedy to protect stolen healthcare information.

Qualitative and Quantitative Risk Analysis

The likelihood distribution in the analysis relies on a simplified FAIR-inspired model, which makes use of the recent healthcare breaches statistics, the familiar ransomware operation, and an evaluation of the existing security measures implemented by NorthBridge.

Risk 1: Ransomware Attack on EHR System

- **Likelihood Rating**: High (3) – The risk is very high due to the rising occurrences of medical institution ransomware attacks, especially EHRs (Mohammed et al., 2025).
- **Impact Rating**: High (3) – Broken healthcare services and possible regulatory fines would lead to colossal losses of business and finances.
- **Estimated Annual Loss**:
  - **Likelihood**: 20% (0.2 probability)
  - **Impact**: $7.5M (midpoint of $5M–$10M)
  - **Expected Annual Loss**: 0.2 × $7.5M = $1.5M annually.

The value aligns with the industry data on the impact of ransomware within healthcare facilities.

Risk 2: Data Breach from Third-Party Vendor

- **Likelihood Rating**: Medium (2) – The risk is moderate since there were prior similar cases when a breach by third parties led to a high percentage of breaches of healthcare data (Reddy et al., 2023).
- **Impact Rating**: High (3) – Exposure and misuse of sensitive patient data would result in legal fines and loss of organizational reputation on a colossal scale.
- **Estimated Annual Loss**:
  - **Likelihood**: 10% (0.1 probability)
  - **Impact**: $3.5M (midpoint of $2M–$5M)
  - **Expected Annual Loss**: 0.1 × $3.5M = $350K annually.

The risk is informed by the reporting of historical data and threat intelligence reports on third-party breaches, which is a concerning trend in healthcare (Mohammed et al., 2025).

Treatment Options & Risk/Cost Trade-offs

Risk 1: Ransomware Attack on EHR System

Treatment Option 1: Enhanced Identity and Access Management (IAM) System

- **Cost**: $400K/year
- **Risk Reduction**: It will decrease ransomware losses by 50%. Better identity management, more rigid access control, and enhanced monitoring diminish the risks of an unauthorized access attempt, and ransomware cannot use weak points of access (Nikhil Ghadge, 2024).
- **Impact**: With risk mitigation, a ransomware attack might have cost a loss of an estimated $1.5M/year, to be reduced to $750K/year.

- **Net Savings**: The investment would yield net savings of $350K/annually, as it would offset the $750K losses of the future at just $400K cost.

Treatment Option 2: Data Encryption and Immutable Backups

- **Cost**: $300K/year
- **Risk Reduction**: 50% reduction in cases of ransomware attacks because data is not lost or compromised. Unchangeable backups and encryption ensure that even in an instance where a ransomware attack manages to encrypt the main systems, the backup data is not compromised, and therefore, the business will go on.
- **Impact**: Encryption and immutable backups will reduce annual loss by $750K, and a $750k risk reduction will be achieved when nothing is done.
- **Net Savings**: The company would incur a cost of $300K/year on it, but the payoff is huge, as it would minimize the threat of ransomware attacks.

Risk 2: Data Breach from Third-Party Vendor

Treatment Option 1: Cloud Security Posture Management (CSPM)

- **Cost**: $300K/year
- **Risk Reduction**: CSPM solutions would eliminate 60% of the risk of misconfigurations and Vendor-based breaches by automatically identifying and recovering cloud infrastructure problems (Jim, 2024). It would guarantee stricter controls on access to sensitive data by third-party vendors.
- **Impact**: A third-party vendor data breach may cause an initial loss of $350K/year. By applying CSPM, that anticipated loss would only be $140K/year with a risk reduction of 210K.

- **Net Savings**: The net savings of CSPM implementation would be $150K/year, taking into account the investment of $300K/year. It is an affordable method of reducing third-party risk.

Treatment Option 2: Enhanced Third-Party Risk Management

- **Cost**: $250K/year
- **Risk Reduction**: Enhancing third-party vendor testing, such as periodic audits, reviewing of contracts, and more stringent controls on access, would mitigate the likelihood of breaches by 50%.
- **Impact**: It would reduce the projected annual loss of third-party breaches to $175K / year, resulting in a risk reduction of $175K compared to no action.
- **Net Savings**: The option offers net savings of $125K/year following the $250K/year investment, which makes it a great choice in addressing vendor-linked cybersecurity risks.

Comparison and Prioritization

The ransomware risk reduction with the Enhanced IAM System offers the best ROI, 50% reduction in ransom losses, and net savings of $350 K/year. The treatment will be prioritized due to the high probability and consequences of ransomware in the healthcare sector (CISA, 2023). Secondly, we should also apply CSPM to third-party risks and cloud misconfigurations (Jim, 2024). It offers a high level of risk reduction at a good annual cost of $300K, which results in a net saving of $150K. Finally, IAM must be implemented first with CSPM to curb the cloud and third-party risks. Both solutions directly decrease the greatest threats to the organization and provide quantifiable financial gains.

Executive Summary and Communication Plan

Summary of Risks

The most common cyber threats to the organization include ransomware attacks, data breaches by third-party vendors, and cloud misconfigurations. The ransomware risk is also high, and the losses are projected at between $1.5M and $5M annually due to operational disruptions and fines. Vendor credential breaches can cost an annual loss of between $350K and $2M because of legal settlements and reputational loss. Cloud misconfigurations, which may reveal sensitive data, pose a medium risk with losses of between $350K and $1.5M per year.

Recommendations

To address the risks, we suggest an Enhanced Identity and Access Management (IAM) System for $400K per year. The system would cut losses related to ransomware by half, cutting projected losses by about $750K a year (Jim, 2024). Another vital suggestion is to implement Cloud Security Posture Management (CSPM) at a cost of $300K/annual, which would lessen cloud misconfiguration and external assault probability by 60%, conserving the organization $210K/annual.

Presentation Plan

During the board briefing, I would utilize a single-slide executive summary and risk heat maps to outline the highest-ranking risks and the financial impact they may have. Important measures like the anticipated loss levels of each risk and the ability of each recommendation to reduce the risk would be highlighted. I would conclude with a particular request to accept the IAM and CSPM solutions, pointing to their affordability and relevance to the risk-reduction objectives of the organization.

References

CISA. (2023, October 19). *#StopRansomware Guide*. CISA. https://www.cisa.gov/resources-tools/resources/stopransomware-guide

Cybersecurity and Infrastructure Security Agency. (2023, July 13). *Threat Hunting*. https://www.dhs.gov/sites/default/files/2023-08/23_0713_cisa_threat_hunting.pdf

Dart, M. (2024). Ransomware: Impacts on Healthcare Critical Infrastructure. In *Ransomware Evolution*. CRC Press.

Jim, M. M. I. (2024). *Cloud Security Posture Management: Automating Risk Identification and Response in Cloud Infrastructures* (SSRN Scholarly Paper No. 5049796). Social Science Research Network. https://doi.org/10.69593/ajsteme.v4i03.103

Khan, M. R. A. (2024). Understanding impacts of a ransomware on medical and health facilities by utilizing LockBit as a case study. *Security and Privacy*, *7*(1), e328. https://doi.org/10.1002/spy2.328

Mohammed, N., Mohammed, A. F., & Balammagary, S. (2025). Ransomware in Healthcare: Reducing Threats to Patient Care. *Journal of Cognitive Computing and Cybernetic Innovations*, *1*(2), 27–33. https://doi.org/10.21276/jccci.2025.v1.i2.5

Nikhil Ghadge. (2024). Enhancing threat detection in Identity and Access Management (IAM) systems. *International Journal of Science and Research Archive*, *11*(2), 2050–2057. https://doi.org/10.30574/ijsra.2024.11.2.0761

Oluwatosin Ilori, Nelly Tochi Nwosu, & Henry Nwapali Ndidi Naiho. (2024). Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. *World Journal of Advanced Research and Reviews*, *22*(3), 213–224. https://doi.org/10.30574/wjarr.2024.22.3.1727

Reddy, J., Elsayed, N., ElSayed, Z., & Ozer, M. (2023). A Review on Data Breaches in Healthcare Security Systems. *International Journal of Computer Applications*, *184*(45), 1–7. https://doi.org/10.5120/ijca2023922333