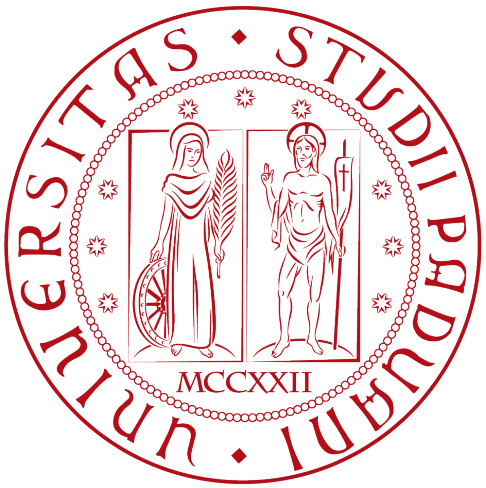

NIST Cybersecurity Assessment for Acme Healthcare Systems Using Generative AI

Security And Risk: Management and Certifications

Gabriel Rovesti - ID: 2103389

June 10, 2024

Index

1. Introduction

1.1. Use case description

Acme Healthcare Systems is a medium-sized regional healthcare provider with multiple clinics and a main hospital in a city. They have approximately 500 staff members, including doctors, nurses, administrative employees, and an in-house IT team. Acme manages confidential patient information like medical records, insurance details, and payment data.

The company's IT setup includes:

- A central data center that houses the electronic medical record (EMR) system, billing software, and other important applications
- Local servers and computers at each clinic, linked to the central data center through a private WAN
- A cloud-based email system and collaboration platform (e.g., Microsoft 365) for communication and file sharing
- Remote access to the EMR system Overall, Acme Healthcare Systems prioritizes the security and efficiency of their IT infrastructure to safeguard patient information and enhance communication among staff.

1.2. Key risks and concerns

The company wants to retain control over the following aspects:

- Identify and categorize critical assets for security measures so as to ensure the proper level of security measures for sensitive patient information
- Implement appropriate access controls to minimize the risk of unauthorized access or internal abuse, particularly on user activation flows and password policy
- Put safety awareness and training programs in place, which prepare personnel for the identification and control of safety risks, thereby reducing the likelihood of human error or social engineering attacks
- Secure the cloud-based email and collaboration suite to protect it from unauthorized access or manipulation of sensitive information
- Ensure compliance with the healthcare regulations (such as HIPAA in the US) and data privacy laws
- Enhance data security measures, including encryption protocols for data in transit and at rest, for ensuring security and prevented unauthorized access or manipulation of financial data
- Strengthen incident response procedures to ensure a timely and effective response to security breaches or incidents to minimize any potential damage and facilitate prompt recovery

1.3. Methodology and workflow

In this cybersecurity assessment, a methodology based on the NIST Cybersecurity Framework (CSF) 2.0, as explained in detail in its parts Section 2, will be applied. It's composed of the following parts:

1. Information Gathering: Acme Healthcare Systems' information will be collecte about its activities, including available documentation, policies, and procedures related to practices of cybersecurity employed. These will include details about IT infrastructure, data assets, access controls, security awareness programs, incident response processes and compliance requirements.
2. Current State Analysis: Acme Healthcare Systems' current cybersecurity posture will be analyzed but also existing controls, gaps, and areas for improvement using all information available. This will be mapped against the NIST CSF categories and subcategories to establish a comprehensive understanding of their security maturity level, implementing countermeasures related to those
3. Control Selection and Tailoring: Based on identified risks and concerns, selected NIST CSF controls to address Acme Healthcare's specific needs will be chosen. These will be drawn from the NIST CSF Core and will be prioritized based on relevance and potential impact on organization's security objectives. This will be further explained in the next subsection, gathering a collective analysis of the problem and understanding how to apply such things.
4. Generative AI Integration: The integration of generative AI enables the use of a generative AI model in understanding the applications, limits, and possible help in conducting a cybersecurity assessment such as this one, present in the report. Such AI model will be involved in the tasks involved in this document, including:
    - Generating draft analyses and recommendations based on the selected NIST CSF controls and commenting if they were applied correctly
    - Providing context-specific insights and suggestions for control implementation, discussing case by case each time
    - Helping to structure and draft sections of the cybersecurity assessment report
5. Refinement, Reporting, and Documenting: The results given by the usage of generative AI will be reported and documented thoroughly, recognizing its value both as a tool and a resource. All AI-generated content will be subjected to a detailed validation process, indicating how much accuracy, relevance, and alignment with Acme Healthcare's specific requirements the presented results had brought. The report will provide a useful use case to finetune the assessment lifecycle during its creation.

The report will follow a clear structure, within the NIST CSF framework, addressing the identified risks, concerns, and control implementation strategies.

The model used is Claude.ai [1] in its base model, as it is excellent at documentation over long prompts and the possibility to use it while giving multiple files per answer and even images. Compared to other models, this one was selected because of its precision over longer prompts and an almost-perfect possibility of giving a response fitting precisely each presented concept.

2. NIST CSF Framework

NIST CSF provides a common taxonomy and mechanisms for organizations to describe their current posture, the target objectives and prioritize improvement opportunities, assessing progress while communicating to stakeholders risks and reducing it establishing specific objectives.

2.1. Core

2.2. Tiers

2.3. Profiles

2.4. Risk and asset management

3. Results

4. Conclusion

Bibliography

[1] Anthropic, “Claude.ai.”