RCI Cybersecurity Analysis Report

0x2A Security

ANALYST: Heather Rosas

DATE: October 22nd 2025

Executive Summary

The recent ransomware incident to Rigel Cybernetics, exposed critical gaps in staff awareness, system monitoring, and data protection. To address these issues effectively and cost-consciously, while keeping your company's core values, we recommend prioritizing the following three actions:

1. Phishing Awareness & Employee Security Training – Ranked highest priority, this addresses the root cause of the attack: employees opening fraudulent patient file requests. Implementing regular training and simulated phishing exercises will prevent future human-error-driven breaches, reduce potential downtime, and protect sensitive patient data. This initiative directly supports the company's goals of delivering exceptional patient care and safeguarding customer privacy, while requiring minimal investment compared to potential incident costs.

2. Continuous Monitoring & Threat Detection (SIEM/EDR) – Weak monitoring allowed ransomware to spread undetected. Deploying real-time monitoring and detection tools will prevent prolonged breaches and enable faster containment of threats. By ensuring system reliability and stability, this solution supports uninterrupted patient care, a secure environment for innovative software development, and ongoing protection of sensitive data—all critical to business continuity and trust.

3. Data Encryption for Patient and Sensitive Records – Unencrypted data made systems an easy target. Encrypting all patient records ensures that even if a breach occurs, data remains unreadable, preventing theft or exposure. This reinforces regulatory compliance and enhances the company's commitment to impeccable privacy protection, while being a cost-effective safeguard against potentially high-impact incidents.

Collectively, these three measures address immediate risk with high impact, are cost-conscious, and align directly with the company's core priorities of patient care, innovation, and privacy protection.

If leadership is interested, we also have **three additional recommendations** that are both impactful and cost-conscious, which could be considered for a phased implementation to further strengthen the organization's cybersecurity posture.

Recommendations

RECOMMENDATION 1: Implement Phishing awareness and Employee Security Training

The ransomware attack began when an employee opened a fake patient file, showing that staff were not fully aware of phishing threats. We recommend implementing regular phishing awareness training and simulated email exercises for all employees. This will prevent future attacks that rely on human error and strengthen the organization's first line of defense. By improving staff awareness, we reduce the risk of system downtime, protect patient information, and maintain the trust essential for exceptional patient care and privacy protection.

RECOMMENDATION 2: Continuous Monitoring and Threat Detection (SIEM/EDR)

Weak monitoring allowed the attack to spread unnoticed. We recommend deploying continuous threat detection tools and central monitoring systems to identify suspicious activity in real time. This solution will prevent prolonged, undetected breaches and allow faster containment of threats. Strong monitoring ensures systems remain reliable for patient care, protects sensitive data, and supports the company's innovative software operations by providing a stable and secure IT environment.

RECOMMENDATION 3: Data Encryption for All Patient and Sensitive Records

Patient records were not encrypted, making it easier for ransomware to access and lock critical data. Encrypting all stored and transmitted patient information will ensure that, even if systems are compromised, data remains unreadable to attackers. This measure prevents data theft, strengthens compliance with healthcare regulations, and reinforces the company's promise of protecting patient privacy—one of its core business values.

RECOMMENDATION 4: Update and Test the Incident Response Plan (IRP)

The existing incident response procedures were outdated and not easily accessible, causing delays and confusion during the attack. We recommend updating the IRP, clearly defining roles, and conducting regular tabletop exercises to ensure staff know exactly how to respond. This will prevent delayed action during future incidents, minimize downtime, and ensure rapid recovery, supporting uninterrupted patient care, safeguarding sensitive data, and maintaining trust in the organization’s operations.

RECOMMENDATION 5: Conduct Regular Security Audits and Tabletop Exercises

No regular audits or exercises meant the ransomware went undetected for an extended period. We recommend implementing a schedule of security audits and simulated exercises to proactively identify vulnerabilities and test response readiness. This approach prevents hidden risks from escalating, ensures systems and processes remain secure, and strengthens organizational resilience, enabling reliable patient care and secure software innovation

RECOMMENDATION 6: Create a Single Source of Truth for IT/OT Assets

Incomplete or outdated asset records left critical systems unmanaged and vulnerable. We recommend establishing a centralized, up-to-date inventory of all IT and operational technology assets. This will prevent untracked systems from becoming security gaps, streamline maintenance and patching, and provide a clear view of the technology environment, supporting safe and efficient delivery of patient care, innovation in software development, and robust protection of patient data.