RCI Cybersecurity Analysis Report

0x2A Security

ANALYST: Jim Combs

DATE: 2/15/26

Executive Summary

Rigel Cybernetics Institute (RCI) recently experienced a significant ransomware incident that exposed critical gaps in foundational security controls and governance processes. While the immediate threat has been contained, our analysis indicates that RCI remains vulnerable to future extortion attempts due to a lack of defense-in-depth and resilient recovery systems.

To immediately reduce risk and ensure business continuity, this report outlines a prioritized remediation roadmap. If RCI could only implement three measures, the following provide the highest Return on Investment (ROI) and risk reduction:

1. **Enforce Foundational Controls (MFA & Encryption):** The recent breach was facilitated by weak access controls. We must immediately mandate Multi-Factor Authentication (MFA) for all remote access and enable AES-256 encryption for data at rest. This prevents credential theft and ensures that even if patient data is exfiltrated, it remains unreadable to attackers.
2. **Deploy Immutable Backup Strategy:** Attackers successfully deleted RCI's online backups, forcing a ransom negotiation. We recommend a "3-2-1" backup strategy with **immutable (write-once)** storage. This prevents anyone including administrators from altering or deleting backups, guaranteeing that RCI can restore operations independently without paying criminals.
3. **Formalize IT Governance & Risk:** The incident response was worsened by outdated playbooks. RCI must establish a formal Risk Register and update the Incident Response Plan (IRP) to include specific ransomware protocols. This ensures that future security decisions are driven by data and legal compliance, protecting the organization's reputation and executive liability.

Implementing these three recommendations will shift RCI from a reactive state to a proactive security posture, restoring stakeholder trust and ensuring compliance with HIPAA regulations.

Recommendations

RECOMMENDATION 1: Enforce Foundational Controls (MFA & Encryption)

RCI must immediately mandate Multi-Factor Authentication (MFA) for all remote access points and enable AES-256 encryption for data at rest. The recent breach was facilitated by weak access controls that allowed attackers to move laterally and access cleartext patient records. Had these controls been in place, the stolen credentials would have been useless without the second factor, and the exfiltrated data would have been unreadable. This is a critical compliance step to meet HIPAA standards and prevent future regulatory fines.

RECOMMENDATION 2: Deploy Immutable Backup Strategy

We recommend implementing the "3-2-1" backup rule: three copies of data, on two different media types, with one copy stored offline or in an immutable state. During the incident, attackers were able to delete RCI's online backups, removing our safety net. Immutable backups cannot be altered or deleted by anyone, including administrators. This ensures that RCI can always restore operations independently, eliminating the need to pay ransoms and ensuring business continuity during a crisis.

RECOMMENDATION 3: Formalize IT Governance & Risk Register

RCI must establish a formal Risk Register and update its Incident Response Plan (IRP) to include specific ransomware playbooks. The chaotic response to the recent incident including the failure to involve legal counsel worsened the financial and reputational damage. A formal governance framework requires executives to sign off on known risks and ensures that future incidents are handled according to legal and ethical standards, protecting the organization from liability.