Microsoft

# Success Story: Lakewood Health's Cybersecurity Journey

**Jim Roeder** says the possibility of a cyberattack keeps him up at night. Roeder, as the Vice President of IT at Lakewood Health System (LHS), a rural hospital in Staples, Minnesota, is keenly aware of the damage a ransomware attack could cause the hospital. Such an attack could dramatically hinder—or completely halt—its ability to care for its patients, some of whom travel up to 50 miles for care.

Staples is a town of roughly **3,000 people** and LHS is recognized by Centers for Medicare and Medicaid (CMS) as a Critical Access Hospital (CAH), the sole hospital within a **25+ mile radius** and serving patients who would otherwise have to travel a significant distance to receive emergency or essential services

Roeder and the Lakewood team are all too familiar with the risks to its network posed by malicious cyber actors—**especially for rural healthcare organizations**. Just a few years ago, the hospital experienced a spear-phishing incident in which the bad actor breached the hospital's email system.

***Jim Roeder***

*Vice President of IT, at Lakewood*

Lakewood's team responded quickly and carefully to resolve the issue, but risks to the hospital's networks remained.

## Refining Lakewood's security posture

In the summer of 2024, Microsoft, the cybersecurity consultancy FSi Strategies, and Lakewood Health embarked on a mission to bolster the security of the hospital's IT environment and mitigate cyber risk as part of **Microsoft's Cybersecurity for Rural Hospitals Program**.

> “
>
> We understand the vital role rural healthcare organizations like Lakewood Health System play in their communities.”
>
> Our cybersecurity efforts protect identities, devices, and data, ensuring these hospitals can continue providing essential care to patients traveling long distances. By partnering with Microsoft, we help these institutions strengthen their defenses against cyber threats, supporting the health and well-being of rural communities.”

**Redha Morsli**

*FSi Strategies's CEO*

As part of this transformation, Lakewood has made significant strides enhancing its **cybersecurity measures**, moving from a baseline with several vulnerabilities to a robust defense system poised to effectively counter cyber threats, as depicted below.

| Cybersecurity Category | Before | After |
|---|---|---|
| Vulnerability Management | Periodic scanning | Continuous, automated scanning |
| Patch Management Processes | 2–5 days to patch | 24–48 hours to patch |
| Multi-Factor Authentication | Incomplete implementation | Mandated for all accounts |
| Email security | Manual interventions | Automatic filtering and removal of suspicious messages |
| Cybersecurity Training | Annual | Monthly |
| Encryption Measures | Inconsistent data encryption | All sensitive data encrypted |
| Incident Response Plan | IT-facing | All organizational stakeholders involved |
| Vendor Management | No systematic cybersecurity measures | Rigorous selection for cybersecurity compliance |

## The future for Lakewood

Lakewood's cybersecurity enhancements reflect a proactive and comprehensive approach to cybersecurity, aligning the hospital with industry best practices and significantly fortifying its defenses against the ever-evolving landscape of cyber threats. The organization's commitment to continuous improvement in cybersecurity not only protects its critical assets but also builds trust among patients and partners.