

CLAIM CASE STUDY

Small Business – Healthcare

How Cowbell helped the policyholder
recover quickly and confidently

Who was affected:

Incident Type: Ransomware

Revenue: \$470,000

Employee Count: 19

What happened?

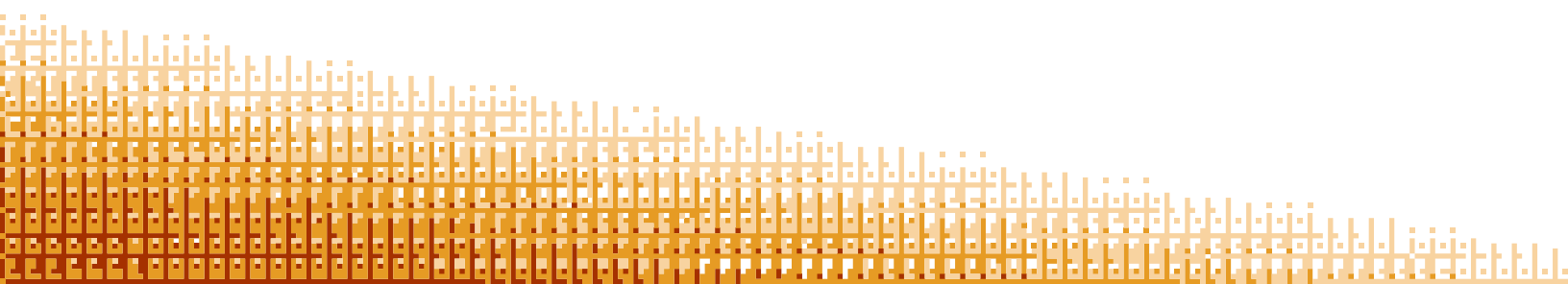
A nurse working for the policyholder arrived at the office early one morning to find ransom notes printed from the company's printer by a threat actor group claiming to have encrypted the organization's systems. The note demanded \$500,000 in Bitcoin to unlock access to patient records and other critical data.

Recognizing the severity of the situation, the policyholder immediately contacted Cowbell's claims team for assistance. Within minutes, Cowbell acknowledged receipt and began coordinating the response.

How Cowbell helped

Cowbell's claims team quickly deployed expert vendors and guided the policyholder through the response process by:

- Assigning breach counsel and forensic specialists to assess the scope of the incident.
- Reviewing and approving vendor workstreams to begin remediation.
- Conducting a preliminary coverage review to confirm policy response.



Outcome

Thanks to Cowbell's prompt coordination and the policyholder's proactive use of data backups, the business was able to restore its systems quickly and minimize business interruption. A forensic investigation confirmed that patient data had not been accessed, and Cowbell's Cybersecurity Services team provided follow-up guidance to strengthen defenses and prevent future incidents.

Key takeaway

Ransomware can be devastating, particularly for small healthcare practices that rely on access to sensitive data and digital systems. With Cowbell's quick action and experienced claims professionals, this policyholder recovered operations swiftly and strengthened its cybersecurity posture for the future.

Need cybersecurity support? Contact our team at cybersecurity@cowbellcyber.ai for tailored guidance from our experts.

Are you experiencing a cyber incident?

Report now! Call **(833) 633-8666** or email our claims team at claims@cowbellcyber.ai.

Cyber incidents don't just affect large enterprises. Small businesses are increasingly targeted by cybercriminals who know that many lack the dedicated security resources of larger organizations. Attacks like phishing and social engineering are often automated, making small businesses equally — if not more — vulnerable.

Cowbell: The Sound Approach to Risk

Cowbell delivers insurance that cuts through complexity and adapts as risks evolve. With streamlined quoting, expert guidance, and protection designed for the realities of today's threats, we make coverage easier to understand and more reliable when it matters most. Behind it all is the Hum—our constant, quiet vigilance—building stronger businesses, trusted partnerships, and the quiet confidence to keep moving forward.



This case study is provided for general informational purposes only and is illustrative in nature. The examples and descriptions included may not represent all possible scenarios or outcomes. Each incident and claim is unique, and actual results may vary. This document does not amend, extend, or form part of any insurance policy. Coverage, terms, limits, and availability may vary and are subject to underwriting approval. Actual coverage is determined solely by the specific terms, conditions, limitations, and exclusions of the issued policy. ©2025 Cowbell Cyber, Inc. All Rights Reserved. Cowbell Insurance Agency LLC, State Licenses: <https://cowbell.insure/state-licenses/>