HEALTHCARE CYBER RECOVERY CASE STUDY · 2024

ASCENSION

When Technical Recovery Became an Ecosystem-Reconnection Challenge

- St. Louis, MO · national system
- May 2024 · ransomware
- Hundreds of vendors reconnected

ASCENSION RESTORED ITS EHR IN ABOUT FIVE WEEKS. RECONNECTING HUNDREDS OF VENDORS TOOK A SEPARATE EFFORT THAT RAN FOR MONTHS.

WHAT HAPPENED

Ascension, one of the nation's largest nonprofit health systems, detected the attack on May 8, 2024. It activated downtime procedures across its ministries, notified partners and authorities, and engaged Mandiant to lead the technical investigation. Critical EHR and patient-portal functions were disrupted; some facilities diverted ambulances and paused elective care while restoration proceeded. Ascension restored EHR access across its ministries by mid-June, roughly five weeks after detection, and continued restoring other systems and revenue-cycle processes for months afterward. [1][2][4]

8–12%	78.4 days	~$874M	95%+
lower same-facility patient volume, May–June 2024	net accounts-receivable days (up from 46.7)	in Medicare & commercial payer advances received	of suppliers reconnected or reconnecting

Source: Ascension FY2024 MD&A; Fierce Healthcare FY2024 financial analysis. Payer advances offset cash-flow disruption; they are not an incident cost.

RECOVERY TIMELINE

1. **May 8 — Detection**
   Investigation, Mandiant engagement, downtime procedures, and partner outreach began.
2. **May–June — Disruption**
   Clinical volume and revenue-cycle effects continued across affected ministries.
3. **Mid-June — Core Restoration**
   EHR access restored across ministries, roughly five weeks after detection.
4. **Late June & Beyond — Normalization**
   Claims, collections, and supplier reconnection continued for months.

THE COST OF RECOVERY

Ascension did not publish a single incident-only dollar total. Its FY2024 financial disclosures instead document the operational and cash-flow effects directly, which is the strongest quantified picture available.

Revenue-cycle delay

Insurance verification, claims submission, and payment processing were delayed across affected ministries.

Lower patient volumes

May and June same-facility volumes averaged 8%–12% below comparable prior-year periods.

Accounts-receivable aging

Net A/R days rose to 78.4 from 46.7 year over year, reflecting a slower conversion of patient-service activity to cash.

Vendor-reconnection burden

Hundreds of vendor negotiations, calls, and webinars created a significant additional resource burden; no public cost allocation was disclosed.

Source: Remparo Combined Financial Consequences and Recovery Costs, Ascension brief. Do not attribute Ascension's FY2024 operating loss to the incident; multiple factors contributed.

WHAT THE RECORD SHOWS

Ascension is the strongest documented example in this series of ecosystem reconnection at scale. The system managed hundreds of individual vendor negotiations, one-to-one calls, eight webinars, and indicator-of-compromise sharing with partner organizations and CISA. More than 95% of suppliers were reported reconnected or reconnecting at the time of reporting.

> ***"Negotiating with hundreds of vendors each with their own unique set of requirements to reconnect was an arduous and time-consuming process."***
>
> **Sean Fitzpatrick**, Vice President of External Communications, Ascension — quoted by *IT Magazine / WIRED*

MEASURED AGAINST RECOGNIZED GUIDANCE

Ascension's response to the May 2024 attack tracked recognized incident-response practice closely, at a scale few of the cases in this series match. The pattern below shows where that discipline paid off, and where even a well-executed response ran into a gap no framework closes.

NIST SP 800-61	Ascension engaged Mandiant to lead the technical investigation and activated downtime procedures immediately on detection, tracking the Preparation and Detection & Analysis phases of NIST's incident-handling model.
CISA #STOPRANSOMWARE	Ascension shared indicators of compromise with CISA and partner health organizations, directly matching CISA's guidance to share threat intelligence so peer organizations can defend themselves.
ISO 22301	Ministry-level downtime procedures and continued, if reduced, patient volumes through the outage reflect a functioning Business Continuity Management System rather than an improvised response.
NIST SP 800-34	SP 800-34 defines recovery in terms of restoring the system itself. It has nothing to say about the hundreds of individual vendor negotiations, each with its own requirements, that Ascension had to run afterward just to reconnect its supply chain.
NO STANDARD ADDRESSES THIS	No NIST or ISO framework defines what evidence a health system owes its business partners before those partners will resume normal transactions with it. Ascension had to invent that process, one-on-one calls and eight webinars, in real time.

Sources: NIST SP 800-61 Rev. 2; NIST SP 800-34 Rev. 1; ISO 22301:2019; CISA #StopRansomware Guide.

Read together, Ascension's response shows what a well-resourced, well-rehearsed incident-response program looks like. The gap that remains isn't a failure of execution, it's a description of ground no recognized framework currently covers: reconnecting an entire ecosystem of counterparties, one relationship at a time.

3 of 5 elements followed recognized guidance

Containment, forensics, and business-continuity practice tracked NIST, ISO, and CISA guidance directly.

2 of 5 mark a gap no framework currently closes

Not a shortfall specific to this organization — a marker of where today's most-cited recovery standards stop measuring the business.

RESTORED IS NOT THE SAME AS TRUSTED

Ascension restored EHR access across its ministries in roughly five weeks, a technically strong outcome for an attack of this scale. That milestone marked the end of the recovery-time clock. It did not mark the end of the business disruption.

> **Disaster recovery does not equal recovered. When counterparties, payers, vendors, banks, also require their own attestation before reconnecting, the business and its operations can remain down while the incident response process is still formally underway, even after every system on the recovery time objective has been restored.**
>
> Remparo Recovery In Depth™ analysis

Ascension's own spokesperson called the vendor-by-vendor reconnection process arduous and time-consuming, and more than 95% of suppliers were only reconnected or reconnecting by the time that was reported, months after EHR access was restored. Net accounts-receivable days rose from 46.7 to 78.4 over the same period, a direct financial signature of a business still working its way back to normal while its systems were already back.

EHR ACCESS RESTORED IN ABOUT FIVE WEEKS. RECONNECTING HUNDREDS OF SUPPLIERS WAS STILL UNFINISHED MONTHS LATER.

WHAT THIS MEANS FOR YOUR EXECUTIVE TEAM

- Maintain a critical-partner inventory sized for hundreds of relationships, not a handful.
- Assign named relationship owners so vendor negotiations don't default to whoever picks up the phone.
- Build scalable briefing formats, webinars and evidence packages, that don't require a bespoke conversation with every counterparty.
- Track reconnect status centrally, and keep alternate claims and payment procedures ready for the gap.

Adapted from Remparo Recovery In Depth™ case research, Ascension (2024).

THE SIX EXECUTIVE QUESTIONS, APPLIED TO ASCENSION

Ascension's public record speaks most directly to four of the six questions Recovery In Depth™ asks every executive team to answer.

How do we keep revenue and cash moving?

Approximately $874 million in Medicare and commercial-payer advances kept Ascension's cash position stable while claims submission and payment processing worked through a months-long backlog.

PAPER 4

How do we rebuild the confidence of everyone we depend on?

Hundreds of individual vendor negotiations, run through one-on-one calls and eight webinars, show ecosystem reconnection functioning as its own recovery track, not a footnote to technical restoration.

PAPER 5

What must keep operating?

Some facilities diverted ambulances and paused elective care while restoration proceeded, evidence that degraded-mode continuity has to function even at a system the size of Ascension.

PAPER 3

How do we communicate?

Hundreds of individual vendor calls ran alongside eight public webinars and indicator-of-compromise sharing with CISA and peer health organizations, treating ecosystem-wide communication as a parallel workstream to technical restoration, not a follow-up to it.

PAPER 1

RECOVERY IN DEPTH™ LESSON

This is the scale problem Remparo Continuity and Vault are built to prevent: keeping eligibility, scheduling, and billing running on infrastructure that never touched the compromised network, so a health system isn't negotiating its way back to normal operations one vendor at a time.

95%+ of suppliers reconnected or reconnecting, after hundreds of individual negotiations.

EVIDENCE-STRENGTH ASSESSMENT

CLAIM AREA	EVIDENCE STRENGTH	BASIS / LIMITATION
Mandiant engagement	High	Official Ascension statement
Mid-June EHR restoration	High	Ascension FY2024 financial disclosure
Revenue-cycle effects (volume, A/R days)	High	Ascension FY2024 financial disclosure
Hundreds of vendor negotiations	High	Direct statement attributed to Ascension spokesperson
95%+ reconnection status	High	Direct statement at time of reporting
Uniform attestation requirement across vendors	Not established	Sources describe differing requirements by vendor

REFERENCES

[1] Ascension, Network Interruption Update. https://about.ascension.org/news/2024/05/network-interruption-update2

[2] Ascension, FY2024 Management Discussion and Analysis. https://about.ascension.org/-/media/project/ascension/about/section-about/financials/2024/ascension-management-discussion-and-analysis-q4-fy24.pdf

[3] IT Magazine / WIRED, vendor-reconnection report. https://itmagazine.com/2024/06/24/how-red-tape-is-exacerbating-the-impact-of-hospital-ransomware-attacks/

[4] Cybersecurity Dive, impact report. https://www.cybersecuritydive.com/news/ascension-cyberattack-data-breach/736183/

[5] Fierce Healthcare, FY2024 financial analysis. https://www.fiercehealthcare.com/ai-and-machine-learning/ascensions-spring-ransomware-attack-sidelines-fy24s-financial-recovery

[6] HIPAA Journal, data-review and notification report. https://www.hipaajournal.com/ascension-cyberattack-2024/

[7] NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[8] NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-34r1.pdf

[9] ISO 22301:2019, Security and resilience — Business continuity management systems. https://www.iso.org/standard/75106.html

[10] CISA, #StopRansomware Guide. https://www.cisa.gov/stopransomware/ransomware-guide

Claims in this case study are limited to the cited public record and Remparo's source-verified Recovery in Depth™ research briefs. Analytical statements are labeled as Recovery in Depth™ analysis and are not statements made by Ascension.