HEALTHCARE CYBER RECOVERY CASE STUDY · 2021

SCRIPPS HEALTH

When Technical Recovery Required External Assurance

- San Diego, CA
- May 2021 · ransomware
- $112.7M total financial impact

SCRIPPS RESTORED ITS CORE SYSTEMS IN ABOUT FOUR WEEKS. GETTING ITS PARTNERS TO SAY YES TOOK A SEPARATE, PARALLEL EFFORT.

WHAT HAPPENED

On May 1, 2021, malware propagated laterally across Scripps Health's network. The San Diego-based system responded with a systemwide shutdown to contain the threat: disconnecting sites, data centers, internet access, remote connectivity, phones, and its Epic EHR. Hospitals reverted to paper. Staff used personal phones. Clinics curtailed activity, and emergency departments began ambulance diversion. Runners and local command structures kept information moving where electronic systems could not. Scripps restored Epic and its other major systems in late May, about three and a half to four weeks after the attack began, and reported $112.7 million in lost revenue and incremental costs through June 30, 2021. [1][2][3]

$112.7M	$91.6M	$21.1M	~30
total financial impact through June 30, 2021	lost patient-service revenue	incremental incident & recovery cost	vendor assurance letters produced

Sources: AHA leadership retrospective; Fierce Healthcare; Becker's Hospital Review; SC Media financial analysis; HIPAA Journal.

RECOVERY TIMELINE

1

May 1 — Detection & Containment

Malware identified inside the network; broad, systemwide isolation began within hours.

2

Early–Late May — Degraded Operations

Paper records, alternate communications, ambulance diversion, and manual clinical workflows across affected sites.

3

May 26–27 — Technical Restoration

Epic, other major systems, and the patient portal restored, roughly four weeks after the attack began.

4

After Restoration — Long-Tail Recovery

Document review, notification, and privacy work continued for months after clinical systems were back online.

THE COST OF RECOVERY

Scripps' $112.7 million estimate, measured through June 30, 2021, breaks into categories its own financial reporting kept separate.

Lost patient-service revenue — $91.6M

Emergency diversions and postponed elective surgeries reduced patient volume and revenue during the roughly four-week outage.

Incident-response & recovery expense — $21.1M

Computer consulting, forensic investigation, restoration, and related response activity.

Insurance timing

Only $5.9M had been accrued by June 30, 2021; another $14.1M was expected later, subject to accounting recognition.

Litigation exposure

Proposed patient class actions were reported. Scripps' published $112.7M estimate did not include a finalized litigation-cost total.

Source: Remparo Combined Financial Consequences and Recovery Costs, Scripps Health brief.

WHAT THE RECORD SHOWS

Scripps produced approximately 30 assurance letters for clinical, business, and administrative software partners, each of whom had to independently decide whether Scripps' environment could be trusted again. Some vendors initially rejected the assurance and asked for more technical documentation, wanting confirmation that independent outside experts had been involved and that the malware had been contained and remediated using reasonable best efforts.

> ***"Initially, there were several vendors that did not accept the assurance letter and requested additional technical documentation and information. However, this was limited and ultimately did not result in a delay to restoring access to systems at Scripps."***
>
> **Shane Thielman**, Chief Information Officer, Scripps Health — quoted by *IT Magazine / WIRED*

MEASURED AGAINST RECOGNIZED GUIDANCE

Scripps Health's early response tracked several elements of recognized incident-response and business-continuity guidance directly. The table below maps documented actions to the frameworks that describe them, and marks the point at which those frameworks stop describing what actually happened next.

NIST SP 800-61	Scripps isolated affected sites, data centers, and remote connectivity within hours of detecting lateral movement, consistent with the Containment, Eradication, and Recovery phase of NIST's Computer Security Incident Handling Guide.
ISO 22301	Paper-based charting, personal-phone communication, and ambulance diversion reflect the kind of manual workaround procedure a mature Business Continuity Management System is meant to define in advance.
CISA #STOPRANSOMWARE	Scripps brought in outside forensic and computer-consulting expertise before restoring systems, matching CISA's guidance to involve trusted third parties in the investigation before returning to normal operations.
NIST SP 800-34	SP 800-34's contingency-planning model measures recovery against a Recovery Time Objective for restoring systems. It has no defined step for the roughly 30 external partners who each separately decided, on their own timeline, whether Scripps' environment could be trusted again.
NIST SP 800-207	Zero Trust architecture governs who gets access inside Scripps' own environment. It was never designed to answer whether a payer, bank, or software vendor outside that environment should extend trust back to Scripps.

Sources: NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide; NIST SP 800-34 Rev. 1, Contingency Planning Guide; NIST SP 800-207, Zero Trust Architecture; ISO 22301:2019; CISA #StopRansomware Guide.

Read together, Scripps followed containment and business-continuity practice about as well as the public record allows us to verify. The unmet items aren't a shortfall specific to Scripps, they describe what today's most-cited recovery standards were built to measure, and what they were never designed to.

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

By late May 2021, Scripps' own restoration effort was essentially done. Epic was back online, and the technical incident-response process had moved into its later phases. But "restored" and "trusted again" turned out to be two different findings, made by two different parties, on two different clocks.

> **Disaster recovery does not equal recovered. When counterparties, payers, banks, software vendors, 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

Scripps produced roughly 30 of those attestations while its clinical teams were still working through the operational backlog the outage had created. Some vendors pushed back and asked for more. None of that shows up in a Recovery Time Objective. It shows up in how long it actually took Scripps to be treated, by the organizations it depends on, as open for business again.

SYSTEMS RESTORED IN ABOUT FOUR WEEKS. THE ~30-LETTER VENDOR ASSURANCE PROCESS RAN ON ITS OWN, SLOWER CLOCK.

WHAT THIS MEANS FOR YOUR EXECUTIVE TEAM

- Predefine a critical-partner inventory before an incident, not during one.
- Name a single owner responsible for assembling and issuing assurance packages to outside partners.
- Pre-approve the technical statements and outside-expert involvement partners are likely to require.
- Track partner acceptance as its own recovery milestone, separate from system restoration.

Adapted from Remparo Recovery In Depth™ case research, Scripps Health (2021).

THE SIX EXECUTIVE QUESTIONS, APPLIED TO SCRIPPS HEALTH

Recovery In Depth™ organizes every cyber event around six questions an executive team has to be able to answer. Scripps' public record speaks most directly to four of them.

What can we still trust?

Scripps' own systems were back online in roughly four weeks. Whether Scripps itself could be trusted by the outside organizations it depended on was a separate, slower-moving question, answered one assurance letter at a time.

PAPER 2

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

Producing around 30 vendor assurance letters, some of which were initially rejected, shows this wasn't a formality. It was a real, resource-intensive workstream that ran in parallel with, not after, technical recovery.

PAPER 5

How do we protect the people affected?

The breach affected approximately 147,267 individuals. Notification and identity-protection work ran alongside, not after, the technical and partner-facing recovery effort.

PAPER 5

How do we keep revenue and cash moving?

Scripps reported $91.6 million in lost patient-service revenue and had only $5.9 million in accrued insurance recovery by June 30, 2021, with another $14.1 million still pending recognition. Its insurer was its own counterparty, moving on its own schedule.

PAPER 4

RECOVERY IN DEPTH™ LESSON

This is exactly the gap Remparo Continuity is built to close: an isolated, HIPAA-compliant environment that was never connected to the compromised network, so eligibility checks, scheduling, and billing keep moving while that proof is still being assembled, not after.

~30 vendor assurance letters, produced while clinical systems were still being restored.

EVIDENCE-STRENGTH ASSESSMENT

CLAIM AREA	EVIDENCE STRENGTH	BASIS / LIMITATION
Outage / restoration timeline	High	Leadership retrospective and dated contemporary reporting
Financial impact ($112.7M)	High	Scripps financial reporting
~30 assurance letters	High	Direct statement attributed to CIO Shane Thielman
Additional evidence requests	High	Direct statement attributed to CIO Shane Thielman
Backup-compromise details	Moderate	Secondary reporting; technical specifics unavailable
Attestation caused restoration delay	Not established	Scripps stated these requests did not delay restoration access

REFERENCES

[1] AHA leadership retrospective, “How to Survive a Cyberattack with Scripps Health.” https://www.aha.org/news/headline/2025-01-13-aha-podcast-how-survive-cyberattack-scripps-health-part-three

[2] Fierce Healthcare, financial report on lost revenue and recovery costs. https://www.fiercehealthcare.com/hospitals/may-cyber-attack-cost-scripps-nearly-113m-lost-revenue-more-costs

[3] Becker’s Hospital Review, EHR restoration report. https://www.beckershospitalreview.com/healthcare-information-technology/cybersecurity/scripps-ehr-back-online-nearly-4-weeks-after-ransomware-attack/

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

[5] HIPAA Journal, backup-impact reporting. https://www.hipaajournal.com/scripps-health-ransomware-attack-cost-113-million/

[6] SC Media, financial analysis. https://www.scworld.com/analysis/scripps-health-cyberattack-ehr-downtime-caused-112-7m-in-lost-revenue-recovery

[7] Becker’s Hospital Review, Q3 operating-loss report. https://www.beckershospitalreview.com/finance/scripps-records-q3-operating-loss-notes-cyberattack-cost-of-112-7m/

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

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

[10] NIST SP 800-207, Zero Trust Architecture. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

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

[12] 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 Scripps Health.