remparo

RECOVERY IN DEPTH™

The Board Case for Recovery In Depth™

What a Breach Actually Costs, and How Long It Actually Lasts

In early 2025, Fitch Ratings downgraded Palomar Health in California from BB+ to B-. Months later, it downgraded Frederick Health Hospital in Maryland from BBB+ to BBB. Both moves cited cyberattacks among the drivers. "That's the first time we've seen an impact from cyber really raise the level of having an impact on the rating," Fitch's Kevin Holloran said. A cyberattack had become a credit event, not just a technology event, and rating agencies started treating it that way.

Boards understand credit events. They approve budgets against them, they report them to lenders, and they know exactly what a downgrade costs the next time the organization borrows. That's the audience for this paper: the case for Recovery In Depth™, made in numbers a finance committee already knows how to read.

1. The State of DR and BC Today

Standard Business Impact Analysis treats financial impact mainly as a planning input. It's priced out in advance to justify a security budget, then handed to insurance and finance to tally retrospectively once incident response formally closes. That habit understates the true cost, because the financial tail of a breach runs for months, sometimes years, after the technical incident is declared closed. Treating it as a one-time remediation line item is the mistake the rest of this paper corrects.

2. Why Recovery In Depth™ Is Needed

Revenue and cash need to be treated as a recovery objective in their own right, not a byproduct of technical recovery. In healthcare, no claims moving means no cash coming in. The same logic holds in financial services, where it's settlement, or in any revenue-dependent business, where it's transactions. Recovery In Depth™ treats the financial and reputational tail as its own live track, run in parallel with incident response from day one, rather than handed off once the technical work is finished.

3. Where This Fits in the Overall Model

Recovery In Depth™ is organized around six questions an executive team has to be able to answer during a cyber event. This paper takes up the fourth:

1. **What can we still trust?**
2. **What must keep operating?**
3. **How do we communicate if our normal channels are suspect?**
4. **How do we keep revenue and cash moving?**
5. **How do we protect customers, patients, employees, and partners?**
6. **How do we rebuild confidence after the technical incident is contained?**

This is the “so what” for a financial audience. It puts the architecture arguments from earlier in this series into dollar terms, for readers who won't sit through the technical detail but will sit through a number that moves a bond rating.

4. Quantifying the Cost

The Direct-Cost Baseline (Cross-Industry)

Putting a number on the cost of a cyberattack starts with what public markets already price in. Academic research on publicly traded firms finds a measurable, immediate market reaction to a disclosed cyberattack. A widely cited NBER study of cyberattack announcements found a significant negative stock-market reaction, concentrated most heavily around attacks involving loss of personal financial information, averaging roughly a 1.1% drop in share value in the days around disclosure and an average loss of about $607 million in shareholder value for the firms studied. The same research found sales growth declines that persist for large firms, a shift toward debt financing with longer maturities, and boards responding by increasing risk oversight and shifting CEO pay away from stock options and bonuses toward restricted stock.

The American Academy of Actuaries models extreme cyber-risk scenarios and puts a catastrophic health-sector cyber event at $6.2 billion to $62.1 billion in the U.S., the widest range of any sector it models, reflecting genuine uncertainty about how far a single incident can cascade. Part of that uncertainty comes from what the Academy calls digital monoculture: when large numbers of organizations run the same operating systems, software, or cloud infrastructure, a single flaw, the way WannaCry exploited one Windows vulnerability, can cascade across sectors that have nothing else in common.

Global data breach costs give a useful baseline before healthcare's own number gets more specific: IBM and the Ponemon Institute put the 2023 global average cost of a data breach at $4.45 million across industries. That's the baseline. Healthcare runs well above it, as the next section shows.

The Healthcare-Specific Cost Curve

IBM's 2024 Cost of a Data Breach Report put the average cost of a healthcare data breach at $9.77 million, a record high and more than double the global cross-industry average. Healthcare has held the highest average breach cost of any industry IBM tracks for over a decade running.

The credit-rating consequence is now directly documented, not theoretical. Beyond the Palomar Health and Frederick Health Hospital downgrades in the opening of this paper, Fitch has warned that the credit effects of a cyberattack can compound with labor pressure and inflation already squeezing not-for-profit hospital margins. The agency's deeper concern is a vicious cycle: cyber insurance premiums are rising faster than other coverage lines, which makes them least affordable for the financially strained, rural, and safety-net hospitals that are also the least equipped to prevent or recover from an attack in the first place.

Microsoft's 2025 analysis of ransomware's effect on hospitals estimated an average revenue loss of $1.9 million for every day of downtime, and found that a typical attack can disable access to critical systems, including electronic health records, for up to 18 days. Multiply the two and the exposure for a single mid-sized incident runs into the tens of millions before a single dollar of remediation, legal, or notification cost is counted.

- **The neighbor effect:** a breach's cost doesn't stay inside the breached organization. A 2023 JAMA Network Open study of the Scripps Health attack found that a nearby, never-breached emergency department absorbing the overflow saw daily patient volume rise 15.1%, patients leaving without being seen rise 127.8%, median wait times rise 47.6%, and stroke code activations rise 74.6%, all during the month Scripps was down. The authors' conclusion is the one worth carrying into a board discussion: plan for a healthcare cyberattack as a regional event, not a single-organization incident.
- **The finance and accounting attack surface:** a 2026 IJRISS study on financial-system cyber vulnerability makes a point worth underlining for any CFO: financial and accounting functions are disproportionately targeted precisely because of the data they hold. A revenue cycle cyberattack is a target in its own right, not just a casualty of a clinical-systems attack, which is exactly what Prospect Medical Holdings' Medicaid-claims disruption in Paper 3 of this series showed in practice.

CASE IN POINT: SCRIPPS HEALTH, 2021

What Insurance Actually Covers

Scripps Health's total documented cost from its May 2021 ransomware attack reached $112.7 million: $91.6 million in lost revenue during the roughly four-week recovery window, plus $21.1 million in incremental response and recovery costs. By the time Scripps reported its figures, cyber insurance had reimbursed $5.9 million, with another $14.1 million expected by fiscal year end, a combined recovery of roughly $20 million against $112.7 million in total cost.

On top of the operational cost, Scripps separately agreed to a $3.57 million settlement addressing the roughly 147,000 patients whose protected health information was affected, a cost that sits outside the recovery figures entirely.

None of this makes cyber insurance worthless. It makes the point precise: insurance reimbursed something like a sixth to a fifth of the total cost. It is risk transfer for a fraction

of the exposure, not a substitute for a recovery capability that keeps the fraction from getting that large in the first place.

Sources: HIPAA Journal; Fierce Healthcare; CBS 8 San Diego settlement reporting.

Change Healthcare, by the Numbers

No single incident makes the ecosystem-scale case better than Change Healthcare, and no single incident better illustrates hospital revenue loss during ransomware at national scale. In a survey taken about one month after the attack, the American Hospital Association found 94% of hospitals reported a financial impact, with more than half calling it significant or serious. Among the hospitals reporting cash-flow effects, more than a third said the impact touched over half their total revenue. Seventy-four percent reported a direct effect on patient care, and nearly 40% said patients had difficulty accessing care because of delays in health plan utilization reviews. Forty-four percent of hospitals expected the negative revenue effects to continue for another two to four months beyond the survey date. UnitedHealth's own disclosed cost reached $872 million in the first quarter of 2024 alone, before the full-year total was tallied.

Systems restored and fully recovered are not the same event. For a meaningful share of hospitals nationwide, the gap between them ran for months, not the days or weeks incident response measures itself by.

The Community-Scale Frame

A hospital's financial disruption isn't only the hospital's problem. The American Hospital Association estimates hospitals directly employ nearly 6 million people nationally, that every hospital job supports roughly two more jobs in the surrounding community, and that every dollar a hospital spends generates about $2.30 in additional local business activity, a combined economic footprint of nearly $3 trillion. A breach severe enough to disrupt a hospital's finances for months is a local-economy event, not a contained IT incident, which is worth keeping in view for board members and community stakeholders who sit outside healthcare entirely.

Documented Financial Impact Across Five Recent Health System Breaches

Organization	Year	Documented Financial Impact
Ascension	2024	~$874M in Medicare/commercial-payer advances received in FY2024; AR days rose 46.7 to 78.4
Scripps Health	2021	$112.7M total ($91.6M lost revenue + $21.1M incremental cost); ~$20M reimbursed by insurance; separate $3.57M patient settlement
CommonSpirit Health	2022	$160M estimated adverse financial effect (company disclosure)
Prospect Medical Holdings	2023	Connecticut alone: state advanced ~$7.5M due to blocked Medicaid claims filing

Organization	Year	Documented Financial Impact
Change Healthcare / UnitedHealth	2024	$872M disclosed cost for Q1 2024 alone; 94% of surveyed hospitals reported financial impact

Five organizations, four years, five different financial mechanisms: payer advances, direct lost revenue, disclosed adverse effect, state Medicaid advances, and a quarter's worth of disclosed cost. None of these figures are directly comparable to each other. That's the point. A single "average cost of a breach" number, however well sourced, can't capture how differently the bill actually arrives.

5. Conclusion

The financial case for Recovery In Depth™ isn't that breaches are expensive. Every organization already knows that. It's that the expense is a multi-year, multi-channel event, financing cost, lost revenue, an insurance gap, spillover to neighboring providers, that a one-time remediation budget line badly understates. Fitch's 2025 downgrades show rating agencies have started pricing that in. Board-level cyber resilience means boards should too, before the next rating action, not after it.

None of this cost is contained by technology alone. It's contained by how fast an organization can rebuild the confidence of patients, regulators, rating agencies, and its own board, which is the last question in this series.

> *"Cyber insurance is risk transfer for a fraction of the exposure, not a substitute for a recovery capability."*

Coming next: "From Contained to Trusted." It closes the series by covering how organizations protect the people affected by a breach and rebuild the confidence of everyone they depend on, and introduces a way for executive teams to score where they stand today.

Recovery In Depth™. Rebuilding trust.

Sources

1. Chief Healthcare Executive and Fierce Healthcare reporting on Fitch Ratings' 2025 downgrades of Palomar Health and Frederick Health Hospital, and Fitch's commentary on cyber-driven credit risk at financially strained hospitals.

2. Kamiya, Kang, Kim, Milidonis & Stulz, "What Is the Impact of Successful Cyberattacks on Target Firms?" NBER Working Paper 24409; summary via Harvard Law School Forum on Corporate Governance.

3. American Academy of Actuaries, "The Economic Impact of Extreme Cyber Risks" (actuary.org).

4. IBM / Ponemon Institute, Cost of a Data Breach Report 2023 (global average) and Cost of a Data Breach Report 2024 (healthcare-industry average).

5. Microsoft, 2025 analysis of ransomware's financial impact on hospital downtime.

6. Dameff et al., "Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US," JAMA Network Open (2023).

7. Zainudin, Basri, Marsam & Ab Majid, "The Vulnerability of the Financial and Accounting System to Cyberattack," International Journal of Research and Innovation in Social Science (IJRISS).

8. Remparo Recovery In Depth™ case research, Scripps Health (2021): HIPAA Journal; Fierce Healthcare; CBS 8 San Diego.

9. American Hospital Association survey, "Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances" (March 2024); UnitedHealth Group First Quarter 2024 Results.

10. American Hospital Association, economic-contribution reporting on hospitals' employment and local economic impact (2025 update).

11. Remparo Recovery In Depth™ case research, Ascension (2024), CommonSpirit Health (2022), and Prospect Medical Holdings (2023): see Papers 2 and 3 in this series for full source lists.