remparo

RECOVERY IN DEPTH™

From Contained to Trusted

Protecting People and Rebuilding Confidence After a Breach

An organization can restore every system it owns and still be unable to operate, because operating depends on counterparties, a payer, a clearinghouse, a supplier, who each make their own separate decision about whether to trust it again. A hospital's own systems can be fully intact and it can still be unable to submit a claim or verify a patient's eligibility. Being recovered is not the same as being reconnected, and nowhere in this series has that gap mattered more than it does here, at the end.

This closing paper takes up the last two of the Six Executive Questions: how an organization protects the people affected by a breach, and how it rebuilds the confidence of everyone it depends on once the technical incident is over. It also closes the loop on the full series, and offers a way for an executive team to score where it actually stands today.

1. The State of DR and BC Today

Neither Disaster Recovery nor Business Continuity Planning has a native answer for the question this paper is about: the technical incident is over, now what. DR stops at systems restored. BCP's Business Impact Analysis hands financial and reputational tracking to insurance and finance retrospectively, as Paper 4 covered, and has even less to say about stakeholder trust specifically.

Trust runs on its own clock, and it's usually the longest of the four this series has covered: technical, operational, financial, and trust. It's also the one most organizations have no plan for at all.

2. Why Recovery In Depth™ Is Needed

Trust has to be planned for. It can't be improvised. Regulators, patients, partners, and an organization's own board each form their own independent judgment about whether it's safe to deal with again, and that judgment doesn't automatically follow from IT declaring systems back online.

Equifax is the cautionary case worth keeping in view here. Its 2017 breach shows technical remediation was the beginning of the recovery process, not the end. Customer trust, regulatory attention, legal exposure, and brand reputation stayed live issues for years after Equifax's systems had stabilized.

3. Where This Fits: The Full Framework, Closed

This series has walked through all six of the questions an executive team has to be able to answer during a cyber event, one or two at a time:

1. **What can we still trust? Paper 2 covered this: strong security architecture answers whether you can detect and contain a threat, not whether you can be trusted again.**
2. **What must keep operating, and how do we communicate? Paper 3 covered this: degraded-mode workflows, pre-trained redeployment, and communications channels that don't depend on the system that's down.**
3. **How do we keep revenue and cash moving? Paper 4 covered this: the financial tail of a breach runs for months or years, in mechanisms a one-time remediation budget doesn't capture.**
4. **How do we protect the people affected?**
5. **How do we rebuild confidence once the technical incident is contained?**

The last two close the loop, and they're the reason "being recovered" and "being reconnected" are different events. Recovered is a technical judgment an organization makes about itself. Reconnected is a judgment everyone else makes about the organization, and it happens on their timeline, not the organization's.

4. Protecting Stakeholders and Rebuilding Confidence

Protecting People

At a practical level, this question covers patient or customer notification, identity-protection services where they're warranted, employee support, and continuity of vendor and partner relationships through the disruption. None of it is exotic. All of it has to be ready to execute quickly, because the notification clock in most jurisdictions starts running whether or not the organization is ready.

- **Ascension (2024):** one of the nation's largest nonprofit health systems, Ascension's ransomware attack took EHR and patient-portal capability offline at some facilities, reportedly forcing ambulance diversions and paused elective care. Clinical recovery and technology recovery weren't the same event: patient notification and the longer work of rebuilding confidence continued well after systems came back, running alongside the financial recovery covered in Paper 4.
- **CommonSpirit Health (2022):** a multi-state EHR access interruption and delayed care were followed months later by formal notification to more than 623,000 patients whose data had been exposed. Three tracks ran at once and on different timelines: technical capability, patient care, and the financial and legal consequences covered in Paper 4, with the CFO as much a recovery stakeholder as the CIO.
- **Capital One (2019):** a cross-industry governance case worth knowing even outside healthcare. Unauthorized access affected roughly 100 million individuals in the United States

and 6 million in Canada. The Office of the Comptroller of the Currency assessed an $80 million penalty for failing to establish effective risk assessment before migrating significant IT operations to a public cloud environment. The trust dimension isn't only about how an organization responds to a breach. It extends to governance and regulatory accountability for how the environment was built in the first place.

Rebuilding Confidence

This is the reconnection problem from Paper 2, revisited from the relationship side rather than the technical one. Third-party attestation, regulator engagement, and communications strategy all need to be designed before a breach happens. Improvised during one, they cost weeks an organization doesn't have.

CASE IN POINT: EQUIFAX, 2017

When Nobody Else Writes the Recovery Narrative

Equifax's 2017 breach remains the clearest example of trust recovery outlasting technical recovery by years, not weeks. The company ultimately agreed to pay up to $700 million to resolve federal and state claims, including at least $575 million and potentially up to $700 million depending on consumer claims, in a settlement with the FTC, the CFPB, and all fifty states, the largest data-breach settlement in U.S. history at the time.

The technical incident closed long before the trust recovery did. Congressional hearings, credit-monitoring obligations, state-level litigation, and sustained media scrutiny continued for years after Equifax's systems were secured. The company hadn't pre-built a communications strategy, an attestation process, or a regulator-engagement plan built for a breach of this scale, and the recovery narrative got written by the people asking the questions rather than the company answering them.

The lesson for this series isn't that a breach this size is unsurvivable. Equifax survived it. It's that an organization that hasn't planned for accountability, customer support, and regulator engagement in advance spends years catching up to a story other people are already telling.

Sources: FTC press release and settlement summary; Consumer Financial Protection Bureau enforcement record; Hunton Andrews Kurth privacy and cybersecurity coverage.

Synthesis: The Full Operating Model

Brought together, the Six Executive Questions form a single checklist an executive team can score itself against, honestly, before the next incident rather than during it. A simple 0 to 3 scale works: 0 means unknown or unplanned, 1 means documented but never tested, 2 means tested in a tabletop exercise, and 3 means operationally validated under realistic conditions.

Most organizations that go through this exercise for the first time are surprised by how many of their six questions score a 0 or a 1. That's the value of doing it before an incident: it turns a vague sense of preparedness into six specific, addressable gaps.

A Starting Point: The Recovery Readiness Checklist

Executive Question	Score Yourself: 0 (Unplanned) to 3 (Validated)
1. What can we still trust?	___
2. What must keep operating?	___
3. How do we communicate if normal channels are suspect?	___
4. How do we keep revenue and cash moving?	___
5. How do we protect the people affected?	___
6. How do we rebuild confidence once contained?	___

Plotted across all six questions, the same scores become a Recovery Readiness Score, a single-glance view of where an organization is strong and where it isn't, the kind of board-level cyber resilience artifact that travels well into a board deck precisely because it doesn't require the reader to have followed this whole series to understand it.

Where Remparo Fits

Remparo builds toward the six questions this series has walked through, not around them. Continuity gives an organization one of the trusted recovery environments this series has been arguing for throughout, a clean, isolated place to operate from when production can't be trusted. Vault holds the records, billing, and vendor information a recovery depends on, staged outside the environment a breach could reach. Hardline gets trusted hardware into the hands of the people who need it when their own equipment can't be trusted. And Advisory helps an executive team run the scoring exercise above, honestly, before an incident forces the question.

If this series has been useful, the next step is straightforward: score your own organization against the six questions above, and visit remparo.com to learn how Continuity, Vault, Hardline, and Advisory map to wherever your gaps turned out to be.

5. Conclusion

Paper 1 established that trust doesn't automatically survive a breach. Papers 2 through 4 covered what to trust, how to keep operating and communicating, and what it costs. This closing paper covered how to protect the people affected and earn confidence back, and how to score where an organization stands today across all six questions. Taken together, the five papers answer the question this series set out to answer: why hospitals fail during recovery even when their technical teams do everything right, and what a genuinely different model looks like instead.

> *"Prevention is the shield. Recovery is the discipline. Trust is the battlefield. Recovery In Depth™ is how the business survives."*

Recovery In Depth™. Rebuilding trust.

Sources

1. Remparo Recovery In Depth™ case research, Ascension (2024): see Paper 2 in this series for full source list.

2. Remparo Recovery In Depth™ case research, CommonSpirit Health (2022): CommonSpirit official update; HIPAA Journal; BleepingComputer; JD Supra notification reporting (623,774 individuals notified).

3. CBS News and CIO Dive reporting on the Capital One (2019) data breach; Office of the Comptroller of the Currency consent order and $80 million civil money penalty (2020).

4. Federal Trade Commission, “Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach” (2019); Consumer Financial Protection Bureau enforcement record; Hunton Andrews Kurth coverage.