From Three Days Offline to 30-Minute Tested Recovery

How a multi-building manufacturer rebuilt after ransomware and created a tested cyber resilience program.

38 acres	3 days	~$1.4M/day	All systems
operating site	minimum recovery	production value at risk	impacted

The Issue

A multi-building industrial manufacturer in the Northeast experienced a ransomware attack that infected workstations, servers, backups, and systems connected to manufacturing equipment. The attack effectively shut down the entire operation.

The incident became visible when a sawmill started unexpectedly.

Personnel investigated the unexplained equipment activity just as computers across the environment began displaying signs of ransomware. Production, file access, and core business systems became unavailable across a five-to-six-building, 38-acre site.

Why It Mattered

- The operation normally ran approximately 14 production hours per day, with roughly $1.4 million in daily production value exposed during a shutdown.
- The ransomware compromised not only endpoints and servers, but also the backups intended to support recovery.
- The network had minimal protection, limited redundancy, and critical equipment operating from an improvised basement environment.
- The business was completely dependent on restoring technology before full production could resume.

The Immediate Response

Calkri was brought in after local IT resources were unable to restore the environment. The first priority was containment and restoring enough capability for the business to operate. Minimum operations returned in approximately three days, followed by an intensive rebuild and hardening effort.

THE FIX

Rebuild for Failure - Not Just Recovery

The goal was not to return the company to its old environment. It was to make the next failure survivable.

PHASE 1

Secure the foundation

Rebuilt the network with redundant next-generation firewalls, managed switching, secured equipment, and cleaner physical infrastructure.

PHASE 2

Improve site reliability

Installed fiber between buildings, replacing less reliable point-to-point wireless connectivity across the industrial site.

PHASE 3

Create independent recovery paths

Added redundant internet, cloud-replicated storage, and full server recovery capabilities so operations were not tied to one physical server or connection.

PHASE 4

Layer security and governance

Added endpoint protection, MFA, segmentation, logging, stronger access controls, protected backups, employee training, and documented recovery procedures.

Recovery Built Into Operations

- Critical devices could reach either the primary server or the cloud recovery environment.
- Recovery covered the full server environment, not just selected files or applications.
- The local MSP was trained on the redesigned environment for ongoing support.
- Controls and documentation were aligned to SOC 2 expectations without claiming formal certification.

The rebuild moved quickly, but the operating model was built for the long term.

Minimum operations returned in about three days; the environment was rebuilt and hardened to the new standard within approximately two months.

THE PROOF

Recovery Was Tested - Not Assumed

Quarterly tests deliberately removed critical infrastructure during business hours to prove the company could keep operating.

~30 min	<=1 hr	Quarterly	6 years
quarterly tested recovery	later real outage	live failover tests	since ransomware event

Quarterly Live Recovery Tests

Once every quarter, the organization deliberately shut down the primary server and disabled one of the firewalls during normal business hours. The team then validated that systems, manufacturing equipment, connectivity, and recovery paths operated as designed.

Full recovery validation routinely took approximately 30 minutes.

The test was not complete until connected equipment and business systems had been checked. Recovery capability became a recurring operating discipline rather than a disaster-recovery document sitting on a shelf.

A Real Server Failure Proved the Design

The primary server later froze because of faulty memory. Spare memory was already kept on-site for this type of failure. While the physical server was repaired, the company operated from the cloud recovery environment and experienced no more than approximately one hour of disruption.

Six Years Later - No Repeat Ransomware Event to Date

It has now been approximately six years since the ransomware incident. During that time, security logs have shown continued attack attempts, including repeated brute-force activity, but the organization has not experienced another successful ransomware event to date.

The result came from layers, not one security product.

Firewalls, visibility, endpoint protection, MFA, segmentation, protected backups, employee training, and recurring testing were designed to reduce both the likelihood and the impact of another incident.

THE OUTCOME

Cyber Resilience as a Business Capability

The organization moved from a complete ransomware shutdown to a tested operating model designed around recovery, evidence, and continuity.

3 days	~30 min	7 years	No repeat
minimum operations restored	tested recovery	semiannual insurer audits	ransomware to date

Insurance and Third-Party Validation

The insurer initially challenged coverage for cybersecurity-related business interruption and recovery costs. The claim process required system logs, security controls, backup and recovery documentation, testing evidence, and detailed remediation records. Calkri provided technical evidence and participated in a formal deposition. The insurance claim was ultimately paid.

What Calkri Led

- Cybersecurity incident coordination and executive status reporting
- Network, server, and physical infrastructure redesign
- Disaster recovery, cloud failover, and business continuity planning
- Security controls, logging, backup protection, and employee training
- Documentation, insurer evidence, deposition support, and audit readiness
- Training and transition support for the local MSP
- Quarterly failover and recovery testing during normal business operations

Recovery became measurable and repeatable.

Following the incident, the insurer required semiannual security audits for seven years. The redesigned environment and documentation were maintained to support those recurring reviews while the business continued operating.

The Bottom Line

A ransomware event that shut down an entire industrial operation for roughly three days became the catalyst for a resilience program that could routinely validate recovery in about 30 minutes. Approximately six years later, the organization has not experienced another ransomware event to date despite continued attack attempts.