# You Think You're Covered. Until You're Not.

How a decade of underinvestment nearly brought down a 24/7 critical operations business, and how our team recovered it overnight.

manawa
NETWORKS

CASE STUDY

While client details have been anonymized, the situation and outcome are real.

## At a Glance

- **Sector:** Critical safety systems monitoring and professional services, with regulatory obligations around continuous uptime and operational resilience.
- **The challenge:** A critical system failure took every virtual machine offline shortly after onboarding, with unverified backups, compromised remote access, and two possible root causes, one of which risked permanent data loss on the wrong move.
- **The outcome:** Full recovery overnight with no data lost, a fully documented environment, and a clear remediation roadmap for the hardware that should have been replaced years earlier.

## The Situation

A newly onboarded client, a critical safety systems monitoring and professional services company with strict 24/7 uptime requirements, experienced a critical system failure shortly after joining Manawa Networks.

As a regulated organization supporting systems that are critical to human safety, their technology environment has to stay live around the clock, every day of the year, with no window in which downtime is ever acceptable.

What first looked like a single hardware fault turned out to be the visible edge of something far larger. The failure had surfaced years of accumulated risk that had sat entirely unseen, quietly building under a previous IT provider who had left the business dangerously exposed.

## What We Found

When our team investigated, the picture that emerged was deeply concerning:

- A **server dating back to roughly 2015,** over a decade old, was still in active use.
- The business was running the **free version of VMware,** which had been unsupported for three to four years.
- A critical RAID controller card, responsible for presenting multiple drives as a single storage volume, **had failed and taken every virtual machine offline.**
- The server firmware had **never been patched** and was still running the version shipped a decade earlier.
- **A known bug in that firmware version** could cause the card to lock up without warning.
- The installed firmware sat **several major versions behind,** at 4.02 against a current release of 7.22, pointing to years of missed updates.

**Every one of these findings traced back to the same root cause: chronic underinvestment that no one had been monitoring. The failure was predictable.**

## The Complication

Recovering a system in this state is not a simple reboot. Our team had to work through several compounding unknowns at the same time:

Remote access to the server was unresponsive. Keystrokes were freezing and sessions were dropping.

Two failure modes were possible: the controller card, or a full storage volume that would corrupt data on reboot if present.

The last known state of the backups was unverified.

The system had only recently been onboarded, so full documentation of the environment was still in progress.

This is the moment where genuine expertise earns its place. A rushed reboot could have caused permanent data loss, but our team took a disciplined, methodical approach: diagnose first, act second.

By carefully ruling out the storage-full scenario and confirming the RAID card as the root cause, we proceeded with a controlled power cycle. The system came back online, and no data was lost.

## What Happened Next

With the system restored, our team kept going. We:

Patched the server firmware to the current version.

Updated all related software components.

Documented the root cause and flagged the hardware as a critical item for planned replacement.

Logged the environment details so the same gaps could not persist undetected.

## The Underlying Message

This client believed they were in a reasonable position because their previous provider had raised no red flags. There were no warning lights until there were.

The risk existed long before we arrived. It had simply not surfaced yet. That is the most dangerous kind of risk, the kind you do not know you are carrying. Ask yourself:

- **Do you know what is running in your IT environment right now?**
- **When was it last audited?**
- **Does your current provider give you proof, not just reassurance?**

## What This Means for Your Business

Your business can carry the same kind of invisible risk. Sensitive data, operational continuity, client trust, and compliance obligations all depend on an environment that may feel sound, but has never actually been verified.

That is why Manawa helps businesses move from wondering to knowing. Instead of relying on assumptions or reassurance, you get clear evidence of what is running, what is exposed, and what needs attention.

The question worth sitting with is simple: do you know your business from the systems up, or are you only relying on the reassurance that everything is probably fine?


## Book your free Cyber Security Risk Snapshot

The fastest way to replace assumptions with evidence is to get a clear snapshot of your environment.

**Book yours today**

manawa NETWORKS

manawa.ca
8855-4-MANAWA

Manawa Networks 85 Scarsdale Road,
Suite 202 Toronto, ON M3B 2R2 Canada