

The \$100,000 Oversight

How a business invested heavily in IT resilience and left the whole thing hanging on a single \$2,000 battery backup.



manawa
NETWORKS

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

At A Glance

- **Industry:** Professional services
- **Challenge:** Redundant power backups sharing one point of failure, with no documented process to catch it
- **Outcome:** Single point of failure identified and removed, change documentation and audit checkpoints introduced
- **Timeline:** Caught during an infrastructure review, before any outage occurred

The Situation

A professional services firm had done something many businesses never get around to: they took IT resilience seriously and put real money behind it.

They'd purchased a high-specification, on-premises storage server, the kind of infrastructure that runs around \$100,000, so their data and operations could withstand disruption.

They'd also invested in redundant power backup units, uninterruptible power supplies (UPS), specifically so that if one failed, the other would keep the system online. They had two backups, belt and suspenders, so they felt covered, but they weren't.

What We Found

When Manawa reviewed the infrastructure, we identified a critical dependency that had been completely overlooked:

- Both UPS units were plugged into wall outlets on the same physical circuit breaker.
- A single power event could take out both backups at once: a surge, a tripped breaker, a lightning strike.
- The \$100,000 storage server bought for resilience was, in practice, sitting behind a single point of failure worth a fraction of that cost.

There was a secondary process risk too. When a UPS unit fails and needs replacing, the quick fix is often to move all the cables onto the remaining unit. That's reasonable as a temporary step.

But if the replacement unit goes in later and nobody documents that the cabling needs moving back, the system slips back to a single point of failure with no one aware of it.

Why This Happens

This comes down to the gap between investment and assurance. Competent people miss it all the time.

The firm made the right call to invest in resilience, and their hardware choices were sound. But resilience is a system. Every component in the chain has to hold up, including the parts that feel too basic to check.

The circuit breaker issue is the kind of detail that slips through when:



As Matt at Manawa puts it, the detail is everything. You can build something that looks completely sound and still have one overlooked component sitting underneath it, waiting.

The Business Impact

In a professional services environment, the cost of downtime is immediate and measurable. People billing by the hour can't get to the files they need. Client deadlines don't move. Trust is hard to rebuild after a failure that could have been prevented.

This was not a hypothetical risk. Had that circuit tripped, through a power surge or routine maintenance, the firm would have been offline. The very investment meant to prevent that outcome would have been rendered useless by a dependency no one had verified.

What Good Looks Like

Following Manawa's review, the firm had, for the first time, a clear picture of their actual risk profile against their assumed one. Once the issue was identified, the remediation was straightforward:

- Redistribute power connections across separate circuit breakers.
- Put a documented process in place for any change to power infrastructure.
- Establish audit checkpoints so temporary fixes are tracked and reversed.
- Build a dependency map of all critical infrastructure, reviewed on a set schedule.

The bigger shift was one of mindset. The firm could now point to evidence that its resilience held up. Assumed resilience and verified resilience are very different things.

The Questions to Ask Your Current Provider

If your IT partner manages your infrastructure, they should be able to answer these without hesitation:



Can you show us a full dependency map of our critical systems?



When were our backup systems last tested end to end, and what was the result?



Do you have a documented process for confirming that changes are correctly reversed?



What would happen to our operations if both our power backups failed at the same time?



If those questions are met with reassurance and nothing to back it up, it's worth asking harder ones.

Key Takeaways for Business Leaders

- Resilience you've paid for still needs to be verified before it counts.
- A six-figure investment can be undone by a component worth a fraction of the cost.
- Temporary fixes become permanent risks without documentation and audit checkpoints.
- Resilience lives in the whole system, including the details that look too small to matter.



Book a complimentary Cyber Risk Snapshot

See where your own dependencies and gaps sit, with no obligation. Book the cyber security risk snapshot

Book yours today



manawa.ca
855-4-MANAWA

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