RedHelm

THE BUSINESS CONTINUITY GAP: WHY DOWNTIME COSTS MORE THAN RECOVERY

Prioritize

Identify which business functions truly matter most.

Many organizations know which servers are critical but have never mapped which business processes generate revenue, serve customers, fulfill contracts, or support operations. Without understanding business priorities, recovery planning often focuses on restoring technology rather than restoring the business.

RedHelm Perspective

You don't recover systems for their own sake. You recover systems because the business depends on them.

Quantify

Understand the true impact of disruption.

Downtime costs extend far beyond IT expenses. Lost productivity, delayed revenue, customer dissatisfaction, operational bottlenecks, regulatory consequences, and reputational damage often create far greater financial impact than the technical outage itself.

Organizations that quantify downtime through a business lens make better decisions about resilience investments and recovery priorities.

RedHelm Perspective

The cost of downtime is rarely measured in minutes. It is measured in business consequences.

RedHelm

Align

Connect recovery objectives to business objectives.

Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) should not be driven solely by technical limitations. They should be driven by business tolerance for disruption.

The systems supporting critical operations may require dramatically different recovery priorities than less impactful systems

RedHelm Perspective

You don't recover systems for their own sake. You recover systems because the business depends on them.

Test

Validate whether recovery plans actually work.

Many organizations maintain disaster recovery documentation that has never been tested under realistic conditions. Recovery plans often contain outdated assumptions, undocumented dependencies, and communication gaps that only become visible during a disruption.

Testing reveals whether recovery capabilities match business expectations.

RedHelm Perspective

A recovery plan is only as good as the last time it was successfully tested.

Sustain

Build operational resilience through continuous improvement.

Business environments change. Technology changes. Threats change.

Resilient organizations continuously evaluate recovery capabilities, business dependencies, cyber risks, and operational priorities. They treat resilience as an ongoing business function rather than an annual compliance exercise.

RedHelm Perspective

The objective is not recovering from the last disruption.
The objective is being prepared for the next one.