The MSP Cyber Resilience Strategy Guide

Your-all-in-one guide to stacking cyber resilience

pax8.com

Cyber Resilience vs. Cybersecurity: What's the Difference?

For SMBs: Cyber Resilience = Survival

Cyber resilience is an organization's ability to prepare, respond to and quickly recover from a cyberattack, power outage or business disruption. If cybersecurity is the fortified wall that keeps threats out, cyber resilience is the battle plan, blueprint and survival strategy to keep operations going.

For MSPs: Cyber Resilience = The Value You Provide

Continuity turns MSPs into trustworthy advisors driving revenue, loyalty and long-term growth. Cyber resilience is your proactive client protection plan. It's the ongoing strategy you deliver as a reliable partner to ensure your clients' continuity (business recovery), no matter the threat.

Continuity: The Backbone of Cyber Resilience

Continuity is the foundation of cyber resilience. It ensures that a business doesn't stop and can recover when attacks or data-compromising incidents happen.

Example scenario:

A busy café working a Monday morning rush is suddenly hit with ransomware. Typically, the café would have to stop taking orders, but with their continuity plan, backups restored the system within the hour and staff switched to offline payments. Sales and orders continued, operations were back to normal by lunchtime and the business didn't pay the ransom. This business has strong cyber resilience.

Continuity keeps business running when the unexpected hits and strengthens your adaptability against cyber incidents.

The Core Elements of Continuity

Backup:
The Foundation

Copies of your data are stored safely to ensure nothing is ever lost. In the event of an incident, this is your primary key to recovery.

Business Continuity (BC):
The Plan for Operations

BC ensures your business can continue operations **DURING** and immediately after a disaster. The goal is to minimize downtime and keep revenue flowing.

Disaster Recovery (DR):
The Restoration Strategy

A DR plan is the roadmap to getting all systems, applications and data back online **AFTER** a major incident has occurred.

Four Key Threats Continuity Protects Against

Ransomware: Resolute, tested backups ensure recovery without paying.

4x

SMBs are targeted **four times more** than large organizations.[1]

Human error: Accidental deletion or overwrites are the top causes of data loss.

26%

Human error accounts for 26% of all corporate breaches.[2]

Outages and disasters: Power failures, storms, server or hardware crashes.

100%

of surveyed cyber professionals at 1000+ employee firms reported $10K-$1M in annual outage losses. [3]

Business incidents: From unauthorized access to insider threats.

47%

47% of cyber professionals claim credential abuse and unauthorized access are top insider threat concerns.[4]

BC/DR is your safety net: Keep running during a crisis and recover systems afterward.

How to Implement a Strong Continuity Plan

Cyber-resilient businesses are built, not born. Lead clients to success with a continuity action plan.

1. Regularly audit and test your backups (cloud and offsite).
2. Segment backups to keep cyberthreats from infecting recovery copies.
3. Establish clear Recovery Point Objective (RPO) and Recovery Time Objective (RTO) goals to limit data loss and recovery time.
4. Test the recovery plan with disaster and recovery drills.
5. Document the BC/DR plan, ensuring it is accessible to all responsible for implementing it.
6. Train employees to recognize and avoid cyberthreats.
7. Explore adaptive continuity models that grow with your business.

The MSP Cyber Resilience Strategy Guide

Business Continuity Checklist

Stay prepared, not surprised. Use this business continuity checklist to sharpen your recovery strategy and strengthen your cyber resilience.

Responsible Party: Department: Location:

Contacts and Communication

- [ ] Identify key internal and external contacts
- [ ] Share emergency contacts and vendor lists with the team
- [ ] Create an emergency communication plan (phone/text chain)
- [ ] Test communication plan annually

Essential Functions and Recovery

- [ ] Define and prioritize essential functions
- [ ] Perform business impact analysis per function
- [ ] Develop recovery steps per function

Resources and Equipment

- [ ] Create equipment, supplies and sensitive items list
- [ ] Verify critical equipment on backup/ emergency power
- [ ] Plan for utility loss (power, water, internet)

Data and Documentation

- [ ] Backup vital documents and files (digital and physical)
- [ ] Secure offsite/duplicate storage for key records
- [ ] Identify peer/collaborator support networks

Relocation and Remote Work

- [ ] Identify alternate site requirements and options
- [ ] Ensure staff have remote work tools and secure access

Plan Maintenance

- [ ] Review and update plan annually
- [ ] Record lessons learned from test simulations and incidents
- [ ] Train employees on continuity procedures
- [ ] Test and exercise the plan regularly

Checklist Source: UW Lab

Build Unstoppable Cyber Resilience with Pax8

At Pax8, we transform your business into a force for continuity. Our Marketplace delivers the expertise, support and scalable security solutions you need to stay resilient, recover quickly and keep business moving no matter what.

Protect your continuity. Strengthen your resilience. Start your journey here.

Safeguarding Tomorrow's Business Today

Schedule a continuity consultation

Sources

1. 2025 Verizon Data Breach Investigations
2. AI Oversight/IBM 2025 Cost of a Data Breach Report
3. The State of Resilience 2025 Report
4. 2024 Insider Threat Report
5. UW Lab Guide to Business Continuity and Recovery Planning