BITSTC TRAINING & CONSULTING

Leading Through Disruption

An executive guide to preparing, responding, recovering, and protecting stakeholder trust.

Resilience is the ability to continue critical operations and recover with confidence - even when assumptions fail.

Five questions every leadership team should answer

01	**What must continue?** Name the products, services, public functions, and obligations that cannot be paused without serious impact.
02	**How long can each critical service be unavailable?** Agree on tolerances before an incident makes the tradeoffs urgent.
03	**What does each service depend on?** Map people, facilities, technology, data, suppliers, utilities, and decision makers.
04	**Who can make high-consequence decisions?** Define authority, alternates, escalation, and communication responsibilities.
05	**How do we know recovery will work?** Test end to end, including leadership decisions, customer communications, and operational workarounds.

Resilience is broader than cybersecurity

Cybersecurity remains a core capability, but leaders must also prepare for technology failure, severe weather, utility interruption, supplier failure, facility loss, workforce disruption, and other business interruptions. A resilient operating model connects cyber response with continuity, recovery, crisis leadership, governance, and communications.

The executive resilience operating model

Capability	Executive question	Evidence of readiness
Governance	Who owns resilience and reports progress?	Named accountable executive, charter, metrics, board cadence
Business impact	What must recover first?	Current critical services, tolerances, dependencies, priorities
Continuity	How will operations continue?	Usable strategies, playbooks, alternates, communications
Disaster recovery	How will technology recover?	Business-aligned RTO/RPO, procedures, protected backups, tests
Crisis leadership	How will decisions be made?	Decision authority, escalation, scenario rehearsals, after-action work
Cyber resilience	How will a cyber event affect operations?	Integrated incident, continuity, communications, and recovery plans

A practical 90-day agenda

01 **Days 1-30:** Confirm executive ownership, scope critical services, gather plans, and identify immediate single points of failure.

02 **Days 31-60:** Validate impact, dependencies, recovery objectives, communications, and decision authority with accountable leaders.

03 **Days 61-90:** Facilitate an executive tabletop, publish the improvement roadmap, assign owners, and establish a board reporting cadence.

During disruption: the executive decision lens

- ✓ Protect life, safety, public trust, and legal or regulatory obligations.
- ✓ Stabilize the critical services with the greatest immediate impact.
- ✓ Separate confirmed facts, working assumptions, and unknowns.
- ✓ Make time-bound decisions with named owners and clear review points.
- ✓ Coordinate operational, technology, cyber, legal, communications, and vendor workstreams.
- ✓ Preserve evidence and a decision log for after-action learning.

Board-level signals to monitor

- ✓ Percentage of critical services with current impact analysis and continuity strategies
- ✓ Percentage of critical technology with tested recovery capability meeting business objectives
- ✓ Age and completion rate of high-priority exercise and incident findings
- ✓ Concentration of critical third-party, data, workforce, facility, or utility dependencies
- ✓ Frequency and maturity of executive and cross-functional exercises

BITSTC helps executive teams connect business continuity, disaster recovery, cyber resilience, crisis management, and governance. Start a conversation at Claude@bitstc.com.