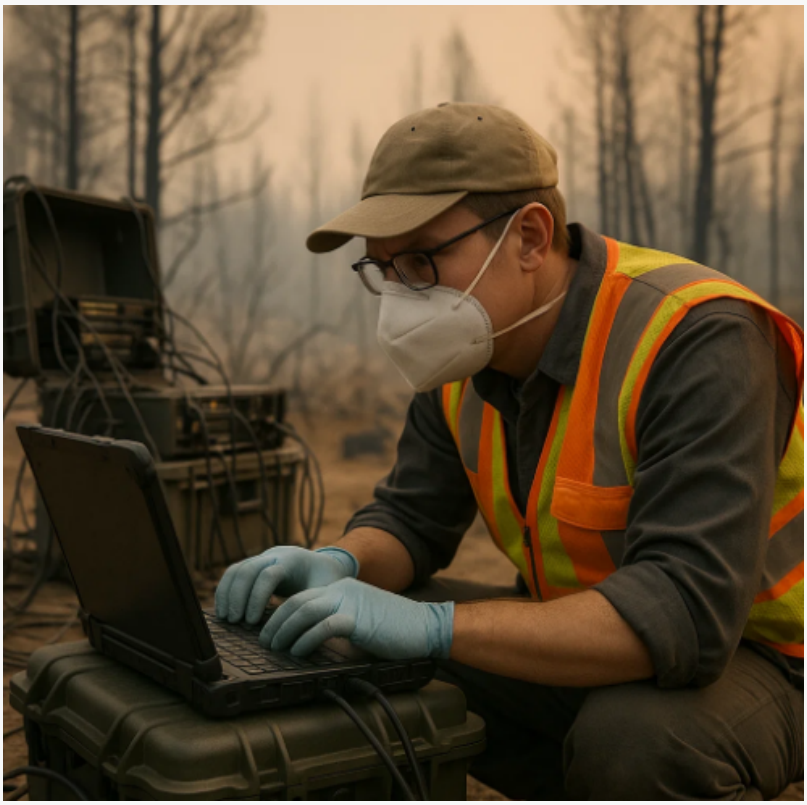
Proactive IT Planning Is Now Essential for Business Continuity in High-Risk Regions, Experts Say

New insights from Los Angeles-based cybersecurity professionals underscore the rising need for integrated disaster readiness and IT resilience.



On-Site Technical Support During Wildfire Season

LOS ANGELES, CA, UNITED STATES, July 8, 2025 /EINPresswire.com/ -- As climate-driven emergencies and cyber incidents increase in frequency and intensity, IT and business leaders are being urged to reevaluate how their organizations approach continuity planning. From natural disasters like wildfires to the growing threat of ransomware, the reality is clear: operational downtime is no longer a rare event—it's an inevitability.

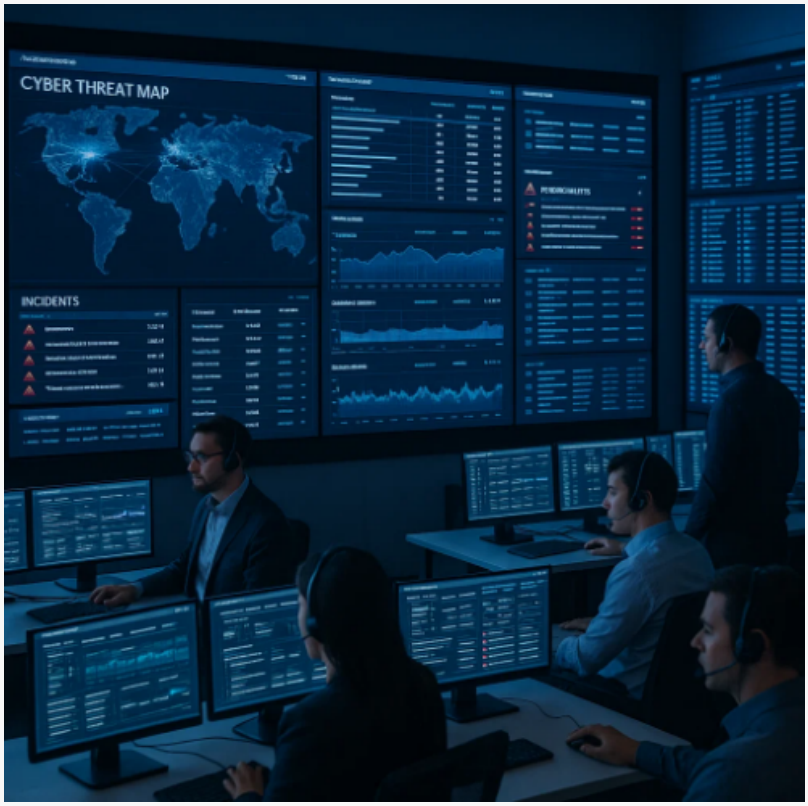
Recent wildfire activity in Ventura and northwest Los Angeles County burned over 6,000 acres in June, disrupting transportation, forcing evacuations, and threatening businesses across multiple sectors. Simultaneously, ransomware attacks targeting Southern California healthcare networks led to significant care delays and system outages, highlighting a critical gap in organizational preparedness.

“We're entering an era where simultaneous threats—climate and cyber—can compound risk and overwhelm systems,” said Michael Cunanan, CISO and CISSP-certified Cyber Security Officer at Global IT. “The ability to continue operations through these disruptions now depends on how integrated and proactive your IT posture is.”

Key Strategies for Business Continuity in 2025 and Beyond

IT experts and cybersecurity professionals recommend organizations—particularly small to midsize enterprises—consider the following steps to ensure continuity:

Develop a disaster-aware infrastructure: Include redundancies for power, data, and connectivity. This could mean off-site backups, remote-ready systems, and multi-location data replication.



Network Operations Center in Action

Establish clear response protocols: Assign roles and rehearse scenarios. “Many organizations have disaster recovery plans, but no one knows where they are or how to execute them under stress,” noted Judah Leon, Project Manager.

Embed cybersecurity into continuity planning: With L.A. County reporting a 40% spike in cyber intrusions in 2025 alone, reactive security is no longer sufficient. Organizations should implement layered defenses, regular audits, and endpoint monitoring that integrates with their business continuity playbooks.

> We were facing an evacuation with no clear plan for how to keep our systems running remotely. This IT team showed up with solutions, not excuses. They were already ten steps ahead.”
>
> *A technology leader impacted by wildfire evacuations*

“Ransomware doesn't just lock data—it halts entire operations,” said Cunanan. “Your cybersecurity plan must assume you’ll be targeted and should be tested under pressure.”

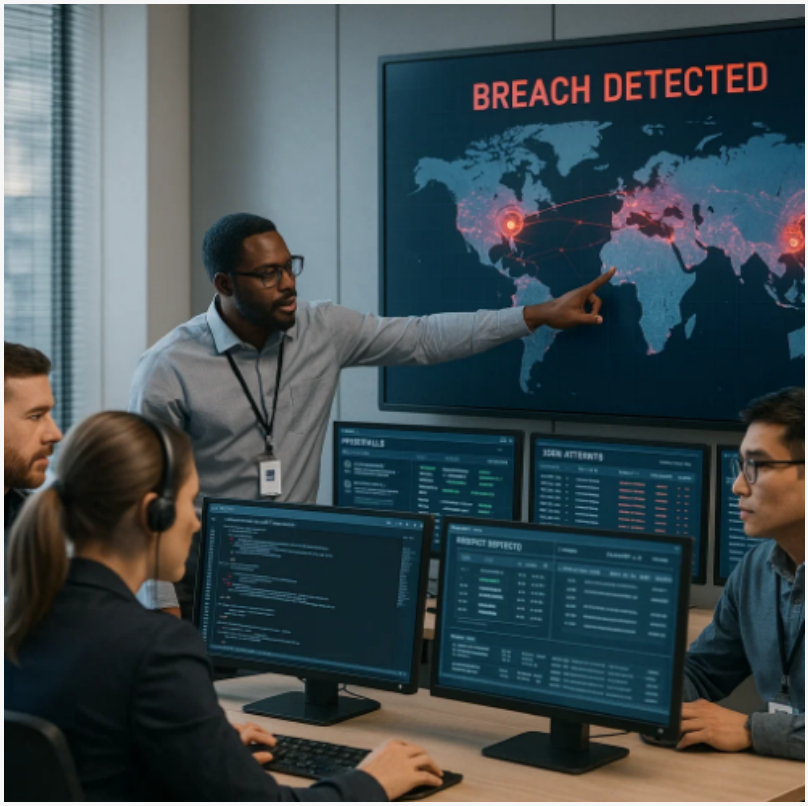
Partner with vendors who provide presence, not just platforms: While many IT service providers focus on tools, businesses increasingly need partners who can act quickly during emergencies.

Learning from Recent Events in California

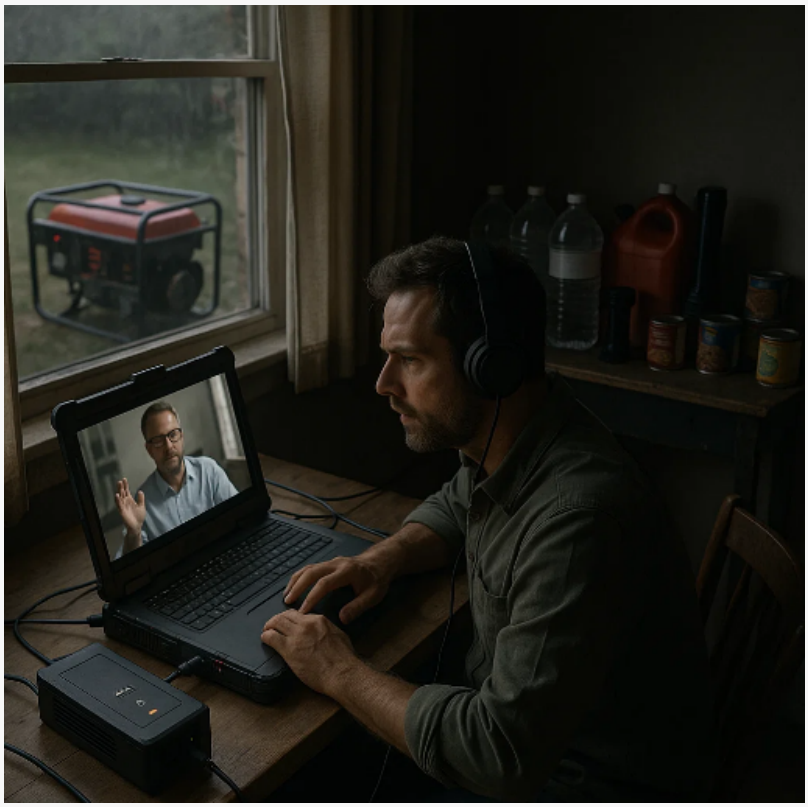
During the recent fire season, several firms in the Los Angeles area were forced to evacuate facilities with little notice. Those that had emergency-ready IT vendors in place were able to pivot quickly—transitioning to remote operations, relocating hardware, and activating backup systems with minimal disruption.

Similarly, businesses affected by cyberattacks saw significantly different recovery times depending on whether their MSP (Managed Services Provider) had 24/7 response capabilities and access to pre-isolated backup environments.

“A surprising number of organizations still rely on single-point-of-failure infrastructure,” said Vanessa Barragan, Communications Operations Manager at Global IT. “What’s needed is a more resilient design, not just faster helpdesk responses.”



Cybersecurity Team at Work

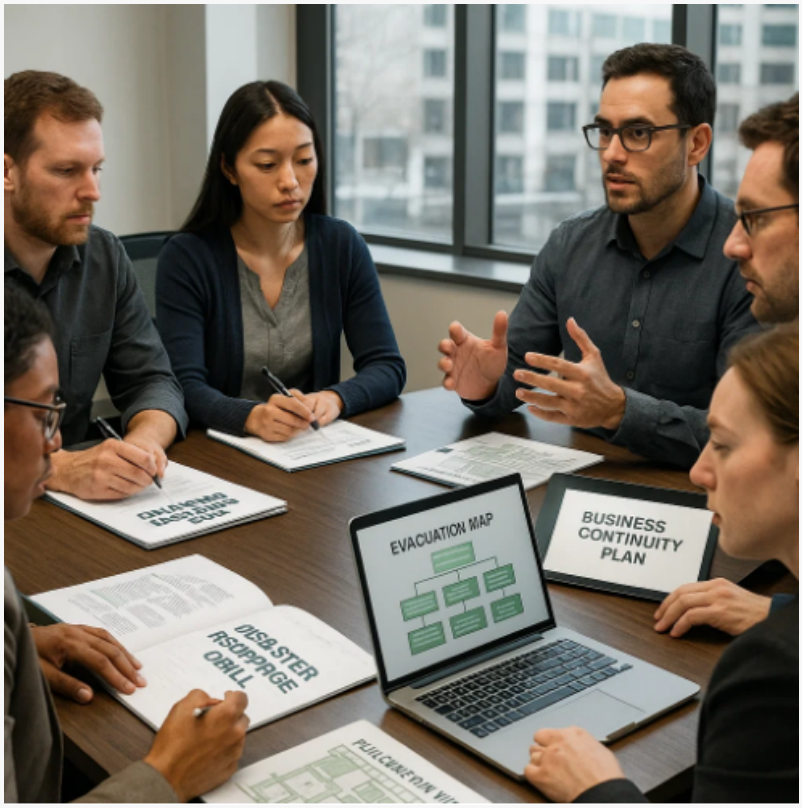

Client in Remote Work Setup During Emergency

The Cost of Downtime—and the Value of Preparation

According to IBM’s 2024 Cost of a Data Breach report, the average breach in the U.S. now costs $9.44 million—with recovery timeframes averaging 24 days. For small and midsize businesses, even one day of downtime can jeopardize contracts, compliance, or survival.

Yet many organizations underinvest in continuity planning or view IT support as a utility rather than a strategic asset.

“Continuity isn’t just a checkbox for compliance—it’s a living, tested process,” said Anthony Williams Rare, CEO of Global IT. “Whether it’s a wildfire, a power outage, or a zero-day exploit, the question is: can you operate tomorrow if everything goes wrong today?”



Disaster Readiness Drill or Planning Session

Final Recommendations

For business leaders looking to strengthen their resilience strategies, experts suggest:

Reviewing and updating continuity plans every 6–12 months

Conducting quarterly cybersecurity penetration testing

Establishing SLAs with vendors that explicitly cover crisis response

Building internal awareness through tabletop exercises and cross-department drills

The ultimate goal: to move from reactive IT troubleshooting to proactive, integrated resilience—where technology, people, and process work in sync to protect operations from the unexpected.

About Global IT

Global IT is a Managed Services Provider based in Los Angeles, specializing in cybersecurity, infrastructure, and business continuity solutions for small and midsize organizations. With a focus on proactive service and disaster readiness, Global IT supports nonprofits, healthcare providers, law firms, and professional services organizations across California and beyond.

Website: www.globalit.com
Address: 5150 Wilshire Blvd, Suite 400, Los Angeles, CA 90036

Media Contact
Thomas Bang
Director of Marketing and Alliances
Global IT
press@globalit.com
(213) 403-0111
globalit.com/services/managed-it-msp-los-angeles

Thomas Bang
Global IT Communications, Inc
+1 213-403-0111
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X
Other
