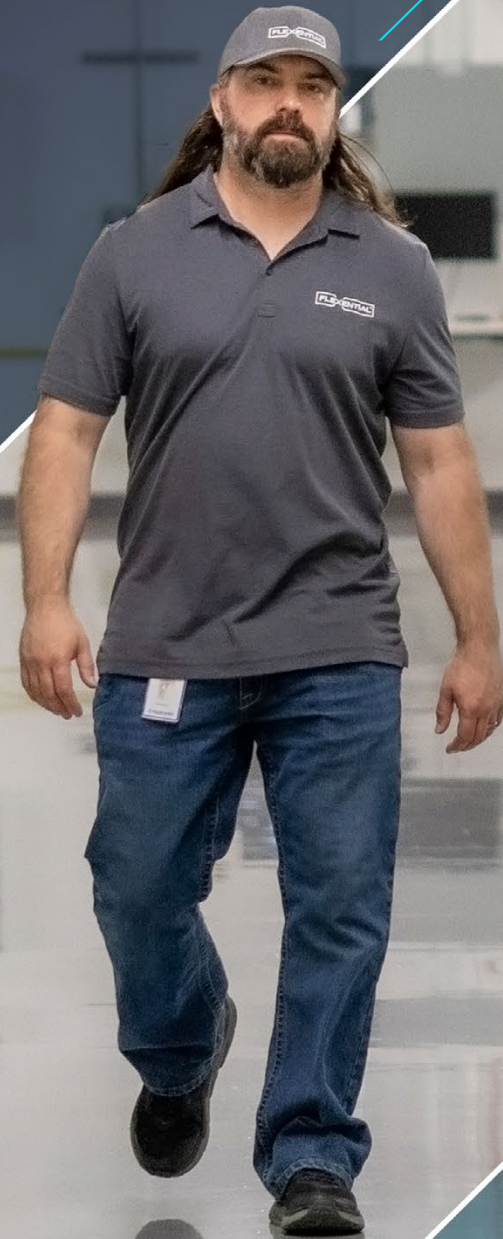




Mastering disaster preparedness

Real-world insights on disaster recovery and business continuity



Introduction

Every organization faces unexpected disruptions, whether severe weather, cyberattacks, or local incidents that no one saw coming. Being prepared is not just about having backups or a checklist. True disaster preparedness means knowing your risks, having a clear plan, and making sure everyone is ready to act when it matters most.

In this guide, you will find practical lessons and firsthand experiences about the frameworks and strategies organizations use to identify risks, document contingency plans, and build real resilience. Whether you are updating your current approach or building a new one from scratch, these pages will help you prepare for what's next and respond with confidence when disaster strikes.

“When we talk about risk and resilience and disaster preparedness, where do we really start? We start with this planning phase, really looking at what our risks are, what are the disasters we're looking at, and there's different considerations in there, identifying those risks, those possible disasters, how widespread they are, what the impacts are.”

– Michael Fitzgerald, Flexential

Who's behind these insights?

This guide is based on a conversation between **Michael Fitzgerald**, Senior Director of Engineering, Professional Services at Flexential, and **Julie Hattel**, Director of Enterprise Risk and Resilience at Flexential. Together, they help organizations build practical strategies for disaster recovery, business continuity, and true resilience.



What disaster preparedness really means

Disaster preparedness is more than a checklist or a one-time exercise. It is an ongoing process that begins with identifying risks and understanding what events could disrupt your operations. As Michael Fitzgerald and Julie Haddel discussed, this includes everything from major weather events and cyberattacks to local incidents like hazardous material spills or infrastructure outages.

It is important to look beyond just the obvious threats. While hurricanes, floods, and storms are common concerns, organizations also need to plan for less predictable events such as ransomware attacks or unexpected disruptions to key services and locations. The real focus is not only on what could happen, but on how these incidents might affect your people, your places of business, your critical platforms, your third-party providers, and your essential processes.

A comprehensive approach also means understanding the difference between disaster recovery (DR) and business continuity (BC).

Disaster recovery is about restoring your technology and infrastructure, while business continuity addresses the bigger picture, making sure your people, processes, and operations can keep moving forward. Both are closely connected and essential for true resilience.

Preparedness starts with asking the right questions and looking at your risks from every angle. With a clear framework and commitment to ongoing evaluation, your organization can be ready for whatever comes next.

Disaster preparedness is about more than planning for a specific event. It is about knowing the impacts, asking what would happen if your people, places, platforms, providers, or processes were disrupted, and having a practical plan for each.



Identifying your biggest risks:

The Five Ps framework

A practical approach to disaster preparedness starts with understanding where your organization is most vulnerable. During the webinar, the Five Ps framework was introduced as a guide for identifying and assessing risks:

PEOPLE

Who is essential to your operation, and what happens if key team members are unavailable?

PLACES

What locations, offices, or data centers could be impacted by an event?

PLATFORMS

Which systems, applications, or technologies are critical for day-to-day business?

PROVIDERS

What third-party vendors or service providers do you depend on, and how resilient are they?

PROCESSES

What procedures or workflows keep your business running, and how would you restore them if disrupted?

This framework helps organizations look beyond the obvious threats and ask the right questions about the full range of potential impacts. For example, planning for hurricane season might include relocating people, preparing alternate workspaces, and securing backup power sources. But it is just as important to consider other scenarios, like a ransomware attack that takes down critical platforms or a local incident that blocks access to your main office.

Using the Five Ps, you can map out where your weak spots are, prioritize which risks need immediate attention, and start to create a clear, actionable recovery plan.

“

By considering the Five Ps—**people, places, platforms, providers, and processes**—you can identify your most important assets and be ready for a wide range of scenarios, even the ones you never expected.”

Planning for reality, not perfection

Disaster preparedness is not about trying to predict every possible event. It's about understanding how different scenarios could affect your business and having practical, written plans you can rely on when the unexpected happens. As Julie and Michael emphasized, documenting your contingency plans is one of the most important steps you can take. Putting your strategy in writing helps you think clearly in calm moments and provides a trusted guide when stress levels are high.

A good contingency plan spells out exactly what needs to be done, who is responsible, and what resources are required. Even simple plans, like making sure everyone knows where to meet during a building evacuation or having up-to-date contact lists, can make a major difference. Real-world events often reveal gaps no one anticipated, which is why learning from experience is crucial. After every incident—big or small—take the time to review what worked, what did not, and how your plan can be improved.

Disaster preparedness is not a one-and-done effort. Plans should be revisited and updated regularly as your organization grows, technology changes, or new risks emerge. This ongoing process is the key to building true resilience.

Real-world example: When plans meet reality

After a major storm closed roads and airports, a company's trained disaster recovery staff were unable to reach their DR site. The only option was to send someone from a remote office—someone who wasn't trained for the recovery plan. This stressful situation highlighted a gap no one had considered: the need to prepare and train backup staff in multiple locations.

THE LESSON?

Even the best plans need regular testing and updates to ensure your team is truly ready when disaster strikes.



Build resilience through testing and continual improvement

Every organization faces unexpected challenges, but with the right preparation, you can turn disruption into an opportunity to build confidence and resilience. By focusing on clear planning, practical frameworks like the Five Ps, and regular testing, your team will be ready to respond to whatever comes next. Remember, disaster preparedness is not a one-time project. It's a continuous process of learning, adapting, and improving together.

Get a closer look at strategies that work, lessons learned from the field, and answers to the questions IT leaders face every day.

Watch the Webinar



[Reach out to our team](#) for guidance, resources, or just a conversation about your disaster preparedness goals.

We're here to help you stay ready!

Looking for more resources?

Ask about our disaster recovery checklists, NIST-based frameworks, or see how real organizations are strengthening their plans with the help of Flexential.

