



Ready Before It Happens

+ The First 72 Hours of Small Business Survival

Created by the **NYSBDC** for National Preparedness Month with

Mike Semel

President & Complianceologist, Semel Consulting

RESOURCE INFORMATION

Contents

The contents of the following document were created collaboratively through human and ChatGPT input. The NYSBDC sincerely thanks Business Continuity Expert and Complianceologist Mike Semel for the *Ready Before It Happens* recommendations he contributed to this free educational resource. *The First 72 Hours of Small Business Survival* section is based on guidance from the U.S. Small Business Administration, Ready.gov/FEMA, OSHA, and the Internal Revenue Service. (See the *Sources & Expert Contributions* section at the end of this document for more information.) The contents of this document were current as of September 2026.

Framework

The 0–24, 24–48, and 48–72 hour groupings are an educational planning framework developed for this resource, not a universal federal response timeline. Actual actions and timing should reflect official instructions, safety conditions, insurance requirements, program eligibility, and a business's unique circumstances.

Disclaimer

Funded in part through a Cooperative Agreement with the U.S. Small Business Administration. All opinions, conclusions, and/or recommendations expressed herein are those of the creators and do not necessarily reflect the views of the SBA or the SBDC. Full funding disclosures are available at <https://nysbdc.org/funding-disclosures>.

READY BEFORE IT HAPPENS

Expert Business Continuity Recommendations Provided by Mike Semel



Mike Semel is recognized as a thought leader in the IT, compliance and business continuity industries. He is the President and Complianceologist at Semel Consulting, focused on regulatory compliance and Business Continuity planning. Mike is a CMMC Certified Assessor (CCA), CMMC Certified

Professional (CCP), CMMC Registered Practitioner (RP), Certified Security Compliance Specialist, ISC2 Certified Governance Risk Compliance, Disaster Recovery Institute Certified Business Continuity Professional & Certified Cyber Resilience Professional, Certified HIPAA Security Professional, and Certified Health IT Specialist. He has owned or managed MSP companies for over 30 years; served as Chief Information Officer (CIO) for a hospital and a K-12 school district; and managed operations at an online backup company. Mike is the only expert who consulted with CompTIA on the original Security Trustmark (2008), the Security Trustmark Plus (2014), and the Cybersecurity Trustmark (2023). He is the best-selling author of *How to Avoid HIPAA Headaches*. If you'd like to get in touch with Mike, [you can email him here](#).



“Address things you don’t want to even think about. I have seen each of these bring businesses down.”



- Death or disability of the owner
- Death or disability of a key employee
- A cancer diagnosis with an extended treatment plan
- Divorce
- Embezzlement or data theft by a trusted employee
- Extended leave by an owner or employee to deal with a family situation
- Loss of a facility
- Extended loss of computers/programs/cloud services
- Ransomware/data theft extortion
- Wills and other estate documents not being current



“Don’t use general theories when planning. I break things down into disruptions, disasters, and Disasters.”



We see real examples of situations every day. Use the news and real stories and consider ‘what if that happened to me?’

- **Disruptions** – temporary business interruptions due to illness, injury, power outages, Internet outages, phone service outages, cloud service outages – even though temporary, these may have big consequences if you miss critical deadlines.
- **disasters** (lower-case d) – These are bigger or longer-term interruptions that only affect your business or your neighborhood. They may be caused by fires, water damage, mistakes, accidents, and employee issues. They are serious, but things you must deal with yourself. These situations often result in temporary sympathy from customers and vendors, but the longer they go on, the more likely you are to lose trust with your customers.
- **Disasters** – the big ones that make the news. You will need outside resources, at first for personal life and safety, and later on for assistance recovering.



“Review your insurance policies and planning resources.”



- **Review your insurance policies** - property and casualty, flood, professional liability, cyber, and auto – to make sure each policy has enough coverage to pay for an incident. As my insurance agent likes to say, “A million dollars used to sound like a lot of money...”
- **Establish relationships** you will need if you have an incident.
- **FEMA (ready.gov) has great resources,**
- Here are some additional considerations.
 - Identify an **employment agency** familiar with your industry that can help you quickly replace a key employee. This is especially important if your employees require licenses, certifications, or special training.
 - **Cybersecurity** is more complex than ever and requires special tools and a certified expert to effectively protect systems, identify and investigate questionable activity, and respond to incidents. Most small IT providers and internal IT technicians do not have the ability to effectively respond to incidents. When possible, prepare by working with a professional cybersecurity service.
 - You might have the best attorney and cybersecurity vendor, but your insurance may not pay for their services after an incident. **Get your specialists pre-approved** by your insurance provider.



“Test your plan.”



An untested plan is words on paper. You don't need to perform elaborate exercises, but you can:

- Have a **tabletop exercise** with your team and your alternate business leader (family member, attorney, accountant, etc.) so they don't meet each other while stressed from an emergency.
- Make sure your alternate business leaders can **access** your bank account and pay bills.
- **Use your written plan** for the exercise. It may show you that contact information is no longer current.
- Test your plan at least **annually**. Things change. Make sure your plan is updated.

“Identify resources likely to be available to manage your business without you.”



- If you select a **family member**, also select an **outside resource** who may not be affected by the same situation as family.
- Work with your accountant and attorney to draft binding **legal documents** that will work with banks, lenders, courts, etc.
- Add **alternate authorized signatures** to your bank account and make sure that the paperwork is in place for your bank to allow your alternate resource to pay bills and employees.
- If you die, credit cards will be frozen. Ensure **alternate vendor payment methods** to keep your business going if cards are frozen.
- Understand what situations will **freeze** loans/lines of credit and result in **immediate payment demands**.

“Expect that your critical systems will fail.”



Most businesses are now Internet dependent for everything from sales and purchases to HR and operations.

- Have **two Internet services** with automatic fail-over if your primary service fails. Purchase a MiFi Internet device that can replace your main Internet service if needed. If that is cost-prohibitive, make plans to use **your phone's hotspot feature**. Test your alternate connection to make sure your systems will work.
- Create **paper forms** that copy what is on computer screens so you can write information and then input it when systems are restored.

“Create a written plan, keep it updated, share it with trusted advisors, and make sure it will be available when needed.”



- You won't believe how difficult it is to remember even basic things when you are under extreme stress. In your plan, list **phone numbers** because you may not be able to access your mobile device or computers. Verify the phone numbers for your insurance agent, attorney, accountant, alternate business leader, and family members.
- **Periodically review** your plan and make **updates** as needed.
- Don't expect your phone, computers, or facility to be accessible. **Print your plan** and store it securely in multiple locations. You don't know which location may be inaccessible.
- Store **passwords, sensitive account access information, and key business documents** separate from your plan in sealed envelopes that only your alternate business leader and attorney know about. Make sure you remember to **update** these when PIN numbers of passwords change.

THE FIRST 72 HOURS OF SMALL BUSINESS SURVIVAL

The first 72 hours after a disaster can be chaotic. You may have a 72-hour kit to take care of yourself during that time. Your small business needs critical care then, too. This guide will take you through smart action suggestions to stabilize the four lifelines of your small business: your **people**, your **operations**, your **money**, and your **records**.



People



Operations



Money



Records



People

*Is everyone safe,
informed, and able to act?*

Prepare Now

- Identify a primary and alternate **decision-maker**.
- Maintain employee and emergency **contact information**.
- Assign **response** and **communication responsibilities**.
- Establish employee **accountability procedures**.
- Decide how staff will receive **instructions** if normal systems are unavailable.

0-24 Hours

- Protect **life** and follow emergency instructions.
- Account for **employees**.
- Activate the **decision-making structure**.
- Tell employees whether to **report, relocate, work remotely, or remain off-site**.
- Establish a **schedule for updates**.

24-48 Hours

- Confirm employee **availability**.
- Reassign **essential responsibilities**.
- Address immediate **staffing needs**.
- Communicate **available support** and **work expectations**.

48-72 Hours

- Establish a temporary **staffing plan**.
- Confirm **who will manage** the next phase of recovery.
- Update employees on **operating status, schedules, and priorities**.



Operations

What must resume first?

Prepare Now

- Identify the business's three most **critical functions**.
- Determine maximum **tolerable downtime** for each.
- Establish **backups** for facilities, technology, utilities, equipment, and suppliers.
- Prepare customer and vendor **communication templates**.
- Test **alternate operating arrangements**.

0-24 Hours

- Assess the **disruption** without placing people at risk.
- Determine which **operations must stop**.
- Activate the **continuity plan**.
- Notify **priority customers** and **vendors**.
- Protect **critical equipment, data, and inventory** when it is safe to do so.

24-48 Hours

- Resume **minimum viable operations**.
- Shift to an **alternate site, remote work, or a backup supplier**.
- Prioritize **essential customers, products, or services**.
- Communicate revised **hours, availability, and delivery expectations**.

48-72 Hours

- Evaluate **operating capacity**.
- Address supply or staffing **gaps**.
- Set **priorities** for the next seven days.
- Establish a regular customer and vendor **update schedule**.



Money

Can the business meet its essential obligations?

Prepare Now

- Estimate the **cost of one day** of interrupted operations.
- Identify **essential expenses**.
- Review **insurance coverage** with an appropriate professional.
- Establish secure **off-site banking access**.
- Identify **emergency reserves** or **available credit**.
- Understand the general categories of **SBA disaster assistance**.

0-24 Hours

- Begin tracking **disaster-related expenses**.
- Notify the **insurer** when appropriate.
- Protect **banking** and **payment systems**.
- Identify **payroll** and **payments** due immediately.
- Avoid making **financial decisions** based on unverified assistance information.

24-48 Hours

- Prepare a short-term **cash-flow estimate**.
- Contact the **bank, accountant, insurer, landlord, lender, and critical vendors**.
- Separate **essential payments** from expenses that may be deferred.
- Monitor **official sources** for available assistance.

48-72 Hours

- Estimate the **financial effect** of continued interruption.
- Confirm **insurance claim requirements**.
- Review official **SBA disaster-assistance information** if applicable.
- Organize the **financial information** needed for recovery decisions.
- Create a seven- or thirty-day **cash-management plan**.



Records

Can you prove what happened and pursue recovery assistance?

Prepare Now

- Back up **tax returns** and **financial statements**.
- Maintain an **inventory** of equipment, property, and stock.
- Photograph important **assets**.
- Secure **insurance policies, leases, licenses, contracts, and payroll records**.
- Make records **accessible** to more than one authorized person.
- Assign people to **document damage** and **track disaster-related expenses**.

0-24 Hours

- Photograph or record **damage** when it is safe.
- Preserve relevant **property** and **evidence** consistent with official and insurer instructions.
- Begin an **incident log**.
- Record **emergency purchases** and **response expenses**.
- Note when operations **stopped** or were **reduced**.

24-48 Hours

- Organize **photographs, receipts, estimates, and correspondence**.
- Document **canceled orders, lost sales, closures, and reduced operating capacity**.
- Obtain **claim** or **incident numbers**.
- Create **one secure location** for all recovery records.

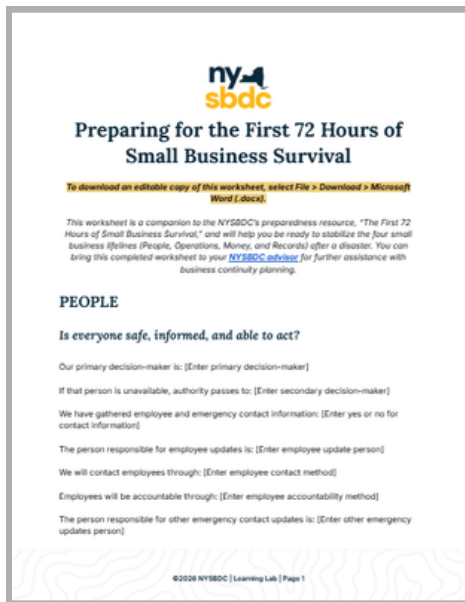
48-72 Hours

- Compare collected records with current **insurer** or **assistance requirements**.
- Identify **missing documents**.
- Prepare **questions** for insurer, SBA, accountant, and/or SBDC advisor.

Don't wait! Take action today!

Congratulations! You've begun preparing your business to face the disaster by going through this resource. Here are more simple steps you can take today

Complete the Companion Worksheet



[Click here to access the companion worksheet for this resource, "Preparing for the First 72 Hours of Small Business Survival."](#) This worksheet will allow you to answer critical questions and gather key information to stabilize your small business during the first 72 hours after a disaster. All four business lifelines (people, operations, money, and records) are covered.

Get Help from an NYSBDC Advisor

For free assistance as you delve deeper into business continuity planning, [contact your local NYSBDC center to schedule an appointment with an advisor.](#)

Access More Free Resources

Don't forget to check out the excellent free resources from several government organizations listed on our **Sources page!**

SOURCES & EXPERT CONTRIBUTIONS

- Business continuity planning. Ready.gov, Federal Emergency Management Agency, U.S. Department of Homeland Security. Not dated.
- Business Resilience Guide: Reducing Risks and Building on Strengths. Office of Disaster Recovery and Resilience, U.S. Small Business Administration. 2025.
- Crisis communications plans. Ready.gov, Federal Emergency Management Agency, U.S. Department of Homeland Security. Not dated.
- Disaster recovery. U.S. Small Business Administration. Not dated.
- Emergency action plans, 29 C.F.R. § 1910.38. Occupational Safety and Health Administration, U.S. Department of Labor. Not dated.
- How to document damages after severe weather events. Federal Emergency Management Agency, U.S. Department of Homeland Security. 2025.
- IRS urges emergency preparedness ahead of peak disaster season. Internal Revenue Service, U.S. Department of the Treasury. September 4, 2025.
- Preparing for a disaster: Taxpayers and businesses. Internal Revenue Service, U.S. Department of the Treasury. Not dated.
- Ready Before It Happens business continuity guidance. Mike Semel, Semel Consulting. Expert contribution provided by email. September 27, 2026.
- SBA Form 5: Disaster Business Loan Application. U.S. Small Business Administration. OMB Control No. 3245-0017. 2023

AI Assistance: The contents of this resource were developed with assistance from ChatGPT (an AI tool from OpenAI) for research synthesis, organization, and drafting. NYSBDC staff reviewed and edited the final product, as well as created the design of the document.

ADVISE. EDUCATE. RESEARCH.



Funded in part through a Cooperative Agreement with the U.S. Small Business Administration. Full funding disclosures are available at <https://nysbdc.org/funding-disclosures/>.