Building a Resilient Business Strategy

Learn how to set your business up for success in a competitive and fast-paced environment.

IRONEDGE®

The Challenge of Business Longevity

Starting a business is hard and takes passion, vision, and determination. But building a business that lasts? That's much harder.

According to the U.S. Bureau of Labor Statistics (BLS),[1] approximately **23% of new businesses fail within the first year of being open**, 48% during the first five years, and 65% during the first 10 years. Only 25% of new businesses make it to 15 years or more. These statistics haven't changed much over time, and have been fairly consistent since the 1990s.[2]

23%

23% of companies fail within their first year of business.

75%

75% of startups won't stay in business for at least 15 years.

Companies don't stay in business for a multitude of reasons, often stemming from fundamental weaknesses in their operational and strategic foundations.

One common pitfall is a failure to adequately identify and address market needs, leading to products or services that don't resonate with consumers. Businesses may also have trouble attracting customers if they don't have an established visible presence, are located in unfavorable areas, or don't understand their audience.

On the flip side, unsustainable expansion efforts, such as rapid scaling without sufficient resources or infrastructure, can lead to overextension and eventual collapse. Poor planning, cash flow issues, and ineffective strategies can exacerbate this issue, leaving businesses without a clear path to success.

Struggling to respond to unexpected challenges, disasters, or market changes can render businesses obsolete in today's fast-paced environment. Recognizing and addressing these potential pitfalls is crucial for businesses seeking long-term viability and success.

Top Reasons Businesses Fail[3]

- Lacking a market
- Poor planning/strategies
- Cash flow issues
- Poor visibility/location
- Not agile/flexible enough
- Unsustainable expansion

5 Underlying Issues That Lead To Failure

1 Rising Inflation

As costs rise, businesses need to cover necessary expenses, reduce spending, and improve profitability.

2 Lacking Capital

Companies that can't convince investors or struggle with cash flow issues can quickly find themselves sinking.

3 Unexpected Disruptions

From sophisticated cyberattacks to natural disasters, there are plenty of issues that can result in unexpected expenses.

4 Poor Planning

Lacking a solid business plan or disaster recovery plan could mean struggling to adjust when issues arise.

5 Inadequate Risk Management

It's good to prepare for the worst and hope for the best, but some businesses don't stop to consider potential threats.

Why Avoid Resiliency?

So, if there are so many threats facing the average business, why aren't more businesses prepared? Only 54% of organizations have an established, company-wide disaster recovery plan.[4]

The simple truth? Many business leaders feel overwhelmed and short on time. Not only do they not know where to start when it comes to a disaster plan, but they don't have the time to dedicate to fully fleshing out a plan. Yet, a staggering **60% of small businesses close within six months of experiencing a cyberattack**.

60% of small businesses close within six months of experiencing a cyberattack.

Business leaders tend to avoid creating a solid disaster recovery strategy because they simply don't know where to start — the process can feel overwhelming and complex.

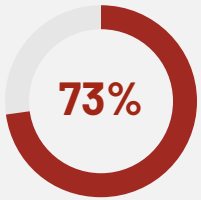
However, there is good news! **Developing a disaster recovery strategy doesn't have to be overly complicated**. By starting with the basics and asking fundamental questions about key business systems and processes, individuals can gradually build a framework for resilience.

It's time to take proactive steps towards disaster preparedness. Every small action taken lays the foundation for building a more resilient business.

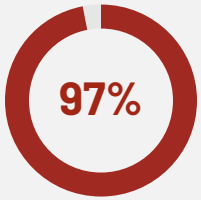
What is the #1 threat for businesses?

While fires, vandalism, and storms are important to plan for, the top threat is **Business Email Compromise (BEC)**.

IronEdge helps clients deal with at least one BEC case per week on average.



73% of organizations reported at least one successful ransomware attack in 2022.[4]



97% of ransomware attacks in 2022 tried to infect both primary systems and backup repositories.[4]

How To Start Planning for Disasters and Threats

1 Identify Key Systems

How long can you survive without key processes and systems? Not every system is crucial to keeping your business going or in a state of protected stasis. While many people want to achieve zero downtime during a disaster or attack, keeping your business going 24/7 is extremely expensive.

So, instead, start by understanding what systems are critical for business operations, the potential impact of downtime, and the available solutions for minimizing disruptions. Then, prioritize the protection and recovery process for these systems in your plans.

2 Start With the One Issue

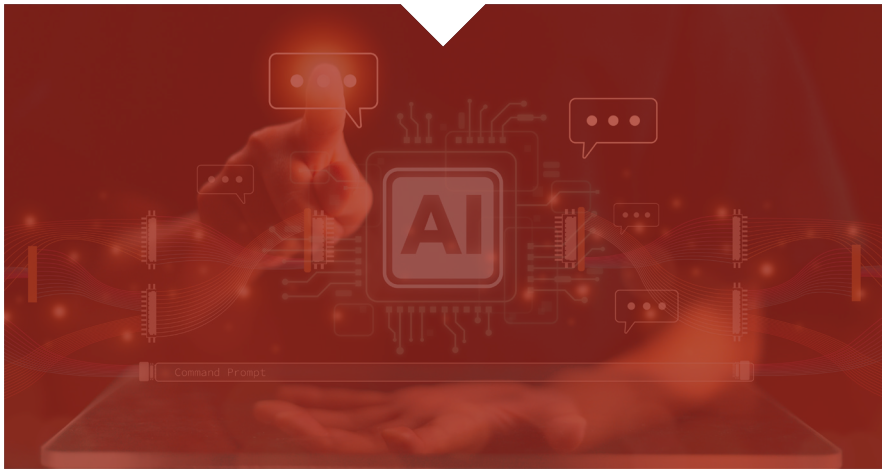
The perceived difficulty of creating a disaster recovery plan and contingency plan often deters people from taking the necessary steps to protect their assets and operations. Some individuals may feel incompetent or lacking in knowledge and resources, further contributing to their reluctance.

To help combat this, you should start with the most pressing threats (like hurricane response and recovery plans as you are entering hurricane season) and keep it simple. If you stick with this process, your plans will become more and more thought-out over time as your business matures.

3 Use AI To Kickstart Your Plan

Feeling a little stuck? You can kickstart your disaster recovery and business continuity planning with AI. Just ask Chat GPT to create a plan and adjust it to fit your business. You can even prompt AI to address a particular disaster scenario, include specific steps, identify potential vulnerabilities, and prioritize key systems.

Harnessing AI can help you avoid the mental block that comes with not knowing how to get started. Once you see a fleshed-out plan and run through it in your mind, you will start to see things you want to tweak, and you can hone it from there.



4 Take Small Steps

Creating plans that are relevant and thorough takes time. A disaster recovery plan doesn't have to be perfect in the first round; it's about starting to think about potential risks and developing strategies to mitigate them. Not only will you find pitfalls and shortcomings in your plan as you go, but your needs will also evolve over time.

The truth is that doing something is better than doing nothing. So, the key is to just get started. Take small, manageable steps and gradually build upon them to reduce your exposure to risks and better safeguard your business continuity.

5 Get Expert Insights

Ideally, you'll choose software and tools that help you support security and disaster recovery efforts. Get expert guidance in selecting software solutions and implementing processes that align with your unique setup while enhancing the effectiveness of your business continuity and disaster recovery plans.

IronEdge offers extensive experience and industry knowledge so you can benefit from tailored recommendations and strategic insights that reduce risks and fit your goals, challenges, and needs. We'll help you streamline your continuity efforts and ensure resilience in the face of unforeseen challenges.

Business Continuity & Disaster Recovery Plan Checklist

Risk Assessment

Ask: What are the potential threats and hazards that could disrupt our business operations, and how likely are they to occur?

- ☑ Identify potential threats and hazards that could disrupt business operations.
- ☑ Assess the likelihood and potential impact of each threat on critical business processes and functions.

Business Impact Analysis (BIA)

Ask: What are the critical business processes and resources that would be impacted by a disruption, and what is the potential financial and operational impact?

- ☑ Determine the impact of disruptions on key business processes and resources.
- ☑ Define recovery time objectives (RTOs) and recovery point objectives (RPOs) for critical systems and data.

Emergency Response Procedures

Ask: Who are the key personnel responsible for initiating the business continuity plan during an emergency, and what are their specific roles and responsibilities?

- ☑ Develop procedures for responding to emergencies and activating the business continuity plan.
- ☑ Outline roles and responsibilities for key personnel during a crisis.

Data Backup and Recovery

Ask: How often are critical data, systems, and applications backed up, and where are backups stored to ensure their security and accessibility?

- ☑ Establish backup procedures for critical data, systems, and applications.
- ☑ Ensure regular backups are performed and stored securely offsite.

IT Disaster Recovery

Ask: What procedures are in place for restoring IT systems and infrastructure in the event of a disaster, and how quickly can alternative work locations be activated?

- ☑ Develop procedures for restoring IT systems and infrastructure.
- ☑ Identify alternative work locations and communication channels for IT staff.

Communication Plan

Ask: What communication channels are available for internal and external stakeholders during a crisis, and how can they be reached in a timely manner?

- ☑ Establish communication protocols for internal and external stakeholders.
- ☑ Ensure contact information for key personnel, vendors, and customers is up to date.

Training and Awareness

Ask: Have employees received training on emergency procedures and their roles during a crisis, and how often are drills and exercises conducted to test their readiness?

- ☑ Provide training for employees on emergency procedures and their roles during a crisis.
- ☑ Conduct regular drills and exercises to test the effectiveness of the plan.

Regular Review and Update

Ask: When was the last time the business continuity and disaster recovery plan was reviewed and updated, and what changes need to be made to ensure its effectiveness in addressing current risks and challenges?

- ☑ Schedule regular reviews of the plan and test it annually to ensure it remains current and relevant.
- ☑ Update the plan as needed to reflect changes in business operations, technology, or regulatory requirements.

Partner With a Provider You Can Trust

IronEdge can help you protect your physical and digital assets with a proactive approach to business resiliency:

- Back up your infrastructure as a core part of our services
- Back up third-party data (like Microsoft, Sharepoint, OneDrive, etc.)
- Get business-level consulting to drive your strategies and solutions
- Access knowledgeable support to guide tech decisions and budget
- Support IT operations with security solutions that limit the scope of disaster
- Educate employees on cybersecurity best practices and using multi-factor authentication (MFA)
- Reduce downtime with robust recovery plans and tools

IronEdge provides many layers to help mitigate disastrous scenarios. We help you consider how your business will grow over the next 3-5 years and then we help you reassess your plans and tools as needed.

Our goal is to be proactive with security and limit the scope of any threat, containing it as quickly as possible. Once an attack is identified, we work with the incident response team to provide them with valuable insights to speed up the review process.

15k **IronEdge supports 15,000 nodes**

24/7 **We provide round-the-clock support**

19 **We offer nearly two decades of industry experience**

CASE STUDY

Example of Disaster Recovery in Action

What happens when things go unexpectedly wrong? When one of our clients chose to install a separate infrastructure on their own, they encountered serious security issues due to insufficient safeguards. The IronEdge team caught a state-sponsored threat actor hacking into the infrastructure. The attack resulted in the closure of all servers and workstations, causing significant disruption to operations.

This situation highlighted the critical need for a comprehensive disaster recovery and business continuity plan. IronEdge swiftly isolated and contained the issue, effectively halting operations and contacting cyber insurance to engage a specialized cybersecurity firm. During the downtime, IronEdge assisted the client in getting operational as quickly as possible, identifying the core systems needed for functionality, and providing crucial support in containing and understanding the threat.

IronEdge's proactive approach not only helped the client recover within a week but also ensured that core systems were protected and operational. Without IronEdge's swift and proactive response, this critical incident could have led to catastrophic consequences for the business.

By collaborating closely with incident response firms, IronEdge was able to provide invaluable insights and assistance, exceeding the expectations of the firm.

Moving forward, IronEdge recommended infrastructure solutions to prevent similar incidents in the future. Our team helped this client increase proactive measures such as blocking, reporting, and preventing threats before they escalate.

IronEdge demonstrated its commitment to providing responsive support and comprehensive cybersecurity solutions tailored to the unique needs of the client.

Increase Your Business Resiliency

Ready to fortify your business against unforeseen disruptions and plan for a resilient future?

IronEdge is here to guide you every step of the way. Our team of experts specializes in developing cybersecurity strategies and tailored solutions that go hand-in-hand with your disaster recovery and business continuity plans.

Partner with our team to fortify your business operations and adaptability amidst evolving threats. With our proactive approach and cutting-edge solutions, we empower businesses to anticipate challenges, mitigate risks, and thrive in an ever-changing business landscape.

Contact us today to learn how IronEdge can help you build a resilient foundation for long-term success.

LET'S TALK

Resources

[1] https://www.lendingtree.com/business/small/failure-rate/

[2] https://www.bls.gov/bdm/us_age_naics_00_table7.txt

[3] https://www.investopedia.com/financial-edge/1010/top-6-reasons-new-businesses-fail.aspx

[4] https://phoenixnap.com/blog/disaster-recovery-statistics

IRONEDGE®