



Building Business Resilience

Your blueprint for creating
effective business continuity

EXIGENT

Building Business Resilience

Your blueprint for creating effective business continuity

Introduction: Preparedness: Isn't Just for Scouts

Chapter 1: The Difference Between Backup/Disaster Recovery and Business Continuity

- Understanding the Scope of Business Continuity
- Where Does Disaster Recovery Fit In?

Chapter 2: Prevent & Prepare Before It's Urgent and Chaotic

- Prevention: The Initial Step in Disaster Recovery Planning
- Where Does Disaster Recovery Fit In?

Chapter 3: Response to Recovery: Navigating Business Continuity

- Creating an Effective Incident Response Plan
- Emphasizing Recovery in Business Continuity

Chapter 4: Best Practices for Compliant Business Continuity

- Understanding the Compliance Landscape
- Challenges with Business Continuity and Compliance
- Integrating Governance, Risk, and Compliance (GRC) into Business Continuity Planning

Final Thoughts: Importance of Comprehensive Business Resilience

Building Business Resilience

Your blueprint for creating effective business continuity

Introduction

Preparedness: Isn't Just for Scouts

For many organizations, disaster preparedness begins and ends with a simple backup plan. However, creating an effective strategy for business continuity requires much more. True protection from disruptions - manmade or natural - only happens when organizations prepare thoroughly, deploy and test solutions for both backup and recovery, and then wrap technology with plans for additional needs such as incident response, crisis communications, and employee training.

Don't leave your organization exposed by procrastinating. Disaster can strike at any time and in many forms. Investing the time to prepare can be the difference between reopening your business and closing your doors forever.

Research repeatedly shows that businesses often don't survive major disruptions: 40% of small businesses never reopen and an additional 25% that manage to reopen end up failing within the year. Acting now to research, plan, and test your strategy can help you avoid becoming a statistic.

In this guide, we will clarify the difference between backup and disaster recovery and business continuity, outline the four elements of an effective business continuity strategy, and share tips for creating a detailed plan to protect your organization. We'll also supply checklists and templates to aid in those efforts.



**40% of businesses never
reopen after major disruption.
25% that do reopen will
fail within the year.**

Building Business Resilience

Your blueprint for creating effective business continuity

Chapter One

The Difference Between Backup/Disaster Recovery and Business Continuity

Amid today's near-constant cybersecurity discussions, one crucial aspect of protecting organizations is often overlooked – the indispensable role of backup and disaster recovery (BDR) solutions in safeguarding your organization. But BDR is only one part of the business continuity strategy that every business needs to weather cyber attacks, natural disasters, and other events that can derail operations, such as hardware failure or even a prolonged power outage.

This leads to a critical question: **Is your company prepared for disruptions to your IT environment?**

To start, let's address a common source of confusion. Many organizations can't differentiate between backup and disaster recovery (BDR) and business continuity planning (BCP). Despite their seemingly interchangeable nature, these two concepts have distinct purposes within emergency preparedness. It is crucial to recognize that while both BDR and business continuity are necessary, their scopes diverge significantly.

Understanding the Scope of Business Continuity

Business continuity is a holistic strategy and roadmap for recovering critical business functions post-disaster. Unlike disaster recovery, which delves into the technicalities of data and IT redundancy and recovery, business continuity addresses the broad spectrum of where, when, who, and how as you plan how to navigate disruption and either maintain or restore operations. This includes orchestrating employee relocation during disasters, managing communication channels with stakeholders, and prioritizing business functions for swift recovery.

The primary goal of business continuity is downtime mitigation and quick resumption of operations to a minimally functional level.

Managed IT services providers (MSPs) play an integral role in crafting the technology infrastructure that supports critical business operations and facilitates data loss prevention and restoration. Collaborative planning across all facets of hardware, software, policies, and communications is essential, with MSPs contributing their expertise to ensure seamless integration of technology into the business continuity plan. Because of their broader point of view, MSPs can often provide best practices for several aspects of an organization's business continuity strategy, pulling examples from their own policies and real-world experience they have had with other clients.



Building Business Resilience

Your blueprint for creating effective business continuity

Where Does Disaster Recovery Fit In?

While business continuity covers every aspect of operations, backup and disaster recovery hones in on the IT-specific elements organizations need to prepare, respond, and recover from catastrophic events. In this digital age, where technology is the backbone of operations for even the smallest organizations, MSPs play a pivotal role in BDR. They guide the backup and recovery process, facilitate decision-making about critical BDR solutions, and spearhead technical efforts for swift data restoration. Additionally, having IT support offsite can be crucial when and if disaster hits your physical location, accelerating recovery processes and providing a logical emergency operations center.

To Recap

The fundamental difference between business continuity and backup and disaster recovery is scope:

- **Business Continuity:** *Encompasses a strategic roadmap for recovering critical business functions holistically, addressing people, processes, technology, and communication plans.*
- **Disaster Recovery:** *Centrally focused on the technical facet of data recovery, backups, system restores, and infrastructure recovery*

The symbiotic relationship between business continuity planning and BDR underscores the necessity of both for comprehensive preparedness.

Collaborative efforts between MSPs and organizational stakeholders at each strategic step are imperative for developing these cohesive, detailed plans.

Having IT support offsite can be **crucial** when and if disaster hits



Building Business Resilience

Your blueprint for creating effective business continuity

Chapter Two

Prevent & Prepare Before It's Urgent and Chaotic

Robust business continuity plans not only shield your organization and its vital data from cyber attacks but also from hardware failures, natural calamities, and human errors. It should come as no surprise that crafting an effective plan takes time and effort, and therefore, planning for disruption is often relegated to the bottom of an organization's "to-do" list. But investing in your strategy before disaster strikes is a must. To start that process, let's review the four essential pillars of business continuity: **Prevention, Preparedness, Response, and Recovery.**

Prevention: The Initial Step in Business Continuity Planning

Implementing foundational measures such as risk identification, cybersecurity assessment, and redundancy establishment significantly bolsters your organization's protection against disasters. These steps create a solid foundation for the actions to follow and are an essential part of a successful strategy.

✓ Conduct a Risk Assessment

Develop a policy for identifying and assessing potential threats, both internal and external, including a regular schedule for ongoing review and revisions. Each organization faces distinct operational threats based on its business nature. It's crucial to understand that a "disruption" doesn't necessarily mean a complete halt but could encompass anything that impedes productivity, affects customer service, or poses safety risks to your employees. Often, organizations focus on uncommon, massive disruptions, such as hurricanes or cyber attacks, but overlook the widespread impact of smaller, more probable hiccups, such as extended internet outages, or even hardware failure.

✓ Network Redundancy Solutions

Incorporate redundancy into critical systems and infrastructure to ensure their resilience against failure, whether from natural disasters or malicious activities. Achieving resiliency might involve redundant hardware, backup power supplies, or geographically dispersed data centers. Many businesses opt for hybrid cloud solutions and leverage the 3-2-1 approach to enhance redundancy, thereby mitigating disaster risks and securing business data.

✓ Implement Data Security Best Practices

Collaborate closely with your MSP to evaluate, strategize, and deploy robust data security measures aimed at minimizing the risk of data breaches and other cyber threats. This includes measures like encryption, access controls, vulnerability scans, and patching. Work with an MSP partner to consider effective ways to protect your data within your backup and disaster recovery processes, where information in motion can be vulnerable.

Why approach business continuity on such a detailed level? The significance of even small disruptions can't be overstated. Research from FEMA indicates that 40% of small businesses never reopen after a disaster and an additional 25% that manage to reopen end up failing within the year. Furthermore, about 60% of businesses forced to close due to a data breach never recover. Given these statistics, investing time in a comprehensive disaster risk assessment and deploying more resilient infrastructure appears to be a wise decision.

Building Business Resilience

Your blueprint for creating effective business continuity



Preparation May Not Be Sexy, But It's Crucial

Preparing your business for disaster entails planning for diverse types of disruptions. Understanding how threats affect your business operations, data, employees, and assets is paramount. That is why research and data from your organization are a vital part of business continuity planning. There are three main actions in the preparation stage:

✓ Business Impact Analysis (BIA)

Identify and prioritize critical business functions and processes, quantifying the potential impact of disruptions on each. This includes assessing factors such as location, importance, backup frequency, and recovery priorities. By sitting down and evaluating what your business needs to operate flawlessly, then considering the impact of specific disruptions – flood, fire, cyber attack, earthquake, etc. – you will start to understand what you need to protect the most and restore the fastest. This exercise provides the basic blueprint for your detailed business continuity plan by forcing your organization to look at each scenario and the processes, tools, people, and facilities needed for your business to remain functional. From there, you can start to prioritize between what you would like to be operational and what you truly need.

✓ Employee Training and Education

Conduct simulated disaster training sessions regularly with your team and employees. Walk through the BCP to ensure everyone understands their roles and responsibilities during various disaster scenarios. Training employees for disaster recovery is crucial to ensure readiness when the need arises. No one will have time to scour a document for instructions when a disruption occurs, so practice often. Also, remember to apply redundancy rules to your BCP document, ensuring multiple team members have access regardless of their location and network availability.

✓ Business Continuity Plan (BCP) Creation

Crafting a meticulous plan outlining how your organization responds to and recovers from different classes of disruptions is perhaps the most challenging aspect of disaster planning. Your BCP encompasses roles and responsibilities for the crisis management team, communication protocols, recovery procedures, and testing schedules. You will need to consider the “who, what, when, where, and how” of every single scenario across your entire business operations. Don't be overwhelmed; you can begin the process with a situation either your business or your MSP has navigated before and use that as a template for other scenarios. It's crucial to ensure your BCP is comprehensive, clear, regularly reviewed, and communicated repeatedly to all employees. Remember to involve stakeholders from across each area of your organization to guard against information gaps and to gain multiple points of view.

While navigating these initial stages of business analysis and preparation may seem daunting, the insights and information gathered during this process provide a significant advantage as you develop your full strategy. Many organizations opt for a task force comprised of representatives from multiple departments to plan for an effective strategy encompassing marketing, IT, operations, and more.

Building Business Resilience

Your blueprint for creating effective business continuity

Chapter Three

Response to Recovery: Navigating Business Continuity



Only 57% of data backups are successful, and just 61% of restoration efforts yield success.

In the previous chapter, we delved into the initial stages of building a robust business continuity plan, emphasizing the prep work necessary as you build toward your comprehensive business continuity strategy. Now, we shift our focus to responding to disasters and executing the crucial steps involved in restoring essential data and assets to resume operations—where the effectiveness of backup and disaster recovery processes shines.

Validation and testing remain indispensable throughout this journey. Consider this: A 2021 study by Veeam revealed that only 57% of backups are successful, and just 61% of restoration efforts yield success. On average, businesses successfully recover their critical data only 35% of the time. Let's not become one of these statistics!

Crafting an Effective Incident Response Plan

As you construct a business continuity blueprint, engage your organization's stakeholders and your MSP to ensure practical execution aligns with all perspectives. Effective communication during emergencies is challenging, and managing crises requires a calm and orderly approach. While your strategy should be tailored to your organization, don't overlook expertise and assistance from key partners such as your MSP, cyber insurance provider, outsourced human resource experts, and marketing agencies.

As you build your plan, you'll find several smaller, highly specific procedures will live within that document. As we discussed earlier, business continuity encompasses much more than data protection and recovery, it also includes incident response, crisis management, personnel, communications, and more. The following page outlines three essential procedural guides you will need.

Crafting an Effective Incident Response Plan



Incident Response Plan

Develop a structured plan outlining how you'll identify, contain, and respond to incidents as they occur. Tailor this plan to address the various threats identified earlier, including instructions for notifying key personnel, assessing damages, and activating your business continuity plan. Create as many elements as possible of that plan in template form, making it easier for your team to learn the process and be comfortable using the plan.



Crisis Management Team

Form a crisis management team responsible for making critical decisions and overseeing response and recovery efforts. Regularly convene this team to review and assess the response plan. Clearly define roles and responsibilities and communicate them throughout the organization.



Communications Plan

Establish protocols for communicating with internal and external stakeholders during disasters. Include strategies for connecting with employees, customers, vendors, and the media. Ensure access to essential contact lists and information, emphasizing the importance of maintaining and accessing backups of such data. Remember to plan in terms of who will run point on communications, who will serve as spokesperson, and the cadence for regular updates to employees, customers, media, and other constituencies. Much like the incident response plan, developing templates that accelerate and simplify the steps helps your team respond more quickly.



Other Considerations

- ✓ Alternative physical locations to be leveraged during a disruption
- ✓ Plans for secondary access points to technology tools, such as a designated coworking site that can provide reliable internet access during an outage
- ✓ Redundancy with personnel to account for access limitations, personal time off, or even injuries that could remove a key person from a critical role

Building Business Resilience

Your blueprint for creating effective business continuity

Emphasizing Recovery in Business Continuity

The final and pivotal aspect of a business continuity strategy is recovery. While data backup falls under preparedness, disaster recovery becomes crucial during the restoration phase. Safeguarding critical data is fundamental, but accessibility and usability are equally paramount. Testing and collaboration with your outsourced IT provider are imperative at this stage.

✓ Data Restoration Best Practices

Outline detailed procedures for promptly restoring data from backups. Regularly test backup and recovery procedures to ensure functionality. Remember those shocking statistics from Veeam? Consider the impact a failed backup would have during a disruption and let that guide the frequency of your testing. Focus on data protection throughout the process and consider implementing a 3-2-1 redundancy for enhanced reliability. Remember that data in motion is more vulnerable to cyber attacks as well as non-malicious issues such as file corruption, so plan appropriately to protect your backup access points, backup and recovery processes, and, of course, encrypt your data.

✓ System Recovery Procedure

This highly specific SOP guides the restoration of critical systems and infrastructure to a functional state. This may involve redundant systems, backup data restoration, or even rebuilding your systems from scratch ("bare-metal restore"). For natural disasters, plan for a temporary office or tech site. Just as you evaluate backup processes, be certain to routinely test your recovery systems – after all, what use is secure, redundant data if you cannot access it? Don't overlook that your team must be able to leverage restored data and systems, so build in contingencies for secondary locations, replacement devices, and more – and communicate those procedures to your team as well.

✓ Testing Disaster Preparedness

We can't stress enough the importance of continuously assessing your business continuity plan and recovery procedures to identify and address weaknesses. Conduct full-scale exercises periodically to simulate real-world scenarios. Involve vendor partners and your managed IT services provider in these tests.



Building Business Resilience

Your blueprint for creating effective business continuity

Chapter Four Best Practices for Compliant Business Continuity

Organizations operating within regulated industries face a unique set of challenges when it comes to crafting a comprehensive business continuity strategy. Regulatory compliance intertwines with business continuity planning, requiring meticulous attention to detail regarding data protection, backup protocols, access controls, data retention policies, and more. In this chapter, we delve into the best practices for developing a compliant business continuity strategy tailored to meet the stringent requirements of regulated sectors.

Understanding the Compliance Landscape

Regulatory mandates emanate from diverse sources, including governmental bodies, industry regulators, and internal corporate guidelines. While the specifics may vary, the shared objective across many compliance standards is robust data protection. Safeguarding sensitive information—be it medical records, personal identification data, financial details, intellectual property, or payment information—is vital. Compliance regulations not only mandate securing data but also comprehensive documentation, detailed logs, and stringent record-keeping regarding data location and movement.

Challenges with Business Continuity and Compliance

Developing a compliance-aware business continuity plan necessitates addressing several fundamental components to ensure alignment with regulatory standards:

- **Data Availability:** *Compliance often dictates specific data retention periods and accessibility requirements. Failure to meet these standards due to system outages or data loss can result in severe penalties. Documenting your data backup and restoration plan in detail confirms to regulatory agencies that sensitive data remains accessible and compliant during disruptions.*
- **Timely Reporting:** *Regulatory agencies mandate prompt reporting of incidents or data breaches. Prioritize communications with relevant agencies during disruptions, and follow up with quick, comprehensive reporting.*
- **Continuity of Processes:** *Adherence to processes and procedures is vital for regulatory compliance. Business continuity plans should incorporate contingency plans to ensure continuity around compliance procedures during disruptions.*
- **Documentation:** *Detailed audit trails are integral to compliance. Disruptions can impede reporting and documentation efforts, emphasizing the need for robust backup mechanisms for compliance-related data.*
- **Data Protection:** *Protecting sensitive information remains a core aspect of compliance. Business continuity strategies must address security vulnerabilities introduced during disruptions and outline measures to safeguard data during recovery.*
- **Human Error:** *Employee training on compliance and business continuity procedures is essential. Emphasize the criticality of maintaining compliance standards amid disruptions.*



Building Business Resilience

Your blueprint for creating effective business continuity

Integrating Governance, Risk, and Compliance (GRC) in BCP

Incorporating governance, risk, and compliance best practices into business resiliency strategies provides a foundational framework aligned with regulatory standards. Governance focuses on processes and documentation, including reporting requirements mandated by compliance standards. Risk assessment aids in identifying threats and vulnerabilities, ensuring a comprehensive approach to business continuity planning. Consistent questioning of compliance needs throughout the planning process ensures appropriate stakeholder involvement and alignment with regulatory mandates.

Leverage MSPs for Compliance Support

Leveraging the expertise of MSPs with compliance expertise is invaluable. They can bridge technology gaps and implementing compliant solutions for data backup, access control, data retention, cybersecurity, and more. Collaborative efforts with MSPs ensure business continuity plans align seamlessly with evolving compliance landscapes, enabling organizations to navigate regulatory complexities effectively.



Building Business Resilience

Your blueprint for creating effective business continuity

Final Thoughts

Importance of Comprehensive Business Resiliency

While creating a business continuity plan can be overwhelming, it is an essential element of developing resiliency in your business. With resilience, your organization is prepared to adapt quickly and navigate through unexpected obstacles, such as business disruptions, without succumbing. While your business may suffer unavoidable consequences, such as downtime and revenue loss, a resilient organization is positioned to weather the storm and resume operations with minimal damage. We've included resources here to help get your team started.

Additional Resources

Disaster Prep Checklist

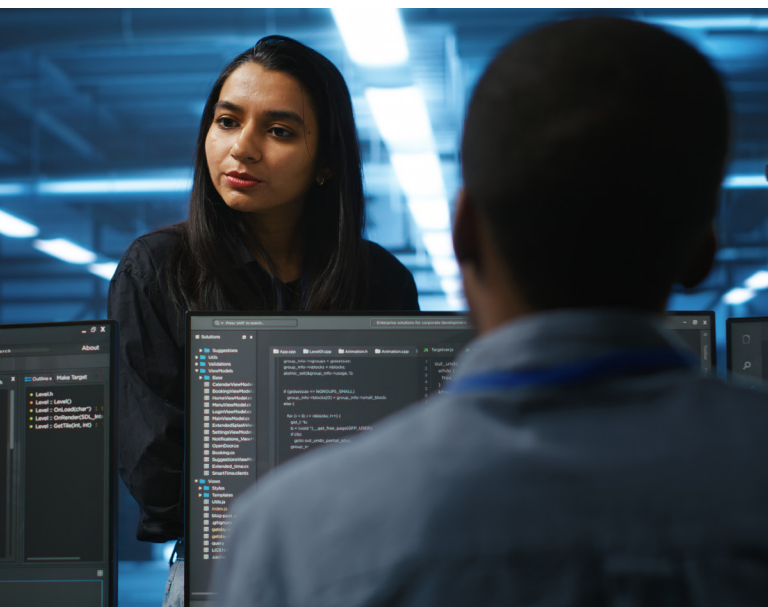
Incident Response Template

CyberSecurity Guide

About Exigent BDR Solutions

About Exigent

Since 1997, Exigent Technologies has combined technical experience and a can-do attitude to consistently deliver exceptional service as a managed IT services provider. With an array of managed services and consulting expertise, we provide end-to-end technology support, accommodating the unique needs of small to midsize organizations and complementing the internal IT resources of larger enterprises. We believe in fostering long-term, strategic partnerships with our clients by actively engaging in their success. This collaborative mindset allows us to align our services with clients' objectives, helping them stay ahead of the competition. Our commitment to true partnership, integrity, and outstanding support is reflected in our average customer tenure of a decade or more. For more information, **visit [exigent.net](https://www.exigent.net)**, or **call 1.877.EXIGENT** or **email learnmore@exigent.net**.



CONTACT US:

877-EXIGENT

EXIGENT.NET

EXIGENT