WHITE PAPER:

The Disaster Survival Guide for Small- and Mid-Size Businesses

The most valuable asset in many of today's businesses is the data stored in their computer systems. In the digital environment, information is money. This is one of many reasons why every organization needs a well-constructed and periodically tested plan to retrieve that precious data in the event of an outage or larger catastrophe.

TeamLogicIT®
Your Technology Advisor

IT experts use terms such as business continuity (BC), disaster recovery (DR) or backup and disaster recovery (BDR) to describe these strategies. Each is acceptable and frequently intermingled in technology discussions, though the former is gaining traction for its straightforward description of the true objective. Business continuity is the ultimate goal for owners, managers, and investors after a disaster.

Failure in this area is unacceptable no matter the size or duration of the emergency. Whether a business is forced offline for a day because of a local internet outage or must completely rebuild its facilities and IT infrastructure after a fire, certain data must be preserved and made readily accessible.

A growing number of government regulations and industry standards include data storage and protection requirements, making effective restoration plans an absolute necessity for nearly all organizations. Covered entities that fail to adhere to these rules may subject themselves to regulatory fines and potential lawsuits from investors, stockholders and other affected parties. Penalties for non-compliance can escalate quickly and could significantly damage an affected organization's already stressed bottom lines, if not put them out of business for good.

While compliance is a great reason to develop a business continuity plan, the ultimate goal is survival. A recent report from the Federal Emergency Management Agency[1] suggests that more than 40% of businesses never reopen after a natural disaster, and only 29% of those that survived were still operating two years later.

Recovery is a costly endeavor. The longer it takes to restore systems and get people back to work, the higher the price tag and the more likely it is that the business won't reopen. IDC research reports 35% of small and medium-sized business (SMB) organizations lost as much as $500,000 in 2017 due to downtime, and for 3% of those businesses the costs reached or exceeded one million dollars.[2] Those numbers clearly illustrate the expense of a poorly constructed (or nonexistent) business continuity plan.

According to IDG, an average of seven hours is required for businesses to resume normal operations after a data loss incident.

Every organization's primary objective should be protecting critical data and vital business systems. If a disaster were to destroy the headquarters and computing infrastructure, how long would it take to restore operations? Most businesses rely heavily on email and voice communications, as well as their customer relationship management (CRM) tools, and require constant access to certain files and data.

1. FEMA, Recovery Mission Overview, fema.gov/media-library-data/1503934487992-04de8b0806cf8fd108be42725a348fa6/2017NationalPreparednessReportRecoveryOverview.pdf

2. 2018 Global State of Information Security Survey, IDG https://www.idg.com/tools-for-marketers/2018-global-state-information-security-survey/

How soon could those systems be restored in a safe location? Every organization should have contingencies written into its business continuity plan, including options such as hosted VoIP, offsite data storage, mobility devices (such as laptops, tablets and smartphones) and a host of cloud-based services. Employees can access and manage those systems from any location with an internet connection—the ultimate disaster recovery scenario.

Data retrieval processes and failover are a big part of recovery expenses. The price of solutions and the responsibility for protecting vital business information increases every year as a slew of new federal, state, local, and industry rules come into play. Many of those requirements center on privacy and security. Ensuring the continued availability of client, employee, and other critical data—even after a natural disaster or ransomware attack—is one of the key value propositions of business continuity plans. That explains why these forward-thinking tactics have become a necessity for every organization today.

A well-planned and frequently tested recovery strategy can minimize those costs. With detailed instructions for restoring access to critical systems and data after an outage, a business continuity plan makes it easier to bring everything and everyone back online in the shortest amount of time possible.

What Could Go Wrong?

Disasters come in all shapes and sizes. In today's internet-centric society any incident that even temporarily interrupts online activities, including email and other forms of electronic communications, can result in major headaches for business owners.

A proactive approach to protecting data can minimize the damage and reduce the stress on those responsible for protecting valuable information and meeting all compliance requirements. A business continuity plan helps companies resume operations as soon as possible following a disruptive event. Those threats come in five categories with varying degrees of severity:

1. **Large-scale emergencies:** Hurricanes, wildfires, earthquakes and major terrorist attacks can inflict tremendous damage to an organization and its computer systems. The first step should be to ensure everyone has been safely evacuated (if needed) and medical attention is provided to those injured during the incident. After addressing the immediate concerns of employees, family members and the community, leaders can then focus on the business recovery process.

2. **Small-scale catastrophes:** These are site-specific events that can significantly disrupt operations, including fires, floods and structural failures. While these situations may be just as devastating as a large-scale emergency for the business, recovery efforts usually start immediately. Operations can often be shifted to a secondary location in hours, if not minutes, if the proper plans are in place.

3. **Short-term computer outages:** Some people may not consider a two-hour ISP (internet service provider) failure to be a significant issue, but the lost time and productivity can be costly for businesses. Other problems that can lead to temporary outages include dropped or water-damaged devices (spilled coffee, soda, etc.), kinked cables, and failed network components. Equipment theft—laptops, smart-phones, and tablets—can also disrupt business operations for the user as well as others they work with or support, including clients. Those incidents can force companies to spend even more time and money enhancing security protocols and addressing possible regulatory compliance violations.

4. **Cybersecurity attacks:** Unchecked ransomware and viruses can completely lock down a company's computer systems. Originating from a single file or infected web link through an email phishing attack, this type of malware spreads rapidly through networks and encrypts or otherwise corrupts valuable business data and files. Ransomware locks down key information systems and can potentially shut down entire organizations, inflicting even greater financial damage than natural disasters and fires.

5. **Power failures:** Dated and overtaxed electric generation equipment is bound to fail at some point. Businesses need to be prepared for outages during peak demand hours (typically 9–5 on extremely cold and hot days), especially when ice, snow, and heavy rainstorms approach.

Regardless of the issue, an effective business continuity plan will help ensure the organization can quickly restore its vital information and computer systems and get everyone back to work. Think of it as an organizational insurance policy for IT.

The Rising Compliance Requirements

Companies face a growing number of federal, state, and local rules relating to data privacy and reporting. In today's high-risk environment—including the threats associated with natural and man-made disasters—organizations must protect sensitive information collected from employees and clients as well as financial and other operations-related data. Many of the latest rules cover the storage, security, retrieval, and restoration of that critical information.

Compliance involves following standards or prescribed best practices, such as the implementation and periodic testing of a business continuity plan. Essentially, regulators want all covered entities to be able to replicate or regain access to critical data in a specific amount of time after suffering business disruptions—whether caused by a natural disaster, fire, or other event.

Organizations that fail to adhere to the rules are subject to regulatory fines and potential lawsuits from investors, stockholders, and other affected parties. Penalties can escalate quickly and significantly damage a company's bottom line, if not force it to close down operations. Common data protection and privacy regulations and rules include:

- **SOX (the Sarbanes-Oxley Act)** requires publicly-traded companies to implement specific internal accounting controls. Section 404 states that the management team is responsible for maintaining an "adequate" internal control structure and requires an annual audit/report on the status of those systems. All financial information must be appropriately safeguarded with its integrity assured, meaning the company should incorporate data backup and security practices into its business continuity plan.[3]

- **FINRA (Financial Industry Regulatory Authority)** is a non-governmental organization that regulates securities brokerage firms and exchange markets in the United States. Member firms are required to create and maintain written business continuity plans to protect all electronic records and email messages in the event of a significant business disruption. FINRA Rule 4370 spells out the required procedures, which may be tailored to meet the size and needs of each organization.[4]

- **HIPAA (Health Insurance Portability and Accountability Act of 1996)** provides data privacy and security provisions for safeguarding medical information. The Security Rule requires that healthcare organizations maintain a viable data backup plan, a disaster recovery plan, and emergency mode operation plan.[5]

- **GDPR (General Data Protection Regulation)** applies to any organization that does business with European Union residents. Article 32 requires companies to be able to restore availability and access to personal data promptly in the event of a physical or technical incident. That rule also mandates a process for regularly testing, assessing and evaluating the effectiveness of those measures.[6]

- **GLBA (Gramm-Leach-Bliley Act)** covers companies that offer consumer products or services such as loans, financial and investment advice, or insurance. Business continuity plans must include specific incident response processes that protect all organizational information from security breaches, data thefts, or denial-of-service attacks.[7]

Most regulatory and industry rules require organizations to test their backup and disaster recovery plans at least annually and update the specifics as needed. For example, when a company switches business continuity-related tools or alters its restoration processes, its business continuity plan should be adjusted to compensate for each change.

3. U.S. Security and Exchange Commission, Final Rule: Retention of Records Relevant to Audits and Reviews https://www.sec.gov/rules/final/33-8180.htm

4. FINRA Business Continuity Planning http://www.finra.org/industry/business-continuity-planning

5. U.S. Department of Health & Human Services, Summary of the HIPAA Security Rule, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

6. Article 32 EU GDPR "Security of processing" http://www.privacy-regulation.eu/en/article-32-security-of-processing-GDPR.htm

7. U.S. Federal Trade Commission, Gramm-Leach-Bliley Act, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

Calculate the Cost of Downtime

If an organization's computer systems went down at this very moment, how long would it take before its operations came to a screeching halt? It probably wouldn't take long, but the price of those failures is often significantly higher than most would expect. From the loss of email and internet applications to a potential interruption in communications (i.e. phone, instant messaging and teleconferencing), a single system failure could be extremely disruptive and costly. Sales losses and diminished productivity can affect bottom-line in no time.

Calculating the potential costs of downtime can help owners and managers understand how much is at risk. The first step is to estimate monthly expenses based on the value of all the resources used to run operations for an hour. A best practice is to use actual payroll numbers (including all benefits) and related expenses to validate the exercise.

For example, an owner of a company with 1 terabyte (1000 GB) of data and 25 employees who rely on key business systems indicates the organization would be willing to go a full day (24 hours) without access and lose 12 hours of server production time. If employee wages average $50 per hour and associated overhead costs equal $100 per hour, with hourly revenue of $1,750, the complete downtime and recovery costs would be $47,688. That figure includes productivity and sales losses during the organization's noted acceptable window for system restoration (one day, three hours and fifteen minutes). (Note: Seasonal businesses often have varied hours of operation, so these figures would need to be calculated at different times to reflect those differences.)

DOWNTIME COST CALCULATION EXAMPLE	
Hours the business can operate without access to critical systems:	24 hours
Server production hours the company can afford to lose:	12 hours
Amount of data on key business systems:	1 TB
Normal back up frequency:	Hourly
Optimal data restoration time:	27.25 hours
Location of data (local network or cloud):	Local
Number of employees affected if key business systems fail:	25
Average hourly wage of employees using key business systems:	$50.00
Average revenue generated (per hour) of employees using key business systems:	$1,750.00
Average hourly overhead cost of an employee using a key business system:	$1,750.00
Total cost to business:	**$47,688.00**

Natural disasters and fires may force organizations to go offline for days, if not weeks or longer. According to IDG, an average of seven hours is required for businesses to resume normal operations after a data loss incident. A number of IT managers (18%) suggest it will take 11 to 24 hours to complete that process, if not longer.

No one can predict how much damage a natural disaster could inflict on buildings, power lines, computer systems, and other infrastructure—until after it occurs. Those factors can significantly affect recovery time. A good best practice is to include all possible worst-case scenarios in the long-term business continuity plan.

Some organizations further refine their downtime cost calculations by factoring in specifics such as:

- **Industry Standing/Reputation:** Significant downtime can negatively impact relationships and leave others with a bad impression of the company, especially in highly competitive markets. These incidents can create public relations nightmares for businesses, and rebuilding reputations can be a long and costly process with absolutely no guarantees.

- **Stress:** Disasters are taxing experiences. The long hours and anxiety associated with downtime can negatively affect morale and increase turnover. While those costs aren't easy to quantify, organizational leaders must understand the impact a stressful work environment can have on their people and their operations.

Some companies take a more simplified approach when estimating downtime expenses, extrapolating their labor and fixed costs for various time periods (one hour, one day, one week, etc.) instead of calculating their complete operational costs. That helps management teams quickly estimate their ROI for various disaster recovery solutions.

Top-Down Support Is Crucial

A solid business continuity plan with well-designed policies, processes, and solutions should be an absolute standard. In today's internet-driven environment, organizations leaders must recognize the value of the data they collect and have a least a basic understanding of system restoration processes.

Management buy-in is essential to success. Top-down support reduces resistance and encourages employees to learn more about their own data management responsibilities. For example, owners can stress the importance of their business continuity strategies in company-wide meetings or emphasize the value of these plans in periodic emails and communications. Those conversations should be ongoing, not just a once-and-done proposition that quickly fades from employees' memories.

An effective business continuity strategy covers all departments, so representatives of each group should be involved in identifying critical data and prioritizing its position in the restoration process. Those individuals can

serve as extensions of the IT team, helping educate co-workers and others on the business continuity plan and their own responsibilities.

That same philosophy applies to empowering the people charged with designing, implementing, and supporting the technological side of these programs. Whether employing an in-house IT team to manage the technologies behind these processes or outsourcing aspects of the business continuity plan to trained specialists, the top-down commitment from management is just as critical.

The complexity of these solutions and processes, combined with ever-changing governmental and industry regulations, make it difficult for most organizations to manage these programs on their own. Developing and running an effective business continuity strategy requires people with a particular set of skills and knowledge—and that expertise gets harder to find and more expensive every year.

In fact, the average salary for an IT manager today is approximately $120,000[8] and can be significantly higher for those with specialized degrees, certifications, and experience. Security and disaster recovery expertise—the skills needed to properly construct and execute a business continuity plan—can drive those rates even higher. For example, the average salary for a CISO (chief information security officer) is more than $220,000 per year and, with demand for their services escalating at a dizzying rate, those numbers look quite conservative.

Finding and hiring these professionals is a difficult process, but the spiraling salary demands for those with this type of security and IT expertise will make it even harder to retain their services in the future. A less-complicated and more cost-effective route is to outsource all or some of the design, implementation and support activities around business continuity.

Whether the company's existing IT team collaborates with a third-party provider or completely hands off those responsibilities, that flexibility allows everyone to concentrate on their field of expertise. An outside perspective on the organization's data collection and management processes, infrastructure and existing security protocols truly helps when building the framework for a business continuity plan.

Craft a Practical Plan

As with any project, many of the most important steps when building a business continuity strategy come before putting pen to paper. Preparation is key to ensuring the long-term viability of the organization.

That process can be time-consuming and difficult. Those with little or no experience building a business continuity plan may struggle with the data identification process and weeding through a myriad of compliance requirements.

8. Salary for an Information Technology Manager in the United States, February 28, 2019; Salary.com

The following seven steps can help those charged with developing these plans make sense of it all.

1. Establish a Baseline

The management team must understand the real risks. Knowing every potential catastrophe that could impact their organization isn't as important as understanding its system vulnerabilities—the things that could fail quickly when unexpected events occur. Is the building below sea level and susceptible to flooding? Are key computer systems located in the most secure environments (away from windows and protected by strong infrastructure)? Do employees know what to do during a short term-outage or when under the threat of a hurricane or flood? These critical steps allow businesses to assess their risks so they can build a viable business continuity plan:

- **Prioritize the data.** Which type of information must be protected and readily retrievable at all times? Which files and applications are essential to the continued operation of the company? Should the main facility and its computer systems fail, this information must be readily available at a secure offsite location, whether at another corporate office or a third-party data center. As the business changes, data priorities may also shift, so periodic re-evaluation should be part of the storage, retention, and business continuity plan.

- **Identify potential site-related hazards** such as natural disasters, flooding, wildfires, landslides, cybersecurity vulnerabilities, and other threats. That makes it easier to sell the business continuity story to key stakeholders. Connecting the potential problems with the solutions will help employees visualize the various scenarios and understand their role in a business continuity plan. These threats can be used as examples when testing the viability of the program (an ongoing process).

- **Identify current and potential compliance requirements.** This is where an experienced chief information security officer can really help by mapping the data security and retention requirements of various federal, state, local and industry rules. Ignorance is not a suitable defense for regulators, so organizations must carefully review these conditions and craft plans that address all compliance concerns. Since those rules are frequently updated, companies must periodically assess and alter their business continuity plans accordingly.

2. Assign Responsibilities

Management, IT and others tasked with implementing a plan must sit down and come to a consensus on the fundamental processes, potential issues, and any remedial work that must be completed before it goes into effect. That team must assign responsibilities to those capable of assessing specific issues and potential problems and researching their various solution options. Their mission is to build a list of standard practices that can be implemented in the event of a disaster or temporary business closure. While that task may sound rather straightforward, there are a few points every organization needs to consider when building a plan that should survive the worst possible disasters.

3. Conduct Research

A lot of thought goes into building a business continuity plan. The team must carefully study and embrace all industry and governmental regulations that apply to their organization so they can address each requirement in their strategy.

The complexity of the processes, from data storage and security methodologies to restoration, will require input from multiple departments with different and sometimes conflicting objectives. While top-down support is critical, a solid business continuity strategy requires buy-in from virtually everyone in the organization. Get those groups involved at the outset by carefully studying their work habits and processes and identifying potential issues, and then elicit their feedback on initial drafts of the document.

Of course, that research must also include solutions. Can existing data backup and disaster recovery systems meet the needs of the company's business continuity plan? Will network and infrastructure improvements or a new internet provider be required? Even if the company has an in-house IT team, this is a great place to consult with a business continuity expert to ensure the proposed systems will be able to support the plan in the event of a disaster.

4. Document

Writing may seem like the easy part. However, many companies struggle when it comes time to organize and document their business continuity strategies. There are scores of templates available from suppliers, regulatory authorities and government agencies[9] (to name a few) designed to simplify the process. Even if everyone agrees on a framework, there will still be a significant amount of writing involved. That responsibility should fall to someone experienced in crafting planning documents or with the ability to create informative guides or short tutorial-type scripts. Business continuity plans must be clear, concise, and focus on each step and explanation.

5. Implement

A business continuity plan is a working document. As such, the implementation is merely a matter of communicating the strategy to employees and other relevant parties (investors, affiliates, and partners) and reviewing individual responsibilities in the event of a fire, flood, hurricane or another type of disaster. Organizations should always clarify the differences between a short-term outage and a major catastrophe and review the appropriate responses for each situation.

For example, businesses usually have several days to prepare for a potential hurricane, which gives employees the time to save their work projects, backup all relevant data, and close down their computer systems. However, the window of opportunity for completing those tasks is often a lot shorter or non-existent. If plugged into a functioning power supply, employees usually have no more than 30 to 60 minutes to save and backup those files. Empowering workers with the knowledge of what to do and when to do it is critical to the success of the business continuity plan.

9. Business Continuity Plan, Ready.Gov, https://www.ready.gov/business/implementation/continuity

6. Test

The most expensive investment is one that doesn't work. To ensure each process in the business continuity plan works, they should be tested periodically. While many regulations require annual verification, reviewing the procedures and equipment more frequently allows team embers to spot potential problems and make needed adjustments to strengthen the plan.

Many companies conduct disaster drills where the IT team and others "walk through" each step to ensure everything works seamlessly. Weekend testing can minimize interference with normal work activities. These simulations should include members of the management team, staff, partner organizations, and even suppliers to completely validate the effectiveness of each procedure.

7. Revise and Repeat

This final step deserves extra emphasis. Business continuity plans are fluid and dynamic and should be altered as often as needed to accommodate technological innovations, new threats, and added regulations and reporting requirements. Unfortunately, that process can be time-consuming and could disrupt operations, which is why it may get pushed aside if the management team isn't fully committed to the plan.

Conclusion

Business leaders never know when a disaster could strike. However, by following established best practices and implementing proven technologies in their business continuity plans, they can be more confident their organizations will fully recover from whatever comes their way.

Whenever possible, businesses should locate backup facilities for key business data and applications in different states or regions to minimize risk profiles. Hurricanes, wildfires, flooding and other disasters often affect multiple communities, so relying on a secondary office in the next town or county would not be a suitable business continuity option. A Forrester Research report found that less than 25% of companies locate their recovery sites less than 50 miles from their primary data center, with many choosing locations from 500 to more than 1000 miles away.[10] One caveat noted in recent studies: the increasing availability of cloud options for critical business applications is shrinking the distance requirements.

A good best practice is to select backup locations with different internet and mobile network providers. That will protect the organization from regional carrier failures.

Top level commitment is essential. There is no excuse for losing vital client and employee information in an era with such great technological innovations and established data retention best practices. Management should

10. Forrester, https://go.forrester.com/blogs/13-10-16-how_far_apart_should_my_primary_and_recovery_data_centers_be_good_question/

actively be involved in business continuity planning and seeking options for backup facilities and mobility initiatives. It's their responsibility to ensure quick restoration of vital operations following a disaster.

Business continuity services are no longer optional for the SMB. Data security and retention is a 24-hour-a-day commitment in today's digital-centric business environment. That's why organizations need experienced and knowledgeable professionals who can fully design, implement, and support these critical programs.

Outsourcing those responsibilities is one option. An IT services provider with strong data management and cybersecurity skills can play an invaluable role in the process, helping organizations develop, implement, and regularly test all aspects of their business continuity plans.

For help with your technology, contact your local TeamLogic IT office.

TeamLogic IT is a national provider of advanced IT management services for businesses. With locations across the U.S. and Canada, TeamLogic IT provides managed services, computer consulting and support services focused on helping companies minimize downtime and improve productivity. TeamLogic IT helps businesses compete better through the effective use of information technology.