SAGACENT®
TECHNOLOGIES
Cybersecurity, IT Management & Compliance

How To Avoid Data Loss with Disaster-recovery and Business-continuity Plans

In 2019, the economic losses from 409 total natural disasters exceeded $232 billion USD, according to a according to an Aon (global professional services firm) report, Weather, Climate & Catastrophe Insight: 2019 Annual Report, and only a fraction of these losses were insured. And while it may be tempting to think that these disasters only impacted a small sliver of companies, that is not the case. Nearly three-quarters (71%) of enterprises[1] experienced a downtime event the next year in 2020. If you read the news, it's clear this is only accelerating.

Disasters that can impact your business IT systems can come in a lot of different forms from a natural disaster to an extended power outage or a cyberattack. Many of these can cause you to lose valuable business data.

There are a number of things you need to do to prevent a catastrophic data loss. Some involve hardening your IT systems to prevent attacks. System redundancy provides workarounds for outages. And data backup can help you recover access to data. But here we'll address what you can do if disaster strikes.

The Difference Between Disaster Recovery and Business Continuity

Disaster recovery is a term that refers to[2] planning a business can enact when responding to a catastrophic event, such as a natural disaster, fire, act of terrorism, or an active shooter. Disaster planning requires the business to determine the responses required to ensure that the company can return to safe and normal operations quickly.

Business continuity refers to planning a business can do to determine how to proceed during and following a disaster. It often includes developing contingency plans and a plan for continuing operations even if the company has to move to an alternate location. In addition, business continuity planning often includes events not covered by a disaster plan, such as planning for extended power outages or minor disruptions.

While both planning for a disaster and planning for business continuity involve efforts to deal with sudden events, there are some key distinctions[3] between the two terms:

- Business continuity emphasizes keeping the business operational during and after a disaster. On the other hand, disaster recovery focuses on restoring data access and IT infrastructure after a disaster. Therefore, business continuity looks at the broad picture and determines how to keep the business operational—even under distressing conditions. At the same time, disaster planning focuses on returning operations to normal as quickly as possible.
- Disaster recovery often involves measures designed to keep employees safe. In addition, these plans may instruct the company to prepare for a disaster by conducting fire drills or procuring emergency supplies. With both plans working together, the company shows an interest in protecting the team and the company's productivity.
- The goals of disaster planning and business continuity planning are different. Disaster planning limits abnormal or inefficient system

> Disasters that can impact your business IT systems can come in a lot of different forms

functions, while business continuity planning limits downtime.

- Disaster planning focuses on efforts to get back to full functionality after a disaster. Business continuity plans frequently also include directions on communication methods used during an emergency. For instance, if your primary method of communication is impacted, a business continuity plan may consist of direction on how to maintain other channels of communication, allowing the company to stay open in some capacity.
- A business continuity plan proactively attempts to prevent and prepare for a disaster. In contrast, a disaster plan is reactive and contains only information and instructions that would be required after a disaster has taken place.

These differences illustrate the precise nature of distinguishing between business continuity planning and disaster planning. Business continuity planning is a strategy taken to ensure continuity of operations while minimizing downtime. On the other hand, disaster recovery planning is focused on restoring data and critical applications when IT systems are impacted by a disaster.

This report outlines key considerations to plan for both.

Plan for Disasters

A disaster recovery plan is a guide that lays out all policies and procedures to recover your IT systems and data as quickly as possible.

It should go through all the different scenarios and identify a plan to respond to each. And, while each scenario and organization will have a different disaster recovery plan, there are key elements[4] that should be present in all plans, including:

1. **Goals:** The disaster recovery plan should outline goals for the organizations and departments. Two common goals that should be included are the recovery-point objective (RPO), which tells you how much data loss is acceptable, and the recovery-time objective (RTO), which tells you the amount of time you need to recover all applications.
2. **Threat analysis**: Anticipating any disaster requires identifying the potential for the event. This process may include identifying potential natural disasters that threaten the area where your operations are based or trends in cyber attacks that may be used in a digital attack.
3. **IT assets:** A disaster recovery plan should include a complete hardware and software inventory. This inventory should also discriminate between essential applications, those you will need within a day, and those that can wait a few days. This information can help you prioritize efforts and focus on those applications needed immediately.
4. **Staff roles:** You will need to identify who is responsible for each action item in a disaster recovery plan. Knowing these duties can ensure that staff and leadership are all on the same page and can respond quickly.
5. **Disaster-recovery sites**: Disaster recovery sites refer to alternative sites that could be used for all of the organization's IT assets to be moved to in the event of a disaster.

6. **Response procedures:** The organization can detail which events to anticipate and outline all steps required to restore operations based on a given event. This section of the plan should discuss communication procedures, data backup procedures, instructions for the response strategy, and any post-disaster activities that should be taken after operations are restored.

7. **A crisis communications plan:** Creating a clear strategy for crisis communication can ensure that employers, vendors, suppliers, and customers all know the information they need and understand what steps are being taken to manage the company after the event occurs.

8. **Testing information:** While it is great to have a plan, it can only be effective if everyone is aware of it and knows how to respond. Running regular practice tests a few times a year gives everyone greater exposure to the plan and its content. You can also look for red flags or procedures in the plan that may need to be optimized. For instance, a practice test may reveal that the internet connection at a backup location is insufficient to restore operations adequately. Running this test in advance allows you to address the issue before an actual disaster occurs.

9. **Plans for updating:** Many comprehensive disaster response plans lose relevance over time. As technology, solutions, and staff members change, the plan can quickly become outdated. Writing deadlines into the plan for regular reviews is one way to ensure you update it to reflect current information.

Because it can present unique challenges, we'd also like to explore what you can do to prevent data loss through a ransomware attack.

> The disaster recovery plan should outline goals for the organizations and departments.

Paying the Ransom Doesn't Mean Your Data Is Returned

As it has for the last several years, ransomware continues to grow as a cyber threat. While it is difficult to estimate the number of ransomware attacks, it was likely around 750 million[5] in 2021. Ransomware attacks present a threat to business continuity and data security.

Many people think that the worst outcome of a ransomware attack is paying the ransom. After that, you get your data back, right? Well, not always. Even if you have paid a ransom, there is no guarantee that you will get your data back. There are many instances[6] where things don't work this way:

- A hospital in Kansas sent money to meet a ransom demand. After, the hackers did not return the data but demanded additional money.
- A small retailer paid a ransom, but the virus malfunctioned and only partially decrypted the company's files.

And these aren't isolated instances. There is a one in five chance6 that you won't get your data back after paying a ransom. There are three common reasons for this:

1. The decryption system could fail
2. The attackers could demand additional money
3. You could become a target again

Unfortunately, it can be very costly to pay the ransom, especially if it doesn't result in the return of your data. The average ransom is approximately $230,000. However, this figure can be substantially higher when the targeted company is in healthcare or finance.

Additionally, the cost of remediation after a ransomware attack is $761,106, and the average downtime a company suffers after an attack is 19 days. This downtime is often accompanied by a substantial loss of revenue.

And in addition to the direct costs of a ransomware attack, companies that have suffered a data breach may be the target of legal action. The bottom line is that ransomware attacks are expensive, and unfortunately, even paying a ransom doesn't always result in a positive outcome.

There is a better alternative. Creating a disaster recovery plan can be the key to weathering a ransomware attack. Approximately 96% of companies[7] with a reliable backup and disaster recovery plan survive a ransomware attack. When these efforts are combined with preventative measures directed at ransomware attacks, you can greatly reduce your risk. And this is much better than relying on cybercriminals to keep their word and return your data.

A disaster recovery plan can ensure business continuity through multiple methods. These methods allow the company to restore critical systems within minutes, even after a ransomware attack. The benefits include:

- The ability to minimize interruptions to normal operations
- Limiting the extent of the disruption and damage
- Minimizing the economic impact of the interruption
- Providing for a smooth and rapid resolution without impacting services or product delivery

In addition to this, a disaster recovery plan will ensure that you still have access to your data, which removes the leverage that cyber attackers have. And without leverage, you have no reason to pay a ransom. You keep your data and your money.

Maintaining Business Continuity

Business continuity refers to planning a business can do to determine how to proceed during and following a disaster. It often includes developing contingency plans and a plan for continuing operations, even if the company has to move to an alternate location. In addition, business continuity planning often includes events not covered by a disaster plan, such as planning for extended power outages or minor disruptions.

Why a Cloud Computing and Remote Work Strategy Should be a Part of Your Business-continuity Plan

Since many organizations have already addressed enhanced security and remote access, they can minimize the impact of a disaster that devastates a central location. For instance, the effects could be devastating when a natural disaster or fire destroyed a building in the past. Not only did the company suffer a loss of space where employees could be productive, they typically lost much of their IT infrastructure and data assets. And a loss of this magnitude could cripple the business for weeks or even months. In some instances, the company may never recover what was lost.

But, with the move to remote operations, many companies have opted to put cloud solutions in place and create a decentralized infrastructure configuration. The benefit of this arrangement is that, in a disaster—even if one location is completely devastated—you will still have digital resources to help recover operations and likely have minimal data loss.

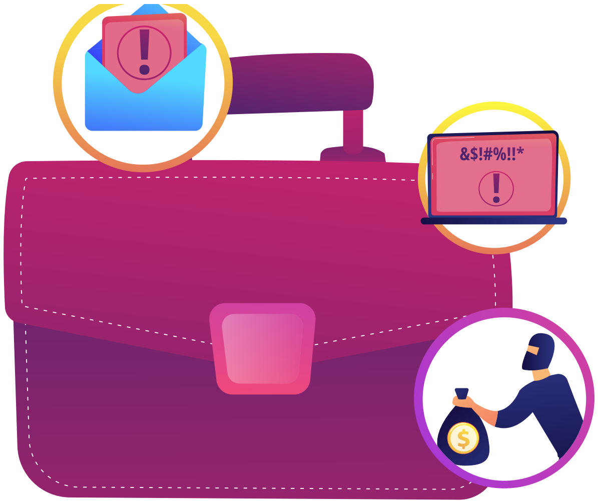
However, business-continuity plans should also identify backup options, which can benefit your business in various ways. Sometimes, simple errors or mistakes can result in data loss when moving to a remote structure. Backup systems identified through disaster planning can be useful in these scenarios, in addition to actual disasters.

Disaster Planning Is Evolving Along with Technology

Remote work strategies and cloud computing are two elements increasingly being seen as part of business-continuity planning. The number of companies offering remote work or hybrid schedules has increased dramatically[8] in the past few years, with 16% of companies reporting that they are fully remote and two-quarters of all U.S. employees working remotely at least part-time. And these statistics only refer to companies where remote operations are a normal part of the organizational structure. Many companies that do not offer remote working options may rely on a remote work strategy in the event of a disaster.

Fortunately, many cost-effective options, such as cloud computing, can also protect business continuity.

Businesses today are using the cloud to provide fast, cost-effective, and easy disaster-recovery solutions—allowing organizations to back up and recover their vital data and tools so that a business-continuity plan can be quickly implemented if a disaster occurs. This addition to a disaster plan can transform your ability to restore operations and help you achieve this goal in minutes rather than days or weeks.



Additional benefits of cloud disaster recovery[9] include:

- **Flexibility:** Relying on cloud services for disaster recovery provides organizations with greater user control in a cost-effective way.
- **Adaptability:** Cloud disaster recovery provides adaptability by allowing organizations to realign and reallocate resources on demand.
- **Availability:** Cloud architecture often relies on multiple data centers to support business-continuity plans. This feature ensures that the apps, platforms, and data resources are available when your company needs them.
- **Scalability:** Cloud resources let your business scale its IT resources up or down with little effort, ensuring that you only pay for the resources you need.
- **Reliability:** Cloud redundancy ensures that data is always there and accessible when you need it. Even if a natural disaster hits the cloud resources in one area, the redundant locations can still provide the resources you need.

As you can see, there are many benefits to incorporating a remote work strategy and cloud computing resources in your business-continuity plan. And while these changes often contribute to enhancing your business's ability to rebound after an event that would otherwise cause a business interruption, they do introduce additional concerns.

For instance, moving data to the cloud may come with compliance concerns. Additionally, your company may lack sufficient security resources to support remote working. It's often beneficial to review your current disaster plan and identify additional needs or resources before relying on cloud computing or a remote-working strategy during a disaster.

Failing To Plan Is Planning To Fail

When companies face difficult challenges, it's crucial to have the proper plans to guide and coordinate multiple efforts to restore business quickly. Without them, the outage or downtime following an event may be prolonged, contributing to additional financial losses.

Therefore, comprehensive planning often requires that your company have both plans, with the disaster recovery plan as a component of a more comprehensive business continuity plan.

Plan with Sagacent Technologies

As you can see, there are many aspects to disaster recovery plans. To learn more about creating a comprehensive disaster recovery plan, the next steps, and solutions that meet your budget and business needs, contact Sagacent Technologies today.

Sagacent Technologies also offers technology management and support, including proactive/ preventative maintenance, onsite and offsite data back-ups, network and security audits, mobility solutions, disaster planning, and emergency business resumption services.

Footnotes

1. https://connect.teradici.com/hubfs/Jumpstart%20Your%20Remote%20Work%20and%20Disaster%20Recovery%20Strategy.pdf
2. https://www.ucf.edu/online/leadership-management/news/business-continuity-vs-disaster-recovery/
3. https://www.insightoutdata.com/blog/business-continuity-vs-disaster-recovery
4. https://thetechportal.com/how-many-ransomware-attacks-have-been-attempted-in2021/
5. https://thetechportal.com/how-many-ransomware-attacks-have-been-attempted-in-2021/
6. https://www.bralin.com/does-paying-ransomware-work/
7. https://www.osgusa.com/backup-disaster-recovery-plan/?msclkid=c16ff97bbc4d11ecbc8e7a30e5322f67
8. https://www.zippia.com/advice/remote-work-statistics/
9. https://www.veritas.com/information-center/cloud-disaster-recovery

Contact Us

2010 El Camino Real #766, Santa Clara, CA 95050-4051
Phone: 408-248-9800 | Fax: 408-248-9700
Service: support@sagacent.com | Sales: sales@sagacent.com | Inquires: info@sagacent.com

SAGACENT TECHNOLOGIES
Cybersecurity, IT Management & Compliance

Visit sagacent.com to learn more.

About Sagacent

Founded and Headquartered in San Jose, CA, in 2000, Sagacent Technologies, Inc. is a leading technology solution provider to small and mid-sized businesses offering our customers a full range of solutions.

Copyright © 2024 Sagacent