SUN DOG

YOUR STRATEGIC IT PARTNER

A recipe for disaster recovery:

3 STATISTICS
your business needs to know

TABLE OF CONTENTS

Why is it important for SMBs to have a disaster recovery plan?

You can never tell when your small- or medium-sized business (SMB) will be hit by disasters like malware attacks, natural calamities, and faulty hardware or software that lead to business disruption, among other things.

For instance, no one could have ever foreseen that the COVID-19 pandemic would significantly affect the operations of many companies around the world. Because employees were forced to work from home, they had to access corporate applications and data using their home internet connections. Unfortunately, home networks are not as secure as corporate networks, so using these could put a company's confidential data at risk of cyberattacks and data loss.

And during the height of the pandemic in 2020, healthcare organizations were targeted by ransomware. In Germany, numerous healthcare facilities were attacked, which led not only to data loss, but also to a patient's death.

To mitigate the negative effects that disasters may cause, you must have a robust disaster recovery (DR) plan.

Why do businesses need a robust DR plan as part of their overall business strategy?

Let's take a look at some reasons why it's essential to have one:

1. **A DR plan protects data from various threats.** Data loss can easily happen due to technical malfunction, physical damage, human error, or other data security threats.
2. **Data security plans aren't foolproof.** With the growing complexity of the cybersecurity landscape, companies are likely to make mistakes with their data and information security.
3. **Data security plans aren't foolproof.** Without data, your employees will most likely have difficulty accomplishing their tasks, which can slow down or completely halt business operations. And the longer data remains unavailable, the greater the negative impact is on your organization.
4. **It's costly to recover lost data.** Data recovery services typically cost between $99 and $2,000. But if you have a DR plan, you'll be able to reduce the scope and amount of damage.
5. **A DR plan can help you resume operations sooner.** A DR plan can minimize the impact of a data loss incident, so you can restore business operations and resume serving your customers. Otherwise, prolonged service interruption could ensue, causing you to lose customers.

DR plans are critical for SMBs as well. Here are three statistics that show why this is the case.

Statistic #1: Almost one in three data breaches involve small businesses

According to insurance and financial services company Nationwide, roughly 68% of small businesses do not have a DR plan in place. When asked why they lack a disaster recovery plan, 21% of small business owners said that having one is not their priority.

These statistics are alarming since the Verizon 2020 Data Breach Investigations Report found that small businesses made up 28% of data breaches. This shows that all businesses — regardless of size — must prioritize cybersecurity.

Why are SMBs vulnerable to cyberattacks?

1. Negligence when it comes to cybersecurity

Many SMBs don't see themselves as cybercrime targets. They believe that their data is not attractive to hackers, so they allocate very little money to cybersecurity. This makes their IT infrastructures easier to infiltrate than those of bigger companies that can invest in robust security.

2. SMBs are gateways to large enterprises

Many large enterprises provide access to their systems and data to SMBs that serve as their contractors or vendors. The problem with this is that cybercriminals are aware of the poor cybersecurity habits of SMBs, so they're exploiting these to gain access to the IT systems of large companies. This shows that a cyberattack can impact not just your business, but also the companies you work with.

To mitigate this risk, invest in security solutions such as antivirus software and intrusion detection systems, virtual private networks, firewalls, and the like. Educate your employees in data security as well; a well-trained workforce plays an important role in reducing the risk of data breaches.

3. Lack of proper cybersecurity training

Your SMB might have gone through cybersecurity training sessions in the past year. But this is all for nothing if you fail to update your protocols or follow up with practical exercises.

Remember that cybersecurity is a constantly changing environment, and cybercriminals will always find new ways to attack businesses. This is why it's ideal to keep your training materials updated. Here are some topic ideas for your next cybersecurity awareness training session:

- **Safe internet habits:** This includes refraining from downloading files or installing programs from unknown sources, and not clicking on suspicious links or emails.
- **Removable media:** External hard drives and flash drives are vulnerable to viruses, spyware, and ransomware, which could threaten the security of your data. Educate your staff about the repercussions of using removable media. You may also opt to disable access to removable storage devices on office computers if necessary.
- **Social media:** Cybercriminals can use information on your social media pages to hack your social media accounts and distribute phishing emails and malware to your partners and clients. Your competition can also assume control of your accounts and post malicious content that may deal a blow to your business's reputation.

  To prevent social media attacks, refrain from revealing too much personal information online and use a unique password for every account you have. Make sure that only the employees managing your social media initiatives can access your company's accounts. Lastly, restrict access to social media sites on work devices
- **Physical security controls:** Disgruntled employees or visitors can steal sensitive information from your company by accessing idle computers, copying handwritten login credentials, or connecting to your Wi-Fi network. To prevent this, use security measures such as installing security cameras and locks on doors to limit physical access to company devices. You must also teach your staff to be aware of their surroundings, especially the people around them.

Statistic #2: Hardware failure is the leading cause of data loss

According to data recovery firm Stellar, hardware failure is the main cause of data loss among businesses, aside from power loss and data corruption. And a StorageCraft study found that among all hardware problems, hard drive failure is the most common one at 80.9%, followed by power source failure at 4.7%. An undetermined failure is almost as likely to happen as a motherboard failure or other internal component failures.

The dangers of hard drive failure

Typically, businesses store their data on their computers' local hard drives. When these drives crash, a mad scramble to recover data always ensues.

Why do hard drives fail? Because hard drives are mechanical devices, they will wear out over time, even with proper care and maintenance. Around 60% of hard drive failures happen because of predictable mechanical failure, while the remaining 40% occur due to misuse. Hard disk failure may happen if any of the following happen:

- The computer is bumped or jostled while it is running.
- The motor that allows the hard drive to spin fails due to bad bearings or other components.
- The computer's air intake is clogged or the filter isn't working properly.
- The computer is too hot while the hard drive is running.
- A sudden power failure happens while the disk is writing or reading information.

Because hardware failure can happen anytime, businesses must always have data backups.

Statistic #3: The costs of downtime are high

Businesses of all sizes will always be at risk of suffering downtime, no matter how well they secure their IT infrastructure. And when a company cannot carry out its core business functions and its employees are unable to serve current and prospective clients, it is bound to suffer losses.

For example, downtime costs businesses between $10,000 and over $5 million per hour. To make things worse, it takes about seven hours on average for organizations to return to normal operations after a data loss incident, with 18% of IT managers saying that it can take 11 to 24 hours, or even longer.

Aside from revenue losses, downtime can also result in the following negative outcomes:

- Business disruption
- Reputational damage
- Loss of customers
- Decreased productivity

For example, in March 2021, IT service management company CompuCom suffered downtime because of a malware attack, forcing it to suspend some of its services. The organization wasn't able to restore some of its operations until 16 days after the cyberattack. CompuCom not only lost about $8 million in revenue, but it also had to spend $20 million to restore its critical operations and resolve other issues stemming from the attack.

Healthcare is one industry that's vulnerable to the financial costs of downtime. According to Comparitech, ransomware attacks cost the healthcare industry $20.8 billion in downtime in 2020, which is twice the number from the previous year. The number of ransomware attempts against the industry in 2020 more than doubled as well, making it difficult for some healthcare organizations to provide patient care during the pandemic.

How do you develop a DR plan?

When it comes to disaster recovery for your business, you can either create your own DR plan or avail of Disaster Recovery-as-a-Service (DRaaS) services. Let's take a closer look at each option:

Option 1: Create, implement, and test your own DR plan

CREATE

To develop a plan, you must first assess your organization's needs and risks. Collaborate with all stakeholders so that everyone's concerns are factored in. Then, test the plan regularly and constantly update it to ensure its effectiveness. Here's how you can create your disaster recovery plan:

1. **Make a list of critical jobs.** Critical jobs are those that keep an organization functioning and often vary from business to business. For example, in an accounting firm, critical personnel would include the accountants.

   Have strategies for keeping critical staff working during a disaster, such as relocating them temporarily or having them work from home.

2. **Select your backup media.** It's important to choose the right storage media when creating your backup plan. Here are a few options:

   - **USB flash drives:** These are data storage devices that have flash memory and integrated USB interfaces. Not only are they portable and inexpensive, but they can also be used to back up data from several devices.

     USB flash drives, however, can easily be misplaced, making them unsuitable for long-term data storage. They are better off used as intermediate backup solutions.

- **External hard drives:** These are portable hard drives that can be connected to a computer through a USB port. They have the lowest cost per gigabyte among backup devices and boast fast transfer rates, enabling businesses to back up a large amount of data in a short time.

  One of the disadvantages of using external hard drives is that you'll need to manually and regularly update your backups to include the latest versions of your files and data. There's also a risk of your hard drives being stolen or misused. For example, a disgruntled employee may deliberately corrupt a hard drive's contents or take the device with them when they leave your company.

- **Network-attached storage (NAS):** NAS is a server for data storage that can also be used as an email server. It can operate either wired or wirelessly, and has a dedicated IP address. NAS also features data redundancy, which generates a backup of your backups to ensure that your files are always available.

  NAS, however, cannot be scaled beyond system limits, so you have to buy additional hard drive bays should you need more capacity. It can also be complicated to configure NAS to protect it from malware.

- **Cloud storage:** The cloud allows users to access data from anywhere at any time using any internet-connected device. It also enables businesses to pay for only the cloud resources they consume. Cloud service providers (CSPs) handle the installation, management, and maintenance themselves, so your team can focus on more important matters.

  Some CSPs, however, don't implement strong security measures, potentially exposing your data to cyberthreats. It's therefore crucial for your business to find a CSP that specializes in data regulations compliance and uses robust cybersecurity protocols.

3. **Make an inventory of essential and supporting office equipment.** Have your employees list essential office equipment. This typically includes office desks and chairs, computers, computer software, and telephones, among other things.

   Consider as well all the office equipment used in the background. For instance, telephones need to be connected to a phone network, while computers must be hooked up to a server. Supporting equipment may also include copies of important software, backup servers, and safes.

4. **Make plans for installing temporary work spaces.** A disaster may necessitate relocation or alternative working arrangements, so you will need to plan for this as well. Scout spaces where your staff can work from temporarily, such as a co-working space in your area, or create a remote work strategy. If your neighboring businesses will allow it, you may consider sharing an office space with them while repairs or restoration works are being made on your own.

5. **Plan your budget and insurance.** You might also need new equipment after a disaster strikes your company. Estimate the cost of the piece from your prepared list of office equipment and factor these into your budget, as well as the cost of insurance. Cyber insurance is essential in helping your company recover after a data breach and save you from costs that can include revenue loss, business disruption, legal fees and equipment damage, among other things. It can even help protect your company before a breach occurs.

6. **Share and secure your DR plan.** It's important for everyone in your organization to know about your DR plan and what it contains so that they know what to do in case a disaster strikes.

   Assign a person or team who will be responsible for implementing your DR plan, and ensure that one or more copies of the plan are stored digitally or off-site. Also, keep copies of all critical software, backups, and documents using a cloud storage service such as Citrix, Dropbox, or OneDrive, or on an external hard drive kept in a secure location.

Typical Structure of a DR plan:

1. **Goals -** The things your company aims to achieve in the face of a disaster, including your recovery point objective (RPO), or the data your business can afford to lose and your recovery time objective (RTO), the maximum downtime allowed for each critical system.
2. **Personnel -** The people resposible for executing your DR plan
3. **IT inventory -** A list of hardware and software assets, their criticality, and whether they are leased, rented, or owned.
4. **Backup procedures -** How and where exactly each data resource is backed up, and how you can restore from a backup.
5. **Disaster recovery procedures -** Your emergency response to minimize damages, and reduce the instaces of last-minute backups.
6. **Disaster recovery sites -** A service that provides fully equipped office facilities immediatedly available for your business to continue critical operations.
7. **Restoration -** The procedures for recovering from total systems loss to restoring full operations

IMPLEMENT

A DR plan isn't executed only when a disaster occurs — it is implemented immediately to mitigate the adverse consequences that a disaster may cause. This means executing your data backup strategy and regularly performing disaster recovery exercises, among other things.

Remember the following when implementing your disaster recovery plan:

- **Have triplicate copies of your data**
  You must have at least three copies of your data. The first copy is the original version that you actively use at work. The second copy should be kept on site, while the third one is your off-site backup that is usually hosted on the cloud.

  Why do you need two data backups? For one, if your on-site copy becomes unavailable due to a power outage or data corruption, you could use your second backup. Secondly, with your on-site copy, you can restore data immediately because you have physical access to your files.

  Off-site backups are especially useful in the event of local disasters. Experts recommend that off-site backups be stored in data centers that are at at least 500 miles from where your primary copy is kept. This means your off-site backups won't be affected by any accident or natural catastrophe that hits your offices. These backups will also be safe from ransomware attacks on your network.
- **Ensure your hardware and software are up to date**
  Cybercriminals exploit software and hardware vulnerabilities to attack systems, as evidenced by past data breaches. By updating your systems regularly, you don't just get new features and an improved performance, but you also patch security holes that may be used to infiltrate your IT infrastructure.

- **Regularly monitor your network and devices**
  Implement a network monitoring tool that can constantly monitor your devices' health and performance. Network monitoring solutions help you detect problems early, enabling you to resolve issues before they can cause disasters.
- **Train your employees**
  Your employees are vulnerable to cyberattacks, so train them on cybersecurity best practices regularly. For example, teach them to be wary of every email or website they open, and refrain from downloading unsolicited attachments.

  You can also simulate a malware or phishing attack to test your employees' reaction times. Such simulations will help you identify your teams' strengths and areas for improvement to prepare your business for future cyberattacks.

TEST

Once you've created your disaster recovery plan, you need to do the following:

1. **Test your DR plan regularly.** It's not enough to just create a disaster recovery plan — you need to evaluate its effectiveness and address any issues. Test your DR plan by running backup simulations to see if they work to check whether employees understand your company's DR protocols.
2. **Always have a postmortem.** After a downtime event, hold an incident postmortem with your team. Discuss the details of the incident: how and why it happened, what were its impacts, what measures were taken, and what should be done to prevent a downtime event from happening again.

Option 2: Avail of DRaaS

Many businesses don't see the importance of disaster recovery until it's too late. But as organizations switch to a remote work setup and find new ways to make data accessible, the general attitude toward DR is finally changing. In fact, it is predicted that the Disaster Recovery-as-a-Service (DRaaS) market will grow by 18.4% between 2021 and 2026.

WHAT IS DRaaS?

DRaaS is a cloud computing service model that allows businesses to back up their data and IT infrastructure on a third-party cloud environment. It also enables companies to provide the DR orchestration to recover IT infrastructure access and functionality after a disaster.

With the DRaaS model, a business doesn't have to own all the resources or handle disaster recovery management. Instead, they can rely on a DRaaS provider.

HOW DOES DRaaS WORK?

DRaaS replicates and hosts a business's servers in a service provider's facilities rather than on the business's premises. In case of a disaster, the disaster recovery plan is executed on the provider's facilities.

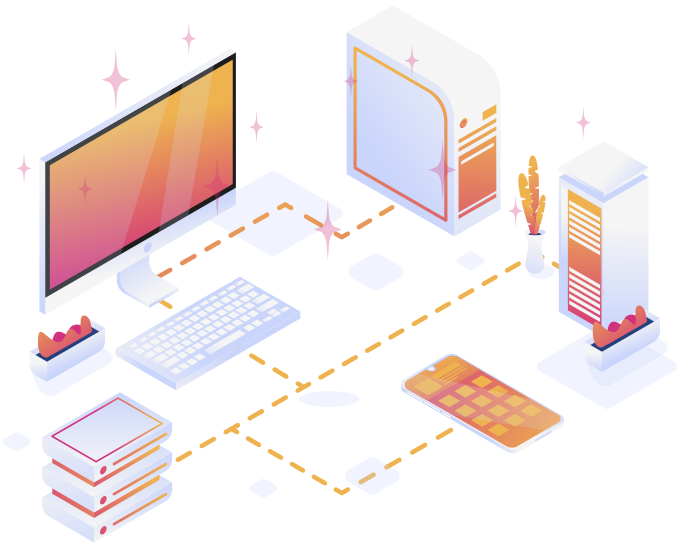
Businesses may purchase DRaaS plans via a subscription model or a pay-as-you-go service that allows them to spend money only when a disaster strikes. This makes DRaaS a cost-effective solution, as it eliminates the need for businesses to maintain their own off-site disaster recovery environment.

It's important to note, however, that issues such as a lack of data redundancy, poor security, or data mismanagement may arise anytime. Make sure that all of your disaster recovery requirements are specified in the service level agreement between you and your provider.

IS DRaaS RIGHT FOR YOU?

Let's take a look at the three most popular DRaaS models:

- **Managed DRaaS:** In this model, the DRaaS service provider takes over all responsibilities related to a business's disaster recovery strategy. This requires the business to remain in close contact with the provider to keep the latter updated on any infrastructure, application, or service changes. A managed DRaaS model is ideal for organizations that don't have the expertise or time to manage their own disaster recovery plan.
- **Assisted DRaaS:** This DRaaS model is ideal for businesses that want to maintain control over some assets of their disaster recovery plan, or have unique applications that might be difficult for a service provider to manage. The provider will only offer their expertise on optimizing disaster recovery strategies.
- **Self-service DRaaS:** In this model, the client is responsible for the planning, testing, and management of their disaster recovery plan. They are also in charge of hosting their own infrastructure backup on virtual machines in a remote area. Self-service DRaaS is ideal for organizations with internal DR expertise and enough IT bandwidth to manage their own recovery environment.

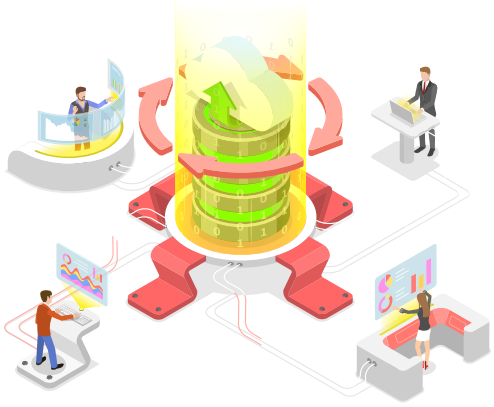


Sundog can help you prepare for any disasters

The last thing you want is for your precious data to be wiped out due to a malware attack, server crash, natural disaster, or large-scale data exfiltration. And without a proper disaster recovery plan, your business may suffer financial losses and reputational damage, among other things.

Fortunately, you don't have to face the challenges of disaster recovery alone. Outsourcing DR planning and implementation to a reliable managed IT services provider like Sundog can help.

As your disaster recovery partner, we'll set up and execute a cost-effective data backup strategy. Our experts will also proactively monitor your IT infrastructure for threats that may affect your business's operations. What's more, we will perform routine restoration tests to ensure that the rate of recovery matches your maximum acceptable downtime. And when disaster strikes, you'll be set up so that your organization can continue to run applications and access data without paying excessive costs. The best part? You only need to pay a flat monthly fee that's cheaper than hiring an in-house disaster recovery team.



Want to learn more about our disaster recovery services?

CONTACT US TODAY!

Phone: **(815) 991-2400** Email: **yourteam@sundogit.com**

SUNDOG
YOUR STRATEGIC IT PARTNER

www.sundogit.com