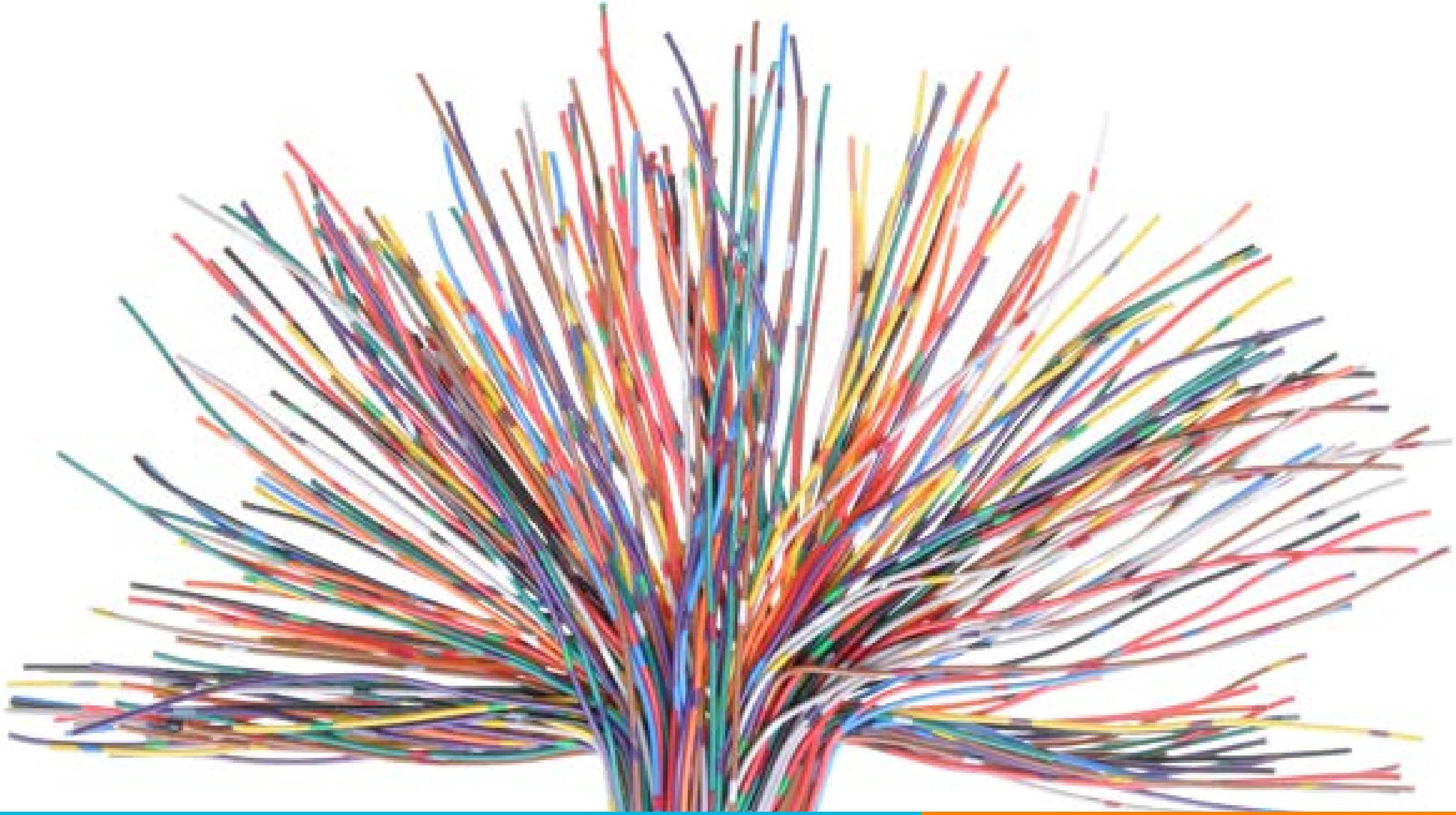
The Resilient Organization

A Guide to IT Disaster Recovery



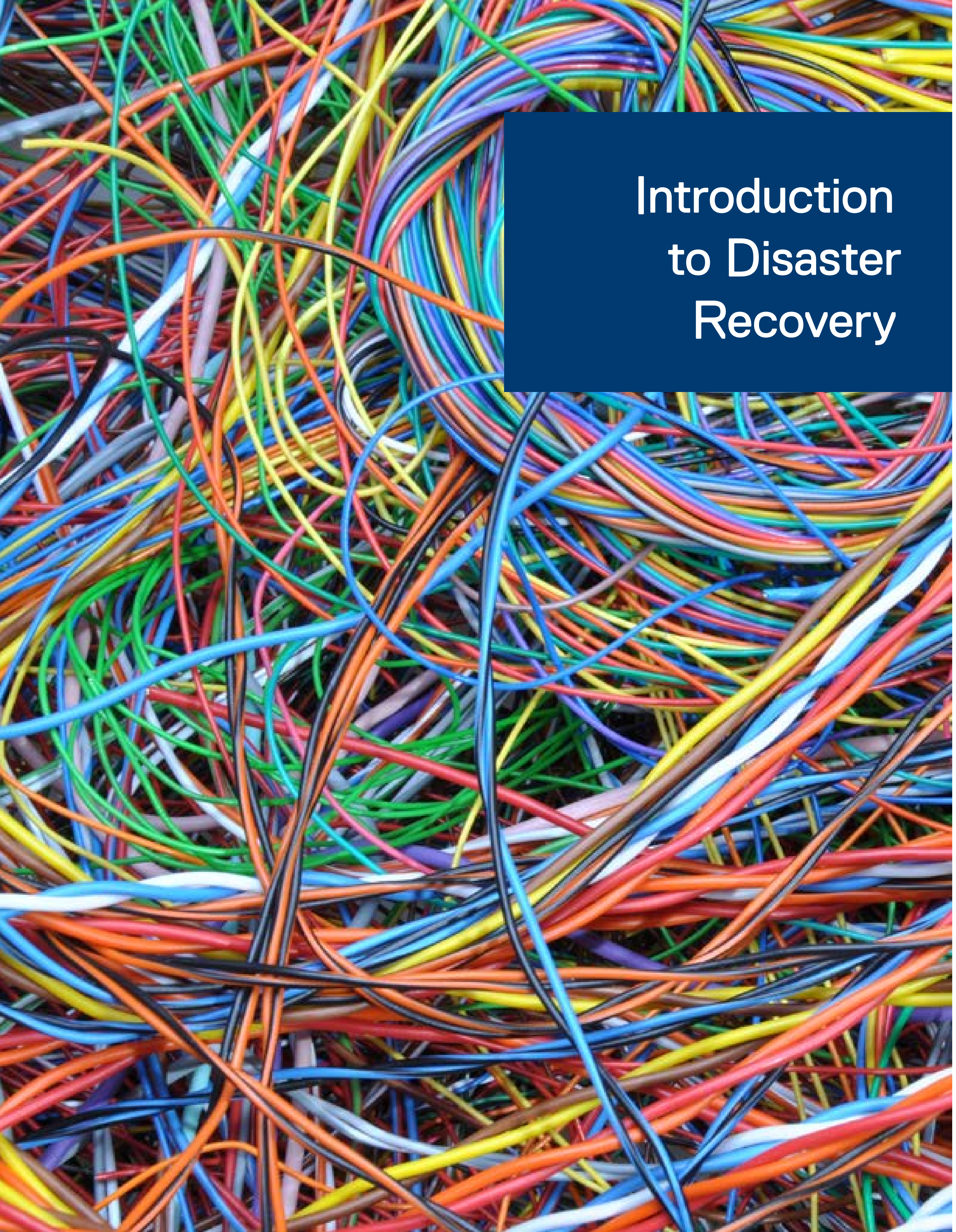
CDP Center for Disaster Philanthropy

techsoup

Contents

Published by TechSoup Global

Modern Nonprofits Use the Cloud



Introduction to Disaster Recovery

This guide is designed for those who have been tasked with moving their organization through the recovery process after a disaster has struck.

You may or may not have any educational or professional background that pertains to information technology. You might have advance warning of a disaster that allows you time to prepare, or you might unexpectedly find yourself in the middle of a disaster.

Don't despair. This guide will provide you with the basics you need to begin recovering from a human-made or natural disaster.

Note

This guide is not intended for organizations whose early rescue or relief operations may put staff members in danger. For those in dangerous situations, please refer to the local Red Cross at http://www.redcross.org/get-help or Red Crescent at http://www.ifrc.org/en/news-and-media/current-operations/.

Recovering from Disaster

Disaster has struck.

You might not have had any warning; you might be unprepared to move forward. Take a deep breath. Recovery is a process, not an event, and nurturing your stamina for the long term will be one of the ways you support your organization.

Or, if you've had the good fortune to prepare for disaster, your prior activities will support your recovery and rebuilding efforts. The careful collection of information and decision making that went into designing your Continuity of Operations Plan (COOP) will launch your organizational triage, and restart your systems and services.

In either case, this section will guide you in rebooting the IT infrastructure of your organization.

We'll walk you through

questions to guide your work plan,
how to reconnect with service providers,
how to retrieve data and files, and
how to assess damage to your equipment.

Rebuilding Your Organization

Initially, your organization will identify what needs to be done and in what order. Then, you can work to obtain the resources, funds, advice, and technology that you will need to begin the recovery process.

Until you have official confirmation from emergency management personnel that it is safe to move away from shelter, do not do so.

If you have access to a phone or electricity and can use the Internet, check for updated safety information with local city or county officials, fire and safety responders and utility providers, FEMA at www.fema.gov, or with early relief providers, such as the Red Cross.

Make sure that you rely on dependable outlets, such as those listed above and others such as disasterphilanthropy.org that provide regular updates on domestic and international disasters and offer helpful tips and support for disaster recovery funding.

Activate your COOP if you have one. Regardless, set up your project teams, and schedule regular meetings (in-person and otherwise) of key decision makers.

Every organization will have different technology priorities after a disaster. However, there are some general guidelines that can help you to develop a good technology triage list:

1 Communication is very important. In most cases, the first priority during and immediately after a disaster is to reestablish communication with the outside world. If the disaster is widespread, communication systems are likely to be overwhelmed, so prioritize who needs to be reached first.

Contact your insurance providers to begin the claims process and to deploy their agents, adjusters, and restoration service providers to your site.

Consider your constituents. Focus on services, functions, programs, and audiences first, before you consider machines, networks, and applications. Refer back to your COOP, if you have one.

Who supports you?

Whom do you support?

Who relies on you the most?

Who might be suffering as a result of the disaster and be in need?

Which programs must continue through the time when you will rebuild?

Which ones can be postponed?

The demand for your services may increase after a disaster, so you need to be realistic about how many constituents you can serve if your organization or members of the staff have suffered damages.

2 Identify any equipment that's been damaged or lost. Insurers may provide temporary equipment while yours is being restored or replaced. Use this information to decide what to do first. Restoration and repair of systems can take a significant amount of time. In order to succeed at triage, you will need to focus your efforts where they will have the most impact.

3 If there will be a delay in restoring Internet service in your office or in the homes of staff members, consider collaborating with another organization whose services may be intact, or working with organizations and businesses that might have large phone and/or computer banks (public libraries, schools and universities, etc.).

Files and Databases

If you have onsite backup storage

Think about your server(s). Recovery of your server may be a high priority, since it is essential in order to recover your data and to restore your network. Attempt to recover the server only if the power and network are in good enough condition to warrant its revival.

If you have data that is stored in a remote system, you might not have the consistent power and bandwidth to restore your system sufficiently. Again, focus on the data and systems that will have an immediate impact post-disaster.

If you have a backup, try to restore it only if your equipment is stable enough for recovery. If you have a network attached storage (NAS) or removable hard drive, verify that its status lights come on. Also check that you do not hear any abnormal sounds when you plug it in. However, if there is even a remote chance that your power is unstable, then you should abandon the attempt to restore.

If you have lost data during a disaster and your backup plan lacks a strategy to address this sort of catastrophe, there's still hope.

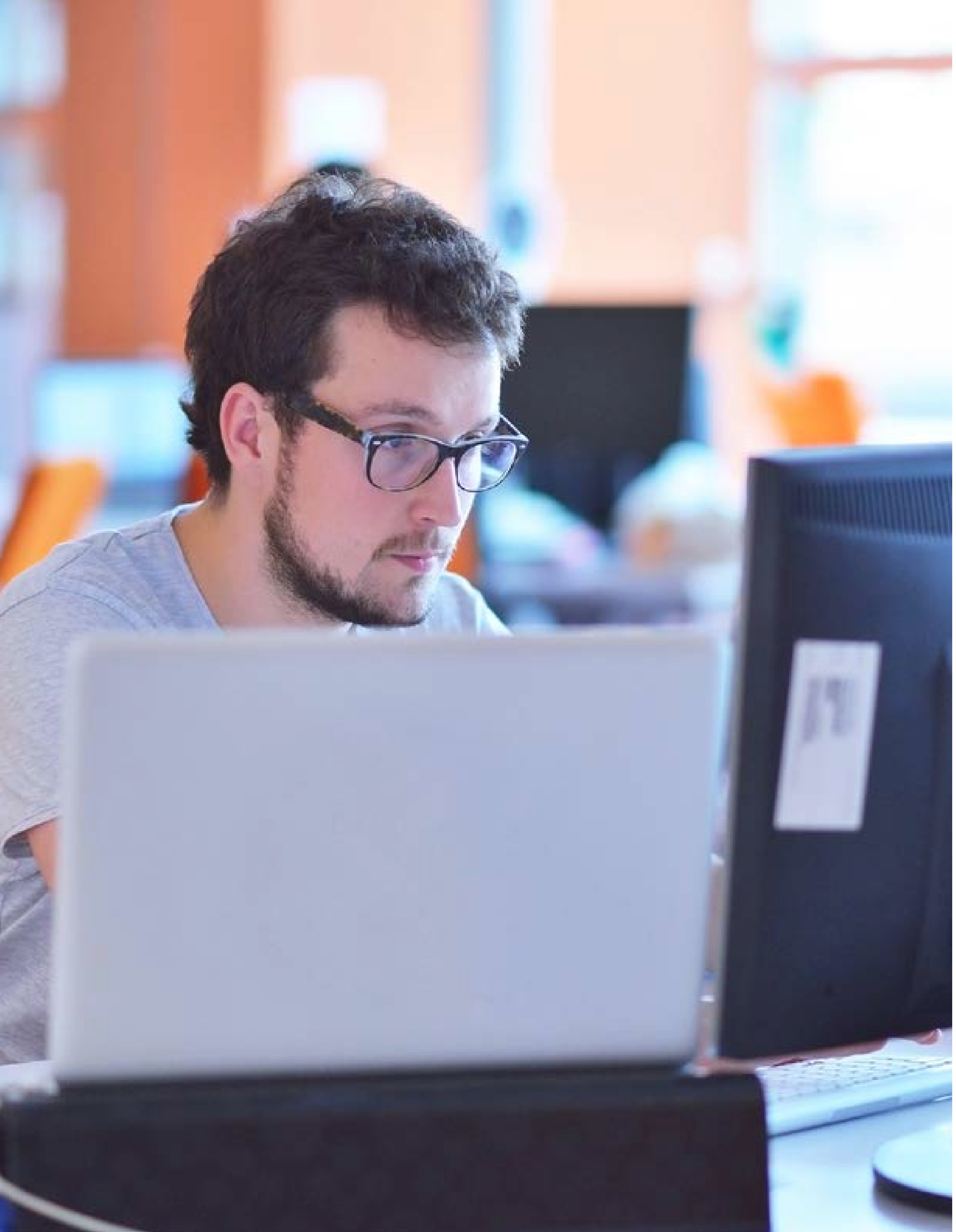
The information that follows can help in your data recovery efforts:

Look for other places where you might have inadvertently stored your data. Perhaps you emailed copies of your files and what you need is an attachment to an email. Perhaps printouts of the data exist that you can re-enter (data entry is often less expensive than hired help from technology experts).

If you do find a copy of your data, back it up and make a copy before you do anything else. Use this copy only and save the original in case something goes wrong with the duplicate backup.

Look for the name, type, and model number of your computer anywhere on the case. Try to find the recovery discs for the operating system. Remember to consider warranties and manufacturer support. Call the manufacturer to see if it can help fix your computer.

In the event that backup media and hardware are unreachable or unusable, you'll need outside help to recover the data. There are many companies that recover data. Costs vary — it depends on the level of damage and the amount of reconstruction that is necessary. Go back to your insurance review to determine if this type of service is covered. If the lost information is extremely important to your mission, such as your donor list, you might want to pay for data recovery.



If your backups are in the cloud

Here are some questions to consider as you plan your recovery:

Do you have the bandwidth and network capacity to restore from cloud backups?

If you plan to restore from the cloud to on-premises infrastructure, how long will that restoration take?

Can your backup provider mail you physical media, in the event that you cannot fully restore via the Internet?

Lost passwords

Even though a system is functional or revived, you still may have lost the passwords to access it.

Here are some ways to restore access.

Windows computers

There are many ways to restore a lost Windows password. Methods vary by Windows version. Generally, you'll need to download an image ISO file to create a boot disk, or download a piece of software to overwrite an existing password. This can be a complicated process, so unless the recovery is extremely urgent, it is advised that you leave this process to your IT consultant or other IT professional.

Apple computers

You can use a Mac OS installation CD to reset the passwords on a computer.

Routers, firewalls, and other network equipment

If you still have it, check the instruction manual that came with the equipment. Most network equipment comes with default passwords. All equipment can be hard-reset to the factory settings — usually you push down the reset button during startup or in a set pattern. If the manual that you need is lost, you might be able to find it online.

Email and Phone

Reestablishing reliable communication — both external and internal — will be essential to rebuilding your infrastructure and continuing your core programs.

Your staff may need to work at home and/or use mobile phones. If so, you can have your office numbers temporarily forwarded to the appropriate landline or mobile numbers. Most hosted Voice over Internet Protocol (VoIP) services allow you to redirect lines to outside numbers.

Your staff members might need to use personal mobile phones for work during the recovery effort. If so, find out whether their mobile plans include enough minutes and data per month to cover the increased usage.

If you have Internet access, consider using Skype or a similar service.

Change all of your outgoing voicemail and email messages to include basic information about your organization's efforts to rebuild. The message should briefly outline any changes in your organization's services and instructions on how to stay informed.

Consider establishing a "help desk" if you anticipate that there will be high demand for information from your organization, screening calls to avoid overwhelming switchboards and personnel.

If your email service has been disrupted, and you need to find a new provider, consider the following. You will need to update what is called your mail exchange (MX) record, which is similar to an update of your website's domain address. Typically, your email host will give you information about what your MX record should be (usually it's an address like mail.mydomain.com or an IP address).

Your Website

Your website is a central way to inform the public about your organization's recovery efforts and any changes to the services that you provide.

You should also take the opportunity to communicate with your allies to coordinate and potentially pool resources.

If power and Internet access is consistent enough, you should be able to update your website normally.

You should also post updates about your organization's recovery efforts on Facebook, Twitter, or whichever social media channels you use most frequently.

Proving your identity

If you have lost login and password information for updating your website or you need to make more substantive changes (such as changing web hosting companies), you may need to contact your domain registrar or hosting company to have your login information reset.

Some companies, given the circumstances, may be flexible around identity verification. However, times of disaster are often ripe for fraud. So it's likely you will still be required to convincingly prove who you are before you can make changes, such as having your login information updated.

You can find information to help you more easily prove your identity by performing a WHOIS lookup. These lookups provide information about your website, such as the admin contact, domain registrar, and more. This information is available via different websites, including

http://DNSstuff.com
(use the "WHOIS Lookup" feature)

https://whois.icann.org

In the best scenario, the person (or entity) listed as the admin contact will match your current contact information. For example, if the “admin email” is an email address you have access to, you should use that email address to communicate with your domain registrar or hosting company.

Sometimes the email address is masked, which makes it harder for you to find out which email address to use to contact the registrar or hosting company. If the street address is correct (and matches your letterhead), you can send written requests.

Details regarding payments made to the company you are contacting can also help prove your identity. If you have access to the date, amount paid, and credit card number used to pay for services, this may help prove your identity.

If records are inaccessible

If you are missing login or password information

You may be able to identify individuals who have this information by performing a WHOIS lookup (see prior "Proving your identity" section for how to do this).

If you can't find login or password information, you will need to contact your web hosting company to change your login and password information. A WHOIS lookup can also provide relevant information to help you prove your identity to the company you need to contact (see prior "Proving your identity" section for how to do this).

If you are uncertain who your current web host is

You can try a WHOIS lookup (see prior "Proving your identity" section for how to do this). Sometimes, it's obvious (you'll see something like dns.webhostcompany.com), whereas other times, all you'll see is just an IP address.

If you don't know who your domain registrar is

You can try a WHOIS lookup (see prior "Proving your identity" section for how to do this).

Equipment and Devices

It may be advisable to maximize your insurance coverage and call in the professionals to repair your damaged equipment and devices. You might be adept at quantifying your IT inventory and having good records in place to confirm your purchases and warranties. But actually taking apart a machine may be the appropriate moment to end your personal IT recovery services. If, however, you have no choice but to attempt repair and restoration yourself, or you are asked to supervise the process, here are some dos and don'ts as to how to proceed.

General safety tips

Ensure that you have a safe environment before you begin the hardware recovery process. For your own safety, observe these precautions.

If the floor, any electrical wiring, or computer equipment is wet, make sure the power is off before you enter the room or touch any metal, wet surfaces, or equipment. If you're certain that the power is off and that it is safe to move the equipment, move it to a safe, dry environment with reliable electrical power.

If you need to use temporary extension cords and cables, make sure that you follow safe procedures. Cords and cables should either be placed where they won't be walked on or taped to the floor to provide protection in high-traffic areas. Be sure that the cables are rated for the device and appliance that they are connected to.

Make sure that tables are sturdy enough to support the equipment placed on them, and that if you stack equipment, it will remain upright and stable, especially when it is connected to cables or other peripherals. Allocate a little extra time to make sure everything is stable, neat, and orderly.

Once you have a safe, dry environment, it's important to make sure that you have good, reliable electrical power before you connect or turn on any computer equipment. A good first step is to plug in an electric light to make sure it shines steadily and provides the same amount of illumination that it normally would. You can also try to plug in things you can afford to lose and test them out. An example of something you can afford to lose might be a radio or any other device that requires only a small amount of power. You may need to purchase or rent power-generating equipment to clean up, charge devices, or verify equipment — it depends on the urgency and situation, and what is being supplied through insurance or volunteer-based services.

To avoid power surges and brownouts, turn off and unplug computers when they will be unused for an extended period. If a lightning storm is expected or the power goes out, turn off and disconnect computers and other sensitive equipment. Keep them off until the power is back on and stable. Power surges often occur when the power returns. Computers should have a backup system for short-term power or an uninterruptible power supply (UPS), which also provides isolation. Laptops are isolated by their power supplies and batteries, but reliable power is still important to avoid damage. Your UPS may have exhausted its battery power during an outage, but its surge protection capabilities may be unaffected.

Ventilation is also very important. Make sure the vents on any equipment are unblocked. Computers can run in a warm environment as long as they have adequate ventilation. Avoid the tendency to put computers right next to each other or position the vents next to desks or cabinets. Use a fan to keep the air in motion in the room and around the computers if you think they might get too hot. Turn computers off if you leave the room and let them cool down before they're turned on again. Consider whether you can work during the cooler part of the day and turn off computer equipment when it's too hot to work comfortably.

Hardware recovery tips

Once you have verified the operating environment, assess the hardware situation independently or with professional guidance. If you think you might require contingency suppliers who are third parties (such as salvage companies, or computer room suppliers who are mobile), notify them of your potential need.

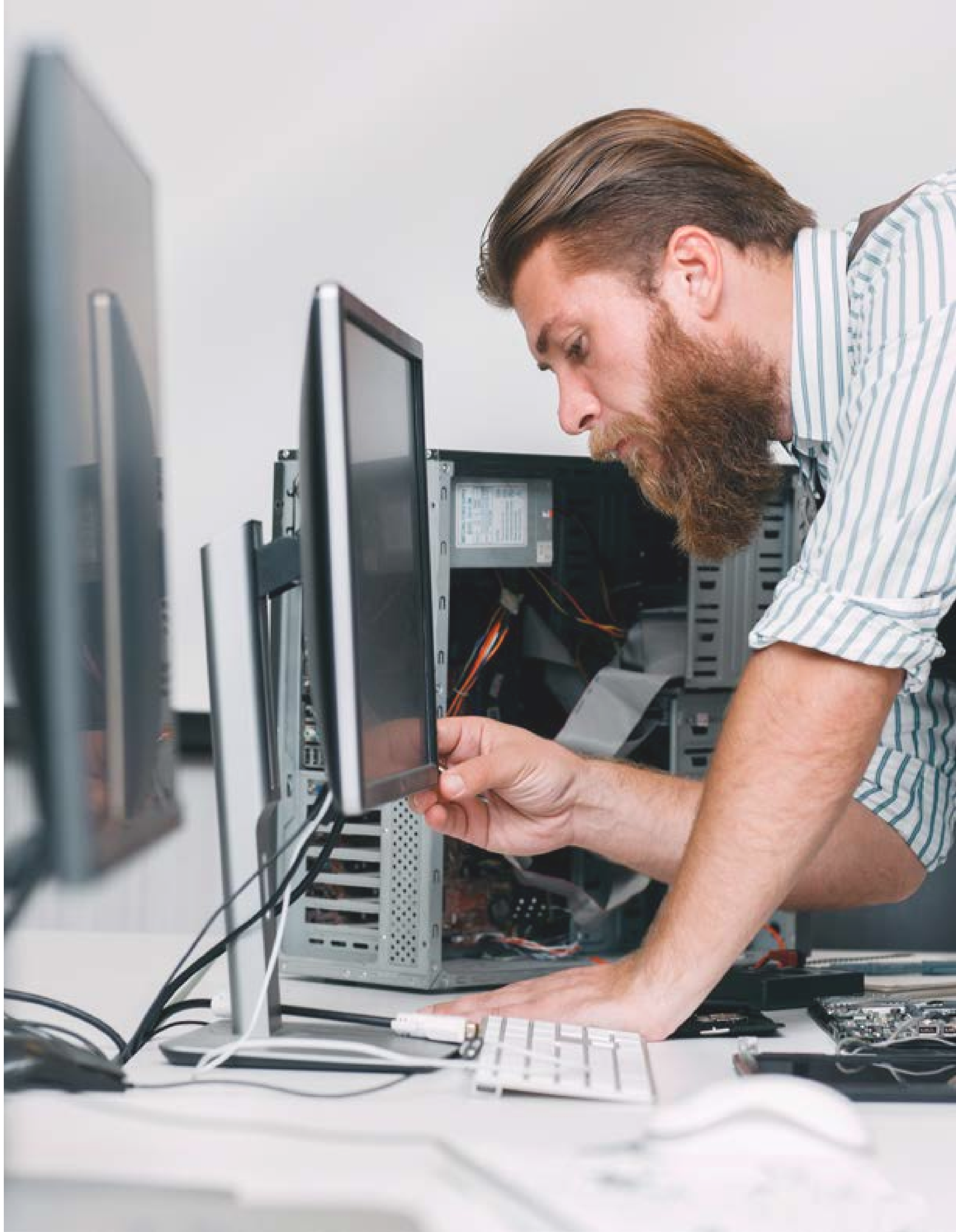
1 Clean and dry hardware that you intend to revive yourself. Postpone or avoid any attempt to plug in or operate a computer until it's completely dry and free of mud, dirt, or other debris. Your computer might work, but if you turn it on prematurely, you can destroy an otherwise healthy machine. It's important to open up the chassis of your computers to make sure they are clean and dry inside and out. If there's any debris, remove it carefully so that you protect the computer from the tendency to overheat from reduced airflow.

2 If you need to touch or put your hand or tools near any part inside the computer, wear a wrist strap with electrostatic discharge (ESD). Or, you can work on an antistatic mat. If you lack a wrist strap or mat, touch a grounded object (such as metal water pipes) before you touch the computer. Before you open the computer's case, be sure all power sources are turned off, the computer is unplugged, and laptop batteries are removed.

3 Make sure devices such as routers, switches, and printers are completely dry before you power them up. If possible, wait to attach peripherals and cables to computers or avoid this entirely, unless you're sure the equipment works properly.

4 Check your components twice. Even if a computer fails to start right away, put it aside to check later. Be sure to sort and label the equipment. These actions allow you to figure out what does work and what is broken. After that, you may be able to build computers that work from operational parts of different broken computers.

5 Once you get a computer to run, back it up if its data is more recent than your backups



Network recovery tips

In the case of a flood or other inundation, a local area network (LAN) can be badly damaged. Network cables can become waterlogged and cease to function. Patch panels and jacks might also be damaged; switches, hubs, routers, and other electronic devices on your network might be shorted out by the water. Full restoration of your network to its original condition can take time and effort. It might be worthwhile to try to get a few devices back on first.

First, verify that the networking devices are safe to use. After this, try to plug in your modem to a reliable power source and see whether the lights come on as they normally would. Usually there would be a green light and a label such as "online" or "power." It's possible that the settings were saved during the outage. If the modem has LAN ports, you can try to connect your computer in directly rather than use your regular networking devices. This is a good short-term solution until you or your IT consultants are ready to do more detailed reconfiguration. If it is safe to do so and there's a need, expand the network by the addition of a hub or a switch.

Once you have a hub or switch that works in place, you can start to connect computers to the network via standard Ethernet cables. Try to run the cables along the base of walls and out of the way of foot traffic. Ethernet cables are easy to trip over, and when pulled abruptly, can break connectors and jacks and pull equipment to the floor. If you need to run a cable across a traffic path, try to tape the cables to the floor to keep them out of the way.

Pro tip:
When you pull up taped-down cables, try to pull the tape off the cable while it is still on the floor. If you pull up the tape and cable together, it's likely that the

tape will wrap around the cable. Then the tape can be very difficult to remove.

If your organization had a wireless network, it may be more efficient to set up that network first to access the Internet, because it is easier to add additional users. A wireless network is also less reliant on a static location. However, you might not have access to certain servers — it depends on your network configuration — so do be aware of potential limitations. You might have had wireless access from your broadband modem previously and your settings might have been retained. If so, then you should be able to use the same wireless settings as before. If wireless access has been lost, you'll need to reconfigure the modem. If possible, refer to the documentation that you have set aside, or the master key of information.

Mobile Internet connectivity

In times of disaster recovery, there will be a greater reliance on mobile networks for both personal and official business. Numerous agencies, private citizens, and relief groups need to use the same networks to communicate with one another within the same region. Therefore, it would be ideal if the organization prioritized the use of this scarce resource.

If regular fixed broadband is currently nonoperational, but your work or personal mobile broadband is available, you should use it as needed.

About the Guide

This is the third major revision of

The Resilient Organization: A Guide for IT Disaster Planning and Recovery

The initial version of this guide was written shortly after Hurricane Katrina struck the southern United States in 2006.

In 2013, we made the information more concise and actionable, and added some key revisions pertaining to cloud and mobile adoption. We also translated the guide into certain languages for our global audience, and produced it in e-book form.

In this latest version, we have split the guide into several parts to better serve organizations who are recovering from a disaster and need support to rebuild their IT infrastructure to resume their primary activities.

This edition of the guide was created in partnership between TechSoup and the Center for Disaster Philanthropy with the generous support of Microsoft.

disasterphilanthropy.org

techsoup

Main Office

TechSoup
435 Brannan Street, Suite 100
San Francisco, CA 94107
(415) 633-9300
Email Customer Service at:
customerservice@techsoup.org

Press Contact

Email PR at:
PR@techsoup.org
(415) 633-9403

Affiliate Accounts

Organizations with multiple members or affiliates, and those looking to place donation requests for 20+ organizations, please contact us at:
accountmanagement@techsoup.org

Business Development

For information about donating products, see Become a Donor Partner at:
http://www.techsoup.org/joining-techsoup/become-a-donor-partner.