THE HIDDEN ASPECT OF DISASTER PLANNING: DATA

Access to data after a fire, flood or other catastrophe can make or break your organization. Here's why your business or agency may be at risk and what you can do to accelerate your time to recovery.

Small and medium-sized businesses (SMBs) and government agencies are the backbone of many communities. In the Western world, from North America to Europe, locals rely on SMBs and the government for everything from health care to groceries to transportation – they're what keeps cities, towns and rural areas operating as they need to. But when you peel back the surface of how these organizations work, it quickly becomes clear how reliant they are on data – and just how vulnerable that data is in the event of a disaster.

Many of these organizations are in remote locations or areas that have low internet bandwidth – and, as a consequence, unreliable access to cloud storage. Even in large metropolitan areas, internet access can be unreliable, slow and expensive. This poses a significant challenge in the case of a fire, flood or other catastrophe, when SMBs and government agencies are unable to access their critical data. SMBs, which account for 99.7 percent of all enterprises in the United States and 99 percent of all enterprises in the EU, depend on customer data and reliable internet access for their livelihood. This enables them to provide products and services, including supplies for government agencies, where and when they're needed on a day-to-day basis and following a disaster. Government agencies need access to data such as local population and geospatial information to deliver timely emergency services and get everyday services such as drinking water and garbage pickup back on track.

When these organizations lose access to data, they often struggle with lengthy post-disaster recovery times. Events as common as a plumbing break or as devastating as a wildfire can have an outsized impact on an organization's ability to recover and operate as needed.

Due to the high consequences of these emergencies and the increasing prevalence of natural disasters, the cloud no longer suffices for data storage at organizations in remote locations or areas with internet connection issues. Physical data must now be a part of disaster planning, regardless of whether an organization is located in a rural area or in a city like Exeter, U.K., which was named the worst-connected city in the country, or Memphis, Tennessee, the U.S. city with the slowest download speeds. Without an effective plan, SMBs and government agencies are unable to prevent longer business downtimes, failure to serve customers or constituents, and an inability to coordinate with first responders and other disaster recovery workers.

HOW DISASTERS CAN AFFECT YOUR ORGANIZATION'S DATA

Most businesses and government agencies are aware that they run the risk of coming under attack by hackers due to well-publicized data breaches such as that of the recent leak of sensitive information in Germany or the growing number of attacks on the IT infrastructure of U.S. cities. As a result, safeguarding data against hackers is now standard operating procedure for most organizations. SMBs and government agencies, however, may not have considered how other real-world events could prevent them from accessing their data.

Plumbing or HVAC breakage can flood buildings and damage computer hardware beyond repair. Building fires can torch devices and eliminate the possibility of data recovery.

And as natural disasters become more common, organizations need to take into account the potential risk to their operations. Wildfires are typically now larger and last longer with even greater effects on local communities. Take, for example, the recent Camp Fire in Paradise, California: A total of 366 commercial buildings were lost in the fire. Seven months after the blaze started, just one of nine schools in the area has reopened, and total insurance losses are reported to be more than $8.3 billion. And in Europe a year earlier, more than 100 wildfires blazed across Portugal and Spain, shuttering a car manufacturing facility and threatening several small cities.

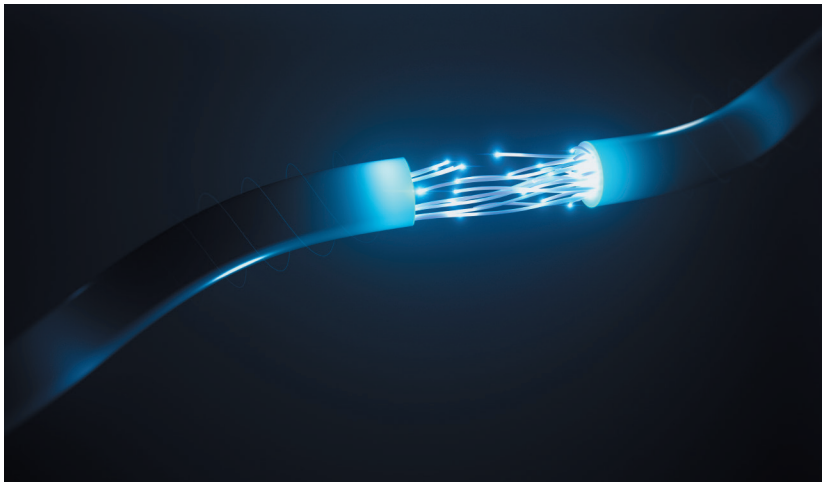
The effect of hurricanes and other heavy storms is increasing as well: Scientists are recording more hurricanes with category four or five strength than ever before, and the widespread flooding damage in Houston following Hurricane Harvey – and in the areas surrounding Carcassonne, France, following violent storms in the fall of 2018 – has put a public eye on how these storms

SPOTLIGHT
DISASTER RISK IN 2019 AND BEYOND

- 4 states are projected to be highly affected by tornadoes in 2019: Oklahoma, Kansas, Texas and Nebraska.
- 25 U.S. states face major or moderate flooding in 2019.
- 89,004 local governments exist in the U.S. – many of which are rural and unable to access high quality internet.
- 35 million U.S. citizens live in the wildland-urban interface fire threat zone.
- 1,500 sq. miles burn due to wildfires each year in the European Union.
- Storms and floods are responsible for more than 70 percent of the world's natural disasters, according to the UN Office for Disaster Risk Reduction.

can devastate entire cities and towns.
Those who live in the U.S.'s Tornado Alley and other tornado-prone areas must also consider the potential for property damage from debris and electrical and water damage that can occur when a tornado hits their community. The U.S. sees an average of 1,200 tornados a year, and Europe, 300, and any of these storms can knock out internet connections, prevent access to the cloud or cause irreparable harm to equipment.

When these disasters strike, SMBs and government agencies need to be able to focus on recovery and assisting their local communities – not on finding a way to access the information they need to do so.



WHY THESE DISASTERS PUT YOUR ORGANIZATION'S DATA AT RISK

Despite the headlines putting a spotlight on new internet connectivity projects like Google Fiber and hundreds of community gigabit internet initiatives launching across the U.S. and Europe, the reality for many organizations today is that internet access is unreliable, slow and expensive. As you'll learn below, that's true regardless whether they're located in a large metro area or in rural countryside – and it can make accessing data online or in the cloud following a disaster difficult or impossible.

In international broadband speed rankings, the U.S. falls far behind top contenders like Singapore, Hong Kong and Monaco. In fact, 17 percent of all Americans – or 55 million people nationwide – lack access to broadband internet.

In the same international internet speed rankings, many European countries don't even make the list: France is

7 CONSIDERATIONS FOR DATA DISASTER PLANNING

1. What internal functions rely on data, and how critical are these to the products or services that your organization provides?

2. Would your business or agency be affected if these functions were to halt during a disaster?

3. What is the scale of impact if you were to temporarily or permanently lose access to that data? How would it effect employees, business value or the community at large?

4. Where is your data stored and can you access the most recent version in its current location in the event that you lose internet?

5. What alternatives and backups do you have in place to ensure your disaster plan includes data recovery?

6. Are your alternatives designed to withstand potential local disasters as well as flooding and building fires?

7. Does your staff understand how to access organizational data, or do they need additional training to ensure continuity?

HOW LOCAL PHYSICAL STORAGE ENABLED FASTER DISASTER RECOVERY FOR THESE BUSINESSES

For many businesses in low internet bandwidth areas, the cloud can be a burden rather than an asset. Take a look at how local physical storage enabled these companies to prepare and recover from disasters faster:

Medical clinic finds data intact after building destroyed by fire
Snoqualmie Valley Medical Clinic in Washington State was devastated when a fire, possibly started by an electrical issue, burned down its $500,000/€450,000 facility. Due to the intensity of the blaze, the center thought it had lost sensitive patient data that was needed to deliver care and stored on an ioSafe network accessible storage device. The clinic asked the fire department to retrieve the unit, and to employees' surprise, the data was fully recoverable.

"I thought the unit was toast," the clinic's IT consultant, Robb Mercer, said. "The casing was badly charred, and external connectors had melted. However, when I extracted the driver from the ioSafe casing and connected it to a computer, I discovered that the data was still there."

Improved workflow with physical storage protects software developer's data
Before implementing a physical storage solution, Humble Daisy backed up its digital assets on a USB drive and Apple Time Machine. Backups were infrequent and often were forgotten or skipped due to time constraints. As a development company, any loss of its data in the event of a disaster would be devastating to the functionality of its products. The company considered cloud solutions but identified network performance and security issues when working with its larger file sizes. It ultimately selected an ioSafe network accessible storage with easy-to-use software that automates backups of the company's data and is both fireproof and waterproof. Now, the company's data is protected from disasters in a manner that's up to par with its security needs.

ranked 14th, and the U.K. and Germany aren't even among the countries with the top 20 fastest speeds. Some metro areas have it particularly bad: The Berlin Chamber of Commerce told NPR recently that 70 percent of businesses in the city have complained about internet speed and reliability.

Rural areas also struggle with low-speed internet: More than half of rural Americans lack access to the minimum speed required for broadband internet, according to an FCC study, and rural areas in the European Union have less than 50 percent broadband coverage, a 2017 European Court of Auditors report found.

Terrible internet bandwidth isn't just a problem when you want to stream Netflix, Hulu, My TF1 or Sky Go at home – it can make the most basic of organizational functions a challenge. To put it in perspective, the speed required for broadband internet in the European Union is 30 Mbps. In the U.S., its 25 Mbps. That's about enough for basic web surfing, email and video but certainly not enough to effectively transfer large quantities of business or government data.

At those speeds, an organization that relies on cloud backups or downloads could find itself waiting days or weeks to replace data – and that's if there's internet access at all following a disaster. Florida municipalities like Panama City, for example, found themselves with unreliable or inaccessible internet for days following Hurricane Michael in 2018. Even a small building fire can destroy internet lines and knock out connections to entire city neighborhoods as recently happened in Roseburg, Oregon, or destroy computer equipment, as one County Clare, Ireland, business experienced.

Organizations that don't have a viable alternative to access data can lose an average of $8,500 - $200,000/€7,600 – €180,000 or more each hour that internet is down. With such high stakes from the inability to utilize data stored online, a solution for local physical data storage and recovery is needed – one that can withstand all the disasters nature or mankind may throw at it.

WHAT TO LOOK FOR IN A PHYSICAL DATA RECOVERY SOLUTION

Local data storage is just one part of a disaster recovery plan, but it can make a huge difference in an SMB or government agency's ability to bounce back swiftly after a catastrophe. When identifying potential storage options, look for a solution that has these characteristics:

Fireproof: When a wildfire or building fire is threatening a building, a computer or storage device is rarely the first object most people think to save. In a building fire, temperatures typically reach temperatures around 100 F/37 C at floor level and up to 1,500 F/815 C at ceiling height. Most wildfires typically burn at about 1,400 F/760 C. Given that a storage device is likely to be left behind during a fire, organizations need options that can withstand fire.

Waterproof: With the National Oceanic and Atmospheric Administration (NOAA) predicting that huge swaths of the U.S. are at risk of long-range river flooding and the European Environment Agency expecting similar outcomes across the continent, waterproof capabilities of up to 10 feet/3 meters are critical. Storage devices can also suffer water damage due to a faulty sprinkler system, leaking HVAC or broken pipe. In all cases, it's unlikely that employees will be able to access a data storage device right away – it could sit in water for several days before it's safe to enter or can be recovered. Look for devices that can keep data safe for at least 72 hours under water.

Ability to support the organization: Of course, in addition to disaster-resistant capabilities, a storage device must be a good fit for an organization's day-to-day data-sharing and archiving needs. Network accessible storage devices with local private cloud capabilities balance between those needs, which means that internet downtime won't prevent employee

access to data following a disaster. It's likely that storage needs will grow as an agency or business does, so look for devices that can expand to at least 50-100 terabytes.

DON'T LEAVE DATA UP TO CHANCE

When an emergency strikes, you shouldn't have to worry about your data. Organizations can protect themselves from future disruption to their operations by adopting a physical data recovery strategy that utilizes fireproof and waterproof storage. Storage devices solve everyday data storage challenges and ensure that your data is accessible after building fires or leaks, flooding, wildfires, tornadoes and hurricanes. By choosing one of these devices for your organization, you can eliminate one of the most difficult and expensive aspects of disaster recovery – access to data – and be better positioned to support the local community following an emergency.