Protecting Your Clients from a DATA DISASTER
Disaster can strike at any time without warning.

Each year natural disasters such as floods, hurricanes, tornadoes and wildfires affect thousands of businesses, as do more common events such as water main breaks and building fires. The damage left in the wake of disasters such as this can be devastating. And while most businesses have insurance to cover the physical loss, how do they overcome those losses that are not physical in nature?

An insurance company can’t recreate customer lists, financial statements or other data that might be lost as a result of a disaster. And insurance companies typically won’t cover losses due to equipment failure or simple human error, which are the causes of most data loss incidents. Instead, as their IT service provider, your clients depend on you to protect them from IT-related losses. And as the amount of data stored on servers and workstations continues to grow, data protection becomes even more paramount.

“70% of small businesses in the U.S. experienced a data loss in the past year due to technical or human disasters.”¹ — AMI-Partners
The Consequences of Lost Data

The consequences of lost data can be extensive and far-reaching. At the very least, businesses will experience decreased productivity and possibly a loss in revenue, depending on the severity of the data loss. There are also high costs incurred to recover the data and if the loss is large in scale, these costs can reach into the thousands. The average loss to small businesses in the U.S. that had experienced an incident of data loss due to a technical or human error was $4,700 per incident in 2009, which equates to approximately $20 billion total.¹

However, these consequences pale in comparison to what could happen if the data loss is catastrophic or if the business loses access to key data for an extended period of time. According to one study, 43% of companies that experience catastrophic data loss never reopen and 51% are closed within two years.² What’s more, DisasterRecoveryPlanning.org reported, “A company denied access to mission-critical data for more than 48 hours will be out of business within one year.”³ Respondents to a Forrester Research study classified approximately 35% of applications and data as mission-critical.⁴

It comes as a surprise, then, that despite the high risk, 56% of enterprises in North America and 30% in Europe don’t have a formal and comprehensive disaster recovery policy in place.⁵

“87% of businesses indicated that failure to recover data would be damaging to the business and 23% said it would be ‘disastrous’.”⁵

- InformationWeek
The Impact of Natural Disasters

Hurricanes. Tropical storms. Tornadoes. Winter storms. Earthquakes. Wind. Hail. Floods. Fire. Natural disasters can occur at any time and no area or region is immune. Sometimes, advance warning is provided, such as with hurricanes and winter storms. Other times there is no warning, as is the case with earthquakes and tornadoes. Thus, businesses must be prepared at all times. According to Steve Fairbanks, Vice President of Product Management at CA Technologies, “A lot of times companies don’t fully understand the cost of not preparing, so as a result they are not willing to spend some dollars to ensure disaster doesn’t occur or they can recover quickly from a disaster.”

Research has shown that at least 25% of businesses that are forced to temporarily close after natural disasters never reopen, and those that do reopen face an uphill battle to stay in business. And yet there are still many businesses that fail to prepare. Small businesses are especially vulnerable, because many lack the resources and knowledge necessary to properly assess the risk of disaster or develop a comprehensive recovery plan. So the onus falls to the IT service provider to educate clients and ensure a proper backup and disaster recovery plan is in place.
Disasters are not only a result of Mother Nature. Even something as simple as human error can cause irreparable harm in a matter of seconds. Terrorist attacks, although rare, are also something to consider, as are hard drive failures, viruses and power outages. In fact, the most common cause of data loss is hard drive failure, which accounts for 38% of data loss incidents. Businesses are much more likely to experience an incident of data loss from disasters such as these than they are from a natural disaster.

Common causes of data loss include:

- Arson
- Theft
- Liquid or heat damage
- File corruption
- Software error
- Virus infection
- Hard drive failure
- Controller failure
- CPU failure
- User error
- Power outages
- Accidental or unknowing data deletion, modification or overwriting
The only way to ensure data isn’t lost in a disaster is by having a disaster recovery plan in place. Because disasters can happen at any time, knowing how data is going to be recovered should be at the forefront of your clients’ business strategy. The best way to safeguard against data loss is to backup data to an off-site location or in the cloud. If stored at an off-site location instead of on the cloud, be sure the physical location is located in a different area of the country. If a storm hits and devastates an entire region, it is very likely that the data storage location would be affected as well.

Backing up data and storing it elsewhere provides your clients with remote access to any and all data whenever it’s needed, regardless of the nature of the disaster that strikes. Other ways IT service providers can help ensure their clients can continue working after a disaster include:

- Ensure backups are successful and rehearse the recovery plan to confirm backed up data can be restored quickly
- Keep equipment and hardware up-to-date and located in safe, dry and dust-free areas
- Encourage the use of battery backup power supplies or a generator so data can be saved or backed up during a power outage
- Provide remote support to your clients’ employees and make sure they know how to access data remotely so they can work from an alternate location if needed
- Create a disaster recovery plan for your own business so you can continue to support clients before, during and after a disaster

One of the biggest hurdles to overcome with backup and recovery efforts is getting clients to understand the catastrophic ramifications of data loss. As an IT service provider, you must educate your clients on the importance of business continuity. It is also important for you to communicate realistic expectations of what clients can expect in terms of service levels and recovery times if disaster strikes.
When it comes to backup and disaster recovery, one size does not fit all. Your clients’ needs vary, so it’s up to you to make sure you’ve got the right solutions in place to help every type of business. From on premise image backups for stand-alone machines to High Availability (HA) offsite image backups, each of your clients is in need of a different solution. So how do you choose the right one?

When looking for a backup and disaster recovery solution, look for one that:

- Integrates with your remote monitoring and management (RMM) solution so you can see the backup status of all your clients under management at-a-glance – even if you are using multiple backup products
- Enables you to remotely create, edit or modify backup jobs for a single device or across multiple machines in real time from a centralized management console
- Provides data protection and recovery for physical machines, virtual machines and the cloud
- Allows you to create disk image backups that contain the full operating system, applications, data and user preferences for true disaster recovery
- Can recover individual files and folders without the need to restore the entire backup archive
- Allows for integrated bare-metal, dissimilar hardware and physical to virtual recovery
- Delivers data recovery in minutes, not hours or days

Selecting a BDR Solution: What You Should Consider

Protecting Your Clients from a Data Disaster  LabTech Software
The bottom line? Whether caused by Mother Nature, human error or some other unforeseen circumstance, disasters will happen. Take steps now to ensure your clients are protected against data loss. Help your clients create a disaster recovery plan and make sure their backups are successful every time. You never know when disaster may strike.

Summary

LabTech Software is the brainchild of a managed service provider (MSP) that struggled with the usual challenges and inefficiencies of a reactive IT maintenance and support model. LabTech—its flagship solution—was born of the urgent need to eliminate technician inefficiencies and the desire to provide preventive and proactive service. Developed with cutting-edge, agent technology, LabTech is the only remote monitoring and management (RMM) platform created by system administrators for system administrators to automate your IT services and eliminate inefficiencies. For more information, please visit labtechsoftware.com or call 877.522.8323.