How would your firm survive a Catastrophe?

A managing partner once told me, "After my people, **our data is our most valuable asset."** The value of data is undeniable. Unfortunately, so is its vulnerability. Critical information can be lost due to server malfunction, hackers, power surges, broken water pipes or any one of a hundred unpredictable disasters. Data backups are important, but they may not be enough.

What Is the Difference Between Data Backup and Disaster Recovery?

In a nutshell, data backups only store the information itself. While this is a crucial step, most companies require a range of different applications to function properly. For example, imagine if your server crashed overnight. You had the foresight to back up all of your clients' information, but you had no access to email or accounting software. Without a disaster recovery plan, your firm could come to a grinding halt.

In cases of catastrophic damage, it can take hours or even days to get everything back online. A proper disaster recovery plan can save you thousands of dollars in lost time, revenue, and opportunity. However, your plan must be in place (and thoroughly tested) before disaster strikes.

What Does a Disaster Recovery Plan Look Like?

Every firm is different, and so is every recovery strategy. It is crucial that your plan reflect what is important to your firm. Two important concepts to keep in mind are:

RTO - Recovery Time Objective: How quickly do we need to recover? Does your firm need to be back online in an hour, or in 24 hours? Faster is always better, but it is also more expensive. You can also narrow this down to certain services. Typically email is more critical than closed cases for example.

RPO - Recovery Point Objective: How much data can we afford to lose? Is a day fine or just a matter of hours? We even have some firms setup where it is less than 15 minutes, but as with RTO, faster is more expensive.

The goal of any disaster recovery plan is to minimize RTO and RPO by bringing crucial systems back online as quickly as possible. For instance, if your company relies on email but the network is down, your plan may allow employees to start sending and receiving new emails within the hour. However, archived emails may not reappear for 8-24 hours. That's why it is important to prioritize which programs and information are most important to your company.

Outside of RTO and RPO, there are other key factors to consider:
What data needs to be protected, and how quickly does it need to be recovered?

What is our budget?

How would you notify employees or clients about an outage (if traditional communication was unavailable)?

In the event of a facility disaster, things become more complex. How will our employees work? From home or another location? Where can our attorneys meet with clients?

How often should you test your disaster plan to make sure it's working?

Remember, the right contingency plan can make or break your business. It is possible for companies to develop the plan in house, but there are proven benefits to consulting a professional legal technology firm like Technology Pointe. We can help determine what kind of services you need, but more importantly, they can help develop a plan that will scale and grow as your firm does.

by *Darry James*

https://www.linkedin.com/in/darry-james