How Law Firms Can Prepare for Hurricanes and Other Extreme Weather

By Chris Owens

Following an unprecedented host of destructive hurricanes this year, many law firms are asking how they can prepare for the next one. Inclement weather can wreak havoc – flooding offices, damaging computers and servers, destroying paper records, and keeping attorneys from reaching their clients. Several days of lost data and billable hours, not to mention damaged facilities, mean big monetary losses.

Practitioners and firms can protect themselves with a range of preparations, depending on how much they are willing to invest in them and on whether they are steeling themselves for a hypothetical storm or for one forecast for the next day.

PLANNING AHEAD: BC/DR

In the legal IT industry, such preparations are called the BC/DR (Business Continuity and Disaster Recovery) technology strategy, which refers to the two main aspects of a plan for extreme weather or other highly disruptive events – a strategy to both stay operational during the storm as well as recover any processes impacted by the event. (Your BC/DR plan is different from the administrative one, which documents where people should go, who declares a disaster, phone trees, operational control, etc.)

Two metrics dictate the development of the BC/DR plan, Recovery Time Objective (RTO) and Recovery Point Objective (RPO). These are, respectively, the maximum amount of time a firm can tolerate being without services and the maximum amount of data that can be lost, usually defined for individual business systems, such as messaging or conflict checking. The ideal metric for each of these is, naturally, zero. It used to be that the closer you wanted to get to zero, the more you had to spend, typically exponentially. Four hours was a common compromise that many firms made for critical systems (that is, four hours without access to systems and four hours of data lost), but recent technological advances have made it possible to get to almost zero loss and minimal outage, even for boutique firms.

Having backups of your data is imperative to the DR portion of your BC/DR strategy. Before the advent of modern solutions, this was accomplished by sending backup tapes offsite. Typically, someone would be deemed responsible for sending it off weekly or even daily with services like Iron Mountain. With contingencies like illnesses and holidays, this was a logistical pain and at best carried a 24-hour RPO with potential RTOs of several days.

To overcome the 24-hour RPO associated with tape recovery from a site-level failure, firms realized they needed to store data sets in a second location and update as frequently as possible. Once a service for only the largest law firm budgets, pricing for storage, network bandwidth and collocation has dropped significantly, allowing all firms to enjoy this protection. As continuous data protection systems developed, not only did the replica data sets serve as a disaster recovery option, but they also replaced traditional backup functions. Today, hardly any firms use tape backups and archiving directly to disk is commonplace.

With RPO commonly approaching zero, firms started to emphasize reduction of RTO, particularly for critical systems like email and documents. Having a data bunker for mitigating RPO was much more cost effective than buying duplicate servers, switches, and software ready to take over production services at a moment's notice. Buying those systems during a disaster could prove problematic and certainly did not decrease RTO. Again, the privilege of having the level of technology and automation to drive down RTO was enjoyed by only the largest of firms.

Enter the cloud service provider and the opportunity to provide BC/DR protections with an operating expense rather than a large capital one. The cloud now makes it possible to back up data continuously as well as spin up environments quickly in the event of a disaster. Zerto, for example, works with virtualized environments such as VMware or Hyper-V to perform near synchronous replication to cloud providers like Microsoft Azure and Amazon Web Services, allowing recovery costs to be on-demand and consumption-based. This pushes RTO down from days or hours to minutes. You can also choose

to replicate to regional cloud solution providers that are part of the Zerto solution partner program.

Alternatively, many law firms practice disaster avoidance, choosing to move their primary IT infrastructure offsite to a colocation facility specializing in 24/7/365 operations (among other reasons such as saving space, streamlining maintenance, and saving on cooling and power costs). For example, if your office is in a city – one beset with construction, poor electric grids, faulty fiber connections, and water options – or somewhere else prone to disruption, such as a coastal zone, a collocation will mitigate chances of an outage. Even if the colocation facility is close to your main site, it is still better equipped to deal with an event that would take down systems in commercial buildings. Manhattan colocation centers stayed running during Hurricane Sandy while the firms with on-premises data centers suffered.

Many of us are moving to the cloud entirely with services like Office 365, in which case the question of disaster recovery and data center locations is moot. Continue to do your research, and don't forget to test your plan. If you do not trust it to work when you need it, you may not even use it when the time comes.

If you do rely on paper files – and a surprising number of offices still do – the advice is less technical. Keep them high. That is, not in the basement, even if you are not in a flood-prone area, and off the floor. When helping law firms set up, we usually put servers and important files about six inches off the floor. You could also start scanning, digitizing, and backing up your files. Aside from hurricane prep, this is generally a good idea. Companies like Iron Mountain can also store your paper files in a secure area for you.

DAY-OF PLANNING FOR IT

Once the news stations start their frantic coverage of an impending hurricane, it is too late to put in place a comprehensive plan and test it. But there are some actions that may minimize the toll of the storm on your business.

First, remind your laptop users to bring their laptops with them in the event they are under an evacuation order. With data center systems up and a working internet connection, the user experience for those with laptops will likely be unaffected, meaning that business is largely unaffected. In addition, ensure other remote access solutions are working properly. Firms that use Citrix, VMware or Microsoft remote access solutions extensively on a daily basis won't need to worry about this. However, many firms only rely on them for the occasional person who needs to work from home. These firms need to ensure that the systems are patched, up to date, scalable to support an influx, and that everyone knows how to use them. You can have the most robust and redundant remote access system, but if nobody knows how to connect to Citrix, it will not be very useful on the day it is most needed.

Know your limits. Many remote access solutions are designed for a specific capacity and may have limits on concurrent licensing. Don't tell 100 users that they can all go home and work from Citrix if you only have 20 concurrent licenses. In the short term, you'll have to deal with the licensing limitations, but for the long term, you should purchase licenses for however many people you want to connect. Also, check that your systems are physically capable of supporting the extra load. Just because you have 100 licenses to support 100 concurrent users does not mean that a single XenApp server with limited RAM will be able to handle it. Some quick things that can be done include augmenting the Citrix farm or adding extra memory to virtual Citrix servers, or increasing the number of total virtual desktops if a Virtual Desktop Infrastructure (VDI) system is used.

TIPS FOR ATTORNEYS AND NON-IT STAFF

Emails from IT routinely get ignored in the inbox in favor of other matters that seem more pressing. It is especially important to read these emails while preparations for inclement weather are underway. Everything may be in place for you to work smoothly, but you may find yourself clueless on the day of, if you haven't been following announcements. And then all your emails, from IT as well as from clients, will be in danger of going unread. Your firm may revert to backup systems if the main infrastructure is affected, for example, and you will need to know how to access them in advance. It may require going to a specific website, enrolling and creating a new password, or some other deviation from routine.

Make sure you know how to use Citrix or whatever your firm uses for remote access before you need to log in. Ask IT any questions you have before the storm hits. Some telephone systems support making and receiving phone calls through your computer or mobile device. If this is available to you, make sure you have a headset and know how to use it. It's also a good idea to have a physical printout of contact information for all staff, or at least critical contacts like IT and management.

If you have a laptop, bring it home with you. Don't forget the power cord.

Chris Owens is the Chief Technology Officer at Kraft Kennedy and leads the Enterprise Client Systems Group from Kraft Kennedy's Houston office. With more than 15 years of technology and management consulting experience, Chris has advised law firms of all sizes. He is an expert in server and storage consolidation, disaster recovery and business continuity, email messaging design and migration, document management, and thin-client architecture. LinkedIn: www.linkedin.com/in/christophermowens. Twitter: @KraftKennedy. Blog: www.kraftkennedy.com/blog/.