Mastering Data Resilience and Business Continuity

Don't be like the farmer who waited to shut the barn door until the animals ran away. Here are suggestions for strengthening the systems for housing law firm data now.

BY JAMES PEARSON

"Of course, my backups are working. My guy swaps out the hard drives every day."

"Backup? No problem, I have that right here in my drawer."

The client who is the source of the first quotation insisted that his server backup was well taken care of by his staff, and they were confident that they could restore it in case of any hardware failure. Yes, they swapped the backup drives daily, but unfortunately, they never tested them. As a result, their most recent backup was 30 days old.

The second quotation indicated that the client and staff were changing their backup drives daily and even checking them. However, a fire broke out, destroying the building and taking all the backups with it.

Natural disasters, human errors (such as accidentally deleting a file), hardware problems, and software glitches (for example, Microsoft releasing an update that caused computers and servers to malfunction) can all result in losing important data. In addition, cyber threats such as ransomware, data breaches, and malware are a constant and growing concern. If you experience any of these issues, not having access to your data and critical systems can quickly bring your practice to a screeching halt.

I have observed in my 35-year career that the biggest mistake people make is assuming that what they are doing is merely "backing up their data." In reality, they are positioning (or failing to position) their businesses for a quick recovery from data loss or disruption.

The harm caused by disruption to computer services or loss of data is significant. The first business owner quoted above said he lost thousands of dollars because of having to close his shop for one day as we restored his failed server. In another situation, a company sent a melted and charred hard drive for data recovery, which cost thousands of dollars, and not all the data could be retrieved.

March 31 is recognized as World Backup Day. This year, I encourage lawyers to focus on the resiliency of their practices and not only on backing up data.

While every firm and network are unique, the keys to designing a business resilience plan in this article should help any business that is harmed by a data disruption to be up and running as quickly as possible, with minimal to no data loss. I hope that lawyers who develop business resilience plans will sleep more easily at night, knowing that they will bounce back from whatever harm might occur to their practices.

Take Inventory and Assess the Environment

It is crucial for lawyers to assess their current situations before implementing a reliable

James Pearson owns the Computer Center, Janesville. He is a Microsoft Certified Professional and a frequent author and speaker on cybersecurity and safety topics. Access the digital article at www.wisbar.org/wl.

james.pearson@computercenter.com

www.thelawyersgeek.com

backup and business continuity plan. Conducting a data inventory is the first step to evaluating resilience.

Many companies struggle to maintain good digital document management practices and, as a result, lose track of their data. With a clear understanding of data's whereabouts, it is easier to make informed decisions on how best to protect it.

Documenting where data resides can be overwhelming, especially if it is stored on various devices and platforms within a network or in the cloud with third parties.

Consider every file, email, calendar appointment, download, and document. Here are some typical devices, locations, and document management systems to check:

- Employer-provided computers
- Lawyers' and staff members' personal devices, such as mobile devices and home computers
- The cloud
- Practice management software
- Email accounts
- File storage and synchronization services, such as OneDrive, Google Drive, and Dropbox
- SharePoint
- Flash and USB drives
- External hard drives
- Backup software
- Vendors
- In-house server
- My Documents folders
- Social media accounts

Data Consolidation

Lawyers should consider consolidating or cleaning up data so that it is in fewer locations, making it easier to back up and find. Many computer users store data wherever convenient unless storage protocols are strictly monitored and enforced within an organization. I have also encountered organizations that use multiple, duplicative services, such as Dropbox, OneDrive, and Google Drive, for no reason except that nobody has decided on nor enforced a standard.

In addition to making it easier to keep track of data or documents, deciding on a common data storage location or service helps improve a company's cybersecurity standing and may reduce costs by eliminating redundant services.

Identify Key Hardware Systems

For purposes of restoring a business (not only data), taking stock of the equipment that is used is essential. Many firms I work with still have in-house servers that they use to house data and software.

If this is your situation, treat the hardware as key to your operations. Instead of backing up its files, leverage software that images the entire computer. This process will significantly reduce the time an IT company or department would take to restore that device to operation.

Evaluate Downtime Tolerance

When considering IT needs and backup solutions, lawyers also need to consider their feelings about and tolerance for downtime. In the past, some of my clients have been able to operate without their computer systems for days. However, others, and most lawyers, are more likely to need to be fully operational again within several hours or less.

Consider two things when evaluating a business continuity solution. First is how quickly you want to return to business. For example, if your tolerance for downtime is low, and your goal is to be back up and running within two hours, that is your recovery time objective. The second detail to focus on is your tolerance for potential data loss. Using a two-hour recovery time objective, with a backup running every two hours, the most data you would have to potentially recreate is the data created within that two-hour window. And, in that case, the disaster would have to happen just before the backup runs in that second hour.

In this situation, you'll need to choose a solution that backs up your data every two hours, and you want a solution that can restore critical data or machines within a two-hour window.

Building Your Plan and Evaluating Your Options

Once lawyers understand where firm data is stored and their tolerance for downtime and have identified critical systems, the next step is to evaluate backup solutions. Rather than going into detail or making specific product recommendations, I provide some criteria for evaluating products, services, and service providers.

Here are the criteria I recommend using when evaluating and selecting a backup and disaster recovery solution:

Automated: During my many years of IT work, I have found that people do not swap backup disks, never check that they are working, and fail at making good backups. Automating backups is essential, but with the caveat that the process be tested and verified regularly.

Encrypted: Encrypting data helps protect it from being stolen, changed, or compromised and has ramifications regarding data-breach-reporting requirements.

Wis. Stat. section 134.98(1)(b) discusses how encrypting your data, including backups, provides a safe harbor from the requirement of reporting a data breach if the data is encrypted. It defines personal information and under what circumstances a data breach must be reported. It reads:

"'Personal information' means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, *if the element is not publicly available information and is not encrypted*, redacted, or altered in a manner that renders the element unreadable:" (emphasis mine).

Tested: A backup that doesn't work might be worthless. Fortunately, many modern backup solutions automatically test and verify backups. They might even scan the backup for suspicious file changes that signify ransomware or other malware infections.

Offsite: Backing up data offsite provides some protection if natural disasters

occur. The approach is commonly called network isolation or air-gapping. An offsite backup offers the advantage of being inaccessible in the event of a successful ransomware attack on a company's computer network. Furthermore, automating the relocation of backups offsite reduces the risk of human error.

Frequent: Picture this scenario: A firm is hit with a ransomware attack at 4:30 p.m., but the most recent backup occurred at 11 p.m. the day before. This puts the firm at risk of losing an entire day's worth of valuable work and data that must be painstakingly replicated. Threat actors that use ransomware target backups, aiming to disable or turn them off to maximize the effect of the ransomware attack. To minimize this risk, I recommend backing up data multiple times throughout the day. Having multiple restore points reduces the potential loss of data dramatically. Backing up every two hours increases the likelihood of a successful backup and minimizes the amount of work that would need to be recreated in the event of a data breach.

Image-based: A backup system that includes frequent snapshots, or images, of an entire critical computer is the best form of protection and the fastest way to recover from a disaster. If there is a snapshot of a vital computer, the computer can be restored to its condition at that time. Doing so is faster than having to reinstall Windows and all software one by one and thus downtime is reduced.

Cloud Backups: Cloud-based data needs some backup attention, too. Products such as OneDrive and Dropbox are synchronization tools, not true backups.

Microsoft employs a shared responsibility model to safeguard and oversee the storage of data within its cloud services. While users are responsible for managing and protecting their data (including backing it up), Microsoft ensures physical security, service uptime, and certain account security aspects.[1]

Although Microsoft offers some redundancy and data retention, the rise of ransomware and other malware poses a significant threat to online accounts and data. Given the constant attacks on Microsoft accounts, adopting a proactive approach to safeguarding cloud-stored data is crucial. My recommendation is to opt for a third-party solution that not only provides encryption but also fulfills all the criteria above. This third-party option serves as an "offsite" location, separate from your primary data storage, ensuring accessibility even during service outages. Moreover, it offers multiple backups across various dates and times, further enhancing data protection.

Conclusion

The month of March includes both World Backup Day and St. Patrick's Day. Despite the latter, the need for the former is a reminder that relying on luck or chance is not a wise tactic as far as protecting business data is concerned.

Having a dependable backup strategy for all essential data and a disaster recovery plan makes a firm more resilient. Online cloud storage services like OneDrive and Dropbox might provide some redundancy and data retention, but they are not proper backups. With the rise of ransomware and other malicious attacks on accounts and data, it is crucial to have a secure offsite backup solution. Consider your comfort level with downtime when designing your data resilience and business continuity plan.

The Computer Center has created a free resource center with additional tips and educational materials on the topic of keeping your business resilient. Visit: https://info.computer-center.com/databackupresources. **WL**

ENDNOTES

[1]Microsoft, *Shared Responsibility in the Cloud* (Sept. 29, 2023), https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility. **WL**