

Data Replication: A Key Element in BCP

by Jason Buffington of NSI Software



The need for business continuity planning is as vital in the legal profession as it is in any major industry — in some ways, more so. Traditional backup systems, commonplace in many firms, do not offer the level of data protection that is critical to professional productivity and practice continuity. This article will explore the key aspects of good planning and good backups.

Business Continuity Planning — a Must-Have for Law Firms

Many benefits accrue from business continuity planning, including high availability of systems, good disaster recovery procedures and better backup systems — all of which mitigate unplanned outages. Additionally, Sarbanes-Oxley and other compliance regulations have impacted data and record retention for many business sectors served by lawyers, including financial (SEC & FDIC), government (DOD 5015.2 and CO-OP) and healthcare (HIPAA and JCAHO).

Two notable factors make business continuity planning in the legal segment especially important:

The average legal practice has the highest percentage of revenue generating workers per company of any major industry in the world. Whereas in a typical company, one might have up to 30 percent in a sales or revenue generating capacity (with the remainder in manufacturing, support and operational roles), the average law practice comprises a broad range of the billable resources, supported by a disproportionately smaller administrative, operational and support structure. This results in an even greater need for high productivity and guaranteed uptime due to the hourly billable nature of the legal workplace. Arguably, a small law firm needs business continuity planning to the same degree that a large international legal practice does. And the need is more prevalent in the legal profession than in similarly-sized organizations across any other industry.

The second characteristic of the legal profession exacerbating the need for business continuity stems from attorney-client privilege. Because of the level of disclosure that clients must give to their own attorneys as part of most major litigations, clients are often forced to trust significant amounts of their own data to their attorneys. By extension, this means that continuity regulations around the viability and security of data arguably transfers to the practice representing those organizations.

Imagine a situation in which a client company has survived a regional crisis through its own business continuity preparations, only to find that the law practice representing them has gone out of business due to loss of client information, billing records or even key discovery contents. A law firm's IT department should focus on the three core aspects of business continuity planning:

High Availability — Protecting Productivity

Disaster Recovery — Protecting the Practice

Better Backups — Protecting the Data

High Availability — Protecting Productivity

In business continuity planning, one of the primary goals most often pursued is that of ensuring uninterrupted productivity.

It's rather obvious that a large firm requires significant uptime for the hundreds of users who depend on the firm's IT resources — what may not be as clear is the small firm's equal dependence on its data. Good data protection is important to firms or law departments of any size.

Small Firm, Large Need for Protection

Consider a small practice, a 25-person office (10 attorneys and 15 support personnel). If the production server goes down in the middle of the day, data loss for both the first part of the day and productivity loss for the entire day will be incurred. We can measure productivity loss as the entire amount of manpower, which either is incapacitated or will need to be reapplied while repeating a task. In this case, we have data loss, plus a productivity loss for the time it takes to replicate lost work, plus the hours where users cannot access their data and may be completely idle.

Using industry statistics, this 25-person office has a manpower cost of \$1,500 per hour (considering average salaries and benefits for partners, lawyers, paralegals, and administrative staff positions). Assuming half a day of data loss and a full day of productivity loss, a single one-day outage will cost this small organization \$23,000 (exclusive of any lost revenue). If we include the average billing rate (assume 60 percent of revenue generators' hours are billable and multiply that by industry-average rates), the firm will lose an additional \$26,000 of revenue. While this small office may have considered itself "too small" for business continuity planning, a single outage per year carries a not-so-small pricetag of \$49,000.

Downtime happens, inevitably. Business continuity planning is about reducing its costs. If \$7,500 can be spent to mitigate a \$49,000 loss and any future \$49,000 losses for the entire time that the business continuity technology is in place, there is a huge return on investment even for the smallest firm.

Economies of Scale

In a larger legal practice, HR costs tend to scale linearly, while billing costs increase at higher rate due to productivity gains from leveraging advanced tools and often higher billable rates. E-discovery technologies, document imaging, online research libraries — all these things improve the productivity of the large practice. But they make the practice even more dependent on its systems, which therefore causes an even higher loss of productivity during any kind of service disruption.

As a final example, if this outage happened to a medium-sized practice of 100 employees, the single outage would cost \$135,000 in manpower plus \$184,000 in lost billing.

For a 250-300 user law firm, the greatest business continuity requirement may not necessarily be about immediate

resumption of activity (high availability described above) as much as about the survivability of the company itself. By definition, an SMB (small or medium business) comprises up to 500 employees. Various surveys, including Gartner, indicate that a medium-sized business (500 users or less) has a 50 percent chance of going out of business after a disaster if they cannot gain access to its data within the first 24 hours following the crisis. There are many factors that contribute to this grim prediction, but a notable point is this: if data cannot be accessed within the first 24 hours after a crisis, it's highly likely that the company cannot begin the rest of its business recovery efforts fast enough to avoid eventually going out of business.

Disaster Recovery — Protecting the Practice

Ironically, it wasn't so long ago that the terms "disaster recovery" and "business continuity" were interchangeable. Today, most industry professionals recognize that business continuity is a broader strategy around uptime, data protection and crisis resilience. We'll focus on the last of these goals, which is still referred to as "disaster recovery." Simply put, disaster recovery means "get the data out of the building" and then plan for how you will access and utilize it.

Insure Yourself

Many disaster recovery plans never get off the ground due to lack of executive sponsorship, which is reflected in an annually deferred budget. Put another way, disaster recovery becomes "something we'll try to do next year." In our earlier example of high-availability, we saw the financial implications of just a single day of downtime. One could extrapolate from those same numbers, stretched over several days but now possibly without the hope of recovering the data, what the cost of a disaster might be. Chances are, that those costs are not in the budget either.

Disaster recovery planning costs ought to be viewed like any type of insurance. Everyone knows that they need it; no one is necessarily excited about spending for it — but the entire motivation is to spend pennies now instead of dollars later. For disaster recovery, a business needs to understand the financial ramifications of a crisis. After looking at the big picture, a firm can typically justify the expense of preparing for a disaster. The advantage of spending for business continuity planning over insurance is that there are benefits that are reaped now, not just after a crisis.

Don't Let Documentation Delay Your Plan

Firms can become myopically focused on grandiose "disaster recovery plans" or binders full of documentation. And while full-scale DR plans should include documentation, the fault lies in delaying implementation pending the completion of grandiose documentation.

Better Backups — Protecting the Data

Why Isn't "Tape" Good Enough?

Imagine having to go to your senior partners or management committee to report that a server crashed in the late afternoon. All of the data for the attorneys, paralegals and some information provided by clientele were all lost. In addition, imagine notifying them that the same server will be down for most of tomorrow while the pieces are being ordered and the server repaired.

In traditional data backup, one should be prepared for the fact that the organization will experience at least half a day of data loss and one day of downtime in what is typically a "best-case scenario." This is not specific to the legal sector, but rather, specific to tape backup in general. If data is backed up nightly, data loss will be measured in "days." In addition, if spare hardware resources aren't readily available, most of the next business day following a crisis will be spent getting the parts to repair the downed server. Many times, an additional day of data loss may occur due to the likelihood that 30 percent of all tapes are not restorable.

And while the above tape scenarios are applicable to all tape backup environments, the effects are more strongly felt in the legal community than in many other industries because of the legal community's dependence on hourly productivity. Law firms and legal departments must protect their data more often than nightly. This takes us from a nightly tape process and into the realm of continuous data protection or real-time replication.

Real-Time Data Replication

With this new scenario, as data is changed, the changes are being transmitted from the production server(s) to redundant server(s) at alternate sites. Instead of having tape-protected data from last night, replicated data on the target server is a virtual twin of that on the production server.

A Boon for the Large Firm

A large multi-location law practice is much like a bank with many branches, a chain of retail stores or any other enterprise with distributed offices. Remote offices tend not to have dedicated IT personnel. While this is obviously notable during a crisis, it also requires a routine burden for remote office personnel to manage system backups. Perhaps an administrative assistant or office manager is tasked with swapping tapes, cleaning cartridges and even validating last night's backup. This process comes with an appreciable manpower cost and introduces the possibility of human error into one's data protection strategy.

One reason that many firms still use this approach is because bandwidth is not available (or cost-effective) to back up the

remote offices to the core data center. However, low bandwidth lines can be used to replicate the data from the remote sites to the IT data center because only the byte level changes are transmitted.

Advantages of Data Replication

From a budget perspective, no other data protection technology is as cost-efficient. Leveraging host-based replication, one need only put a simple software license on each production server and then point it at an offsite location.

Replication will transparently, automatically and without routine manual intervention, send the data to a remote site, which by definition is the beginning of disaster preparedness.

Instead of each site handling its own tape backups (and changing tapes, cleaning cartridges, monitoring jobs, etc.), all of the data on the production servers have a consistent copy at the core data facility, and the centralized IT team can perform centralized backups. Tape backups can be done during the day from the replicated copy of data.

Backups of the remote offices can occur, even though the remote office production data is actually still in use on their real servers. This results in fewer backup jobs to manage and maintain regardless of the size of the environment(s).

In Summary

A major difference in the business continuity needs of law firms from those other types of business is their notably higher dependence on hourly productivity and data protection. This is compounded by the regulatory requirements that many law practices must comply with as part of supporting their clientele in various specific industries such as healthcare, financial and government.

Unlike other industries in which only larger organizations place a priority on business continuity, we have seen how even the smallest of practices have significant uptime requirements and data dependencies. And of course, as the firms get larger, the needs are further exacerbated. Traditional methods of data protection simply do not fit the vast majority of law firms. Because of the manpower associated with the creation of data, its loss is intolerable; and nightly tape backups simply do not provide sufficient protection.

Data replication technology may be the solution that addresses your firm's needs to protect its data, its productivity and therefore, its practice.