

❖ Protecting the Heart of Your Firm

by John Hall of Integration Appliance (IntApp)

Most law firms do not have comprehensive disaster recovery or business continuity plans in place. Given the importance of information technology to the practice of law, this assertion would be hard to accept without proof. But proof comes straight from ILTA's membership.

According to ILTA's annual technology survey of over 430 firms, released in December 2005, only 36 percent of firms have such plans in place. Most firms, over 50 percent according to the survey, list their plans as "under development."

This article offers some advice to firms building their plans and identifies several key issues those with plans in place may be well served to consider.

A Common Approach to Planning

Law firms frequently consider disaster recovery planning and response in terms of three key areas:

Availability of Services and Applications — How do we ensure that Internet access never goes down? How do we make sure that staff has access to the tools they need to be productive when disaster strikes?

"If a firm is a living organism, the data that flows among timekeepers, staff and applications is its lifeblood."

Protection of Information — How do we make sure our document management infrastructure is synchronized, backed up and restorable in response to crashes . . . or worse?

Personnel Response — What's our plan and how do we train and educate our people on what to expect and how to respond when things go wrong? Will people be able to adapt and respond in the midst of unexpected change?

To address these issues, firms typically employ a standard set of strategies such as deploying redundant systems, using backup and data mirroring tools and documenting processes.

An apt metaphor here is that of the firm as a living organism. In this context, IT services and software applications comprise the body of the firm — serving functions analogous to hands, eyes, ears and other appendages. Of course the body requires a brain to function — the brain is the people who staff the firm, without whom there would be no organization, no identity. Finally, the information typically at the heart of DR planning represents memory, skills and knowledge — the understanding of how to function as a law firm.

The Missing Piece

But there's a piece of the recovery/continuity equation that's often overlooked: application and data integration. Consider how important it is that information moves among people and applications during the normal course of business. Integration is the glue that connects applications, data, people and processes and enables that movement.

Whenever an organization ties together different systems, the tools and business logic enabling these integrations become a valuable asset which must be protected. Should these integrations become unavailable, a variety of business operations may be impacted or even become impossible.

Thus, if a firm is a living organism, the data that flows among timekeepers, staff and applications is its lifeblood. And integration, the means used to transport that information, is the body's circulatory system and heart. Protecting it is vitally important for firms seeking true business continuity in the face of real-world disaster.

Understanding the Integration Challenge

Because most legal applications provide limited native means for broad data sharing, IT organizations often develop custom workarounds to connect systems. For example, a firm may use a batch script to move data between DM libraries or manually rekey new client matter numbers into time tracking and cost recovery systems. Approaches firms commonly use include:

Manual processes performed by humans

Custom-developed batch scripts

Third-party tools designed for application-specific connections

Centralized integration platforms (either commercial or custom-developed)

Typically, firms use multiple approaches. This makes integration a complicated affair. This complexity exacerbates disaster recovery and business continuity challenges, creating questions that frequently go unasked such as:

Do we have an inventory of the batch scripts we're using? Do we know who owns them and manages them? Are they backed up and restorable? Are they optimally designed to account for BC/DR considerations?

Are all of our processes documented, or do they live in peoples' heads? Are these definitions centrally stored, accessible and secure?



Is there a plan in place to protect and communicate information when applications fail? If the integrations themselves fail? Or if the people who execute manual processes become unavailable?

In many instances the answer is “sort of” or just plain “no.” And there is more than anecdotal evidence to support this assertion. A 2005 survey of over 280 legal IT professionals by Askew Network Solutions (a consultancy headed by a former law firm CIO) reported not only the expected — 82 percent of respondents stated that disaster recovery was a “top” or “very important” priority — but also a stark gap between priority and reality:

“Specifically, only 13 percent of organizations maintain backups of the tools, scripts or configuration rules they use to communicate information between applications. This means that in the event of disaster, many systems may be restored, but the ties between systems that keep the legal data ecosystem functioning, ensure that information stays current and enable internal processes to run smoothly may be lost.”

(“2005 Legal IT Integration Survey Results,” Askew Network Solutions, www.askew.net.)

Preserving Business Continuity by Protecting Information Integration

In order to fully safeguard themselves, firms should act to address three key scenarios:

When Integrated Applications Fail: There are two categories of potential failure to consider, “upstream” and “downstream.” Upstream failure occurs when a data source is unavailable; downstream when a destination system dependent on an update goes down. In both instances, firms should use approaches that preserve data integrity in the event of downtime. For example, in the case of source systems, make sure that data isn’t lost if a temporary outage or network unavailability occurs; and similarly, in the case of downstream systems, queuing upstream updates locally and employing mechanisms to propagate those updates to destination systems when they become available. The end goal is ensuring that if infrastructure is unavailable, key data isn’t lost.

When Integration Tools Themselves Fail: Ideally, the tools used to communicate information among applications and automate business processes should themselves be quickly restorable in the event of disaster. More importantly, the business logic controlling those tools should be similarly secured. The end goal is ensuring the pieces that tie the firm’s body together are themselves protected.

When Key Staff Becomes Unavailable: It is critically important not to overlook the role individuals play in the context of integration and disaster recovery. Situations may arise where key staff resources may become unavailable either temporarily, due to illness or injury, or permanently, due to turnover or unforeseen calamity. Whatever the reason, organizations are certain to struggle when those with specialized technical knowledge or process know-how are absent. For example, if legacy integration systems such as batch scripts need to be modified, teams may face significant delays as they struggle to decipher the work of others. The best way to address these issues is through defined, accessible processes and centralized, standardized integration technology. The end goal is to help available staff maintain normal business operations.

The Next Level

Firms that address these three key areas effectively will be much better prepared for more complex business continuity planning — for example, putting in place data sharing and process models that respond and adjust automatically in the face of disasters or adding sophisticated monitoring, tracking and notification capabilities across their business infrastructure.

By incorporating data integration protection into BC/DR planning, firms can rest more easily knowing that the systems that connect their applications, data, people and processes are safeguarded — in short, that the firm is “heart healthy.”

About our author :: :: ::

John Hall is the President of Integration Appliance. He has presented at several industry events on topics including business process automation, conflicts checking, ethical walls management, new business intake and financial process optimization. John can be reached at john.hall@intapp.com.