When lightning strikes . . .

are you prepared?

It can be as devastating as a fire, a major theft or other physical calamity that has the potential to wipe out your practice.

Or it can be as manageable as a power outage that puts you out of commission for a few hours.

Regardless of the scale, unpredictable events put the focus on you and how prepared you are for a practice interruption.

A topic – like the process of preparing for practice interruptions – is not necessarily an easy one. It takes time, effort and resources – all of which you are tempted to allocate to your immediate business pressures – to ensure that you and your practice are prepared for the unplanned. But as the events of September 11, 2001, have driven home, preparing your practice for business continuity is, in both the short and long term, good for business.

This issue of LAWPRO magazine focuses on how you can prepare your practice to weather virtually any "storm." The seven firms interviewed for our article represent a cross-section of firm sizes, practice areas and geo-graphic locations. For all of the firms interviewed, the issue of practice continuity is a priority; but the plan and preparations underfoot vary significantly. Although larger firms have the resources to plan, smaller firms are often better positioned to manage business interruptions simply because their processes and needs are less complex. In this article, we profile the "best practices" implemented by these firms, as one way of facilitating the exchange of ideas and information on this vital and topical issue within the legal community. Specifically, we examine this topic of practice continuity in four principal areas: preparing the plan, the people, the premises, and the practice.

The plan

"Accidents don't make appointments."

For most law firms, the events of last September reinforced this conventional wisdom and the need to prepare for virtually any kind of eventuality.

"It was a bit of a wake-up call for us all," admits Jamie Trimble, partner with Hughes, Amys.

"It made disaster planning a very topical issue for TLOMA (Toronto Law Office Managers Association) which in turn kick-started the planning process for many, many firms I know about," says Millie Waicus, network administrator with Bereskin & Parr.

"Without a doubt, it fast-tracked both planning and implementation of disaster recovery efforts," adds Arthur Shiff, senior partner at Davies Ward Phillips & Vineberg LLP.

But almost a year later, most firms are still grappling with the planning process.

At Goodmans LLP, the events of 9-11 prompted a major change in the scope of its business interruption planning. "Previously, we'd looked primarily at the technological issues," says Joseph Siu, the firm's chief technology officer. "After September 11, we refocused on the larger topic of business continuity planning: how do we stay in business if we cannot access our main office, how do we communicate with staff, how do we regroup."

Addressing those questions has raised even more issues that have further expanded the project's scope. "We're finding that certain ideas are not as feasible as we thought: There are back end issues related to moving data around to accommodate our decision to maintain a hot site that affects the front end – from both a resource and timing point of view. We've discovered we need to

Millie Waicus and Dennis Nault, Bereskin & Parr

Tom Troughton and Karen Curtis

upgrade all servers so that we can replicate information between our current and hot site; we need to accelerate the timeline for phasing out our Novell servers. These are all major issues from a resource point of view."

Developing and implementing the plan has become a "massive undertaking, with us doing two years of work in one." His goal: to finish compiling the master plan by the end of the current year so that Goodmans is prepared to meet its principal objective: To have the firm back in practice within 24 hours of a disaster.

Time and resources are more critical issues for smaller firms, which, by necessity, have opted to focus their recovery planning efforts on what Rick Mount calls "the mission critical issue: being able to service

clients." The ice storm of several years ago, as well as two virus invasions that ground the firm to a halt, have provided Mount Clark Yemensky Bowman with first-hand experience at preparing for the unpredictable.

"Our plan, though not written down, focuses on eight key areas: premises, phones, computers, technical support, database access, client document access, client files and accounting records," says Rick, a partner and the firm's "tech expert." Using this roadmap, he's assessed the firm's key vulnerabilities, outlined how to respond and the costs involved, and implemented a number of measures to minimize the impact of a business interruption on many of these core areas. For example, a spate of thefts at Ottawa-

Nepean area law offices prompted the firm to install its own office alarm system; renovations provided an opportunity to install a separate electrical system (with insulated, isolated circuits) and panel dedicated only to the firm's computer system. But Rick drew the line on changing passwords every two to three months: "You always have to balance risk against practicality and productivity," he points out.

It's this kind of pragmatism that is crucial to recovery planning, says Hughes, Amys' Jamie Trimble. "It is essential for every firm to work through a process of risk assessment: where do the most real risks lie; how do you eliminate or minimize them; and if you cannot eliminate or minimize the risk, how to finance them; as well, as lawyers, we need to take into

account the regulatory constraints we all face." In Toronto, for example, power outages are "almost epidemic – but this is a very manageable problem. You put surge protection and UPS (uninterruptible power supplies) on all systems." Similarly, the danger of virus contamination is much bigger than a server melt-down. "So virus protection software is a top priority – for our network, our laptops and anything that hooks into our systems."

Millie Waicus took the assessment process one step further, developing a "vulnerability assessment" spreadsheet that Bereskin & Parr now uses as its initial implementation guide. "Going through this process pointed out some critical but simple things we could do to reduce our exposure – in areas such as a power failure, theft and even flood." Drip pans have been installed over the firm's server area, to minimize damage that could be caused by a malfunction of overhead air conditioning units; the firm has reconfigured some of its computer equipment to ensure everything is on surge protectors and on a UPS; and it has created redundancies to allow for a backup capacity on its servers.

The next steps, adds Dennis Nault, director of administration and finance at the firm, are to "expand what we have on paper and itemize what we still have to do, especially when it comes to preparing for major disasters, and then bring everyone from management to staff into the loop."

But committing the plan to paper, say all firms, is only the first step: By definition, planning is a dynamic process. "Every firm should be doing a risk analysis on an ongoing basis," says Jamie Trimble.

"Once a year – usually during insurance renewal – is a good time to take stock, and turn your mind to the kinds of things you are doing to protect your practice overall," adds Tom Troughton, a Kingston-based sole practitioner.

Adds Mike McArthur of Cline Backus Nightingale McArthur in Simcoe: "We need to talk about this (recovery planning) a lot more as a profession. Technology, and what we now demand from technology, will fundamentally change the way we practise law. We have to be more management and systems focused – and that means looking at how we protect these systems on an ongoing basis".

practicePRO has created a spreadsheet that you can use to identify and assess your vulnerabilities. It is available for download at www.practicepro.ca/disasterrecovery.

Joseph Siu, Goodmans LLP

Russ Doucet & Mike McArthur, Cline Backus Nightingale & McArthur
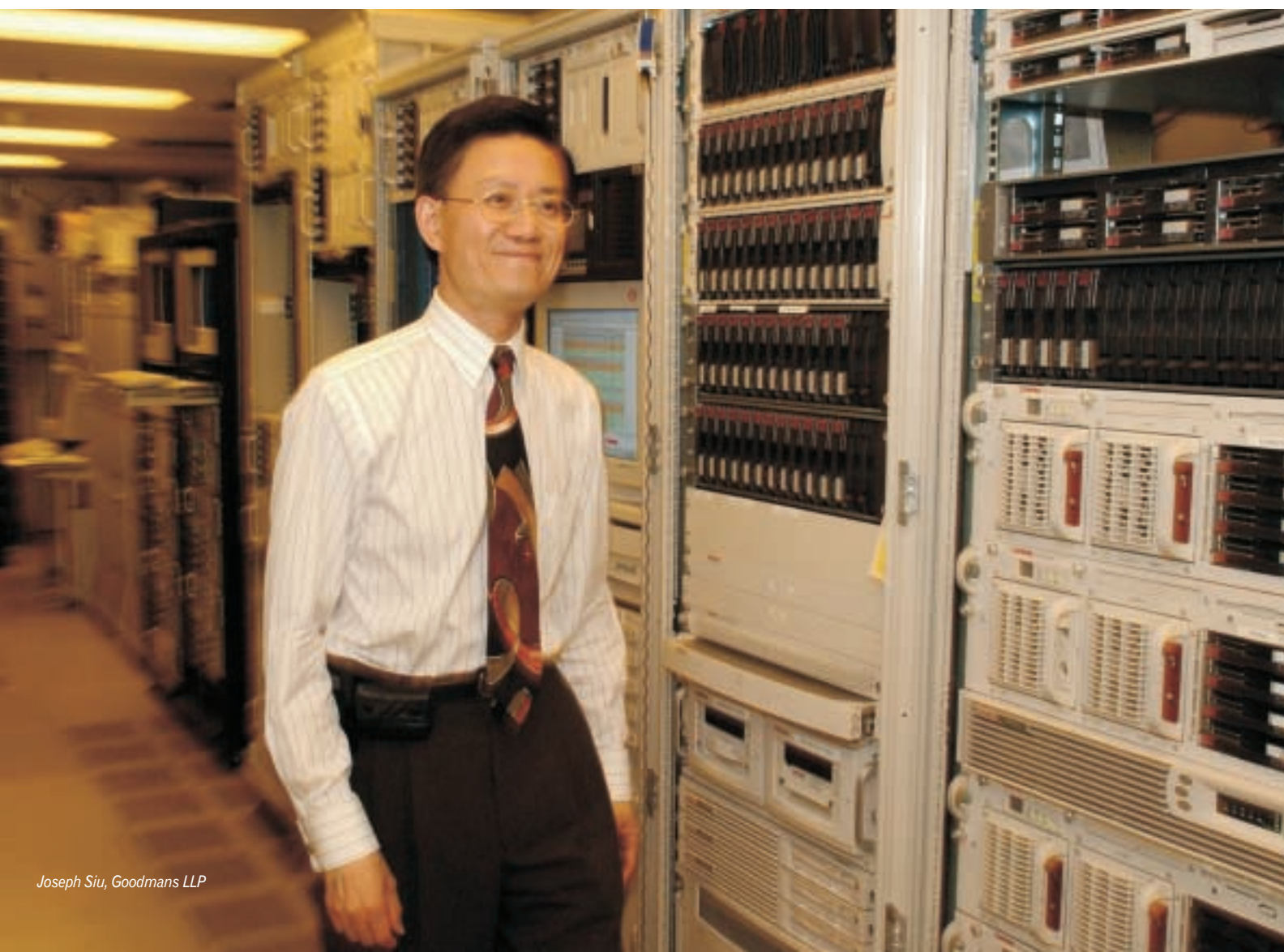
Preparing your people

Protecting the safety of their employees is a top priority for all law firms participating in this article. Many law firms maintain computerized staff lists with current home telephone numbers, e-mail addresses and even emergency contact names and numbers. Some have even established "telephone trees" with designated contact persons responsible for phoning others in case of emergency.

Goodmans plans to create a separate Web page that would provide clients and staff with access to critical information on next steps and contacts.

Davies Ward, like others, maintains a central number to which staff can call in for instructions in cases of emergencies; that line is used even now during major snowstorms, downtown power outages or other unforeseen events. The firm also provides seminars for staff to upgrade their first aid/CPR skills, and keeps first aid kits (and, in the case of Davies Ward and Bereskin & Parr, oxygen) on their premises. Like many firms, Bereskin & Parr has established pre-set meeting spots outside the building where staff are to congregate for a head count in case of a building evacuation.

Firms operating in highrises face unique people issues centred around evacuation, the ability to account for staff after an emergency, and staff ability to provide emergency first aid, points out Jamie Trimble. For Hughes, Amys, this meant pressing its building administration for more fire drills and evacuation exercises post 9-11; the firm pays special attention to the training of its fire marshalls and floor wardens. Davies Ward retained an engineering firm to ensure that, in an emergency, all doors would disengage and not lock staff in.

"When all is said and done, a firm's major asset is its people. We have to make sure that they are safe and equipped to handle any of these situations," says Jamie.

Protecting property and premises

Even the smallest of law practices today are computer-dependent. So it comes as no surprise that a principal concern for all law firms is the need to safeguard both its computer hardware and software and databases.

Regular backups a key

For many law firms, last fall drove home the need to not only do regular, thorough backups of all systems and databases, but to also store backups offsite and, for Toronto law firms, outside the downtown core.

Most larger law firms report doing full, daily backups that encompass client records, personnel records, accounting and supplier information; some send tapes offsite daily, others on a weekly basis. Bereskin & Parr has its two main client servers backed up remotely via the web on a nightly basis, as well as backing up all systems onto tapes that go offsite; plans call for all systems and databases to be backed up remotely starting this summer, thus ensuring two levels of redundancy for all of its online records and databases, reports Millie Waicus.

Goodmans has taken the backup process one step further, establishing a full hot site at a remote location outside the downtown core; the servers housed at the hot site are a replicate of its main servers, ensuring that the firm can be operational within 24 hours of losing its downtown location. Providing access to the hot site for a large number of staff, however, has created its own share of problems, reports Joseph. "Our Citrix system, which now supports 20 to 30 people, will need to be able to support 200 or more staff, making this server a much more important part of our overall plan than it was. And this change has significant resource implications."

A vital link in the technological equation, adds Rick Mount, is the technology support person used by the firm. Mount Clark has opted for a firm that maintains a VPN (Virtual Private Network), enabling its tech support firm to troubleshoot from offsite. The value of having the tech support firm also maintain identical backup systems was driven home recently when the law firm's central server "fried."

"Our tech support guy brought in his backup, boosted the RAM and had us up and running within hours, with one of our staff computers acting as the server," says Rick.

To ensure the integrity of its backups, Cline Backus Nightingale's Russ Doucet (the firm's information technology specialist), encourages staff to store all information on a server and not on their desktops. "We also remind staff to synchronize laptops and PDAs (Personal Digital Assistants) with our main network, so that we can ensure full backup of all of our work."

Protecting yourself by doing backups, maintains Tom Troughton, is as important for the sole practitioner as for the largest law firm. He and his secretary back up each other's desktop computers regularly. He also backs up onto an external hard drive, then copies the data onto his computer at home. "For a sole practice, especially, it is critical that you turn your attention to protecting your work – and to make your support person a vital link of that backup system, as she is absolutely essential to your practice," explains Tom.

THE NEWEST ONE:

Equally essential, even for a small practice says Tom, is to plan an alternative site in case your principal work site is unavailable.

He maintains at home the necessary equipment to operate an off-site office, being a computer, fax machine, copier, and Internet connection. His secretary has at her home both a fax machine and a computer that is connected to the Internet. This gives her the option of working from home, both now, and in the event of an emergency. From their respective homes, Tom and his secretary can communicate and share data with each other, as well as clients and other counsel, via telephone, fax or e-mail. Copies of the office backup diskette are taken home by his secretary. For security and confidentiality reasons the diskette is stored separate from her computer. She can access it on her home computer if necessary. This gives her all the information she needs to work from home, and provides additional safety as a second off-site location for storing the backup.

Nor is the home office concept limited to sole or small firms. Goodmans' initial plan would have lawyers working at home on an interim basis, likely with support staff working out of the lawyers' homes. This type of arrangement would complement a small working office, at a still-to-be-determined space outside the downtown Toronto core, which would accommodate core functionalities on an interim basis, says Joseph. Similarly, Rick Mount has equipped his own home office with additional circuits and wiring that would allow his home to act as a contingency site for several firm employees.

Law firms operating out of several locations, such as Davies Ward, plan to make one of their other sites a designated alternative site. In the case of Davies, its Montreal location likely will be designated a hot site at which the firm will replicate its Toronto systems; Bereskin & Parr plans to put backup servers into its newly opened Mississauga office, to facilitate business continuity. Hughes, Amys' Hamilton office would serve as an alternative site if a catastrophe hit its Toronto offices.

Protecting your practice

A law firm's stock in trade is knowledge – the information resident in its client records; and the intellectual capital of its employees.

Protecting client records from destruction therefore is a principal concern. Most firms use fireproof cabinets and/or storage vaults to protect critical client documents such as wills, powers of attorney, as well as other critical business papers. Tom Troughton has opted to store his critical client records in a vault in a main bank branch, for additional security. Mount Clark Yemensky sends its minute books offsite, to a secure storage facility. Rick Mount recently had that facility improve its insurance coverage, to better protect the firm in case any of those records were destroyed accidentally. Its location – a renovated service centre – has given Cline Backus the opportunity to house its critical client files in a concrete enclosed area in the basement.

Equally important – but less frequently acknowledged – in an effective recovery plan is the need to protect the firm's access to its intellectual capital, says Jamie Trimble. "It is essential, short and long term, to foster a culture that makes sharing of knowledge and information a way of doing business in the

firm," says Jamie. "You need to make it a policy that your people take intellectual capital out of their head and put it on the network – be it contact lists, precedents, research, or anything else. Intellectual capital cannot be proprietary and resident with one individual; it must be shared." Complementing this aspect of business interruption planning at Hughes, Amys is a policy of maintaining key man insurance on the firm's principals, as well as succession planning that addresses, among other issues, the need for partners to maintain powers of attorney on each other.

For sole practitioners like Tom Troughton, a backup "buddy" system is an essential part of protecting their practice. For the past 15 years, he and another sole practitioner in the Kingston area have covered for each other during vacations and other situations; both have also named each other as estate executors, and have powers of attorney for each other. An essential part of this buddy system, for Tom, is a periodic summary of next immediate steps for all of his open files: these summaries not only help evaluate his own practice but can also enable the buddy lawyer to step into Tom's shoes and service his clients on a "business as usual" basis. Maintaining a team approach with his support staff (under which their functions are complementary) and using this periodic summary makes easier another lawyer being efficiently involved if Tom is incapacitated.

And business as usual is what planning for the unpredictable is all about.

Rick Mount, Mount Clark Yemensky Brown

The interviewees

Mike McArthur is a partner with Simcoe-based Cline Backus Nightingale & McArthur. The seven-lawyer, fully computerized firm provides litigation, corporate and real estate services to clients in south-west Ontario. **Russ Doucet** is the firm's information technology specialist.

Rick Mount is a partner and technology expert with Mount Clark Yemensky Bowman in Nepean, just outside Ottawa. The six-lawyer firm provides a wide range of legal services (excluding intellectual property and criminal law) and makes extensive use of technologies in its offices.

Tom Troughton is a sole practitioner in general practice in the Kingston area, now practising on a semi-retired basis. A former teacher, university lecturer and college dean, he also served as president and director of CSALT (Canadian Society for Advancement of Legal Technology).

Joseph Siu is chief technology officer with Goodmans LLP, a 170-lawyer firm headquartered in Toronto but with offices in Vancouver and Hong Kong.

Arthur Shiff is a senior at Davies Ward Phillips and Vineberg LLP. The 225-lawyer firm has offices in Toronto, Montreal, New York and Beijing.

Dennis Nault is director of administration and finance with Bereskin & Parr in Toronto. **Millie Waicus** is the firm's network administrator. The practice of the firm extends to all aspects of intellectual property law.

Jamie Trimble is a partner with Hughes, Amys, a fully computerized, boutique litigation firm, helping clients from across Canada resolve their disputes. Hughes, Amys' 29 lawyers serve their clients from offices in Toronto and Hamilton. Because of his insurance-based practice, Jamie has a particular interest in risk management issues and matters.

Backup best practices

The following checklist is an extract from a more thorough discussion of computer-related issues in a new publication from practicePRO: managing PRACTICE interruptions. This full booklet is included as an insert with this issue of LAWPRO magazine, and is available for download in PDF format at www.practicepro.ca/disasterrecovery.

- **Do a full backup:** Full backups are preferred to partial backups. Having everything that was on your hard drive is better than finding out you need a critical file that isn't in your backup and is not otherwise available.

- **Do backups daily:** Modern backup hardware is able to do complete backups of large hard drives in a matter of hours. Backups can be set to run automatically, usually in the middle of the night. Doing a daily backup ensures you are as up-to-date as possible as you have all of the work and data that you created up until the end of the previous day.

- **Identify responsible person(s) and alternatives:** Doing the backup should be a mandatory responsibility that is assigned to a specific individual, and a specific alternate individual. You want to ensure that a backup is done every day, without fail.

- **Review the backup log:** Most backup software programs create a log report when a backup is completed. This report details what was backed up, and if there were any problems.

- **Regularly do test restores:** Don't believe the backup log. Periodically it will report successfully completing a backup, despite the fact that some or all of the data to be backed up was missed. The only way to truly test your back up is to regularly do a test restore of selected files and folders.

- **Identify offsite storage location:** Tapes left on top of your server in your office will be destroyed or taken along with your server if there is a fire or theft. You should store at least some backup tapes in one or more safe off-site locations.

- **Rotate and keep generations of tapes:** Don't use the same tape over and over; rotate your backup tapes. For example, use a series of five tapes, one for each night of the week. This can be helpful when database corruption is detected sometime after it occurred. Having an older backup will allow you to reach back to an earlier date if necessary. Some firms keep end of week, end of month or end of year backups.

- **Replace tapes regularly:** Backup tapes degrade over time and with use. You should replace your backup tapes every six months. When they get to the end of their life, rotate them out as end of month tape etc.

- **Don't forget data on desktops, laptops and PDAs:** Usually server backups are configured to only backup data on servers. Make sure that data on desktop computers, laptops and PDAs (Personal Digital Assistants) gets backed up as well. Also have staff backup the phone numbers stored in their cell phones.

- **Make sure open files are being backed up:** Some backup software, and in particular older versions, will not back up files that are in use or "open" by other programs. Central accounting system, e-mail and other database files often remain open 24 hours a day. Make sure that your backup is getting all open files.

- **Create written instructions for restoring:** Many offices have one or two people who know how to do a backup, but no one who knows how to restore backed up data. Create written instructions and train several people to do this task.

- **Find a hardware backup buddy:** If your backup server and tape unit are destroyed or stolen, you could find yourself with a good backup tape and no compatible tape unit to do a restore. Ideally find someone who has a server and tape unit that is identical to yours.

A partial backup from last week is better than no backup at all. If you aren't doing full regular backups, at least spend some time backing up some of your important files. It is easy to copy files onto a CD or some type of removable storage device. It is even easier to simply copy them to another computer on the network. This won't help if your office burns down, but it will if you have a hard drive failure.