



ERIN BRERETON

Owner
Chicago Journalist Media

“It could be any type of calamity. It could be a fire, your biggest referral source saying, ‘I’m not sending you any more cases,’ the death of a partner. A business continuity plan is just being prepared. I’m not trying to downplay the heartache and the tears I had watching my building burn, but I was organized and ready.”

Where Firms Are Falling Short on Business Continuity

Is your firm prepared for sudden employee departures, natural disasters and other unforeseen circumstances?

In 2007, shortly after being jolted awake at 4 a.m. by a phone call, Michael Morse found himself standing in front of the office building that housed his law firm — which was on fire and burning down.

The gravity of the situation wasn’t lost on Morse.

“I had client calls that were going to be coming in the next few hours,” he says. “I had lawyers who had to be in court. Most people would have been out of commission for weeks, if not months. But because we had a written-down playbook, we were up and running within a few hours. We didn’t miss a beat.”

While the COVID-19 pandemic has undoubtedly highlighted the need to be prepared for sudden challenges, less than half of law firms — 41% — said they had a disaster recovery or business continuity plan in place in a 2019 American Bar Association survey.

A number of the firms that do have merged the two plans into one comprehensive approach to unexpected events, according to Sharon Nelson, an attorney and President of Sensei Enterprises, which provides managed IT support and cybersecurity services to law firms.

“More often, we’ve seen a single unified incident response plan, and it covers both disasters and cyberattacks,” Nelson says. “It’s more hybrid now than it used to be.”

Whether your firm eventually faces a fire, a partner becoming seriously ill or other major event, having a plan in place that clearly outlines what to do — and who will do it — can position your organization to react promptly and effectively.

“The first seven days are usually the worst because on top of having to secure business continuity, you have to secure life continuity. You’re still a parent, a spouse, a child of somebody who will need your assistance during that turbulent time.”

If your firm hasn’t created a plan to address continuity challenges yet — or may need to revisit and revise the one it’s using — you may want to consider including some of the following elements.

DESIGNATED ROLES

Morse, Founder of the Michigan-based Mike Morse Law Firm, now coaches firms on operational practices and has co-written a book on the topic, *Fireproof: A Five-Step Model to Take Your Law Firm from Unpredictable to Wildly Profitable*. Morse notes the book is named “Fireproof” partially because it addresses preparing for misfortune. He says his firm was able to bounce back so quickly because it had put processes in place to address any major occurrences.

On the morning of the fire, by 8 a.m., firm members were answering calls in the parking lot and accessing files on their laptops. In the following days, individual employees tackled various tasks — somebody found new office space; another person dealt with server-related needs; a separate employee addressed the phone system.

“It could be any type of calamity,” Morse says. “It could be a fire, your biggest referral source saying, ‘I’m not sending you any more cases,’ the death of a partner. A business continuity plan is just being prepared. I’m not trying to downplay the heartache and the tears I had watching my building burn, but I was organized and ready.”

Delegating responsibilities — ranging from who will head up a hiring committee to who will regularly come into the office when it’s closed to pick up the mail — can help save time and confusion when it’s time to enact the response plan.

Nelson advises listing position titles as being responsible for specific tasks in the plan, though, instead of employee names.

“People come and go,” she says. “You want to identify the position, as opposed to the person.”

Renata Castro, Founder of Castro Legal Group, an immigration law firm with 38 employees, has designated a repository attorney to facilitate information being shared and prevent continuity gaps if she ever becomes ill.

Castro is also a proponent of preparing team members to step in for each other if necessary.

“You always want to cross-train people because if someone, God forbid, gets sick, gives notice, moves across the state — that happens,” she says. “You want to be quick on your feet on making that transition because your clients are going to be really sensitive, anxious, concerned — and you want to be able to address it.”

COMMUNICATION PROCEDURES

Your firm’s approach to sharing critical news and updates internally and externally will likely vary somewhat, based on the circumstances. However, a provision to address how those decisions will be made can be built into a response plan.

“Do you tell your employees about any of this?” Nelson says. “What if it spreads? Then you’ve got real reputational damage, which is why some people actually keep a PR person [listed] on the incident response plan.”

You’ll also need to confirm ahead of time that the firm has a way to disseminate information to the correct parties. While firms should have an up-to-date employee contact information list, instituting a client communication process can also be helpful.

Castro’s firm uses a messaging system to distribute important news to clients after events such as a hurricane.

“We can text clients in a certain area,” she says. “That’s the importance of collecting data on your clients. It really is about making sure every time you connect with a client, you validate their information — is this still your mailing address? Is this still your email address? Is this still your phone number?”

INSURANCE CONSIDERATIONS

Law firms may want to look into business continuity insurance, which can potentially help offset the revenue an employee would have generated until the person is able to return or be replaced. That said, it won’t provide absolute protection, says James Chittenden, the Founder of business consulting service OneClickAdvisor.com, who worked with Castro to create her firm’s continuity plan.

“If you have a key person who is sick and remains sick, that’s actually insurable,” Chittenden says. “But you want to have redundancy. You don’t want to have everything pinned on one person. [If] I’ve got all this important knowledge [and] get hit by a car, where does that leave the business? Insurance is just one small part of the planning.”

Along with specifications to contact any professionals you’ll need to work with — such as a data breach lawyer and digital forensics specialist after a cyber incident — plans should include any moves your cyber insurance policy requires you to make after a breach, according to Nelson.

For example, to be covered, a firm may need to file a formal claim, in addition to notifying its insurer.

“There are so many steps you have to take in any incident response plan,” Nelson says. “The plan has to contain all of the laws relative to a data breach or ethics in a disaster. For instance, if it’s a data breach, you’ve got to have the data breach notification law for your state.”

Your insurance company and a data breach attorney can provide guidance on how to handle informing clients about an incident. Although if their data has been compromised, Nelson says, in a ransomware or other attack, there’s no question they need to be told.

“That’s within the rules of all of the states,” she says. “You’ve got to put them in the best possible position and make sure they know that their data’s been exposed or taken. That doesn’t mean you have to make it public, but if you don’t pay the ransom, the bad guys have the client [contact information] — and they’re going to tell the clients they have your data. So you better have gotten there first.”

METHODS TO KEEP THE PLAN CURRENT

Once you’ve got a solid response plan in place, testing its feasibility is also important.

“You have to practice incident response plans,” Nelson says. “Most firms do tabletop exercises. You pretend that not only did you have a data breach, but the electric grid went down, and how does that impact everything? What do you do when the lights all go out?”

Frequency is also crucial. Firms need to look at their plan at least once a year, according to Nelson.

Now may be a good time. Given the pandemic’s effect on how law firms and other businesses operate, reviewing your



response processes can be beneficial, Sensei’s Vice President John Simek says. “The conditions have changed quite a bit. Should there be a problem with the electric distribution, what is your comfort factor? Do you think that you need to have potential facilities 20 miles away that might not be impacted, or is 2 [miles] good enough? Do you plan to rent or have on retainer data center space that has backup generators and offices where you can very quickly temporarily set up shop? Those are all things that should be part of your plan,” says Simek.

With revisions — or if you’re penning a new plan — preparing for the worst-case scenario can help ensure the response to whatever your firm encounters will be thorough, Castro says.

“Continuity is just making sure you have all your ducks in a row,” she says. “The first seven days are usually the worst because on top of having to secure business continuity, you have to secure life continuity. You’re still a parent, a spouse, a child of somebody who will need your assistance during that turbulent time. The last thing you want to be thinking of is, ‘Who will answer the phones now that we cannot get to the office?’ Just having basic steps in place helps a great deal.”

ABOUT THE AUTHOR

Erin Breton is a freelance writer, editor and content strategist who has written about the legal industry, business, technology and other topics for 20 years.

 breretonerin@gmail.com

 twitter.com/erbrer09

 chicagojournalist.com