DISASTER PREVENTION AND RECOVERY: UNDERSTAND AND ADDRESS YOUR RISKS TODAY

Ellen Freedman, CLM

I have been on the soapbox of disaster prevention and recovery planning for a very long time. If you've attended one of my seminars on this topic, you know I have experienced in my career-to-date many more disasters, of every type imaginable, than most will witness in a lifetime. I believe that the Pharaoh in Egypt and Job probably surpassed me, but fortunately for them they lived in simpler times, before technology and armed citizens added an additional layer of threat.

I have written extensively on this topic. Over the years my articles have appeared in the PBA *Solo & Small Firm Section Newsletter*, the PBA "*Solo & Small Firm Section Tech Report"*, *The Pennsylvania Lawyer*, the American Bar Association's *Law Practice Today*, and in countless newsletters and websites.

My first speaking appearance at LegalTech New York was a scant two weeks after 9/11. Due to the events, my topic was changed at the last minute to disaster prevention and recovery. My co-presenter —the late, great Ross Kodner — was much calmer about the sudden switch in gears, but I was unsettled. It was a huge responsibility. With the smell of acrid smoke still hanging in the air, we spoke to a room packed with intent listeners who wrote notes feverishly.

I say all this not to impress. Rather, I want you to understand that this is a serious topic to which I have consistently and continuously devoted a great deal of time and attention. I will not rest until the majority of law firms in PA have been sufficiently influenced as to take some real action to protect themselves, their employees, and their clients.

The appropriate outcome for your firm should not be a 100-page bound volume that gets parked on a shelf to gather dust. Rather, it should be a collection of checklists, some infrastructure improvements, regular education, and some change to or creation of policies and procedures. The very difficult areas have long been worked out by others, and there are resources to assist your firm. You can do this!

Surveys indicate that as high as 75% of U.S. businesses do not consciously prepare for disaster recovery. Chances are pretty good that you're one of them.

Unfortunately, statistics also indicate that businesses that actually experience a disaster will fail within five years. The smaller the firm, the more likely it will not recover. That's pretty grim.

If survival itself is not a sufficient motivator, consider that you have both ethical and legal obligations which require you to be proactive in this area. It's not optional. This is not something you can indefinitely put on the back burner any longer. Depending on the types of law you practice, the rules and regulations that apply will vary, as will the penalties and consequences for failing to establish good prevention, oversight and reporting procedures. At a minimum the following rules come into play:

Rule 1.1 [Competence]

Rule 1.15 [Safekeeping Property]

Rule 1.4 [Communications]

Rule 1.6 [Confidentiality]

Rules 5.2 and 5.3 [Supervision]

If your practice areas require that you handle sensitive information such as medical records (referred to as Protected Health Information or PHI); Social Security numbers; personal financial/credit information; information regarding mergers, acquisitions or public-owned companies and more, you have additional responsibilities under such regulations as the Pennsylvania Breach of Personal Information Notification Act (and similar legislation in other states or countries where your firm may represent clients), the federal Health Insurance Portability and Accountability Act (HIPAA) and the Securities Exchange Act of 1934.

To get started, let's define the world of disasters your firm might face. Risk will vary depending on your geographic location(s), firm size, and practice area(s). Many of the risks will require the same planning for response, recovery, and perhaps even prevention. So while the list is long, stay optimistic that your planning will not be. Generally speaking, disasters fall within certain broad categories.

1. **Natural Disasters.** Pennsylvania lawyers have contacted me over the years following crippling experiences with all of the following:

    - Floods
    - Hurricanes
    - Fires

- Lightning strikes
- Mudflows
- Blizzards / winds
- Extreme heat or cold accompanied by power loss.

2. **Technological Disasters.** I have received calls about and personally experienced such events as:

    - Equipment failures
    - Sewer main breaks
    - Water main breaks
    - Internet outages
    - Environmental hazards
    - Hard drive failures
    - Corrupted or unusable backups
    - Computer viruses and Spyware.

3. **Personal Disasters.** The crippling effects here are so severe that most of you have made it a point to attend one or more seminars dealing with the following:

    - Sudden death or disability of one or more firm owners
    - Sudden death or disability of a key staff person
    - Addiction, gambling, mental illness
    - Loss of mental faculties
    - Violence in the workplace, neighborhood, or employee home.

4. **Human Caused Disasters – Intentional or Unintentional.** Disasters caused just by unintentional human error are almost too numerous to list. Unfortunately, there has been a definite uptick in intentional harm. Consider such events as:

    - Intentional or unintentional deletion or harm to files, forms, software and/or data
    - Third-party crimes including cybercrime, fraudulent bank checks, and identity theft
    - Crippling or theft of computer systems
    - Theft of digital client information found on everything from dictation devices to firm copiers or old computers
    - Metadata transmission / exposure
    - Ransomware

- Data breach
- Acts of terrorism
- Theft of client funds / fraud
- Breach of client confidentiality
- Missed deadlines
- Clerical errors.

Whew, that's quite a list, isn't it? Do I detect some beads of sweat on foreheads? Some of you have already dealt with some of these issues and perhaps others I haven't even thought to include, in which case I encourage you to send me a note and let me know what happened. If you've been lucky enough to escape the possibilities noted above, it's unlikely you will get to the end of your career unscathed. As the saying goes, it's not a question of ***if*** one or more of these will occur, it's a question of ***when***! And let me remind you that you have an obligation to stay sufficiently competent with technology in order to understand and address risks and advise clients as well.

So what to do? First, we take a hard look at prevention strategies. The best and most productive use of your time will be to focus on prevention. Avoiding a problem is the best and most cost-effective solution. Directing some dollars toward prevention may seem like an undesired or unnecessary expense, but not when viewed as offsetting potential losses magnitudes higher.

Do you know anyone whose firm has been a victim of ransomware? Trust me, the cost of just the ransom — which provides no guarantee of getting the decryption key — is higher than the cost of prevention strategies. If the firm can't get the key, the cost to recover data and get the firm's computer(s) back in operation will also be magnitudes greater than prevention costs.

I'm going to get you started thinking about prevention. Space precludes me from covering all of the strategies you might employ for the risks identified above. The good news is that you're all very smart people, and there are loads of resources to help you.

Let's first address disasters that impact employee safety and possible prevention strategies. Whether it's violence in the neighborhood or a hurricane or fire at a local chemical plant that releases toxic fumes, there will be times when you need to be prepared to shelter in place to keep people safe. That means that you need to make some arrangements in advance. Do you have people with medical conditions which may require medication, such as insulin or glucose tablets, to be

kept on premises? Do you have ample water and sources of protein to take care of everyone for 24 – 48 hours?

Do you have an established communication protocol in event of an emergency so that everyone knows how to find out whether the office is open or closed, where to report, and so forth? What's your backup plan if the communication tools required for that fail? Is your emergency contact list up to date? How long will it take you to determine everyone's status? Following 9/11, it took some law firms over 72 hours to determine whether everyone was accounted for. That's too long!

If your office is in a converted home, consider purchasing a wireless doorbell at the local hardware store for about $15. Put the button under the receptionist's desk, and the chime back where people can hear it. That way your office can be alerted quickly if a threat presents itself. This simple strategy can save lives.

When it comes to fire prevention, I pay special attention. I lived through one fire at work so bad that the tips of my eyelashes melted before I was able to escape. My employer had no protocol and had evacuated everyone ***except*** me! Yes, it was traumatic.

Do you have sufficient fire extinguishers? Have people been instructed on how to use them? How about fire alarms? They're pretty cheap to add. Are your smoke detectors tested to see if the batteries are still charged? Have you held fire drills so that people know the various escape routes? When your office is in a converted house, there are often "dead ends" where people might be trapped by fire. Ensure windows in those areas can be opened and provide an emergency escape ladder. Then don't forget to tell employees and remind them regularly. In the event of an emergency evacuation, how certain are you that you will be able to account for everyone who was in the office within minutes?

Most natural and technological disasters involve destruction of client files. There's no gusset file in the world which can withstand a fire hose, a flood or a foot of mud. I can tell you from personal experience that a regular file cabinet, when closed, will usually provide sufficient protection of contents so that they can be professionally restored. But what sits out on a desk, on the floor and on open shelves is usually unrecoverable.

The only way to make sure your client files are safe is to digitize them. When your office operates in a paper-independent fashion, you are protected from the loss

of client files. You just need to make sure your methodology is well thought out and closely followed and ensure that you have two forms of daily backup: hard drive and cloud. Be sure to the backups regularly – at least monthly.

Paper independence also enables one to work effectively from anywhere at any time. The efficiency of locating information improves significantly with the introduction of document management / practice management software. Plus, malpractice risk is reduced.

I acknowledge that many of you prefer working with paper files. You can still do that. However, you should not reject digitizing files as a risk management and avoidance strategy based on your personal work preference. Remember, you don't go backwards in time when you start digitizing. You start with only active and new files and go forward with the new strategy.

Nowadays we all know that we must address data security. Once again, prevention is the first course of strategic action. That begins with a data security audit. That sounds difficult and pricey, but it's not.

If you have a regular information technology support vendor, you will be tempted to ask them to perform the audit. I don't recommend that. What you will get is a recommendation for lots of expenditures to improve your data security. But it's rare that an existing vendor will objectively examine and test your system and identify weaknesses in the design they have created or maintained for you. So use a third party. They can be physically located anywhere. They usually charge a modest flat fee. They test your system to determine vulnerabilities and provide you with a report and recommendations. Think of the movie "Catch Me If You Can" about the legendary forger. Your audit, if done properly, will be a thorough attempt to hack into your system through a variety of methods. You also want to test security on mobile computing devices.

With the report in hand, you can then work with your existing IT vendor to prioritize and implement solutions. Typical problems found at firms include missing or weak passwords, unpatched software, lack of end-user training on detection of phishing and malicious links, firewall appliances (routers and switches) with unchanged factory-default passwords, out of date antivirus or spyware software and more. I am currently upgrading the infrastructure of my own office technology. I was shocked to find out that the main firewall router still had the factory-default password of 123456! So much for the support company I ***was*** using.

Despite the fact that many attorneys are still uncomfortable with written policies, it's well proven that written policies serve to protect the firm. I've worked with firms where employees have illegally procured and installed specialty application software, without informing the firm. Including anti-piracy language in a computer-use policy may effectively insulate the firm from heavy penalties should the piracy be discovered by a routine software license audit. You have probably read or heard a horror story or two about improper use of social media, or improper use of a firm's computers to conduct personal business, manage a private business venture on firm time, or even attempt to intimidate others by sending demands under the firm's electronic masthead. For all these reasons and more, every firm should have a written computer-use policy. PBA members may contact me for some sample language.

Along with inevitable technology improvements, you should address training, revise or create written computer use policies, and develop your required response plan in case of a data breach. In addition to outside companies that will test your data security, there are companies that concentrate in training. Some even do follow-up testing of your employees to determine whether they are adhering to the guidelines they've been taught,

Lastly, this article would not be sufficiently comprehensive without focusing on personal disasters. If you are a solo or small firm practitioner, you should be aware that you have additional responsibilities to preplan so that your client's representation is protected in the event of your death or disability, or something of similar significance. My seminar on this topic is "Survival 101: Law Practice Emergency Planning for Death or Disability," and provides one ethics credit. If you have not yet attended this seminar, ask your continuing legal education director to get it scheduled. Or you can take it for credit on your own; you will find it (me) in the On-Demand CLE section of the Pennsylvania Bar Institute website, www.pbi.org.

In the event a personal disaster occurs, failure to preplan properly could lead to the appointment of a conservator by the court. The conservator will quickly disburse all active matters and escrow funds to attorneys suitable to continue representation. You could return to the office to find no active files, serious lapses in payment of business liabilities such as rent, payroll and insurance premiums, plus malpractice claims, and lost employees. Probably 30 percent or more of our Pennsylvania counties have had at least one solo attorney return from an unexpected disability to find his or her practice dismantled and unrecoverable. Don't let this happen to you!

Freedman Consulting, Inc.
(215) 628-9422

I expect that the weight of what you've just read may cause you to simply shut down in response. I know this can seem overwhelming. So I remind you again that there are vast resources already created. You don't need to reinvent the wheel. Please don't fail to act. If you're a PBA member, reach out to me so we can discuss how to take a baby-step-at-a-time approach to getting your disaster prevention and recovery plan in order.

A version of this article originally appeared in the March-April 2018 issue of The Pennsylvania Lawyer.

Freedman Consulting, Inc.
(215) 628-9422