zolasuite

Is Your Firm Prepared for a Disaster?

Is Your Firm Prepared for a Disaster?

This resource was created from a series of blog posts, written by Gail Ruopp, which were originally published on zolasuite.com.

Disasters can take many forms for an organization. They might include a compromised computer, a power outage, severe weather, an active shooter situation, a bombing, or a virus. Some of these situations are not as severe as others, but all need a plan to protect employees, clients, business partners, data, and files.

The Federal Emergency Management Agency (FEMA) estimates that 40 percent of businesses do not reopen after a disaster, and another 25 percent fail within one year. The factor underlying this failure rate is business' fundamental under-preparedness.

An organization needs a plan which:

- **Identifies levels of disasters and responses**
- **Identifies systems, tasks and processes that are critical to the operation of the company**
- **Identifies personnel responsible for business recovery activities**
- **Identifies alternate operations and processing locations**
- **Identifies the resources required to continue to effectively function, such as:**
  - Vital Records
  - Office Furniture and Equipment
  - Data Processing Hardware and Software
  - Supplies
  - Business Partners

The basic objectives of a disaster recovery plan should be:

- **To protect personnel, assets and informational resources from further injury or damage**
- **To minimize economic losses resulting from interruptions of business activities**
- **To provide a plan of action to facilitate an orderly recovery of business operations**

In the pages ahead, we explore the key components of a comprehensive disaster recovery plan. Our hope is that this information will help your firm begin down the path of creating a plan that delivers business continuity and peace of mind during challenging times.

Disaster Definitions

- **Level 1** disasters are considered a loss of power or other business sustaining services for an expected period of up to 48 hours. Damage is not large scale. It may consist of minor damage to the building, lack of access due to weather or city infrastructure conditions or significant hardware/software damage.
- **Level 2** disasters are ones in which the outage is expected to last from two to five days. Damage is more serious than Level 1 and may mean heavier losses to equipment and documentation (files, reports, contracts) due to prolonged events (fire, flooding).
- **Level 3** disasters are ones in which the outage is anticipated to last in excess of five days. Damage could extend to total destruction of the building, requiring replacement and/or significant renovation of the facilities. If a health pandemic occurs, consider this a Level 3 disaster.
- **Level 4** disasters involve immediate danger of possible injury, such as an active shooter situation. These disasters should be addressed separately because they require active participation immediately from all personnel.

Disaster Recovery Team (DRT)

The Disaster Recovery Team (DRT) must include members who understand specific aspects of the business. This may include business partners, such as data providers, and technology. The team should meet regularly – perhaps quarterly. If members are not at the same location, connect via a conference site, such as Zoom. Becoming familiar with a product like Zoom or Go To Meeting will better prepare the team to respond to a disaster when everyone is not at the same location.

A meeting which includes vital members of the organization and the team should meet twice a year.

Recovery efforts eat up 25% of staff time.

Emergency Phone Numbers

- **The first list** should include only employee phone numbers. It is highly recommended that team members maintain this list of numbers either in a smartphone or in an address book that is kept off-site. Identify the members of the team who will maintain this list. Send “test” messages occasionally to ensure the sender knows how to do it and the phone list is current.

  Choose methods of communication. VoiceShot allows the team to populate a distribution list and send a voicemail or text message to everyone affected. A member of the marketing department should immediately post a message on the landing page of the firm’s website. It is recommended that members of the DRT should practice using VoiceShot or a similar communicator.

  Normally, a member of the human resources department would be a good choice to maintain this list with one or two DRT members as secondary.

- **The second list** should include main phone numbers of business partners. This list may be maintained electronically and in hard copy by each member of the DRT. There is no need to send test emails to these entities via VoiceShot or similar messaging software. This list should include:

  - **Building Management** for every location. Even if a disaster occurs in one location, all management companies should be notified.
  - **IT Providers**: this should include providers for the cloud, time & billing, document management, the website, outsourced help desks, and internet and phone providers.
  - **Other Providers**: this includes your offsite storage, accountants, and all insurance brokers.
  - **Emergency Entities**: this may vary depending on location, but the team should include: the American Red Cross, area hospitals for all locations, the FBI, FEMA, local police departments, local fire departments, and poison control centers.

Staging Areas

When a disaster strikes, it is critical to know where everyone is located.

- **Wardens**

  For this purpose, wardens should be appointed, each to be responsible for a specific list of employees. A warden should also be appointed to contact business partners. Contact can be accomplished via VoiceShot or another mass communication platform.

- **Locations**

  Identify staging areas for each office location. The employees at each location should determine the most prudent, safe places to meet in case of an emergency. Locations should be within easy walking distance, but far enough from the building to address a bomb threat. Specifically, identify these staging areas by location.

- **Groups**

  It makes sense not to designate more than 20 people to report to any one staging area. A warden will be responsible for matching people at the staging area to names on a list, so it's important not to make any list too long. Things usually become chaotic during emergencies. Keep things simple, so that no one is easily forgotten.

- **Drills**

  At least twice a year, a drill should be implemented at each location. The times and frequency of running these drills may vary between offices, but drills are very important. When a disaster strikes, people will need to react automatically. For this reason, it is important for everyone to participate in these drills.

  It may make sense to schedule the disaster drills when the building management does its fire drills. It is the responsibility of the wardens to account for the people on their lists, and to have their groups go to their staging areas. Expect people to complain, but if they don't practice when it is not an emergency, they may not survive when it is.

Alternative Facilities

Prepare beforehand. Alternative facilities should be designated to accommodate those disasters that will continue for some time. When seeking alternative facility options, it is critical to be able to properly access all technological applications and documents remotely. It is important to review all current leases to determine if rent has to be paid when the building is not accessible.

- **Working From Home** may be the best option. This alternative has become quite common since the Coronavirus pandemic. However, many people do not know how to work from home for an extended period and how to effectively interact with colleagues and clients. For this reason, a work-from-home policy should be prepared, reviewed and endorsed by each employee. This policy should:

  - **Include a "home office" provision.** All employees are to be based in a primary office—this will accommodate an employer that may not want to abide by another states' labor laws.

  - **Ensure that employees have a safe work area in their homes.** All communications must be secure, which requires that the internet in each home be secure.

  - **Specify the party responsible for each expense** and explain that all the company's employment policies apply when working remotely. It would be worth the investment to hire an employment attorney to review the policy to ensure that the company is compliant with all labor laws.

  - **Offer classes throughout the year** that teach employees how to properly work and communicate effectively when working remotely. It is also possible to find courses dealing with these subjects that include certification credits (CLM, CLE, CPE). It may make sense to offer this accredited training at least once a year.

Remote work has grown 44% over the last five years.

  - **Sublease Space**. When dealing with a disaster, if it becomes necessary to sublet space, it is important that the new space be secure, both from the disaster and technologically, and that all documents are stored in a confidential area. Be sure to properly evaluate the environment, however; it may make more sense for employees to work from home.

Shelter in Place

Schools routinely instruct students how to behave when there is an active shooter in the vicinity. They practice what to do and what not to do.

- **Training**

  Many police departments offer free active shooter training to instruct employees what to do in such cases. Though much of this information may be found online, it can be of great advantage to have the police visit the location; they can determine the best action to be taken at each specific facility.

  When a disaster recovery team attempts to present this type of training, fellow employees tend to dismiss it. But when the police present the training, their expertise in these matters is usually well-received.

Education

- **Employees**

  Educating employees is an ongoing initiative. While not every employee needs the same level of education, it is critical to continue the disaster education process throughout the year for all employees.

- **Wardens**

  The level of disaster education for wardens is more intense. Wardens must be better prepared and be willing to actively participate in training. CPR training is recommended. Appropriate training is available and emergency kits are easily affordable.

  Wardens should routinely communicate with the employees on their lists. To help them achieve this goal, scheduling break-out group meetings after company-wide meetings is a good idea.

  Routine training is critical. This is not “one and you’re done” training. Training for all employees should occur, at the very least, annually. It is recommended that disaster-training presenters be brought in from outside the company since people tend to pay more attention to outside presenters. Wardens should schedule their group meetings prior to or after these training sessions.

  Training should include how to use Zoom or Go To Meeting applications to accommodate people who may need to use FaceTime on their cell phones. (Most office phones, today, can transfer incoming calls to cell phones.)

  It may be prudent to maintain a staggered schedule requiring departments or groups of employees to work remotely once a month or quarter; this will keep the workforce familiarized with the use of various disaster-related technologies.

According to the 2019 ABA Legal Technology Survey Report, only 41% of lawyers say their law firms have disaster recovery plans.

Communications

Communication is critical during a disaster. Contacting each client and business partner via phone or email may not be prudent depending on the situation so here are some other options:

- **Websites**

  Websites are now widely used to research a company. It may make sense to post press releases on the company's homepage. It is important to keep all information on the website current, so removing outdated press releases is critical.

- **Sample Press Release**

  (Date of press release) COMPANY NAME (specify offices if relevant) has sustained damage from (an explosion, a fire, a flood, etc.). No employees were injured. The source of the (explosion, fire, flood, etc.) is under investigation.

  For security reasons, we have been asked not to make further comments at this time.

  Following a standard procedure, put in place some time ago, key employees have been temporarily moved to (address and telephone/fax numbers) and business will commence as usual (time and date). While we will endeavor to continue normal service, we ask our clients to bear with any minor delays in responding. Our aim is to run a seamless operation from our temporary post.

  Further information will be announced as soon as possible.

- **Social Media**

  LinkedIn is being used more and more. The company probably has a page on this social media platform. It makes sense to update the company's page with a brief reference; remember to update it and remove it as necessary.

- **Direct Communication to Clients**

  The size of an organization should determine how best to communicate with each client and when.

  Provide an active client list to various teams. Each team should contact assigned clients via telephone.

  The team should provide active clients with an immediate update and progress report to assure them that the company is continuing to address their business.

  Prepare an email that can be sent to inactive clients to assure them that the company's services remain available to them. Take this opportunity to let inactive clients know that they should not hesitate to reach out for new business or other resources that the company may provide.

  If a disaster continues for an extended period, it is best to include relevant narrative on all emails in the signature area. Most companies include a confidentiality notice in signature lines. It would be prudent to add narrative stating that employees are working remotely or that the company is closed and to indicate how best to communicate.

- **Potential Lawsuits**

  Document, document and document. Keep all correspondence. Confirm a conversation with an email. Expect employees, clients, and business partners to litigate. Check with workers compensation, employment practice, professional liability, and commercial insurance brokers to ensure that the company is properly covered in case of an emergency or disaster and that there are no exclusions.

- **Post Disaster**

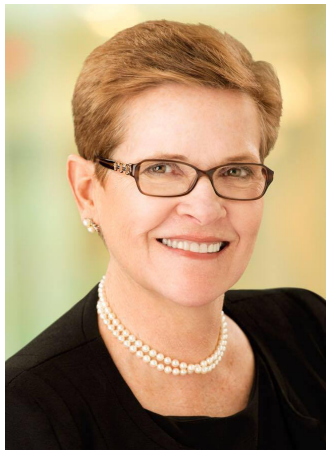
  Document, document and document. Keep all correspondence. Confirm a conversation with an email. Expect employees, clients, and business partners to litigate. Check with workers compensation, employment practice, professional liability, and commercial insurance brokers to ensure that the company is properly covered in case of an emergency or disaster and that there are no exclusions.

Businesses are affected by many unforeseen circumstances. Establishing business continuity and disaster recovery plans are essential to help your firm prepare for, and bounce back from, threats to your firm's operations.

About the Author

Gail Ruopp has acquired more than 25 years of professional experience in senior law firm management, initiating best practices in administrative operations, including: financials, accounting, lateral recruiting, personnel, day-to-day operations, systems management, and firm marketing.

Gail has served as an Executive Director at New York City and Philadelphia area law firms dealing with various areas of practice. www.gailruopp.com



Zola Suite is a secure, cloud-based legal practice management platform that allows you to access your firm's matters, files and financials from any location at any time. Zola Suite employs state-of-the-art technology to detect, investigate and stop threats before they can impact your firm's operations.

Deployed on Amazon Web Services (AWS)

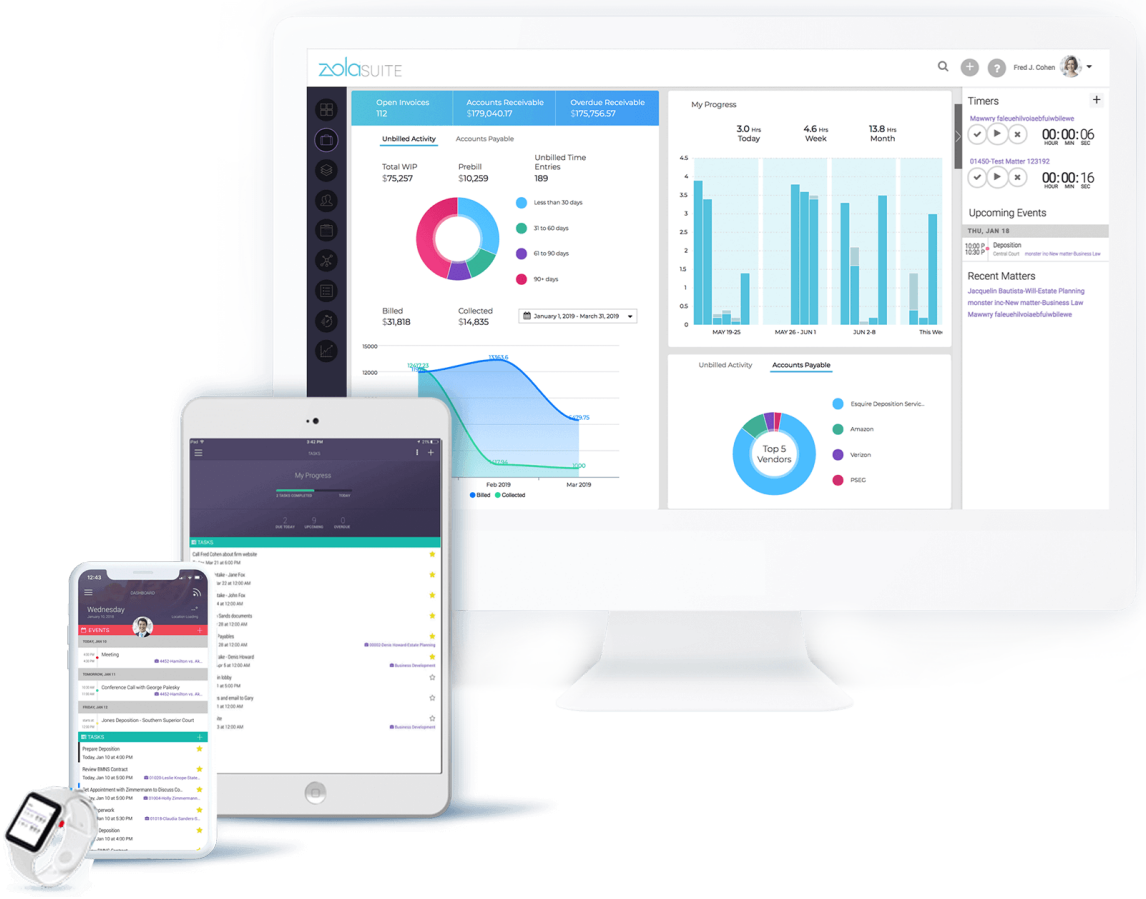
Two-Factor Authentication

Strict Password Strength

Detailed Logging of All Activities Within the Account

Infrastructure Certifications Include ISO 9001, ISO 27001, SOC 1/ISAE 3402, SOC 2, and SOC 3, PCI DSS and HIPAA

Bank-Grade TLS Encryption



Schedule a demo at zolasuite.com/demo

zolaSUITE

Citations

Wackrow, J. (2017, May 3). A guide to business continuity planning in the face of natural disasters. Retrieved from https://www.csoonline.com/article/3193616/a-guide-to-business-continuity-planning-in-the-face-of-natural-disasters.html

Rock, T. (2018, January 31). 2017 Disaster Recovery Statistics that Businesses Must Take Seriously. Retrieved from https://invenioit.com/continuity/2017-disaster-recovery-statistics/

Hering, B. (2020, February 13). Remote Work Statistics: Shifting Norms and Expectations. Retrieved from https://www.flexjobs.com/blog/post/remote-work-statistics/

Despite coronavirus, most law firms lack disaster plans. (n.d.). Retrieved from https://www.americanbar.org/news/abanews/aba-news-archives/2020/03/coronavirus-and-disaster-response/