Protecting your Vital Records from Natural and Man-Made Disasters

By Cadence Group's Records and Information Management Practice Group

There is no place on earth that is 100% safe from disasters. Whether man-made or natural, disasters can strike at any time, at any location, and to anybody.

- In August, 2017 Hurricane Harvey, the first major hurricane impact on the U.S. since the famous 2005 hurricane season, dumped a year's worth of rain in Southeast Texas and Louisiana in a matter of days. The human and financial toll from this storm is likely to be felt for decades.
- Huge wildfires out West ignite every year, consuming homes and businesses in paths that can span over thousands of acres – causing untold devastation in their wake.
- Earthquakes, flash floods, snow storms, and tornados are wreaking damage throughout the world, often with little or no warning.
- On the man-made front, arsonists, insider threats, industrial espionage, and accidents can bring a business to its knees overnight – and don't forget, cyber security experts routinely warn that it is not a matter of IF a cyber event happens, but WHEN…

Considering these "once every X-Years" storms appear to be occurring with increasing frequency, and the news is filled daily with a wide-ranging gamut of other catastrophes, the need has never been more urgent for organizations to protect their information assets, in all formats and media. They must identify, locate and track, as well as protect their vital records from natural and man-made disasters. And if the worst happens, they must ensure that vital records recovery is built into their disaster recovery plans.

What are Vital Records?

First it is important to understand what constitutes business records, as well as how to identify the portion of records that meet the criteria for being vital. According to ARMA International, records are defined as "recorded information, regardless of medium or characteristics, made or received by an organization in pursuance of legal obligations or in the transaction of business." Simply put, a record is information used by an organization's employees to do their jobs. A vital record is a subset, defined by ARMA as information "fundamental to the functioning of an organization and necessary to continue operations without delay under abnormal conditions." Vital records are typically divided into two categories. First are ***emergency operating records***. These are records you would need in the first hours or days of a crisis, as well as mission critical

records, which cannot be lost for any length of time without causing irreparable harm to the organization. Whether your organization is a business, non-profit, or government agency, emergency operating records should include records such as emergency contact lists (employee information and disaster recovery contractors), orders of succession/delegations of authority, continuity of operations or business continuity plans, and emergency operations manuals. The second category of vital records is ***legal and financial rights and interests records***. These include records that protect the rights of the organization as well as those affected by the organization (employees or stakeholders (citizens or customers)). These might include contracts, employee files, customer case files and the like.

Vital Records Protection Plan

Regardless of category, vital records need to be identified, located/accounted for and protected in a vital records protection plan. Here is a simple five-step plan, adapted from the U.S. EPA's Records Management website, for identifying and protecting your organization's vital records.

1. ***Identify your vital records categories/types***. The first thing you need to do is to review the information and records maintained by your organization and determine what information would be needed in an emergency. There are three types of information that rises to the level of vital records:

    - **During the Emergency** – Records/information necessary to respond to the emergency at hand. These records pertain only to that work which is necessary to handle the crisis. It is assumed that no day-to-day work will be done during the disaster and that you may not have complete access to your records.
    - **Immediate Aftermath** – Records/information necessary in the first few hours after the crisis. These records can include delegations of authority, vital records inventories, and other information needed in the near-term.
    - **Long-term Continuity of Operations / Recovery Records** – records that involve activities which are the most critical to the organization's mission. This assumes that your records are completely inaccessible for a prolonged period of time and the few most critical activities will need to be continued off-site without interruption.

    To facilitate identification of vital record types, consult with department heads, legal counsel, executive leaders, and other subject matter experts with knowledge of your organization. In addition you can review the Records Retention Schedules and mission statements, organization charts or other material documenting your organization's key functions and processes.

2. ***Conduct an inventory of your vital records***. Next you need to prepare a listing, or inventory, of the records identified in Step 1. Decide who needs to have copies and

establish a procedure to ensure the inventory is updated and sent to the appropriate people. In order to conduct this inventory, you will need to have the help and cooperation from a number of parts of the organization including:

- People in business units who are familiar with the various records created or used in their portion of organization. They serve as vital records coordinators and implement the vital records program for their business unit, including preparing the inventory and working with office staff to ensure records are protected. They may also have to compile information, such as a list of access methods.
- Management - Make a vital records program a priority as quickly as possible. This includes revising priorities of the staff to allow time to implement the program.
- IT (Database Managers and Network Administrators) - Ensure electronic systems in their control are regularly backed up and accessible in an emergency. This may require storing copies and equipment to read the copies offsite.
- Staff - Be as cooperative as possible and assist where needed.

3. ***Determine how you will protect your vital records***. Now that you know which records in your office are vital and where they are located, you need to determine how to protect them. There are two basic choices: (1) duplicate them and store them offsite; or (2) collect them from other sources and recreate them.

   The following is a list of questions that will assist you in making your decision.

   - Can these records be found in locations other than your office and geographic location (e.g., a regional office, offsite storage center, a State, or another organization (such as a Federal agency or subcontractor, etc.)
   - For physical records, is the information contained therein also available in an electronic system or database?
   - What is the most cost effective manner to recreate these vital records (e.g., storage on electronic media, photocopying, collecting them from another organization)?
   - Do these records contain any sensitive information which would require special handling?
   - How often does the information need to be updated and who will be responsible for updating it?

   Note: If you will be duplicating information, use electronic media whenever possible since the cost to reproduce and store information electronically will be less than duplicating and storing paper. It is also critical to have a backup in case the primary

electronic system fails. This can be accomplished by copying onto portable electronic media or cloud storage. We will discuss secure electronic storage later in this article.

4. ***Designate an off-site location, or locations, for your vital records storage***. Based on the decisions made in Step 3, it is likely you will need to find at least one offsite location to store duplicates. If you work for a public agency or large business with multiple locations, a facility may have already been identified, or you may want to identify multiple facilities. If not, here are some things to consider when selecting a location:

    a. 30 miles is usually considered sufficiently close for access, but far enough away so that physical records will not be vulnerable for most emergencies. If you are located in an area at risk (vulnerable to large storms, lies in a floodplain, or near a fault line) you might consider a greater distance, and preferably further inland or less vulnerable locality

    b. Physical records which will be needed immediately, such as the emergency preparedness plan and telephone tree, can be stored in a manager's home. However, it is important that another copy be stored in the central location for off-site storage. That will allow access to the record if the manager is not available.

    c. Other organizational offices, as well as local company off-site records centers or commercial offsite storage, may be appropriate choices.

    d. Don’t forget any equipment you may need to access the records.

    e. The records will need to be immediately accessible; therefore, physical records should be stored as close to the facility for emergency off-site operations as feasible, given geographical vulnerabilities. Commercial storage allows immediate access to the records at all times, which may not be possible at a secured organizational facility. Electronic information can be stored further away as long as access is not adversely impacted.

    f. Consider incorporating telecommuting options as part of your disaster plan, unless your organization does not have the infrastructure or ability to support telecommuting. Allowing appropriate employees to work from home or other locations outside of the office during a recovery period is a good option, especially for disasters requiring extended recovery times. Remember, however, that this ability may be restricted if there are widespread interruptions in the power or telecommunications systems.

5. ***Document location and protection decisions in your vital records inventory***. Once you have decided what to protect, how the records are to be protected, how they will be kept up-to-date (refresh rates) and any contingency options, add the information to your inventory. The inventory should show:

    a. The method of protection (e.g., backups, photocopies, etc.);

    b. How often the records are updated (the rotation schedule), including who does it and how is access tested/validated;

    c. Contact/Access information if the records are to be collected from other locations or accessed via cloud/offline storage mechanisms

Records should be updated as often as necessary to ensure that the information remains relevant if you need to use it. Weigh the risk to the recovery effort if the information is out of date against costs of keeping it updated.

Ensure that any other documents which contain information related to your organization's vital records program, such as the office's continuity of operations or business continuity plan, reflect the most updated vital records program-related information, and that the information is communicated to all individuals who will need to follow the procedures.

Create a resource list of disaster recovery firms for your geographic area and update the information at least annually.

Don't forget to test your plan to be sure the recovery runs smoothly. Include drills on using the equipment, supplies, and procedures for vital records recovery.

Securing Electronic Vital Records

Large organizations typically have secure electronic storage and backup systems that support continuity of operations in the event of a disaster. As previously noted, it is important to test these capabilities on a regular basis. For smaller organizations, it is important to properly research your needs and create tools and a governance process that so it fits the needs and budget of the organization.

For very small organizations, it might be practical to securely back up information on a regular basis to a portable device or multiple devices and remove the device(s) to a safe distance from the business premises on a regular rotating basis. Storage devices have become much smaller and more reliable in recent years making this a viable option. The device(s) can them be stored

either at another facility that belongs to the organization, or at a commercial off-site storage facility. Many of these facilities offer pick-up/delivery services as well.

Many organizations, large and small, are discontinuing the practice of backing up electronic records in favor of remote "cloud" storage ". When selecting a cloud provider, it is important to examine your needs and the prices and options available. The first set of options to consider is the frequency of backups. Backups can typically be scheduled on a daily, weekly, or monthly basis. Some services also offer an on-demand option and now services also are offering automatic or constant updating, where files are updated as they are saved. Some even offer versioning so you can access previous iterations of a file.

Cloud providers generally offer remote accessibility, whereby authorized personnel do not need access to the organization's physical assets to access electronic information. Remote accessibility makes your organization's information available, regardless of the condition of the physical office space. As with network or shared drives, robust access controls must be implemented and reviewed regularly to protect company information from unauthorized access.

Security options vary from service to service and might include user name and password authentication, encryption (128 or 256 bit) and internet protocol such as secured socket layer (SSL) or Transport Layer Security (TLS). Some services run on redundant server grids and some also have data centers with 24/7 staffing and backup generators to ensure access to your information. As with any service where your information is in the custody of a 3rd party, you need to review the terms and conditions of the service carefully to make sure you understand any issues that pertain to the ownership and use of the information and your costs and ability to remove it from the service. If you have any legal or regulatory obligations that may restrict where and/or how you store your information, you should have those reviewed as well.

Conclusion

Unfortunately, it often takes an event like Harvey, Snowzilla, or WannaCry ransomware attack for organizational leaders to assess disaster readiness. When (not if) a disaster strikes, the organizations that incorporate vital records into regularly-updated disaster recovery plans are the ones that will survive. The organizations that put information governance on the "backburner" become afterthoughts. Given the high price of failure, it only makes sense for organizations to invest in the protection of their vital records or, as we like to say, "Business Survival Insurance." Start today to safeguard the records that are vital to your organization's survival.

For more information on how to kick-start your organization's vital records program, please contact our team of certified records managers at 888-246-8125 or email us by completing the Information Request Form located on our website (www.cadence-group.com/contact) and clicking on the Submit button.

* * *

About Cadence Group®

Cadence Group® is a certified woman-owned small business and GSA Contract Holder that has offered sustainable and integrated information management services for over 25 years.

Other Resources

National Archives and Records Administration (NARA)
Federal Agencies: Preservation of Records in Emergencies
https://www.archives.gov/preservation/records-emergency/federal

Environmental Protection Agency (EPA)
EPA National Records Management Program
https://www.epa.gov/records