Managing the Crisis: Disaster Planning and Records Management

Abigail Bibee, Mê-Linh Lê, and Nazi Torabi. School of Library, Archival, and Information Studies. University of British Columbia

VITAL RECORDS PROGRAM

WHAT ARE VITAL RECORDS?

Vital records are records essential to the operation and functioning of an organization. They may be unique records that are not easily reproduced that provide information about :

- Financial and legal status of the organization
- Rights of employees, stakeholders and customers

DEVELOPING A VITAL RECORDS PROGRAM

Perform a risk assessment: Identify all possible risks to the organization and its records including : natural (e.g. earthquake), technical and mechanical (e.g. power outage) and/or human (e.g. mishandled records)

Risk Assessment Formula: R = P x C
R = Risk of the loss of a vital records series due to a disaster
P = Probability that the threat will occur in any given year
C = Cost of the loss if the threat occurs[1]

Conduct a business impact analysis: Determine the **critical** functions of the organization and **identify** the vital records necessary to perform these tasks. Assesses the impact the loss of vital records would have on the organization to determine which records are most valuable.

Create a business continuity plan : Outline specific resources, actions and data necessary to respond to and recover from a crisis. Include the results of the business impact analysis and the risk assessment.

PROTECTION OF VITAL RECORDS

Dispersal & Duplication: Actual duplication of records; transfer of duplicates to another location
Pros: Cheap, easy, built into regular routine, can protect vital and non-vital records
Cons: Sheer number of duplicates can be overwhelming

Protection Storage: Specially designed fire-resistant or environmentally controlled equipment, storage containers, or vaults to hold material, e.g., Granite Mountain, Utah (picture below)
Pros: On or off-site, protects duplicates
Cons: On-site records could be destroyed in disaster; off-site makes it hard for vital records need to be easily accessible

→ What's best? A combination of dispersal and protective storage

VITAL RECORDS SCHEDULE

Inventory All Records: Gather information to determine which records are vital (will vary by organization)

Classify and Inventory Vital Records and Information: Different classes of vital records (e.g., Class 1 is irreplaceable and vital to the business; Class 4 are non-essential records that do not prevent the business from resuming following a disaster

Set Priorities: Vital records assessed to determine which are absolutely necessary to resume business following a disaster; this will determine the protection method used

Select Protection Methods: Most appropriate protection method for each record must be listed on the schedule

Compile a Vital Records Schedule: Schedule based on all information collected in steps above. Schedule should include a unique ID code, the location(s) of the record, its format, its electronic application, its usage level, protection methods and vulnerabilities, and classification and priority.

ELECTRONIC RECORDS

COMPONENTS FOR PROTECTING VITAL RECORDS

Identify electronic vital records; covering all platforms (not only mainframe or network servers)

Determine electronic application(s)

Maintain local hard drives & shared repositories

ID appropriate electronic replication methods and quality control during duplication to ensure that the tapes or optical media are legible and understandable

Determine the number of copies (single or multiple copies)

Establish procedures on regular transfer of digital records from local drive to network servers

Establish suitable storage conditions and locations; considering environmental problems, including the avoidance of dust, water, and magnetic fields[2]

E-MAIL MANAGEMENT

E-mail as one of the most critical communication mediums in organizations plays an important role in decision-making processes because e-mail outages may lead to:

⇩

The corporate e-mails become substitute by employees private e-mail accounts.

⇩

The corporate e-mails become fragmented.

⇩

Legal discovery processes and production of evidence for litigation may be impaired.

⇩

Loss in revenue[3]

Factors to be considered during e-mail recovering plan process:
- The number of e-mail users
- The budget
- The importance of e-mail in the organization's operations[4].

CASE STUDIES

TERRORIST ATTACK – 9/11

The attack on the World Trade Center on September 11, 2001 (9/11), resulted in the loss of thousands of lives and the destruction of countless records. Records stored in paper format were destroyed in the attack, unless they were carried out by survivors. Organizations that relied solely on paper records were vulnerable to significant losses.

> "No one planned for a wholesale destruction of human assets and information assets at the same time."[5]

Lessons Learned

- After 9/11 organizations re-examined their disaster plans to include worst-case scenarios. A survey conducted at the Disaster Recovery Conference revealed that 97% of respondents admitted to revising their organization's disaster plan after the 9/11 attacks[6].
- The attack highlighted the superiority of storing vital records off-site, as opposed to on-site, as records may be lost if a building is destroyed. Relying on vital records stored on-site in paper format poses many risks.

NATURAL DISASTER – HURRICANE KATRINA

In 2005 Hurricane Katrina swept across the southern US. Little attention was paid to the destruction and loss of vital records. Items lost include:

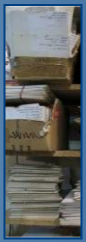
- Medical records, school records, law enforcement records, court records and driver's records.
- Medical offices were destroyed, legal evidence was submerged in standing contaminated water for months, and individuals returning to save records were confronted by alligators.
- Without records, individuals and organizations faced enormous difficulty in proving who they were, what they owned, and where they lived [7]

Lessons Learned

- Medical offices and hospitals that used electronic health records (EHRs) were able to continue operations and resume business much quicker
- More organizations must consider the transfer of vital records to a digital format
- Disasters of this magnitude may require a relaxation in identity requirements
- Proper disaster preparedness must take the worst possible case (and more!) into account
  - Disasters often break or succeed previous records or expectations of the "worst that can happen".

> "Unless you experienced the disaster and understand the full impact of a loss of information data, it's just a mindset - we'll get to it when we can." [8]

CONCLUSIONS



- Assessments must be conducted to identify risks to vital records
- The best way to protect vital records is to use a combination of dispersal and protective storage
- The creation of a vital records schedule is a critical step in any records management plan
- Email is a critical communication tool and an email recovery plan should be part of any vital records plan
- Organizations that have a vital record plan in place are much more likely to quickly and smoothly resume business after a disaster, are better equipped to help their customers, and are less likely to go under
- More organizations must consider moving vital records to a digital format