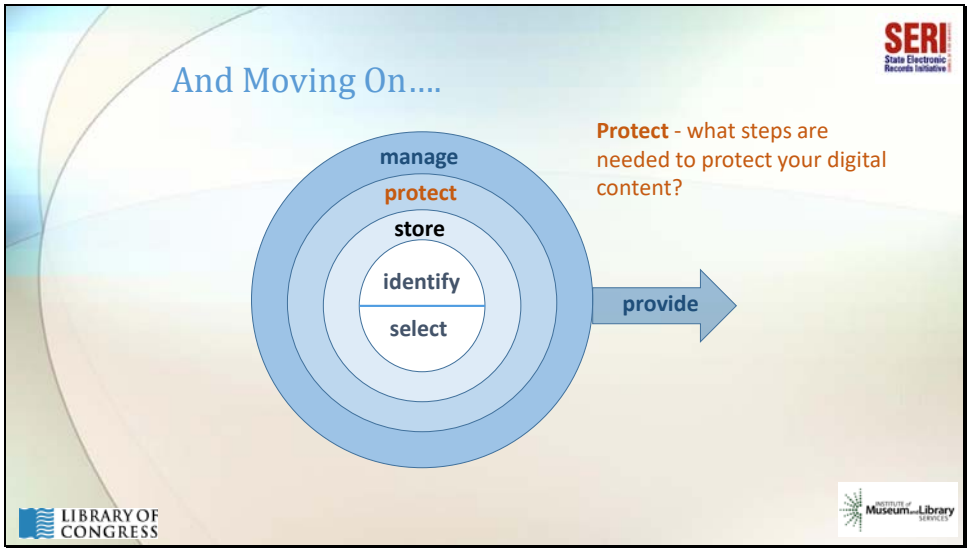
Slide 1

Welcome to Managing Digital Content Over Time. This training was produced by the State Electronic Records Initiative in coordination with the Council of State Archivists. It was developed under a grant from the Institute of Museum and Library Services and based primarily on training created by the Library of Congress. It is designed to help archivists and others who manage digital content understand the necessary steps of digital preservation. This is module 4, Protect.

Slide 2



What steps are needed to protect your digital content?

Slide 3

Many of you probably have some kind of institutional disaster preparedness plan for your physical items. But often there isn't anything in those plans that specifically addresses digital content. Digital content faces different threats than physical items but they are also very similar threats. So we are going to talk about the various types of threats facing digital materials and how to address them and learn about the types of policies that can assist with protecting your content.

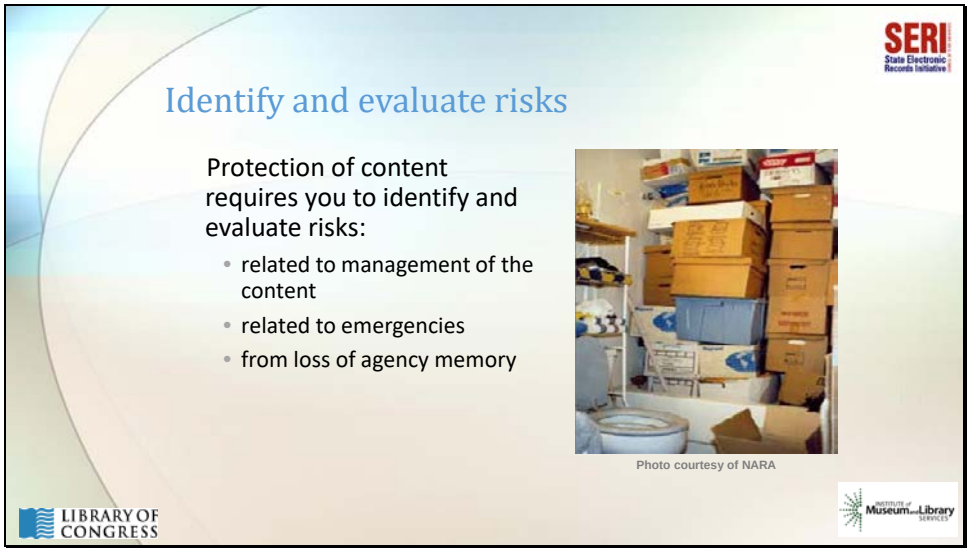
Slide 4

What are you protecting?

There is the obvious…

And the unspoken.

Slide 5



Protection of content requires you to identify and evaluate risks related to management of the content, related to emergencies, and from loss of agency memory. Regarding the loss of agency memory, if someone leaves, do you know what they managed, and do you know where it is?

Slide 6

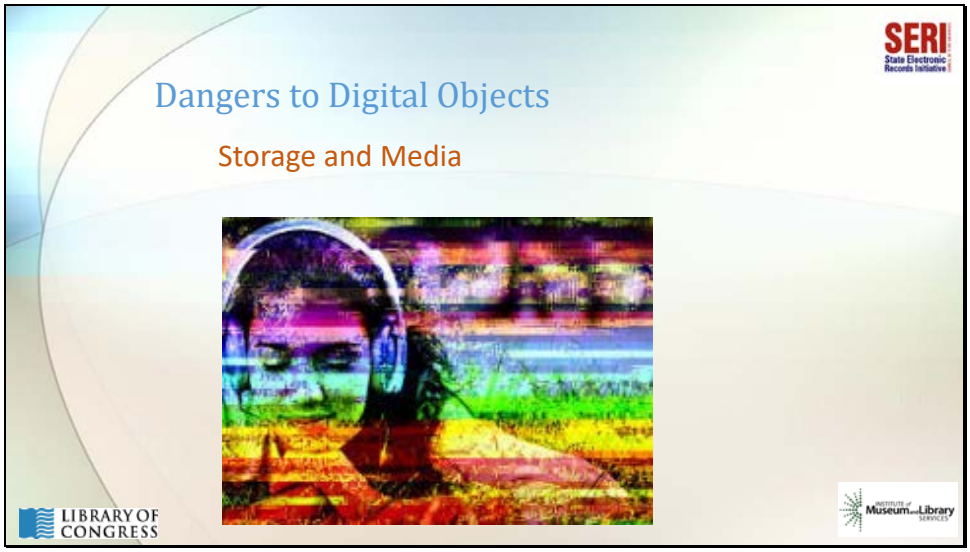
Have you ever lost any digital assets?

What steps are needed to “protect” your digital assets?
We will be talking about 2 different aspects of protection

1) Immediate day-to-day concerns
2) Business continuity and emergency planning

What exactly are we protecting our assets from?

Slide 7



Have you lost content, or had a close call? This is common and often an incentive for organizations to do more about preservation, disaster planning and business continuity for preservation.

Corruption of data – Bit rot

Drive failure –

While you can lose bits and bytes in any digital content – it tends to show up most obviously in images.

It could be due to storage practices, or the media it's stored on.

Slide 8

Dangers to digital objects include lost or stolen computers, mobile devices, and external media.

Rights access – who has access to your treasures? Can the wrong people come in and delete or change your content?

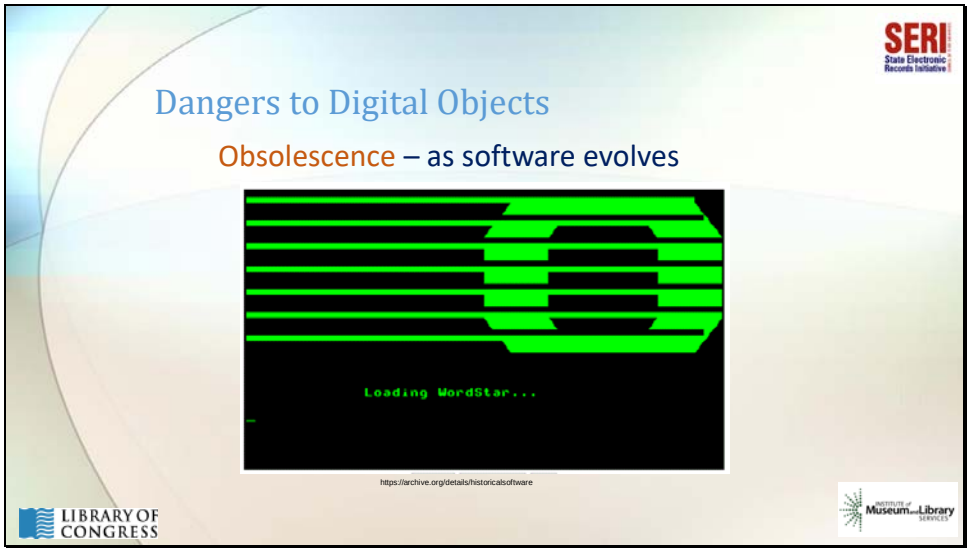
Could they steal your content and possibly disclose personal information?
Are you protecting against viruses?

This issue also applies to management of paper records, right?

Slide 9

In September 1956 IBM launched the 305 RAMAC, the first computer with a hard disk drive (HDD).
This photo is the IBM 350 disk storage unit utilized by the IBM 305 RAMAC and you could lease it for $3,200 per month.
The HDD weighed over a ton and stored 5MB of data.

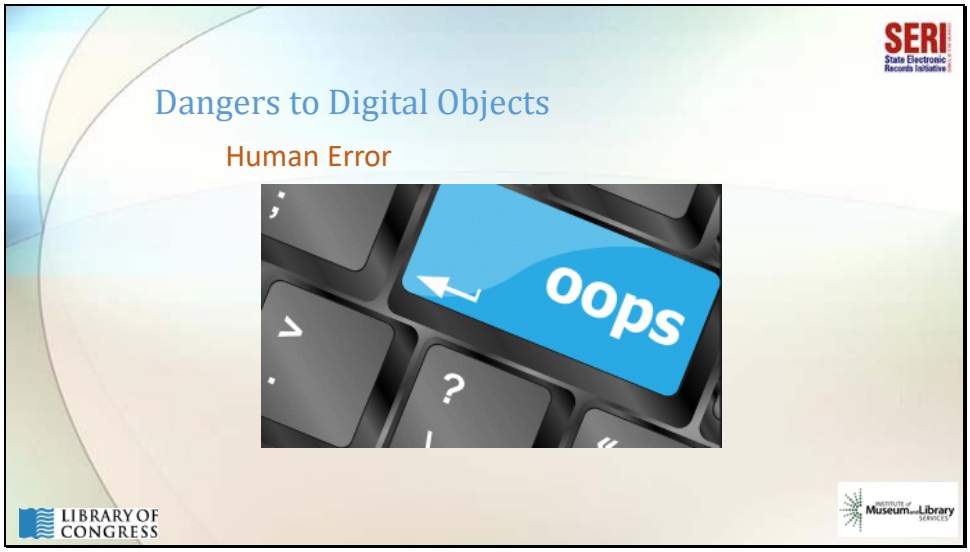
Slide 10



Also file obsolescence. File formats continue to evolve and change.

What kinds of things are you currently managing that may become obsolete, or that would you like to access that you can't because you don't have the technology or proprietary software to access it?

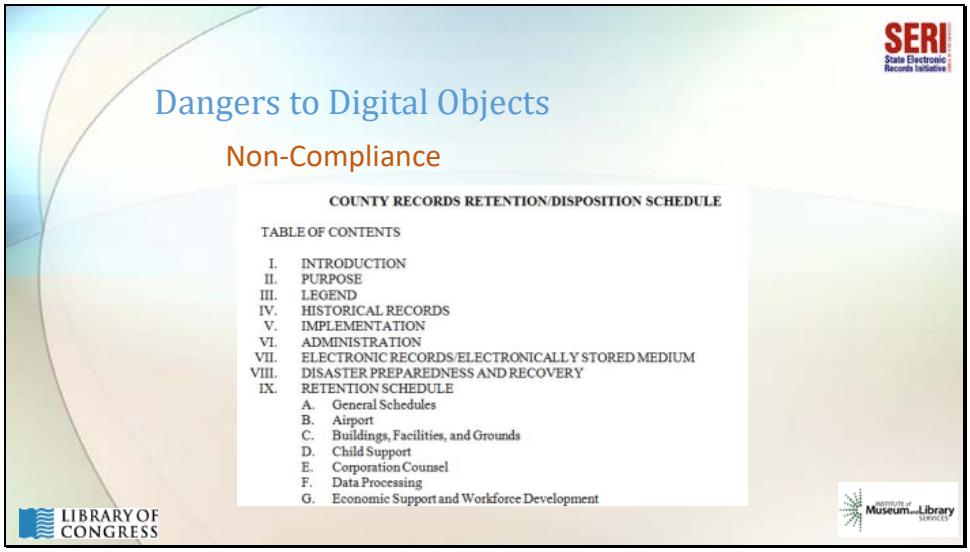
Slide 11



Human error includes deleting, overwriting or misplacing content.

Again – also a paper records management issue

Slide 12



Non-compliance means someone didn't follow a schedule and deleted something they should not have.

It's easy to find examples of where both paper or digital content was deleted and shouldn't have been.

Slide 13

What kinds of Natural Disasters might affect you? These are the BIG things: Hurricanes, Floods, Earthquakes, tornadoes.

What happens if one of these things hit where you are? What happens to the paper, what happens to the digital systems? Can you protect those things that are most important to you?

Slide 14

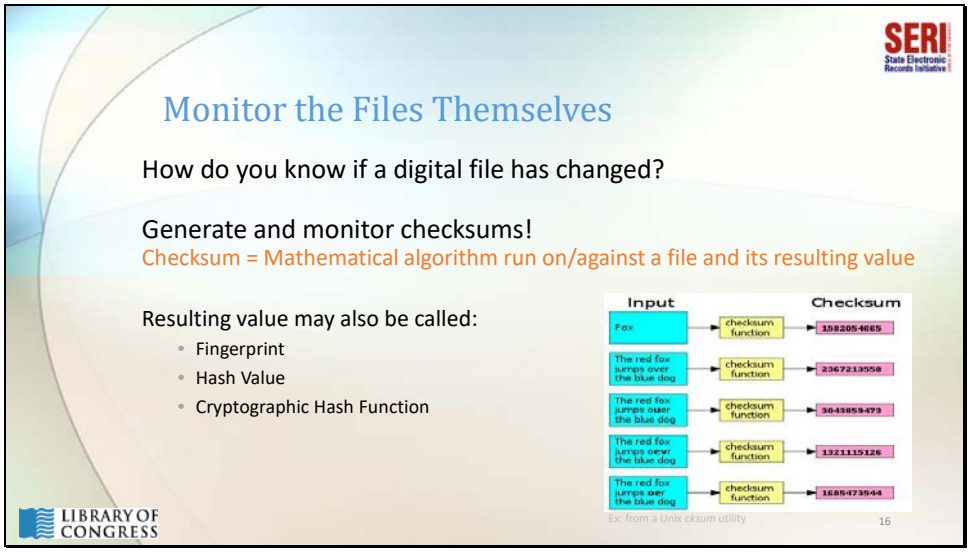
Moving on …

You can potentially face emergencies of all kinds. Disasters tend to speak for themselves. Some disasters may be more likely depending on your particular circumstances. If you work in an older building, you may face a number of threats due to old infrastructure. In the building pictured, water disasters are much more likely and probable. This is currently more of a threat to the repository's physical collections but a definite concern for digital content. If multiple copies of our digitized materials aren't kept, they could be destroyed by one disaster.

Slide 15

Have multiple copies. Know where your content is location. Know who can have access to it, and know who accesses your secure information. Continual caution and awareness help avoid day-to-day threats to digital content. Each one of these tasks requires some kind of metadata, which may be stored in the same or a different system as your descriptive and preservation metadata.

Slide 16



Being able to verify that a file has not changed when you copy it from one storage medium to another, or become corrupt over time, is extremely important and can be done by creating and monitoring the fixity (or stability) of a file. There are various types of programs that can help monitor fixity.

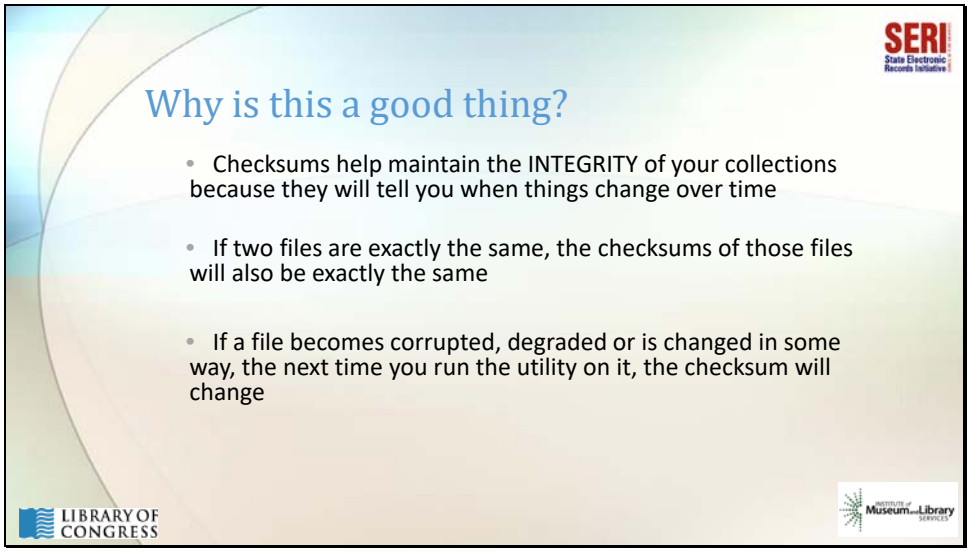
One of the simplest methods for monitoring fixity of your files is to generate checksums.

A checksum is an algorithm run on a document whose resulting number is referred to as the checksum value. The resulting checksum is a short sequence of letters and/or numbers that uniquely identifies that file based on the document's content at the bit level. After this checksum value is known, a checksum can be re-calculated on the document again at any time.

When you compare checksum values between the first time you run it and subsequent runs, if the numbers are identical then the document has not changed; if the same number was not generated then the document has changed somehow.

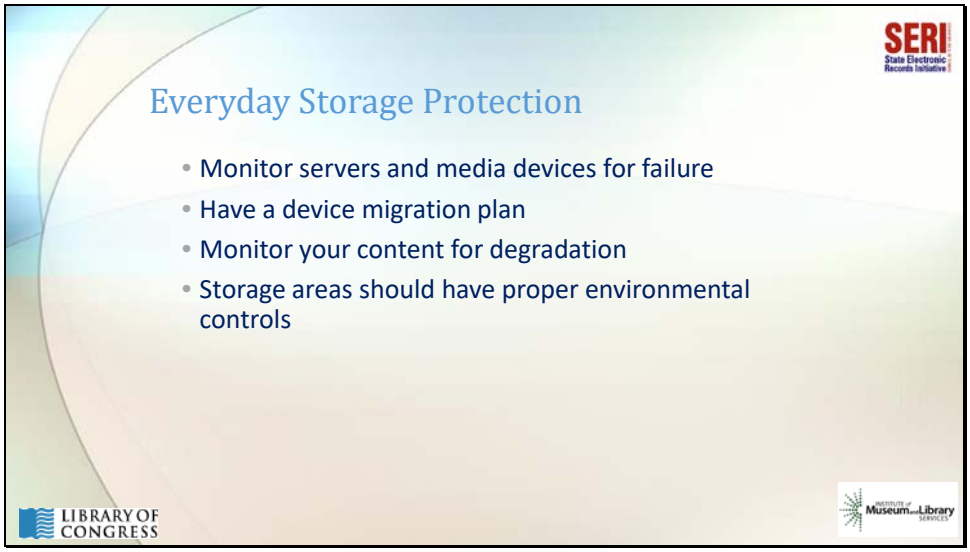
If differences are detected, this method does not tell you what has changed or when something was changed, just that the two documents are no longer identical at the bit level.

Slide 17



Maintaining integrity is important for both Legal and Audit purposes. Check your checksums on a regular basis so you can replace a corrupted file with a clean 2nd copy promptly.

Slide 18



Monitor servers and media devices for failure. Have a device migration plan. Monitor your content for degradation. Storage areas should have proper environmental controls.

Slide 19

Continual caution and awareness can help avoid day-to-day threats to digital content.

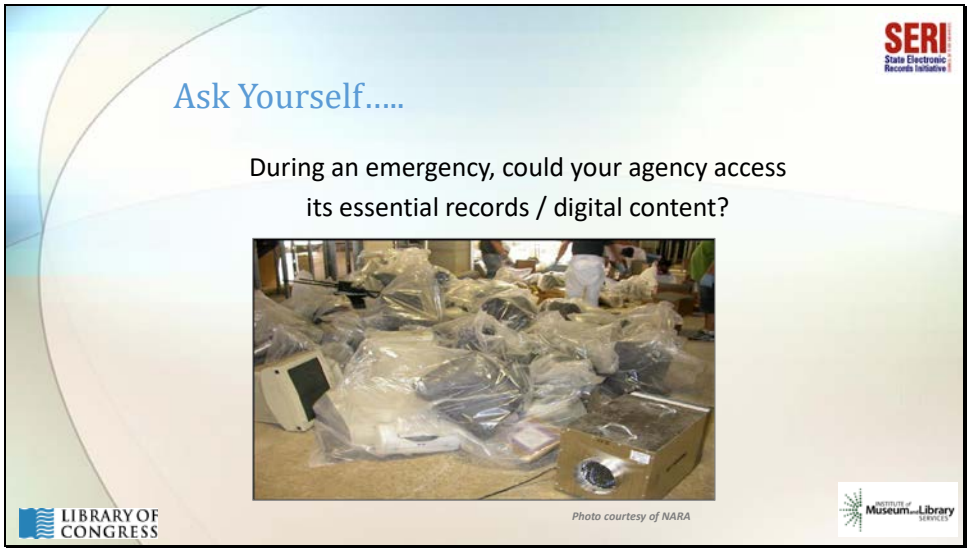
[LOCATION]
Onsite and offsite; online and offline

[Who has ACCESS?]
All staff or just certain people, IT staff, others?
How about the servers themselves? Could someone just pick it up and leave with it or is it in a secured room?

[AUTHENTICATION]
It's a good idea to have more than one person that has access - But not so many that you lose control over access.
What level of access do they have? – Can they read it, write or change it, delete it?
Access to your records should be documented and recorded

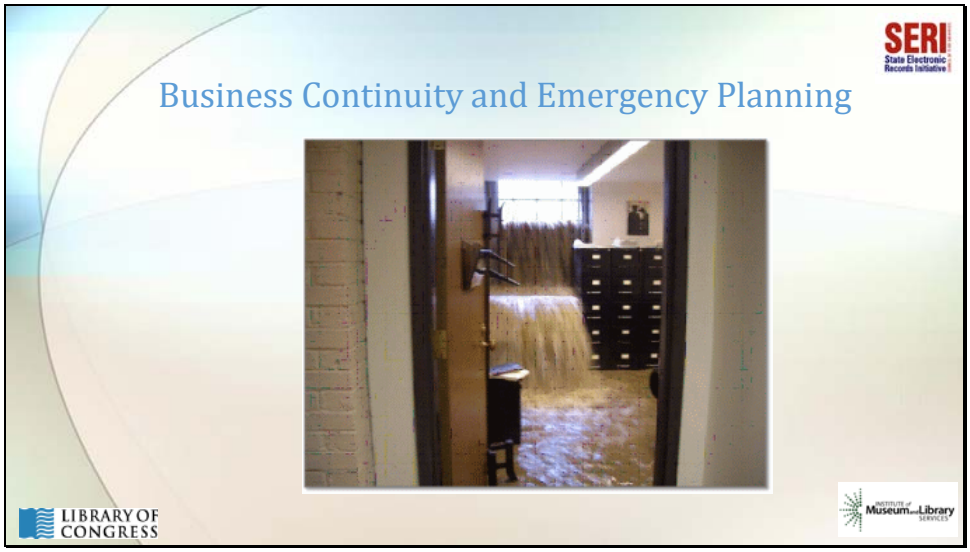
[USAGE]
Usage helps identify the most significant content, and prioritize preservation.
It includes web use, internal use and activities, plus maintenance.

Slide 20



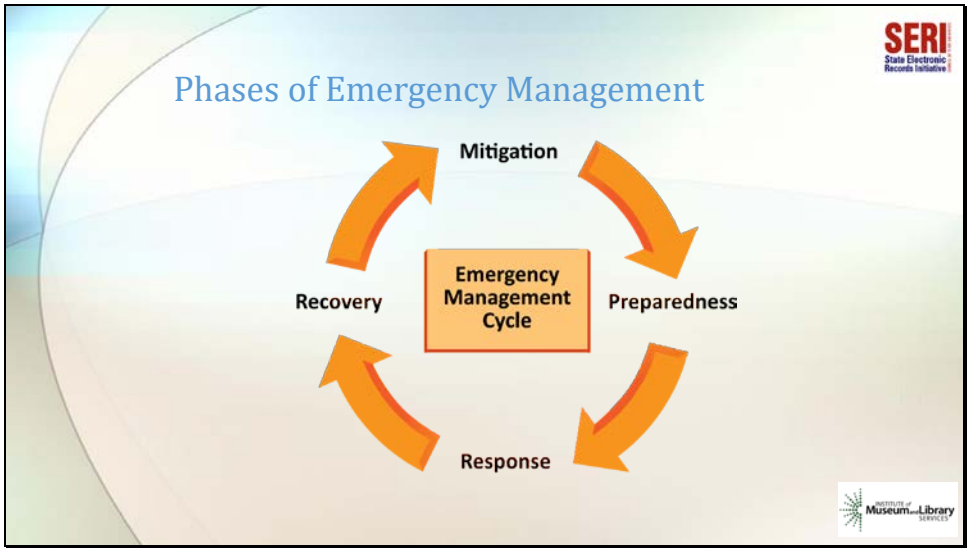
Ask yourself: During an emergency, could your agency access its essential records or digital content?

Slide 21



So now we are going to talk a little bit about Business Continuity and Emergency planning within your organization.

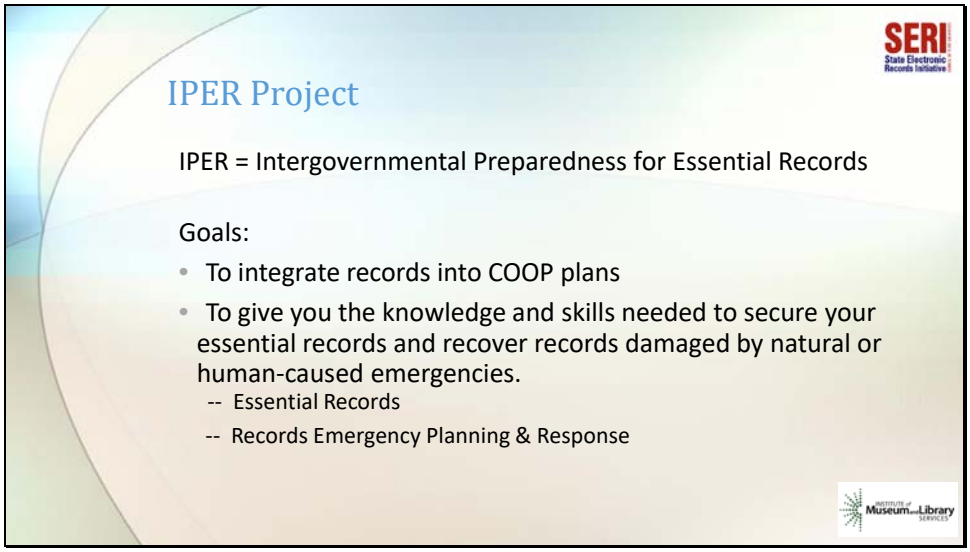
Slide 22



These are the key phases of the Emergency Management Lifecycle
We are going to start with the “preparedness” step –

- Identifying areas of risk to records
- Identifying essential records
- preparing for emergencies

Slide 23



As part of that, we are going to wrap in a little bit about the IPER project. IPER stands for Intergovernmental Preparedness for Essential Records (IPER) Project, which grew out of the Katrina disaster.

Recognizing that emergency preparedness is critical for archives and records centers, CoSA created these self-directed online courses with the support of FEMA to help state archives and other institutional users continue improvement of their preparedness and training programs.

There are 2 key goals with this program…
First - Too often, the COOP (Continuity of Operations Plans) process neglects the identification and protection of essential records.

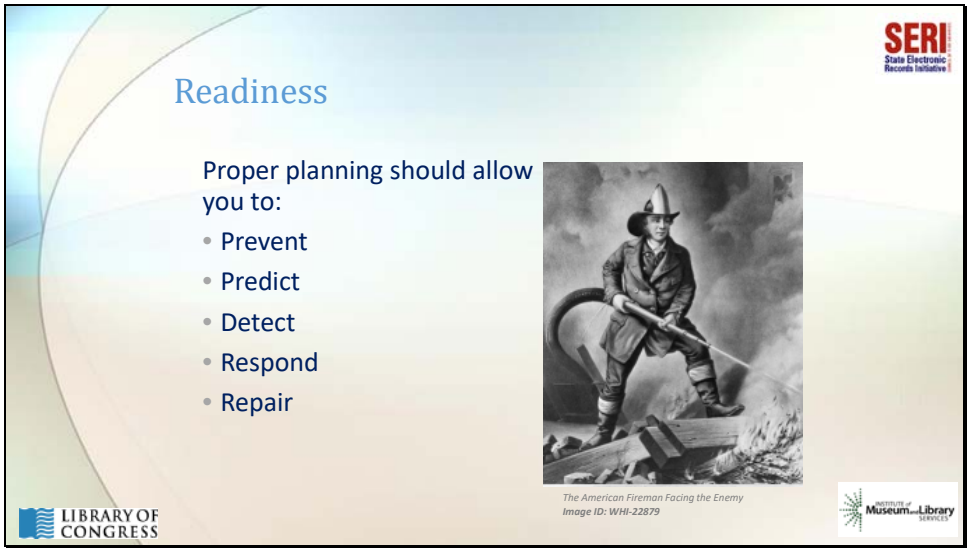
Records custodians must be prepared to protect their essential records so that, in the event of an emergency, their offices can recover quickly and return to service for the residents of their state or locality.

Second – Secure your essential records and recover records – which it does through two courses.

The goal of this course is to enable participants to establish and administer an essential records program, and also to train participants to develop and activate a Records Emergency Action Plan in order to protect, mitigate damage to, and recover records in the event of an emergency.

For today – we will be looking at this planning process broadly in terms of essential records – but from the repository standpoint – you may well consider the materials you collect physically and electronically your “essential records”. Collecting, preserving and providing access is your ultimate goal, and to lose those things due to any one of the above issues would be a disaster on an intellectual and historical scale.

Slide 24

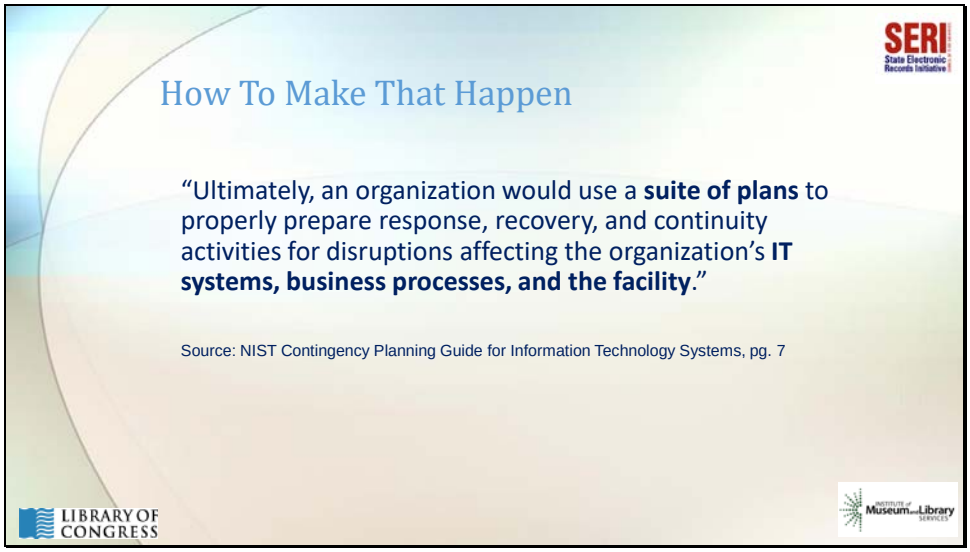


Proper planning should allow you to prevent, predict, detect, respond, and repair.

Why?
Many times organizations only realize gaps in their readiness when something happens. Being prepared is good practice, and saves time and money. Readiness protects investments in digital content.

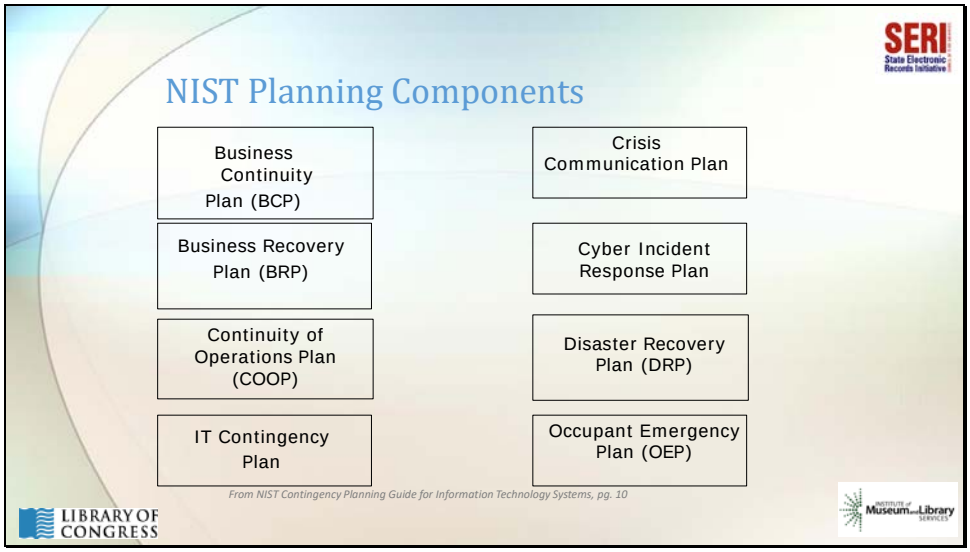
•Prevent – undesirable outcomes
•Predict – most likely risks and threats
•Detect – errors, problems, damage
•Respond – with appropriate measures
•Repair – damage or possible loss

Slide 25



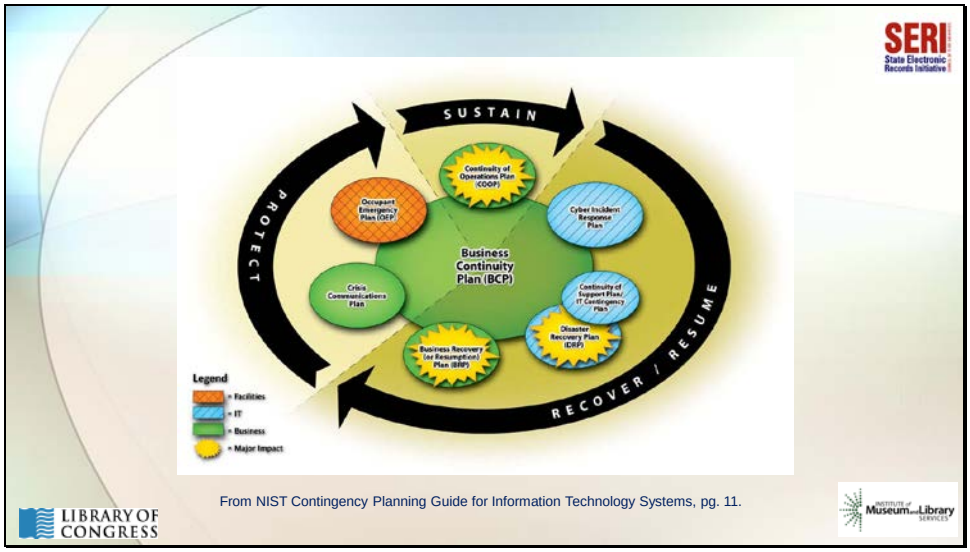
Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's IT systems, business processes, and the facility.

Slide 26



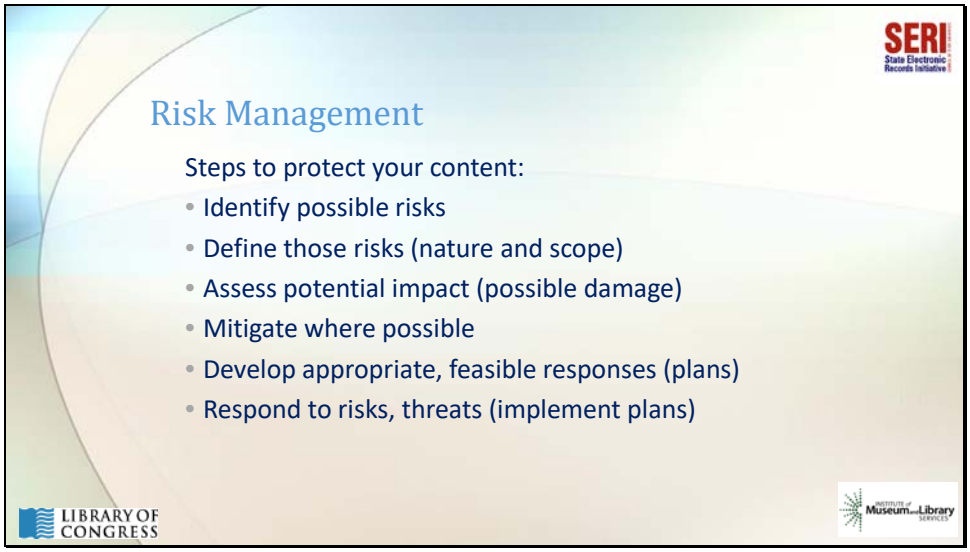
So what types of plans would work here?

Slide 27



This diagram distinguishes between things that may be affected (listed in the Legend) and the arrows map the planning documents to phases of an emergency – protect, sustain, recover/resume. Training for emergencies that includes what to do about digital content should be provided to all staff and emphasized with regular reminders.

Slide 28



The Risk Management process is really made up of several steps. For this example, we are going to tie it back to digital content, but it could be related to a storage room of physical records as well.

- Identify possible risks: It could be something as simple as - you've got a construction project going on outside the wall of where you have some of your records stored on CDs

- Define those risks. Risk of a pipe being punctured and causing a gas leak or water damage, for instance. The scope of a gas leak could be widespread: throughout the whole building. Water damage would probably be confined to the room. Is the likelihood of such an incident occurring high, medium or low? May be high while the project is going on. When the workers start covering up the pipe it probably is reduced to medium. After the area is paved over it may move to "low."

- I might add another factor: mitigation. Perhaps there are measures that can be taken to reduce the probability of loss during an emergency, such as move the CDs to another area.

Sometimes it's easy to get bogged down in identifying risks without identifying appropriate responses to relevant risks.

•Identify possible outcomes and prepare
  – the media (CDs) are damaged or destroyed

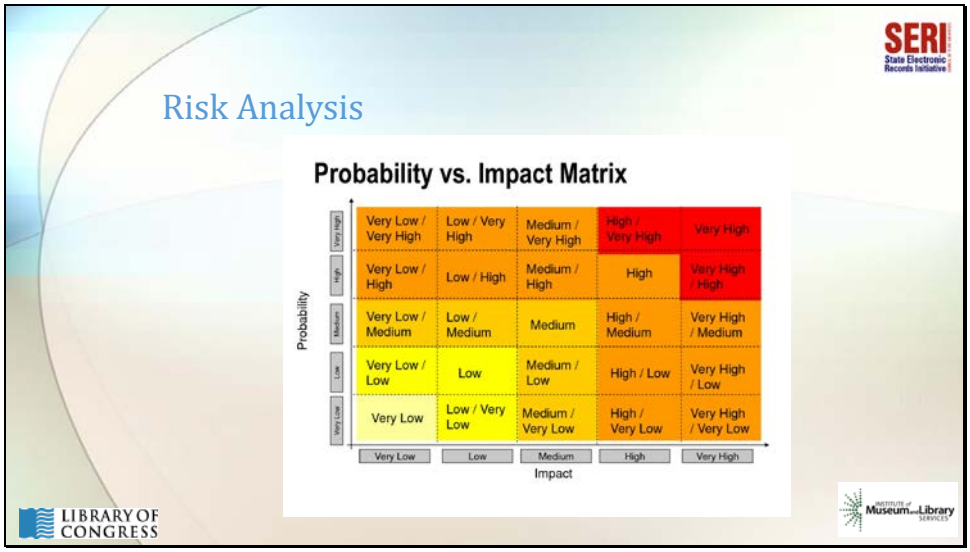
– but you discover that these CDs are just backups. The impact on your operation would be minimal.

- start developing specific plans or actions accordingly.

- Provides an opportunity to engage with other stakeholders in your institution or organization

- Including others in the planning process is key to increase awareness and involvement in the development of a digital preservation strategy

Slide 29

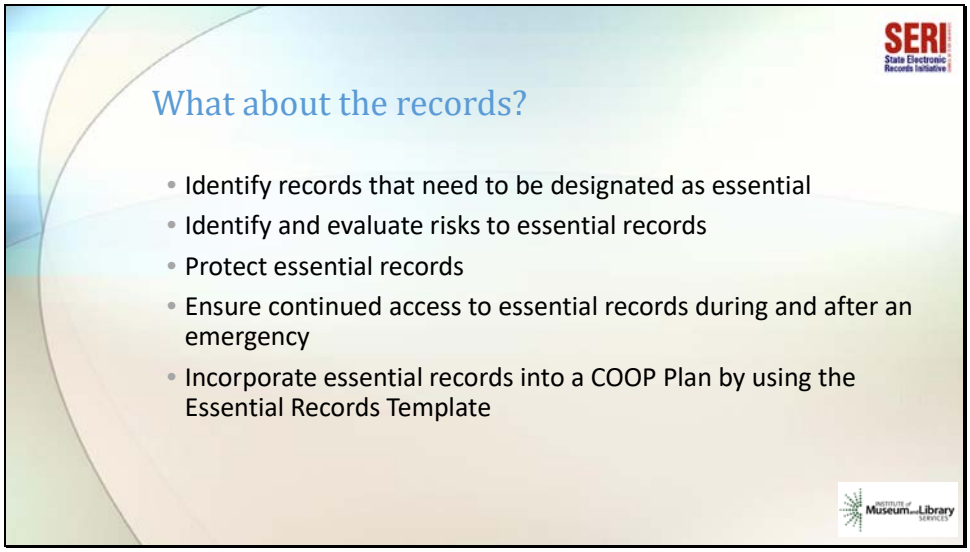


A Risk Analysis chart like the one shown here can help you determine which things pose the greatest risk to your organization.

Use some of the examples we discussed already to see where they fall on this matrix. You will want to really focus on the items that fall in the upper right part of the matrix.

Run through examples of how to use matrix.
Do you live in Tornado Alley? Subject to earthquakes? How often do you lose power? Do you have a lot of people working with digital content or only one or two?
Looking at your collections -
Obsolescence – what amount is at risk? How fast?
Virus? Hackers?

Slide 30



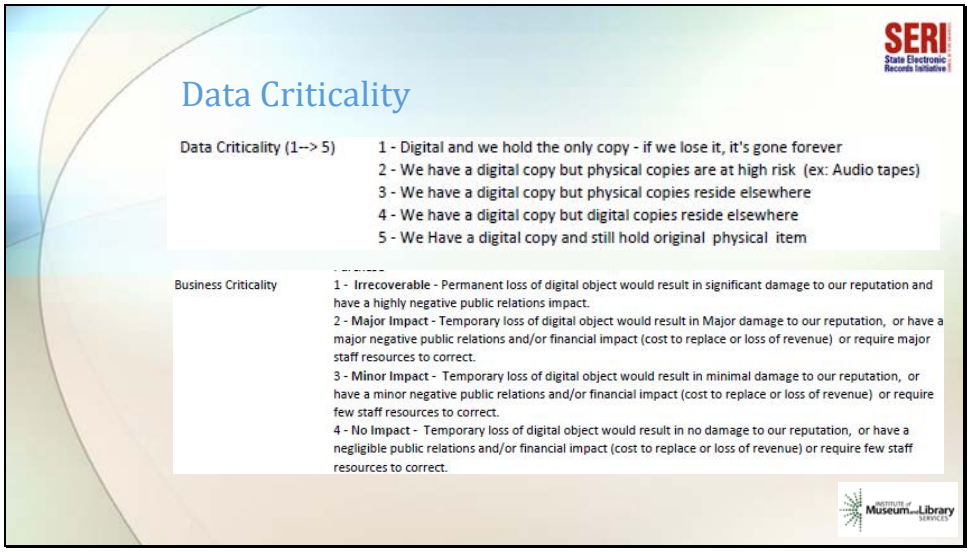
Identify records that need to be designated as essential. Identify and evaluate risks to essential records. Protect essential records. Ensure continued access to essential records during and after and emergency. Incorporate essential records into a COOP Plan by using the Essential Records Template.

Slide 31

Essential records can be found in paper and digitally …. Or both.
And it is critical that they are all identified.

For the archives – beyond your institutional Essential records - The inventory and select process is really the basis for determining your "Archival" essential records.

Slide 32



Remember this slide from when we were talking about the Selection process.
Your essential records are going to rank near the top of these lists…

This is where the multiple copies in several locations becomes really important. For those items at the top – maybe more copies than normal would be a good thing to plan.

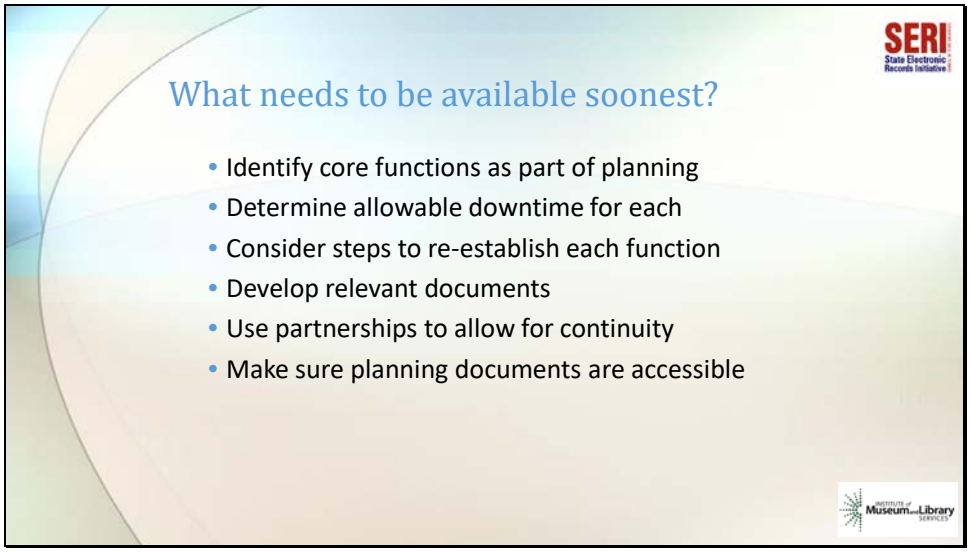
Slide 33

Often, you must continue to function and provide services to the public under emergency operating conditions, and must be able to resume normal business afterward.

Essential records make this possible.

All equipment & keys or access codes needed to read essential records will be available in case of emergency.

Slide 34



For the archives or any governmental entity, you need to determine what services need to be brought online first.

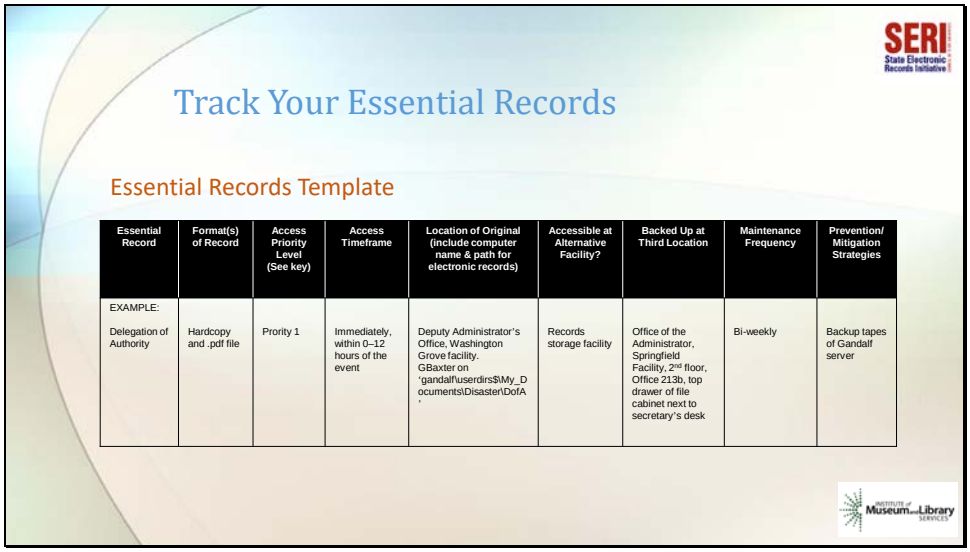
As you are developing your plans, think through what would need to be restored first. It's not possible to do everything at once. What is an acceptable timeframe for restoring core functions, if possible – minutes, days, weeks?

Sometimes restoring means rebooting computers that may have shut down abruptly and sometimes it means fixing equipment and facilities before they can used again.

Documents should plan the entire process. And should identify who determines priorities in the event of an emergency – and restoring digital content should be on the list.

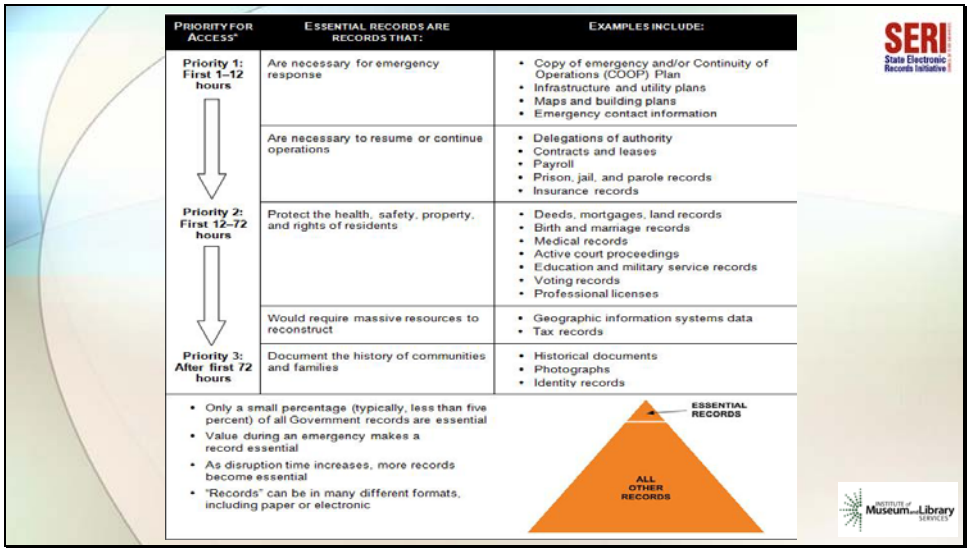
Partner organizations can have a copy of phone trees or planning documents to help with continuity; could be physical copies or the password to a simple website

Slide 35



Track your essential records using information gathered in the inventory. You can list by record series if they are at the same location and in the same medium or media. You will need to provide the key to the access priority rating system: others will not know this.

Slide 36



Priority 1—First 12 hours

Needed immediately, to respond to the incident

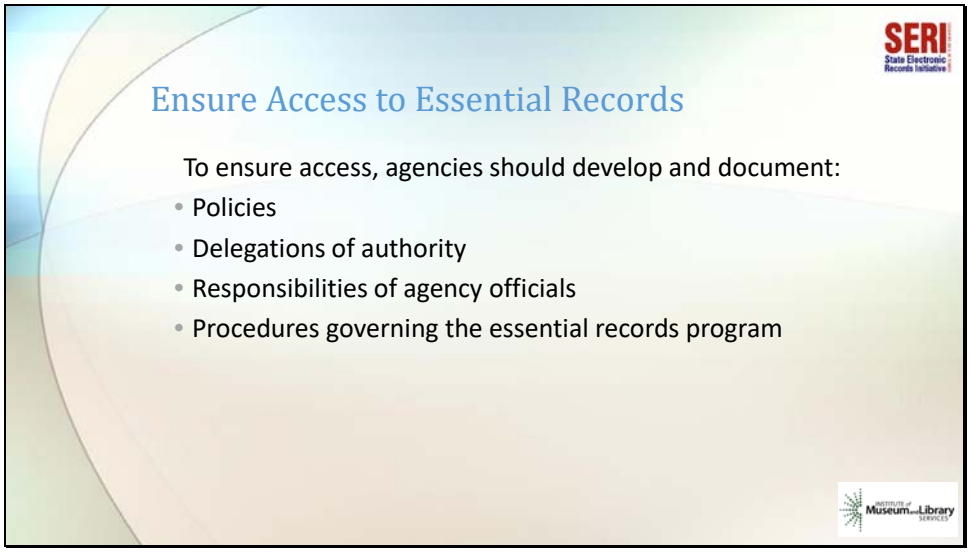
Priority 2—First 12–72 hours

Needed to manage the incident and resume operations

Priority 3—After first 72 hours

Needed to continue essential functions and for long-term recovery

Slide 37



To ensure access, agencies should develop and document policies, delegations of authority, responsibilities of agency officials, and procedures governing the essential records program.

Slide 38

"Grab and Go" kits contain more than just essential records. They contain a water supply, first aid kit, etc. Developing the kits is mainly the responsibility of a safety manager or COOP planner, however records management can contribute what goes into them.

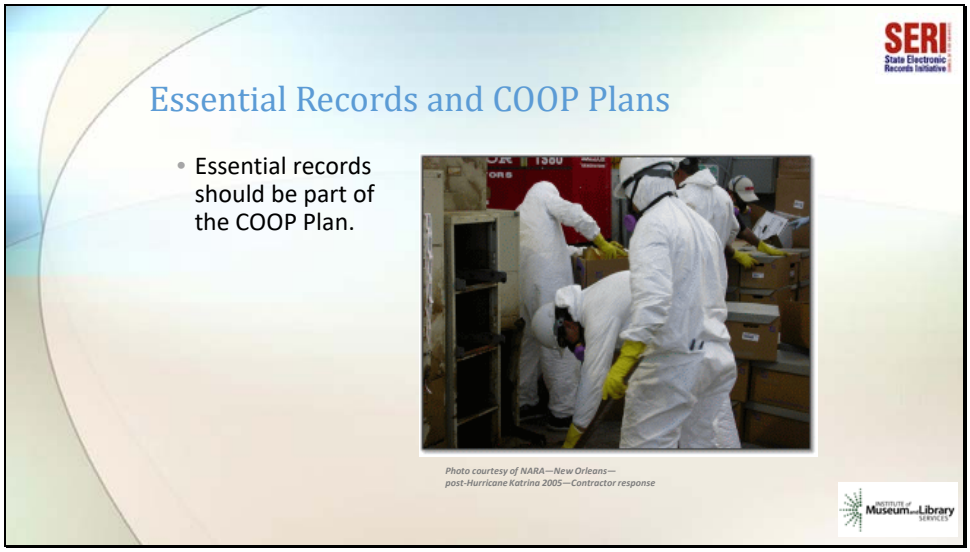
"Grab and Go" kits should be kept by all essential personnel "on their person" (at home or in their vehicles) and should include specific Priority 1 documents (those needed during & immediately after an emergency. The essential records in these kits should be updated or cycled on the same schedule as all your essential records so that the kit remains current.

Examples of the types of essential records & information to include in a "Grab and Go" kit are:
COOP plan. It would be embarrassing to say the least if you arrived on the site of your burning building and realized your plan of what to do in case of emergency was in the burning building!
Delegations of authority
Media procedures
Emergency telephone lists
Passwords
Access codes
Directions to a "hot" site
Hard drives containing essential records

Keep in mind that some of these documents may contain highly sensitive security information. If they must be readily available in an emergency, you must take precautions so that sensitive

information does not fall into the hands of unauthorized personnel. If you store information on an e-device make sure it's password-protected.

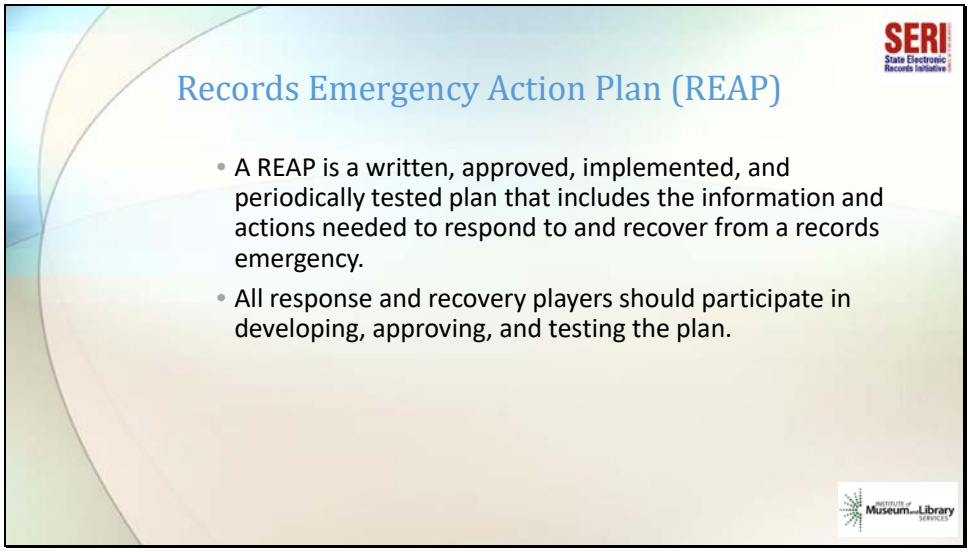
Slide 39



Records are critical for responding to an emergency and for continuing operations. These include the COOP Plan itself, as well as occupant emergency plans, telephone trees, delegations of authority, security clearance rosters, building blueprints, media policy directives, and essential records inventory lists.

Local Jurisdiction Mission Essential Functions. Every level of government should identify and characterize those MEFs for which it is responsible and that it must accomplish during a disruption or crisis. Just as Federal, State, territorial, and tribal governments should identify and ensure continued performance of their MEFs, local governments (including counties, cities, towns, and parishes) also should identify their jurisdictional MEFs and ensure the continued performance of those MEFs.

Slide 40



The REAP plan is part of the COOP as well.

Why is it important?

Even if you have an excellent, trained staff that has knowledge of emergency response & recovery techniques, it is still important to have a written REAP, which will serve as a vital organizational tool in the event of an emergency. The chaos associated with emergency situations can make the most efficient person forget important response priorities, such as:

- Where keys are located
- Where the water shutoff valve is located
- How to find an employee's phone #
- What to do if an important emergency team member is away on vacation

Without written instructions, plans & checklists, others are left behind to guess what to do, and the middle of an emergency is not the time to guess.

Slide 41

The REAP fits within your agency's or department's overarching disaster plans: whether a so-called emergency plan or COOP Plan. The REAP is not a general plan such as these, because it specifically addresses only records emergencies.

It should not duplicate or conflict with the general disaster plan.

The general disaster plan should incorporate the REAP via reference & policy.

Finally, it should work in sync with county disaster plans. Each county has an Emergency Management department or individuals within administration who do this work. They can help you with the plan and alert you to services they can provide in case of emergency. i.e. This 21-foot fully self-contained command post trailer is available to local communities to use.

Slide 42

- Even if there are no other disaster plans or COOP in place, develop a REAP now.

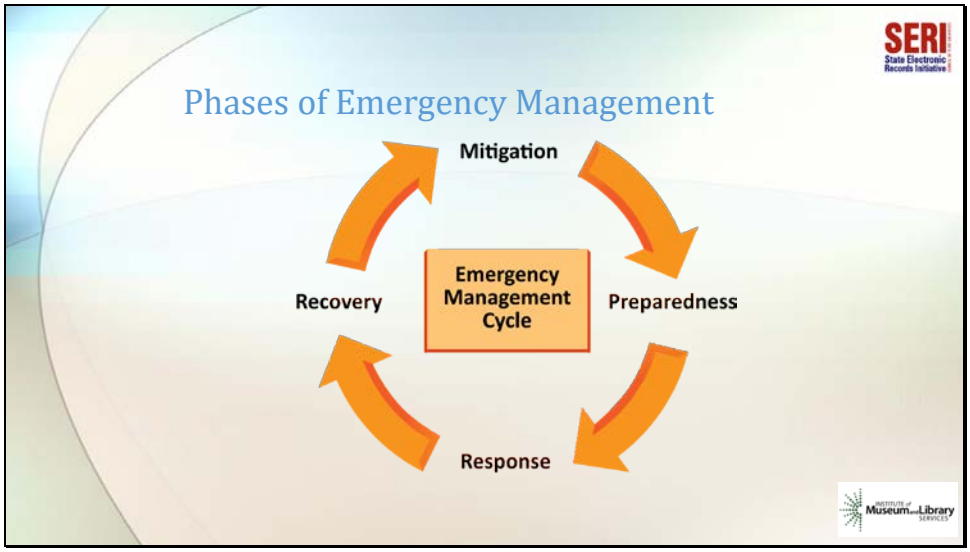
One of the many lessons we can take from Hurricane Katrina is to prepare now. It is much easier to prepare for an emergency when people are calm and rational and you have the luxury of time and resources, than to play catch-up after one has occurred.

- You can minimize the disruption of an incident by protecting the records that keep you functioning.
- If in the course of developing a REAP you involve other municipal personnel who are not knowledgeable about records, they gain an appreciation of good records management practice. They will learn the importance of identifying, protecting, & maintaining business information.
- Having a REAP demonstrates due diligence. If you're unprepared for an emergency, it's bad news for the government and for the records.

Slide 43

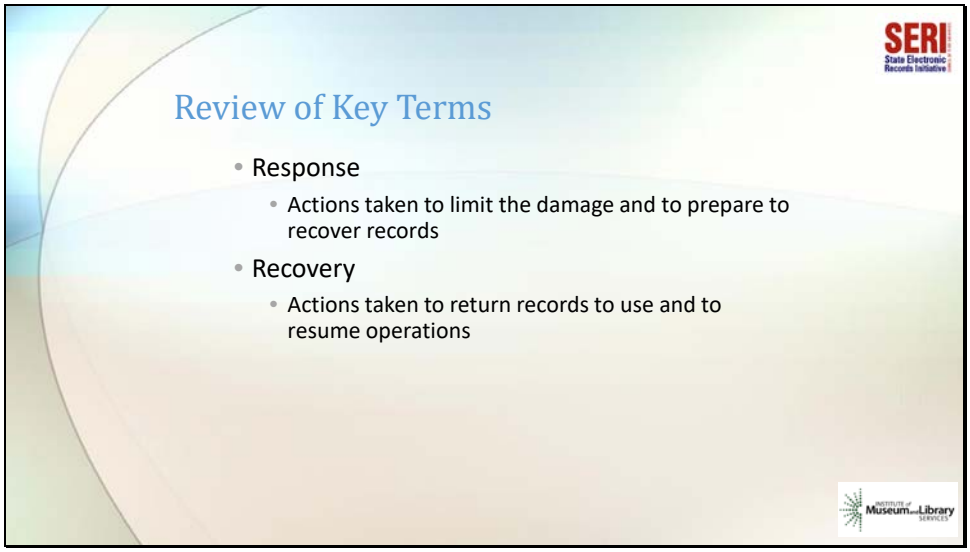
This is important because the REAP provides the basis for response & recovery actions.

Slide 44



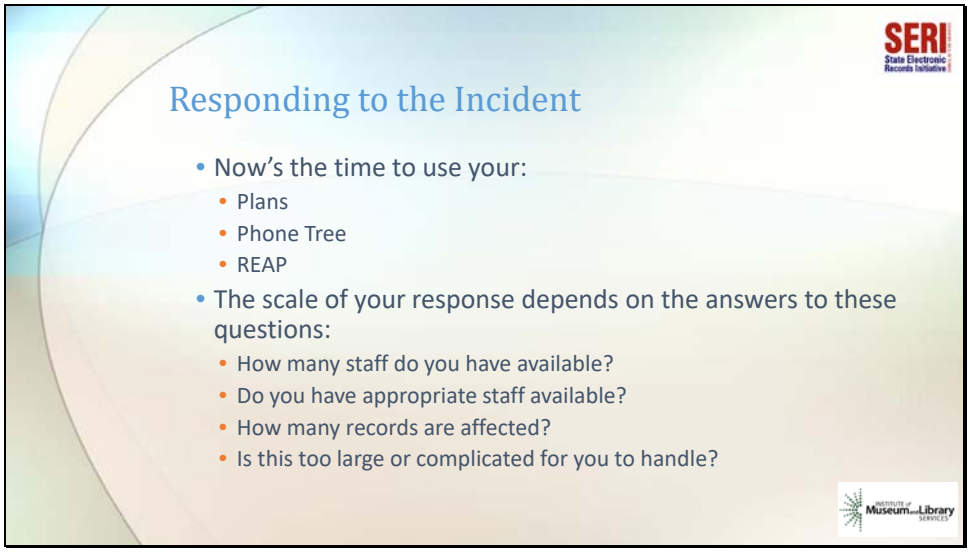
Moving on to Response and Recovery…

Slide 45



Response - actions taken to limit the damage and to prepare to recover records. Recovery - actions taken to return records to use and to resume operations.

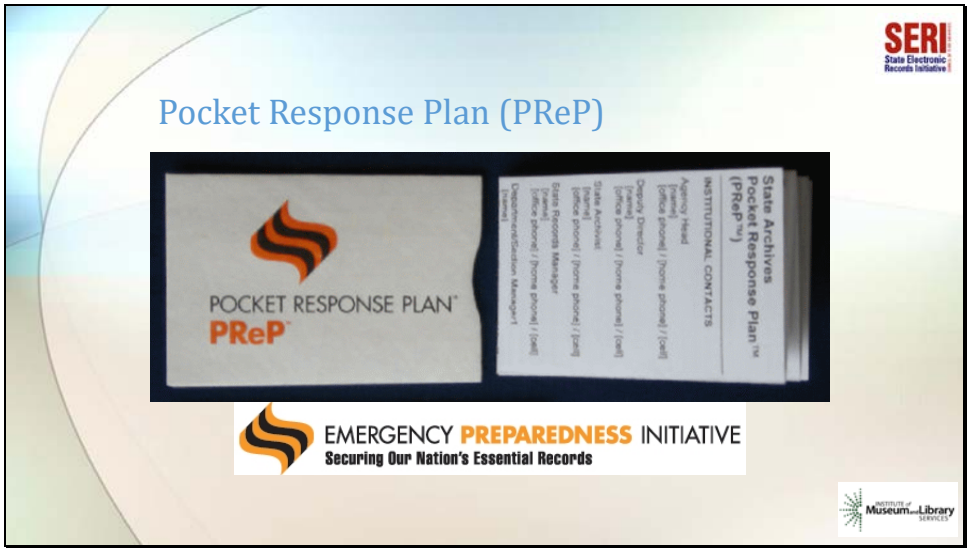
Slide 46



Responding to the Incident: Now is the time to use your plans, phone tree, and REAP. The scale of your response depends on the answers to these questions:

- How many staff do you have available?
- Do you have appropriate staff available?
- How many records are affected?
- Is this too large or complicated for you to handle?

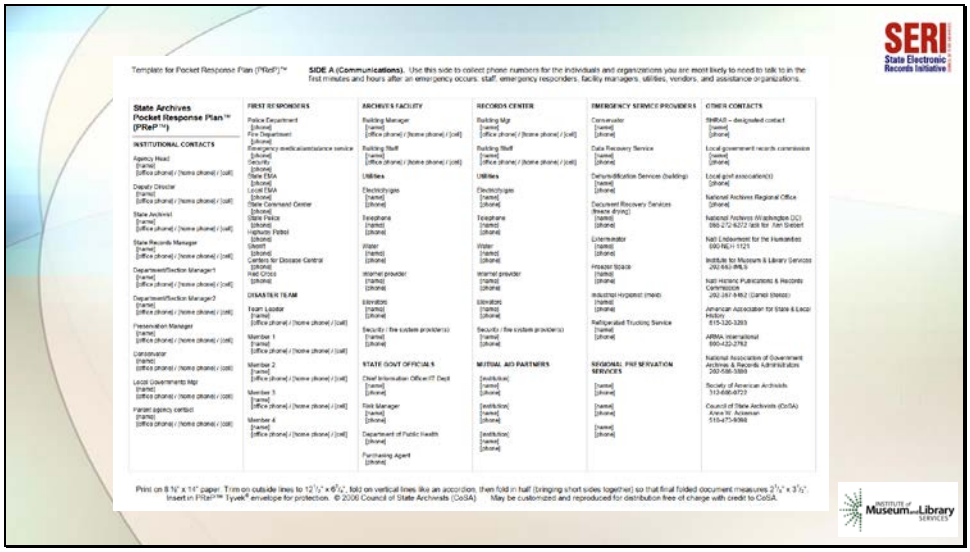
Slide 47



Feeling a bit overwhelmed? Fear not. You do not need to start from scratch. Several resources are available that can either complement your REAP or help you create your REAP. I'm going to highlight just one of these:

As a complement to, not a substitute for, your REAP, COSA created the pocket response plan, a concise document for recording essential information needed by staff in case of emergency. Designed to be carried by each staff member who has responsibilities during emergencies. Focus on information and guidance needed during the first 24-72 hours. Formatted as a 2-sided, legal-sized document that can be folded to the size of a credit card, inserted in a Tyvek envelope for protection and carried in a wallet.

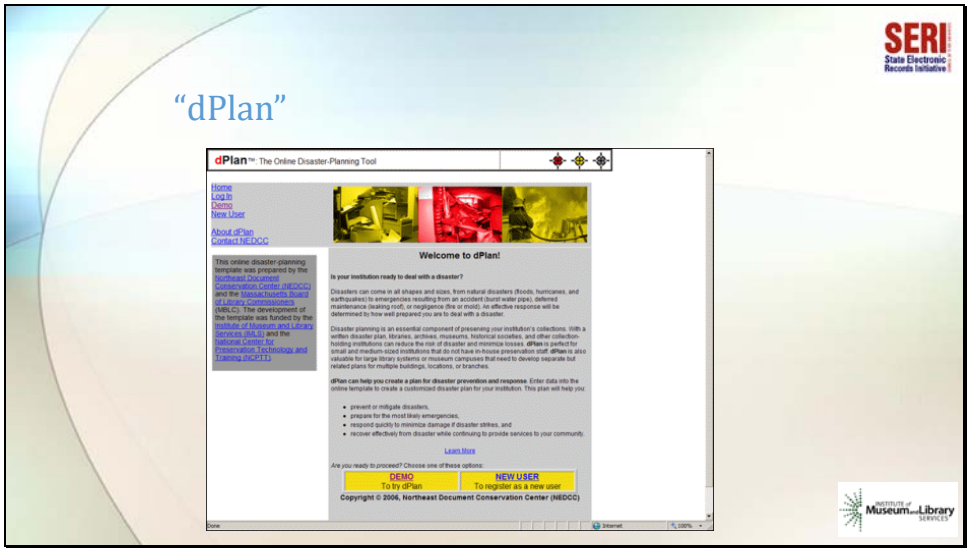
Slide 48



Side 1 is all about communications and who to call – institutional contacts, disaster team – emergency personnel around buildings and people - first responders (police, fire), facilities, utilities, Emergency contacts around your materials - in terms of data recovery, exterminators, and mold testing.

Side 2 is a checklist to go through in case of emergency.
Activating your agency's response disaster plan,
Steps through the assessment, salvage and recovery phase,
Communication to the public and other agencies, and
Vital records recovery and reestablishing services

Slide 49



A free on-line tool called dPlan will help you to create a REAP. It simplifies the process of writing a disaster plan for your collections. It offers a comprehensive fill-in-the-blanks template into which you enter information about your institution. It generates a printed disaster plan specific to your institution.

There are two ways to use it: dPlan: in Depth & dPlan Lite.
Recommend dPlan Lite: displays only those data entry forms that are most important in preparing a plan for emergency response.

Data is stored on dPlan's servers so be sure to check with your IT staff about potential security & control issues that using dPlan may present.

Available on-line at http://www.dplan.org. You must allow cookies to be set from the site.

Slide 50

Heritage Preservation is an organization that offers a field guide to emergency response as well as an emergency response salvage wheel.

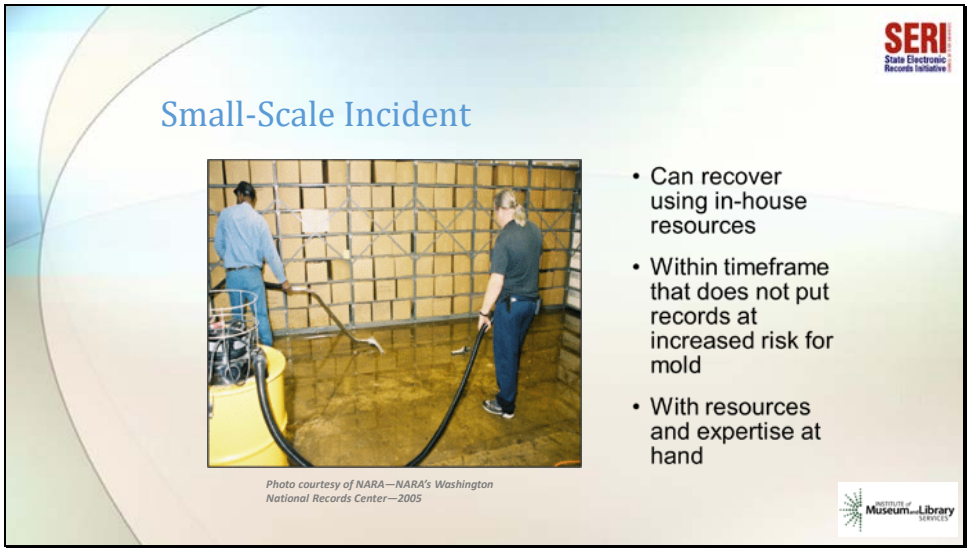
This Field Guide provides step-by-step instructions on how to respond to an emergency, form a response team, and stabilize your records and information.

The Salvage Wheel is a hands-on-tool that helps you:

- Find reliable info instantly
- Protect essential records
- Take steps to save damaged objects

(THERE IS A COST FOR THIS) The website is www.heritagepreservation.org

Slide 51



The definition of an incident that can be handled in-house includes a small area, a few hard copy records, and clean water.

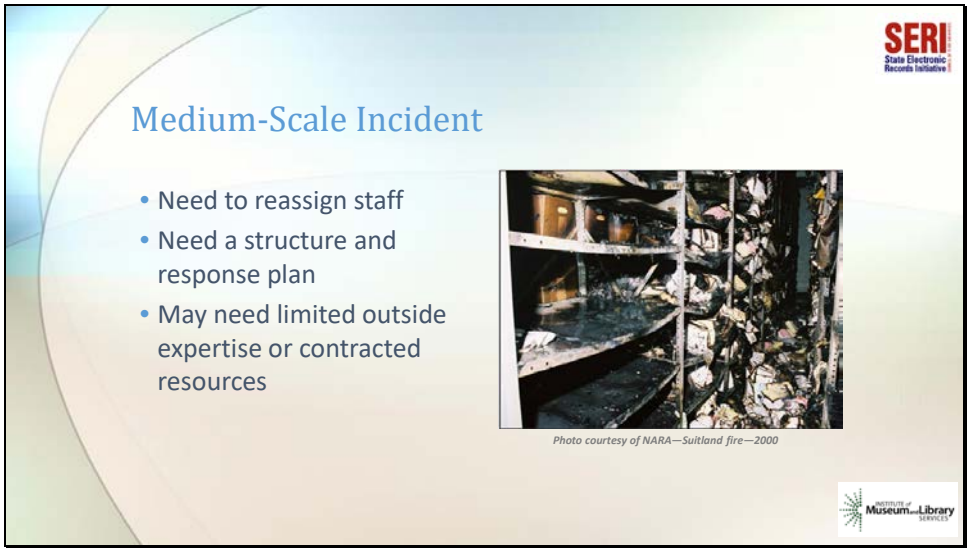
Clean-water damage that affects fewer than 10 boxes of records is the most common occurrence and can be easy to recover from with sufficiently trained staff, space and appropriate supplies.

Has anyone had a small-scale incident that you dealt with on site and with your regular staff?

Remember that small water incidents left untreated can cause mold which can turn a possible in-house recovery into one that requires a paid contractor to resolve.

If you think the incident can't be handled in-house, it is better to err on the side of requesting assistance sooner rather than later before the situation becomes more complex.

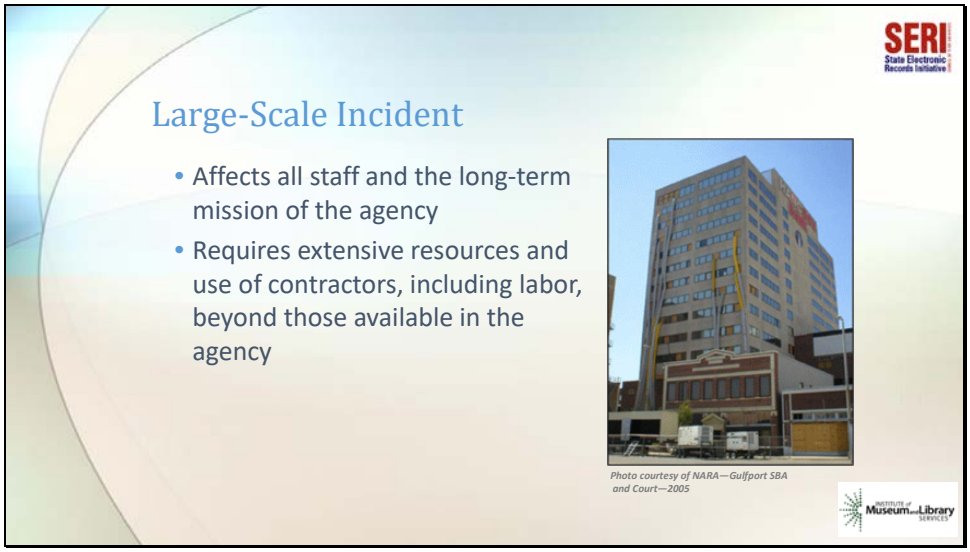
Slide 52



A medium-scale event affects all the staff in an agency. You will need to reassign staff to respond to the crisis and may need a limited contractor response.

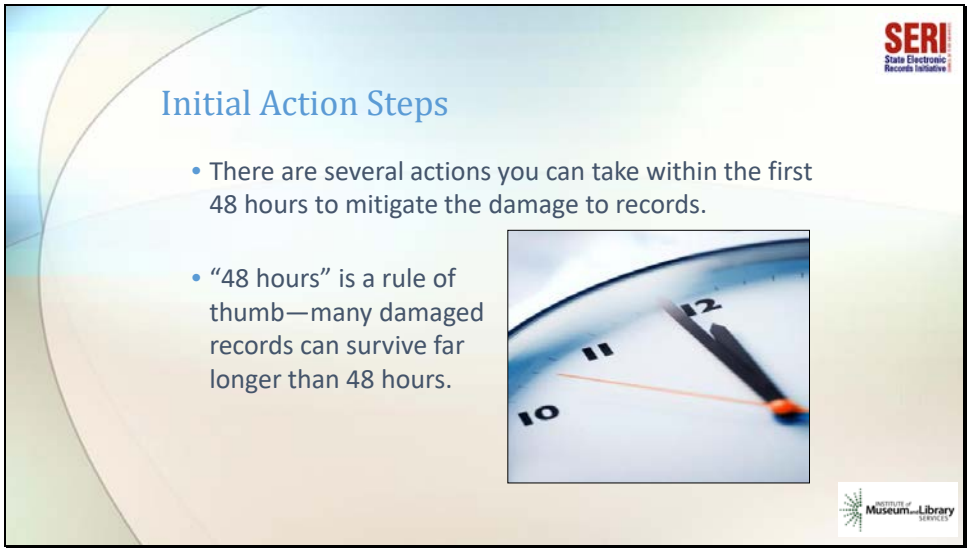
What is considered a medium-scale incident depends to a great extent on the resources of the agency.

Slide 53



A large-scale incident is an incident that will require external resources and/or contractors. It is a large volume of records, extensive and serious damage, and records on special media and formats.

Slide 54



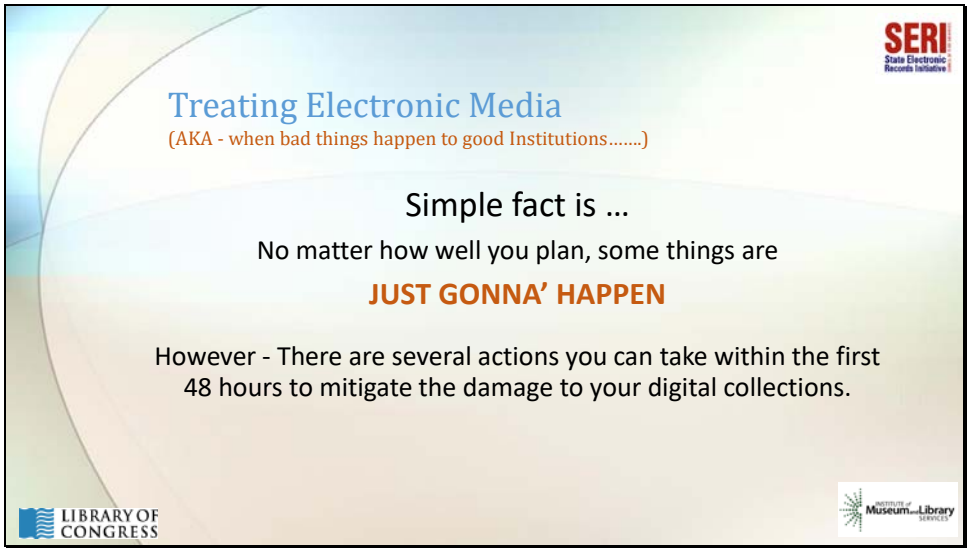
Initial action steps include:

- Cover materials with plastic if water is dripping on them
- Remove standing water
- Drop the temperature to 65 F or lower
- Drop relative humidity to below 50% & monitor
- Use fans to circulate air, unless the records are contaminated by mold

If you don't have access to the records you can still take steps to mitigate damage:

- Start whatever planning is possible before actually seeing the damage
- Order the recovery materials you know you'll need
- Get in touch with any outside help (for instance, document restoration professionals) you may need

Slide 55

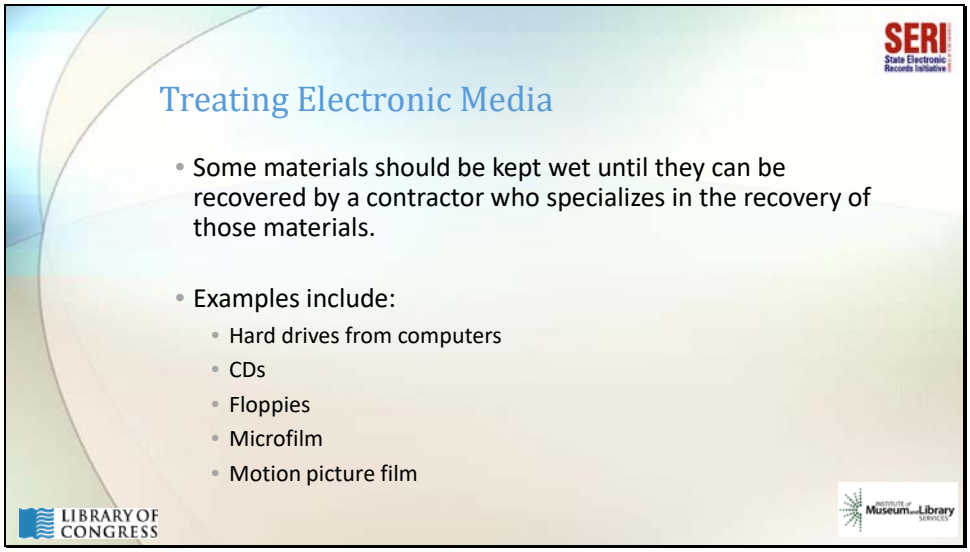


We've talked a lot about planning – but those physical or natural disasters we discussed earlier can be planned for, so if they DO happen, you have a response ready to get back up and running quickly. You need to look at your situation (where you live, etc), weigh the risks of the likelihood of something happening, and then make a plan.

While all of those possible problems have their own issues, a common denominator in many of these is often water damage
Extreme cold = burst water pipes
Fire = sprinklers / water from hoses
Tornadoes = minor damage to building = burst water pipes again
Excessive snow and collapsed buildings = melting snow (maybe) and water pipes
Earthquakes = the same

If something DOES happen – the first 48 hours are critical to mitigating the damage to your collections, but you need to be ready to act.
In the next slides, we are going to take a look at ways to mitigate water damage specifically and tie this into some of the topics we've been discussing.

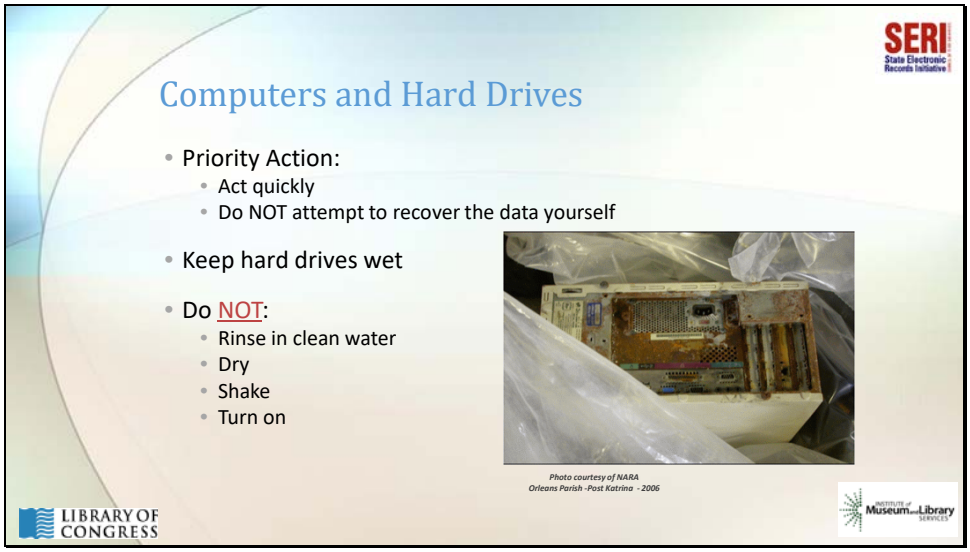
Slide 56



Some materials should be kept wet until they can be recovered by a contractor who specializes in the recovery of those materials. Examples include:

- Hard drives from computers
- CDs
- Floppies
- Microfilm and
- Motion picture film

Slide 57



The image here is a CPU that was allowed to dry and rust in New Orleans after Katrina. This illustrates the need to wrap and seal in plastic and recover immediately.

Depending on where you store your collection servers, this one is probably relevant to you. If you keep it onsite (as opposed to a managed cloud somewhere), this may be what you are facing after an event. Think about where all of your data lives outside of the collection server…are there workstations where collections being processed are stored? Hard drives that are being used as temporary storage? This emphasizes what was mentioned earlier about multiple copies and multiple locations. If your servers and backups are co-located in the same building, what are you going to restore your files from?

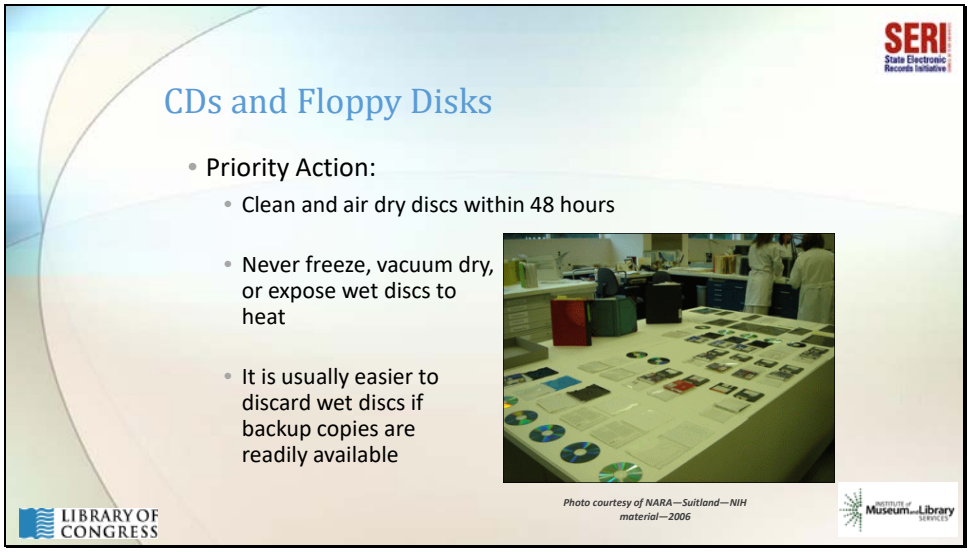
Act Quickly - The sooner a data recovery attempt can be made, the better the chance for successful recovery of data

Do NOT attempt to recover the data yourself
o Salvage of electronic media and equipment is most successfully carried out by a firm specializing in data recovery
o Some issues to consider when discussing a contract with a data recovery vendor include: protection of the data from a security and access perspective; what to do if data cannot be recovered; how the recovered data should be returned; whether the original hardware should be returned or disposed of with appropriate documentation, etc.

Recommendations:

• **Keep hard drives wet if that is the condition in which they were found**
o Keeping hard drives wet will help prevent further corrosion of mineral deposits and crystallization on the platters
o Keep hard disk drives in a sealed container to keep the drives wet
• **Do not rinse hard drives in clean water**
o Best practice is to leave hard disks alone until they can be salvaged by a firm that specializes in data recovery
• **Do not dry hard disk drives out or subject them to high temperatures**
o When hard disk drives get wet and then dry out, contaminants are usually left on the platters and heads. Any residue will cause physical degradation of the platters and will result in loss of data
NEVER attempt to power up wet or visibly damaged drives
• **Handle gently** o Do not shake or disassemble hard drives that are wet or damaged

Slide 58



This image is of CDs and floppy disks air drying.

We are talking about this, because collections are transferred using this type of media, and a disaster may occur before you have removed the data. Or sometimes you use this media for storage.

Recovery of CDs/DVDs is time sensitive
o The metal reflective layer responsible for conveying disc data is thin and easily damaged
o High quality discs have an outer protective layer that is water resistant during short exposures (less than 2 days)
o Poor quality discs will incur damage sooner

Avoid scratching the surface of the disc during the cleaning process

Floppies are fairly water-resistant – you don't necessarily want to save it – just get it to a point you can transfer data
o Data on water stained diskettes is usually recoverable unless diskette itself is magnetically damaged or warped
o Immediate salvage is preferable

• It may be safest to send disks to a professional data recovery vendor for data recovery
o If so, pack wet disks vertically in sealed plastic bags and ship overnight to a computer recovery service vendor for data recovery
o Do not dry disks first as dried impurities can scratch magnetic coating

Slide 59

This image is about the proper positioning to air dry audio and video cassettes

Priority Action:
Air dry within **48** hours. **Do not freeze** magnetic tapes.

Do not freeze dry. This can result in hardening of contaminants and adhesion of debris and contaminants on the tape surface.

• Damage to wet tapes is **time sensitive**
- o Short-term exposure to water will not destroy most tapes
- o But delay in recovery is likely to destroy most tapes

NEVER attempt to play back wet tapes (this will cause irreversible damage)

• Guidance provides information about how to prioritize damaged tapes for recovery:
- Unmastered originals over masters
- Masters over reference copies
- Older tapes over newer tapes
- Acetate over polyester-based tapes
- Smaller sized tapes over larger tapes

Recommendations: Lots of them – but here are a few key points
Minimize Handling -

Water compromises the physical structure of magnetic tapes, making them much more susceptible to stretching, tearing, and edge damage

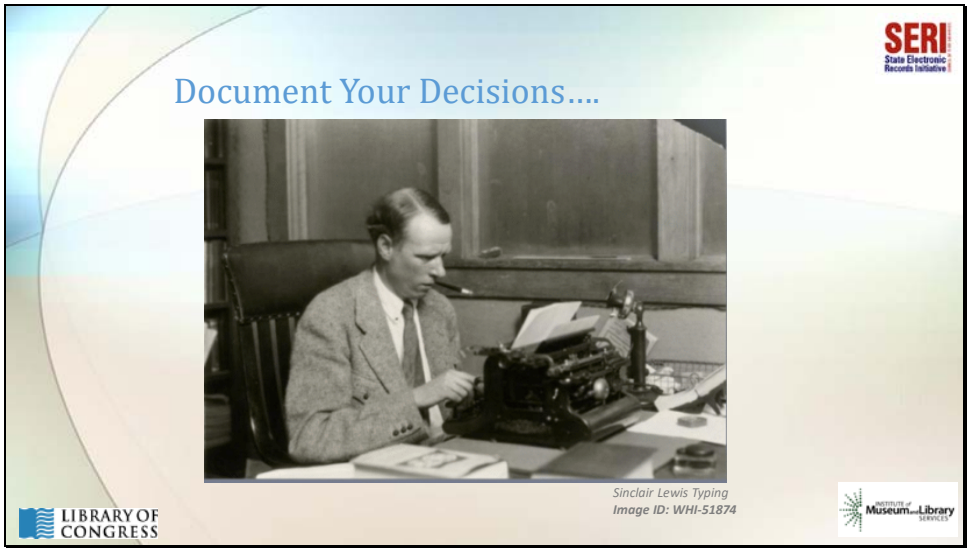
Use portable dehumidifiers to remove moisture from the area and objects

Keep tapes in an area that is cool and well ventilated until recovery begins

Slide 60

There are lots of resources that can help – look for relevant examples.

Slide 61



Document your decisions.

Engage in ongoing disaster planning

–Establish a committee and share information

–Develop and maintain documents

Slide 62

Often, digital content is left out of disaster planning. Find out what your status is. It can be challenging to get people to focus on emergency planning when there isn't an emergency, but if they don't, when an emergency happens, it's too late. Make sure information about emergency response isn't only available online or in digital form. Make sure key people can have access even if internet access is down or computers are unavailable. Run through a practice scenario annually to make sure people know what to do. Remember that restoring all preservation copies within some days after an emergency may be sufficient. Users will want access restored right away, but preservation happens over time and doesn't have to move as quickly as access does.

Slide 63

When planning for emergencies, we often need to start at the institutional level and identify our priorities.

Think through what would need to be restored first – it's not possible to do everything at once. What is an acceptable timeframe for restoring core functions, if possible – minutes, days, weeks? Sometimes restoring means rebooting computers that may have shut down abruptly and sometimes it means fixing equipment and facilities before they can used again. Planning should identify who determines priorities in the event of an emergency – and restoring digital content should be on the list.

Users will want access restored right away, but preservation happens over time.

Slide 64

We talked briefly about the large scale institutional disaster management planning that should take place, but there are some things you can plan for at the repository level that can be integrated into the institutional documents. In some ways, your planning is somewhat easier, because digital content can live anywhere with proper care and feeding and isn't restricted to a building like records storage or artifacts might be.

Planning – see if there is any mention of the digital collections and if not, see how that can be incorporated

Planning team – to fill in gaps that you find with the institutional plans

Inventory –
Backups - Do you know where the backups are for each collection? Sometimes they are co-located on a server, but sometimes they live on various hard drives, etc. You may want to add a category which describes location of any secondary copies of the collection or digital object.

Restoration – This is based on how important or at risk some of your collections are

Recovery time - Statement describing recovery time needed in the event of a system-wide failure

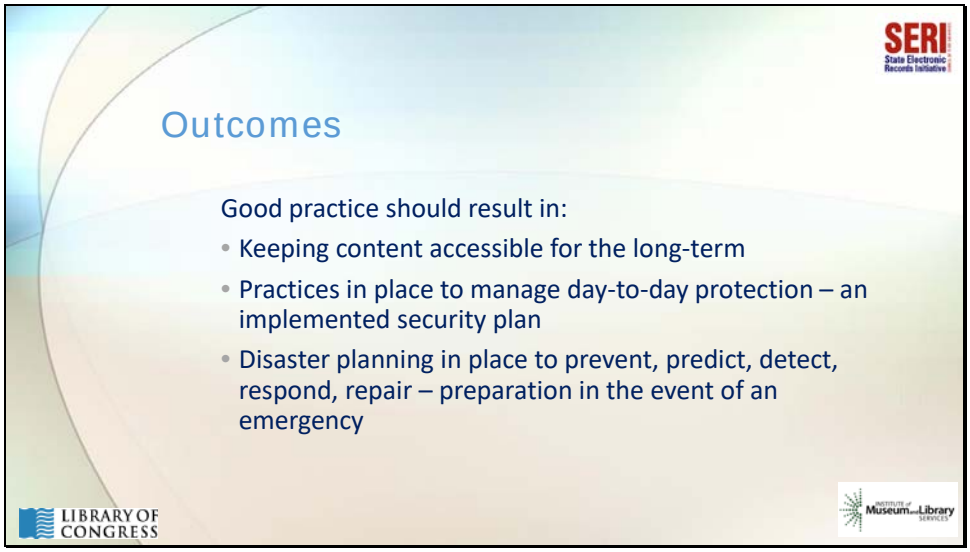
Other things – Phone Trees
You may want to create a list of contractors that will be part of your recovery team should you need them.

Add a Workflow about recovering from backup.

Slide 65

Next steps: Implement practices to manage day-to-day protection - an implemented security plan. Make sure disaster plans are in place to prevent, predict, detect, respond, and repair your records in the event of an emergency. Perform periodic practice drills. Ensure that emergency documents are available both digitally and in hard-copy.

Slide 66



Good practice should result in:

- keeping content accessible for the long-term
- Practices in place to manage day-to-day protection--an implemented security plan and
- Disaster planning in place to prevent, predict, detect, respond, and repair - preparation in the event of an emergency

Slide 67

This completes module 4, Protect. If you are using these modules in order, the next one is module 5, Manage. For additional resources on electronic records preservation and management, please visit the State Electronic Records Initiative webpage. This link is on your screen.