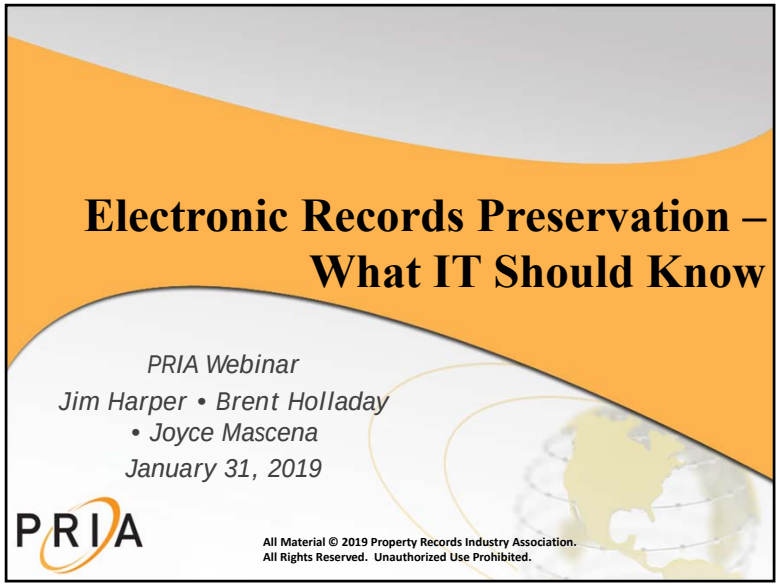
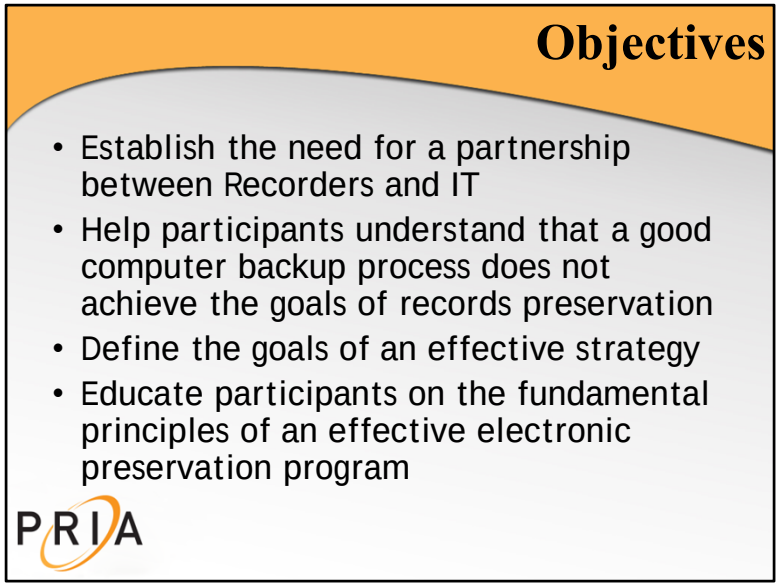


BRENT:

Welcome to this PRIA webinar about the importance of preserving electronic records. We are going to provide IT with some insight as to how to navigate a conversation with the Recorder about the permanent preservation and protection of the records under the care and custody of the Recorder.

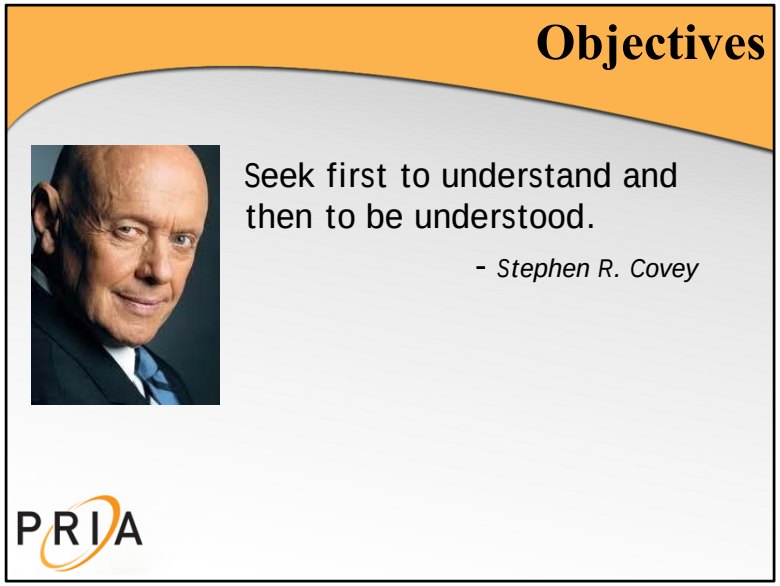


BRENT:

These are the published objectives for this webinar:

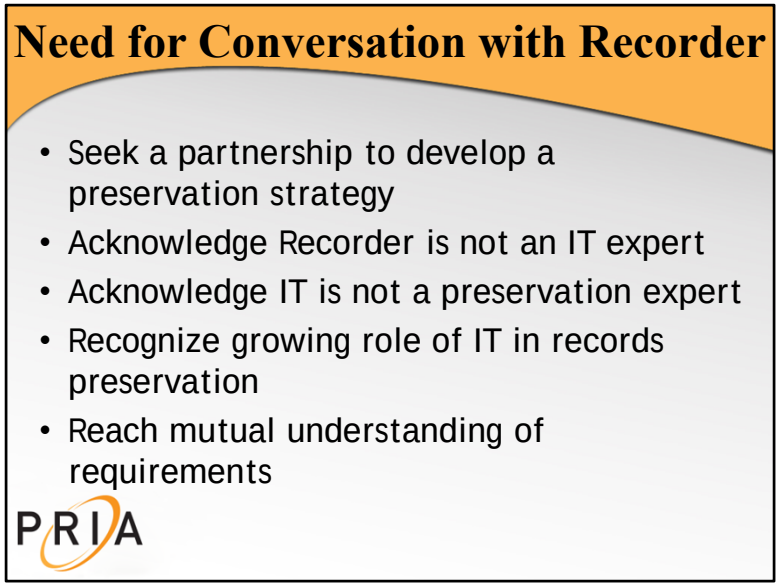
- The importance of developing a partnership between IT and the Recorder
- Understanding that certain traditional IT processes, such as computer backups, don't necessarily meet records preservation goals
- Understanding the goals of an effective preservation strategy
- Educating all parties about the fundamental principles of an ePreservation program

Although this presentation focuses on recorders and their IT department, we want you to know that the principles of an effective electronic preservation program apply whether you are a government organization or a business.



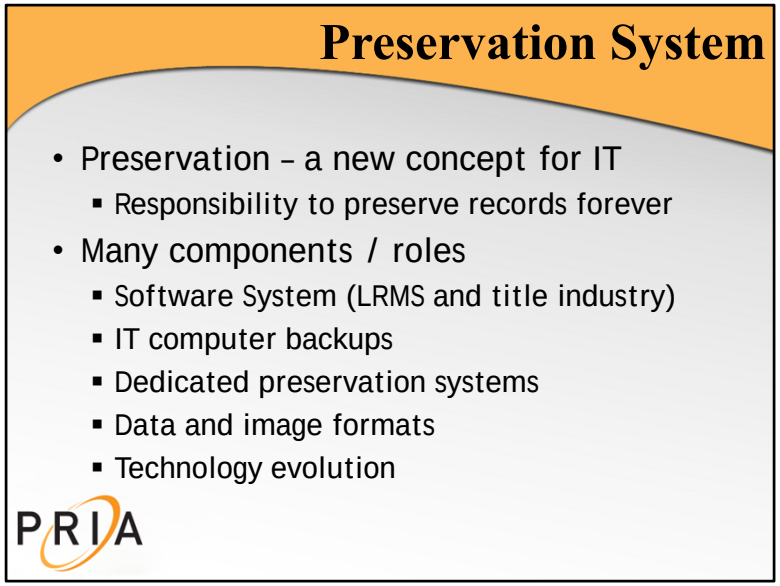
BRENT:

The famous author Stephen R. Covey advised that we "seek first to understand and then to be understood." When we recently talked to the Recorders, we asked them to first seek to understand what you are doing as IT professionals and then to help you understand the end goal of electronic records preservation. In this session, we will start by helping you to understand the end goals of electronic records preservation and then explain where traditional IT processes may be falling short of these end goals.



JOYCE:

- IT professionals and Recorders need to seek to develop a partnership and work in tandem.
- As a general rule, Recorders are not IT experts, nor do should they need to be, but they do need to be knowledgeable so they can converse with IT professionals in a productive way.
- IT professionals shouldn't be expected to be preservation experts either but have to recognize their ever increasing role in aiding their Recorder in implementing a successful electronic records preservation program.
- As we move forward, we need to learn each other's language, come to a mutual understanding on the requirements and share records retention and preservation responsibilities.
- Therefore, it is key that there needs to be ongoing communication between the IT professionals and the Recorder.

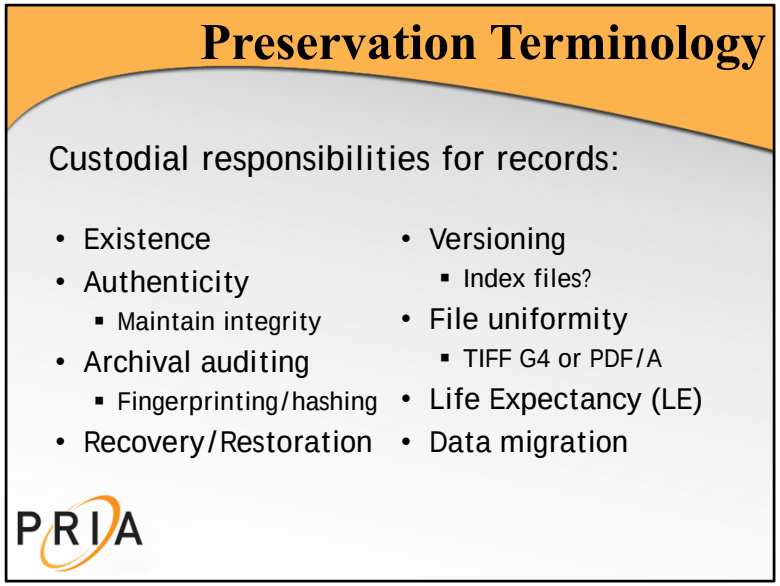


JIM: As Brent mentioned, we have flipped this presentation from the one we shared with Recorders. Our goal today is to help you understand where Recorders and IT need to go, essentially together on a journey, so that you will end up with a mutually agreeable strategy to preserve electronic information. We will begin that journey by educating you, as IT professionals, on what preservation means and then we'll return to talking about technology.

Electronic records preservation is about preserving everything forever, which goes beyond customary IT processes. Permanent records are traditionally written to microfilm to satisfy this permanent records requirement. Because microfilm is beginning a slow exit from the scene, IT will need to be prepared to adopt technologies that will provide the same level of comfort and capability that microfilm delivered. Assuming responsibility for all facets of a preservation program ***will likely be a new concept to your IT team***. There are many components & roles related to a preservation strategy. We'll discuss the roles later, but introduce the concepts here so that each of you can look for the areas that pertain to your situation. Here are some points we'd like you to understand:

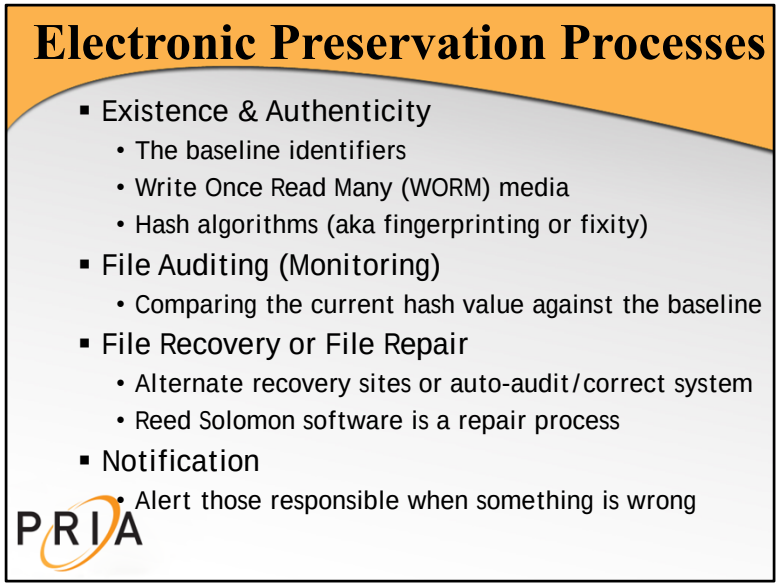
- Preservation is relevant to both public and private sectors so software capabilities can apply to both recording and title insurance systems
- Even though it's not considered preservation, the value of the traditional IT backup process should not be discounted
- Be aware that there are dedicated preservation & recovery systems commercially available today
- Awareness of image and data formats and the inevitable evolution of technology are important considerations

And finally, don't assume that the Recorder's records management production system has addressed preservation needs because in all likelihood it hasn't. While there are innovative land records systems that leverage leading edge Cloud technology, it is highly doubtful that they incorporate the necessary preservation strategies that we are presenting here.



JIM: As the custodian of the record, the Recorder has a legal responsibility to maintain in perpetuity the documents they record. Traditionally, moving the management of records from a manual process to an electronic one did not guarantee that the requirements needed for preservation were being covered. This is because they were being handled by the offsite storage of microfilm. Because preservation encompasses more than the traditional data backup process, the principles behind true preservation must be introduced and understood. These principles are more thoroughly described in the PRIA paper Electronic Records Preservation, which will be published very soon.. Here's brief description of what these terms mean:

- Existence – Does the record exist on the County's system?
- Authenticity – Is the record that is currently on the system identical to the record that was originally recorded?
- Archival auditing – This is the process identifies the unique characteristics of a record and has the ability to continuously monitor that identifier to detect any type of change to those characteristics. Mathematical hashing algorithms are most commonly used for this process.
- Recovery/Restoration – The ability to faithfully and confidently reinstate a lost or corrupted record.
- Versioning – The ability to track changes to a record and retain every iteration.
- File uniformity – Continuity in and awareness of the types of image file formats that are accepted and stored. TIFF version 6 using ITU G4 compression (our "de facto" industry standard) and PDF are examples of common used image formats.
- Life Expectancy – The useful period of time that a storage medium will perform its intended task. For example, the LE for today's silver, polyester base microfilm is 500 years. There is no consensus for the Life Expectancy of electronic media.
- Data migration – The process of moving image or index data from one system to another.



JIM:

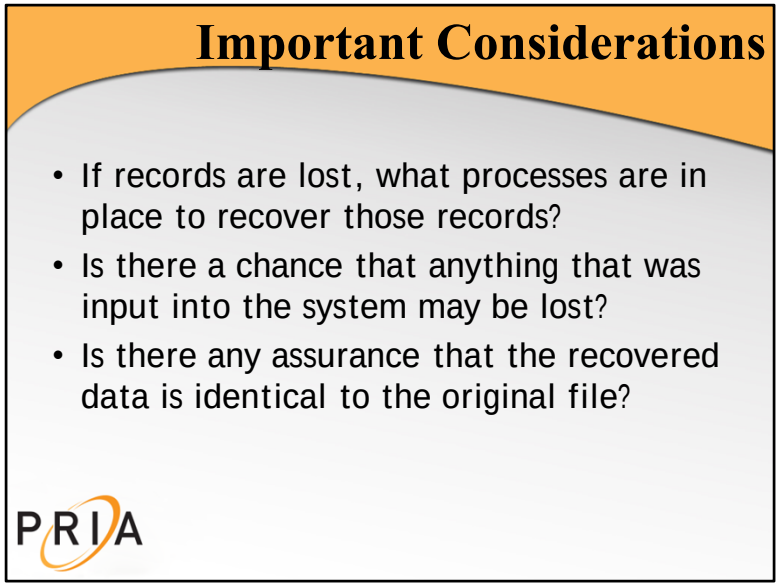
Here are examples of tools that are available to manage these issues.

A baseline identifier for each file needs to be established as soon as possible after the recording process is completed and, over time, you'll need to ensure the existence and authenticity of these electronically stored records. This process is key to creating confidence that stored records are identical to the those captured at the time of recording. Technologies such as secure hash algorithms have been around for years and can be used to perform this function. If you are using a file identification technology, are you deploying it in a way that creates a true electronic records preservation system? For example, relying on an electronic "time stamp" can be a useful too to help determine a file's authenticity but it does not address the issue of existence.

Even when there are safeguards to establish existence and authenticity a true preservation strategy includes an awareness of the health of the data on an ongoing basis. We call this process file auditing or monitoring. The idea is to have a process in place that continually examines every electronic file and compares its current condition to its original condition. For example, if you use hashing algorithms, there needs to be a process in place to systematically check that the current identity value of a file is consistent with its baseline value. If they are not identical, you must be able to either recover the original record or repair the record to its original condition. An alternate recovery site or file repair strategy along the lines of Reed Solomon error-correcting coding are examples of recovery and repair strategies.

If the monitoring process discovers a problem, will the responsible parties be notified and, if so, how? Or, if a repair is automatically performed, will the responsible parties be notified?

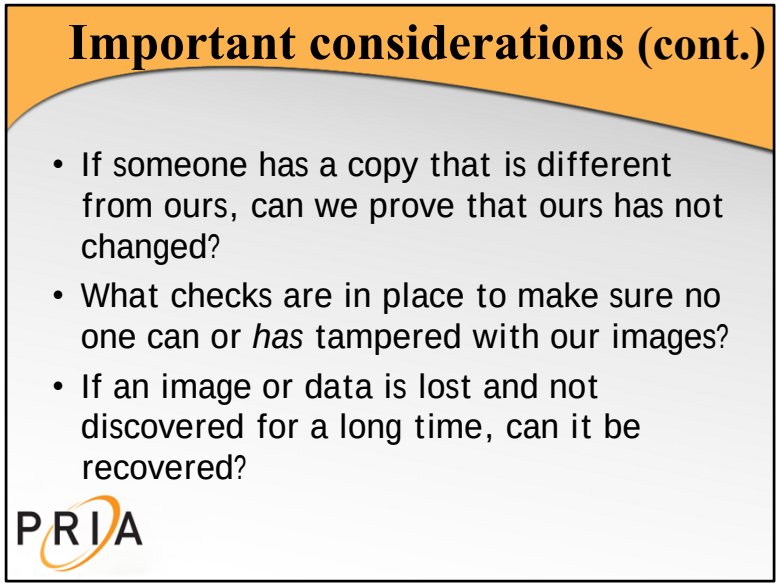
The bottom line is, what technologies does your IT group have in place or could put in place to accomplish any or all of these functions.



BRENT:

Picking up on what Jim just shared, let's review some important considerations:

- Can data, any data, be lost? If you don't think it can, why not?
- If it can be lost, what is the plan and process to recover lost records?
- What processes are in place to ensure that the recovered records are authentic?



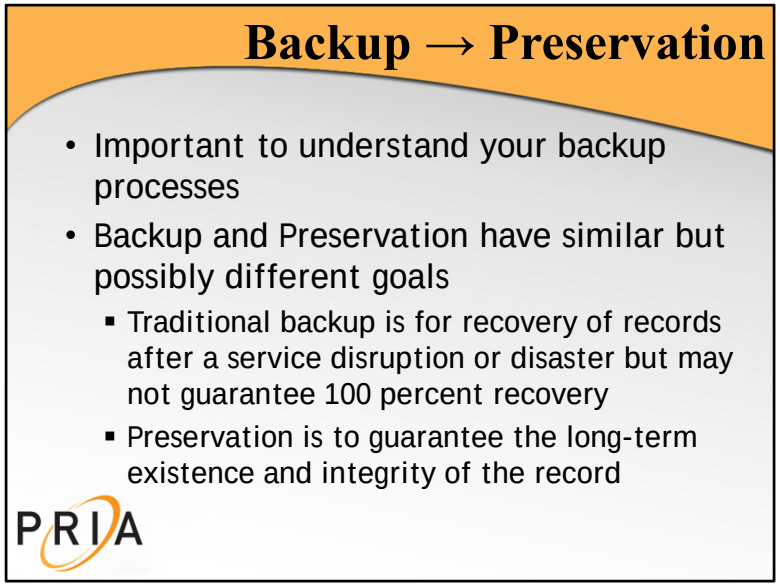
BRENT:

Continuing:

If someone were to produce a document different from yours, how would you prove that your record is the authentic (the real) record?

What checks are in place to make sure no one can or has tampered with your images – ever?

What processes are in place to recover either accidently or maliciously lost images or index data either on an ongoing basis on in a situation where the lost image is not discovered for a long time after the loss? I'll share an example of this momentarily.

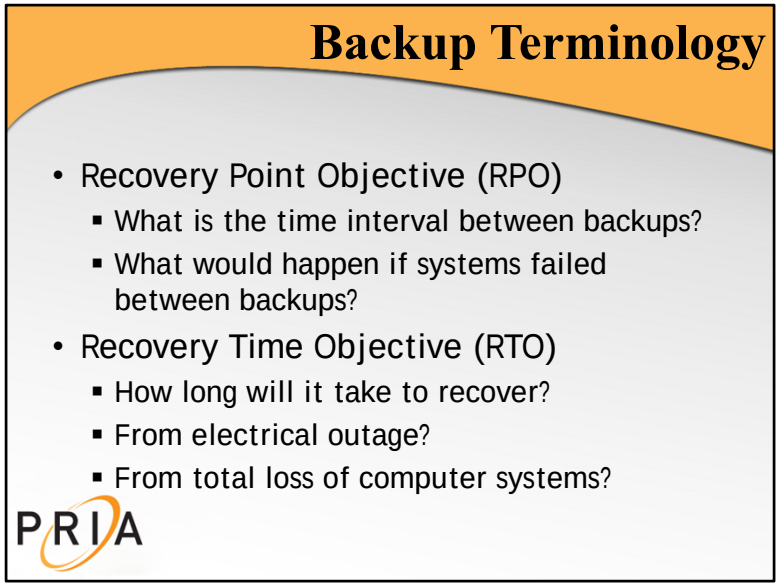


BRENT:

With the questions we just listed in mind, let's review some of the traditional IT processes and see how we can evolve them to the preservation environment we have described.

The traditional role of IT has been to create, secure and maintain the computer infrastructure, and to provide recovery after a failure or disaster through a process that we generically refer to as "backup." For this presentation, we are focusing on "backup." We recognize that "backup" in one of the components of your IT operations and also one component of a preservation program. So, you can extend our conversation to the broader context of your own operations. With the understanding of what we have just discussed, I think we can see that the traditional "backup" strategy does not provide for all aspects of an electronic records preservation program. However, as IT professionals (and I refer to my former life a year and more ago), we all know that over the last 5 to 10 years there have been great strides in backup technology so that most of you are a lot closer to a preservation environment that with the more traditional processes. Your IT backup processes may be ahead of some of the fundamental processes I will discuss. The key will be to think about what supplementary processes you have in place, in addition to what I will discuss, that take you beyond traditional backup, into the world of preservation. I hope you will all leave with some confidence that you're on the road to preservation and that our discussion will prompt you regarding what the next step is that you can take along with your Recorder to develop a true Electronic Preservation strategy.

Currently, it's likely that the goals of your IT Backup program do not achieve the goals of true records preservation. Let's discuss why that may be the case:



BRENT:

The backup process traditionally is to provide for business continuity in the event of any type of disaster or loss. Let me review two terms that I think we're all familiar with and see what they mean with respect to preservation. The first is:

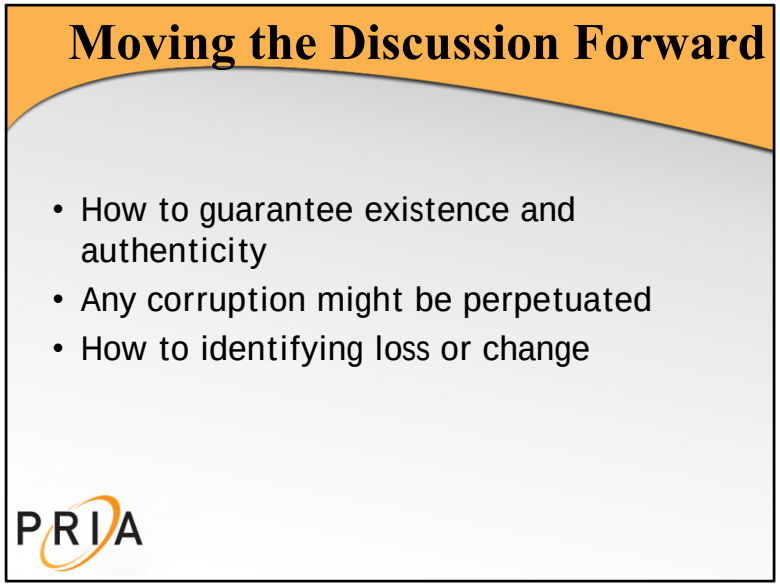
RPO – which is the time interval between backups. If there is a failure, what is the time interval from when the last backup copy was made. For preservation there can be no loss, i.e., this interval must effectively be 0.

a. We know that backup systems today may provide a virtually instantaneous backup, meaning that there is no loss of data, the RPO=0. You input something into the computer and it is backed up. Ten years ago, many backups were made daily, meaning that you might lose a whole day's worth of work. Over time that interval has reduced significantly. What is your RPO? Even if backups are a few minutes apart, you need to formulate a strategy to recover what was input during that interval. Thus, if there's any potential for loss, you and your Recorder need to develop an acceptable objective to make sure you can recover information that may have been input during the loss interval, if there is one. As an IT professional, I remember asking our recording staff if they could determine what they did for the last 30 minutes at a time that our RPO was 30 minutes. You need to know what you would do to recover anything that might be lost between backups.

RTO – this refers to how long it will be until the computer system is back up and running; before you can continue regular operations. Of course, different interruptions may have different RTO's. In the case of a total failure, the time to recovery could be several days. Currently, you probably all have some form or RAID or redundancy of systems to reduce the RTO for various types of disasters. Is what you're doing adequate? Think of the fires in CA and the recent hurricanes in the southeast that wiped out data centers. How protected are you, really, especially if your electronic records are your only source of records preservation? I've talked to some jurisdictions that have taken the step to eliminate microfilm as a layer of protection. After some conversation, I have wondered if they did so prematurely.

a. Also, after a major disaster, what do you do while you are waiting to rebuild your systems?

b. If you must record, what are your processes to do so, and how do you preserve those records?



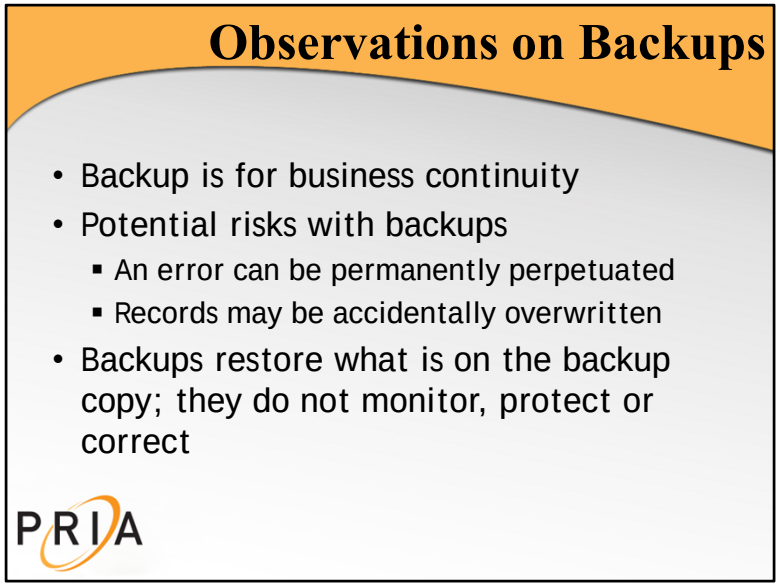
BRENT:

Here are a couple of related issues that move the discussion towards preservation and that address the questions we introduced at the beginning of this presentation.

a. How is the existence or authenticity of the recorded document guaranteed? (i.e., how do you know the record was created and backed up correctly?)

b. If a corruption is introduced, it might it be perpetuated. We mentioned this earlier. This may be a function of how long each backup instance is maintained. For example: Daily backups may be kept for a week. Then a weekly backup may be kept for 3 months and then those tapes are rotated and reused. The basic assumption in such a case is that after 3 months, what's in the database is assumed to be correct. The old backup information is then overwritten with a new backup. Let me give a real live example where this did not work. I am familiar with a Recorder's Office where the test system with a new version of the software was pointed to live database resulting in 100 images in the live database being overwritten. This error was discovered 120 days after it occurred, but this jurisdiction only kept backups of the database for 3 months, so backups could not be used to recover the original documents. Fortunately, they had still maintained microfilm and used the microfilm to recover the original images. After that, this jurisdiction started storing every instance of an image to the cloud upon capture. This is an important point that we'll mention again later: that is that ***preservation begins at capture.*** Again, that jurisdiction used their cloud process of preserving every new image and any new version of that image immediately upon capture. That alone does not do everything related to existence and authenticity. But, it was a good step down the road.

c. The associated question is: If a particular instance of an image or record is overwritten or destroyed, is there a way to identify that loss or change, and to correct the corruption or loss. That's another step down the road.



BRENT:

To summarize our discussion:

a. Backups are primarily for business continuity and do not necessarily guarantee preservation of a record.
b. Backup processes have risks such as perpetuating errors, whether accidental or intentional, and
c. Backup copies restore what was backed up; they do not monitor, protect or correct.
d. Preservation on the other hand is about ensuring the existence and integrity of the record.
e. So, how did your organization score as we discussed these principles? What are your next steps towards electronic records preservation?

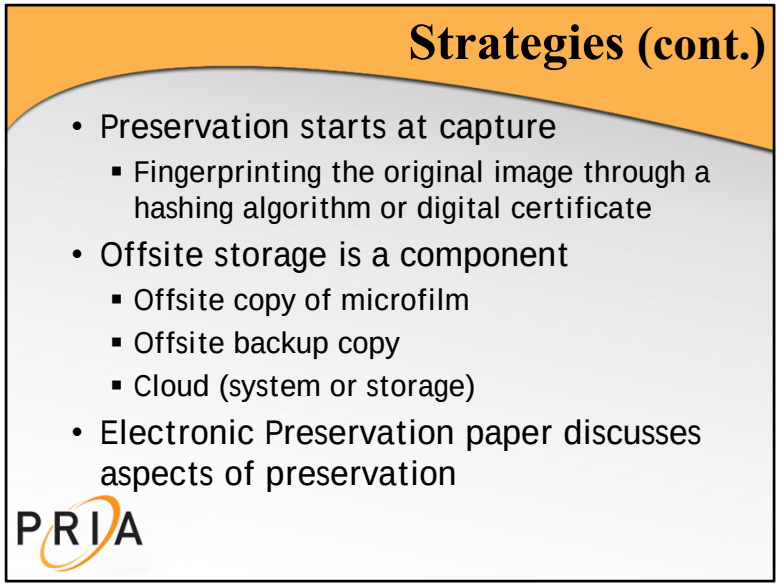
May I also note that electronic preservation is not something that you may be doing now or even in the near future. Your preservation media may still be on microfilm. But, the day ***may*** come or you may at least want to head down the road towards electronic records preservation. It will take time and money. So what's your strategy??

JIM:

It's evident that a comprehensive plan is needed and that it's comprised of multiple components. The PRIA Electronic Records Preservation paper considers:

- The role of IT's backup
- The role of the records management software and hardware
- The value of an independent data auditing and recovery system
- The value of diverse media types
- And the continuing role of existing microfilm and paper records

PRIA calls this a "Layers of Insurance" strategy where various preservation techniques and technologies complement each other.

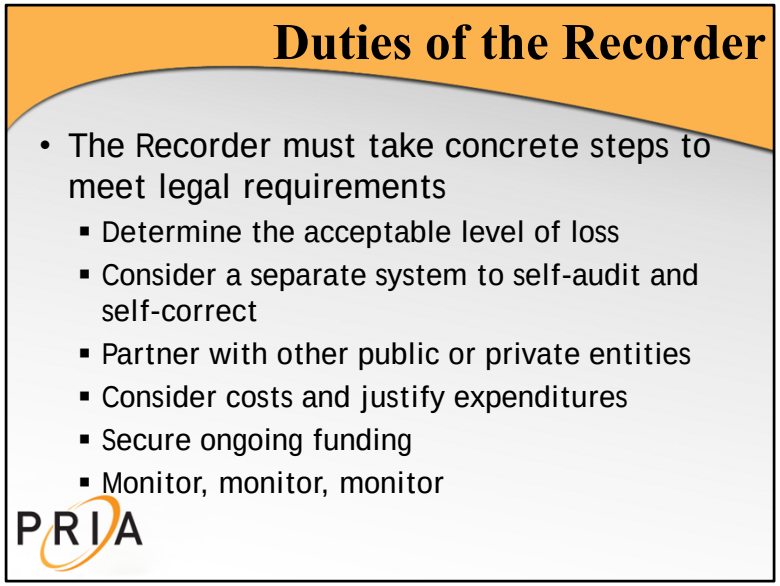


JIM:

There are three additional points that cannot be overlooked:

1. The importance of quality image capture and accurate index data. Retaining marginal or illegible images or inaccurate index data isn't a preservation practice.
2. Applying the file identification process as soon as possible after recording increases the likelihood of the record's existence and integrity. Preferably, this function should be incorporated into the LRMS.
3. Finally, copies of preservation data must be store sufficiently far from the recording location. How far will depend on the type of disasters that the recording jurisdiction experiences.

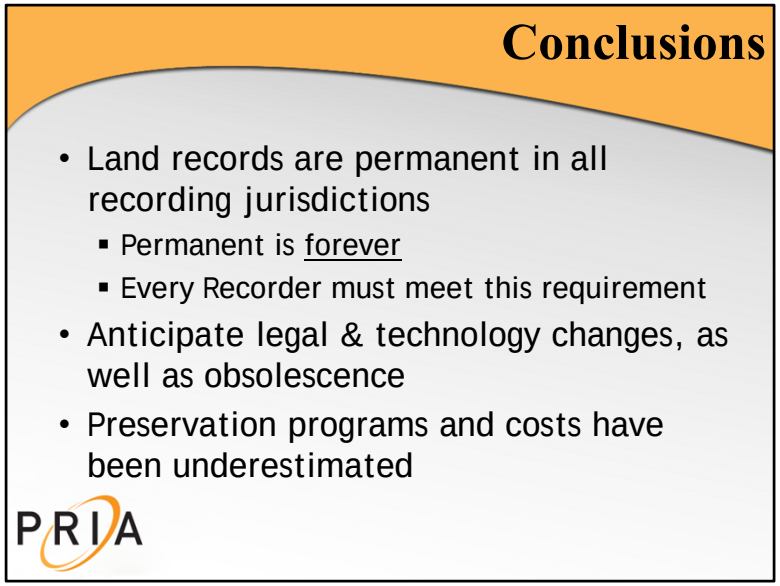
The PRIA paper discusses these and other aspects of the electronic preservation process.



JOYCE:

As a precursor to the conclusion, we want to summarize the duties of the Recorder. As we do so, please think of what your corresponding duties are as the IT professionals that are supporting your Recorder as you move in partnership towards a true electronic records preservation program.

- The Recorder, whether elected or appointed, has a duty to meet the legal requirements of preserving all permanent records past, present and future – and forever.
- For a variety of reasons, microfilm is slowly exiting the scene as a preservation strategy.
- We need to come up with new, effective strategies for electronic records and perfect the next generation of protection before we are forced to give up microfilm.
- We also have to ask ourselves, is there an acceptable level of loss? In my mind the answer is no.
- If a recorder thinks any loss is acceptable, how and by whom would that be determined?
- I certainly don't want to be the Recorder to tell one of my property owners that I don't have their record.
- Does the Recorder have a way to self-audit and self-correct what is in the system? There is a difference between being proactive and reactive.
- Are there other groups with which to partner? Look to partner with others to save costs and reinforce with the funding board the necessity of the strategy.
- What is the cost for an adequate electronic records preservation system? We must justify and explain those costs.
- We need to look at what the cost was to convert these electronic records. It's an investment worth protecting.
- It's very important to secure funding for today and into the future for an electronic records preservation system.
- And this point can't be stressed enough, don't abandon existing methods and media, which are a vital piece of our current layers of insurance, until other electronic methods are well proven out so starting the process early is a must.
- Finally, learn from our collective past. Processes put into place but not checked or evaluated regularly have proven to create gaps with missing data and images.
- So whatever program and process you put into place, you will have to monitor, monitor, monitor – leading right back to self-audits and self corrections.



JOYCE

In conclusion:

- Based on a 2017 PRIA survey, land records are permanent public records in all 50 states.
- Permanent is forever and forever is a very long time, not just the 500 years microfilm is projected to last if stored properly. This is a very tall order.
- Every recorder must take concrete steps to meet this statutory obligation of the office; we can't just talk about it and do then do nothing.
- We have to act but we cannot do it alone. We need our IT professionals.
- When establishing and revising an electronic records preservation program, legal and technology changes must be addressed – as well as the obsolescence of equipment, media and software.
- For far too long, preservation programs and costs have been understated and underestimated; it's often the last thing any organization starts to do and the first thing they stop doing.
- With an increasing dependence on electronic records and the potential for dramatic losses, these oversights must be acknowledged – and resolved.
- Recorders must make every effort to understand IT terms and processes and IT professionals must try to bridge the information gaps and understand basic preservation strategy goals.
- Only then will we find ways to work together to protect these most valuable permanent public records.
- We hope this presentation and conversation has helped you realize the importance of your role in protecting your Recorder's permanent electronic records, and in forming valuable partnerships with your Recorders.

- Before opening it up to questions, Brent and Jim, do you have anything else you would like to add?

JIM: For decades we've been focused on building the infrastructure to mange electronic information. Because most information is not considered permanent, electronic preservation strategies have been overlooked. In our industry, it is time to shift our focus to protecting the existence and integrity of the real property records that contribute to the strength of our economy. To do this will not only require teamwork at a technical level but at a political level as raising awareness with regard to value of these records will be needed to support future funding for the implementation of these important preservation strategies.

PRIA Presenters

Jim Harper
PFA, Inc.
jharper@pfainc.com
(800) 429-8200

Brent Holladay
Seminole County Florida - IT
bholladay@seminoleclerk.org
(407) 665-4475

Joyce Mascena
Glastonbury, CT - Town Clerk
joyce.mascena@glastonbury-ct.gov
(860) 652-7616