SDC 20

BY Developers FOR Developers

Storage Developer Conference
September 22-23, 2020

Data Preservation & Retention 101

Thomas Rivera, CISSP
Co-Chair, SNIA Data Protection & Privacy Committee

About the Speaker

- Co-Chair, SNIA Data Protection & Privacy Committee
- Secretary, IEEE CS Cybersecurity & Privacy Standards Committee
- Chair, IEEE Zero Trust Working Group
- Member, American Bar Association – Science & Technology (SciTech) Law Section

Thomas Rivera, CISSP

Security/Privacy Professional

Abstract

There are many instances in which the terms "retention" and "preservation" are used interchangeably and incorrectly. This can result in different and conflicting requirements that govern how the same information is maintained, how long it must be kept, and whether and how it is protected and secured. This session highlights the differences between retention and preservation.

- What will be covered in this presentation:
  - The difference between Data Preservation and Retention
  - Issues and considerations for Data Preservation and Retention
  - Guidelines and Best Practices for Data Preservation and Retention

Agenda

- Defining “Business Record”
- Overview of Data Preservation and Retention
- Data Preservation vs Retention
- Issues & Considerations
- Best Practices
- Key Takeaways

Defining a “Business Record”

“Business Record” Defined

- A record is documentary material, in any media, that is created or received in the normal course of business, and that:
  - Is worth preserving, either temporarily or permanently, because it provides evidence of the organization’s policies, procedures, activities, decisions and:
  - Has technical, administrative, historical, and/or legal value

Note: There is usually data that an organization has, which would not be considered a “business record”, e.g., lunch menu…

“Business Record”: What’s the Big Deal?

- ISO TR 18492:2005 notes that electronic document-based information constitutes the “*business memory*” of daily business actions or events, and enables entities to later review, analyze or document these actions and events
- As such, these “*records*” are evidence of business transactions that enable entities to support current & future management decisions, satisfy customers, achieve regulatory compliance and protect against adverse litigation
- To achieve this goal, the “records” should be retained and appropriately preserved

Overview of Data Preservation and Retention

Data Preservation: Defined

- The processes & operations involved in ensuring the ability to read, interpret, authenticate, protect, and secure information, data, and metadata throughout their lifecycle
  - Preservation requirements often take on:
    - Usability Focus (processes ensuring ability to use the data records)

    – and/or –

    - Legal Focus (addressing evidentiary requirements)

Source: SNIA Dictionary

Data Retention: Defined

- Involves defining the *policies* for meeting legal and/or business needs, to preserve the existence and integrity of data (business records) for a specific period of time, and/or until certain events have transpired
- Overriding normal/default data handling
  - Example: keep email for 6 months
  - If email is not a “business record”, then the p
    eliminate the email
  - eDiscovery event: over-rides normal policy

Source: SNIA Dictionary

Data Prevention vs Data Retention

Data Preservation vs Data Retention

- Data Preservation has to do with maintaining the *safety, integrity,* and continued *existence* of data

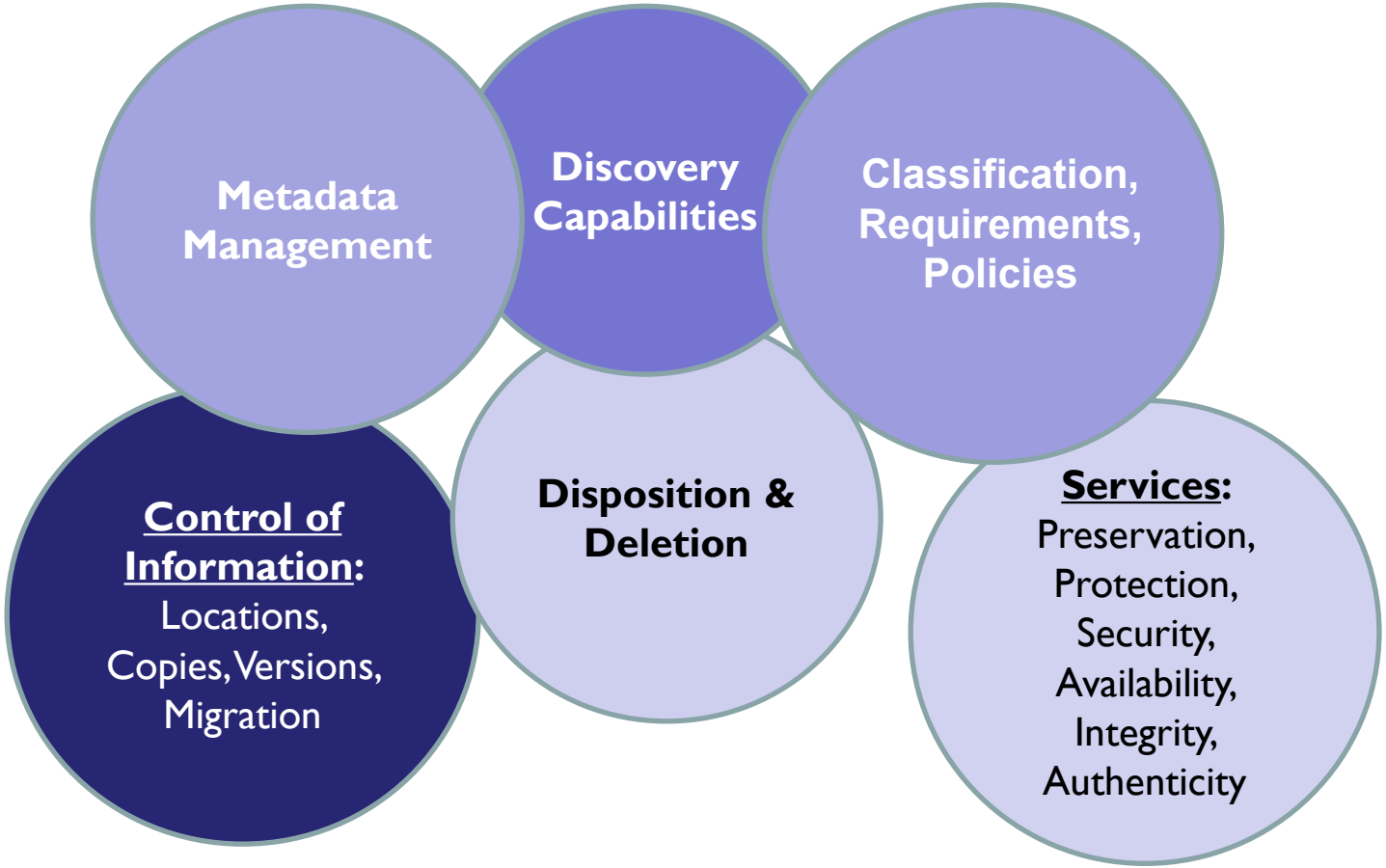
Whereas:

- Data Retention includes defining the *policies* for meeting legal and/or business needs – for a defined period of time

Preservation: Authenticity

- A property of information object's content & metadata that identifies that it is currently what it was originally and verifies that its content has not changed over time
  - Maintaining authenticity requires maintenance of the information's digital integrity, using:
    - Verification that it is the original
    - Auditing access
    - Providing a means to detect change (hashing, audit trails, etc.)

Retention: Activities



Retention: Records Management

- Developing an Electronic Retention Schedule
  - Conduct an electronic records inventory
  - Conduct legal research to obtain regulatory and legal retention requirements
  - Work with various organization members to establish business, legal, compliance, & security retention requirements
  - Identify vital records & publish, educate, and implement

ARMA International

RECORDS RETENTION AND DISPOSITION SCHEDULE

Listing by Department

Records Series Code	Records Series Title	Responsible Department	Total Retention Period	Vital Record?
02.010000	Activity Reports Committees Headquarters	CORPORATE	3 years	
04.010000	Administrative Letters	CORPORATE	10 years after superseded	
01.020000	Articles of Incorporation	CORPORATE	Life of Association	Yes
04.030000	Bylaws	CORPORATE	Life of Association	Yes
02.060000	Certificates of Destruction	CORPORATE	10 years after records are destroyed	
04.040000	Charters Chapters Regions	CORPORATE	Life of Association	Yes
04.050000	Contracts/Leases	CORPORATE	6 years after contract expires	Yes
01.060000	Copyrights	CORPORATE	Life of Association	Yes
02.030000	Correspondence (General) Ad Hoc Associations (Other) Chapters Committees & Publications Headquarters Officers Regions	CORPORATE	3 years	
02.031000	Elections/Nominations Ballots List of Elected Officers	CORPORATE	3 years	
02.025000	Email Messages Inbox & Sent Items	CORPORATE	90 days maximum	
	Insurance Policies			

Retention: Processes

- Electronic Records Processes & Controls
  - Appraisal
  - Ingest
  - Storage
  - Preservation actions
  - Access
  - Disposition

Issues & Considerations

Why is Preservation a Problem?

- Who Cares?
  - Data preservation is at the bottom of the IT hierarchy & lacks adequate funding
  - Mitigating risk (insurance)
- Drivers are relatively new (compliance, legal...)
- Technologies are Incomplete & Immature
  - Archivists rely on intensive care & best practices – these approaches don't scale to the datacenter
- Failure to Collaborate (isolated responsibilities)

Preservation & Retention Obligations

- Statutory, Regulatory, & Legal Requirements
  - SEC, SOX, HIPAA, FRCP, Intellectual Property litigation, etc.
  - GDPR
- Corporate governance (business requirements)
  - Internal controls such as:
    - Intellectual Property, HR documents (PII), etc.

IT Preservation Practices

- What are the preservation requirements? (Many do not know!)
- Many still rely on Backup (Wrong!)
- Record to Tape and ‘Lose it’ (Sad but true!)
- Migration by Crisis:
  - Small percentage Migrate every 3-5 years if on disk
  - Even smaller percentage migrate regularly if on tape
  - If an app changes, it forces a ‘crisis’ migration

Collaboration

- Legal – Assist with information identification and its importance to the organization (legal, business, compliance)
- Records Managers – Evaluate policies & procedures, analyze risk, regular reviews, determine retention requirements
- IT – Implement the policies & define systems for storage & security of the digital records (including metadata, logs, audit trails, etc.)
- Business/Operations – Create / Receive / Store records & metadata
- Security – Define Security / Confidentiality / Compliance policies
- Archivists – Preserve digital records

What about Data Loss?

- The questions are: how much & when is it a problem?
  - Lack of clear retention policies
  - Corruption or damage & inability to recover or decrypt
  - Cannot: Find it / Read it / Interpret it
  - Security theft or changes
  - No longer have the “original” records
  - Inability to access 3rd Party sites/systems
  - Failure to control & prove the integrity & authenticity of the information and its metadata
  - Migration/transformation to other formats

Data Security Services

An organization needs to be ready for potential litigation, in which records will need to address data authenticity, provenance and chain of custody, and this means that the following security services should be used:

- “Identification / Authentication Service”
  - Confirms the identities of users
- “Access Control Service”
  - Prevents unauthorized use
- “Data Integrity Service”
  - Ensures that the records are not altered or destroyed in an unauthorized manner
- “Data Confidentiality Service”
  - Ensures records are not accessed by unauthorized folks
- “Non-repudiation Service”
  - Ensures engaged parties cannot deny involvement

Source: ISO 14721

Best Practices

Retention Best Practices

- Use Preservation-aware applications
  - ILM-based practices repositories
  - It's not enough to make a single "super reliable" copy
- Conduct a records inventory
  - Must be consistently adhered to
- Obtain the organization's regulatory & legal retention requirements
- Identify vital records, then publish, educate and implement

Metadata Counts

- "Changing or enhancing the metadata of legacy ESI (any ESI retained as a record…) should be considered with care if it being retained for compliance because this could be construed as "altering" an existing record."

- Metadata associated with an immutable object:
  - Could refer to metadata that identifies characteristics of the object, and may not impact the validity of the object

Source: Report of the Judicial Conference: Rules of Practice & Procedure, Federal Rules of Civil Procedure, September 2005

Best Practices: What, How, Who…

Typical Process

- Goals and Strategy
- C-Level Sponsorship
- Methodologies
- Terminology
- Identify Information Assets
- Classification
- Set Requirements
- Policy Definitions
- Service Level Objectives
- Design and Implement
- Measure and Improve

Typical Frameworks

- Service Management
- Info Governance
- Projects – Compliance & Risk Reduction
- Information Lifecycle Management

Stakeholders

- IT
- Records & Info Mgmt
- Legal
- Security
- Business
- Finance
- Risk Management

Best Practices: Solve the Disconnects

- Failure to Collaborate
  - Need all the Stakeholders to assist in setting requirements
    - RIM, IT, Legal, Business, Risk Management, Finance, Security

- Reduce Complexity
  - Large bucket/small bucket classification practices
  - What specifically needs to be retained
    - **"Business Records"** vs everything
    - Implement Deletion, as appropriate

Collaborate, Identify, Classify, Set Requirements

Best Practices: Change in Mentality

- Replace the old ‘archive’ mentality with ‘retention & preservation’ from the beginning of the data lifecycle
- Change Disposition:
  - From: an event at ‘end of information lifecycle’
  - To: a requirement and policy at creation
  - Note: This does not affect ‘Legal Holds’

Process Controls: Storage

- Storage Media – Must ensure readability, integrity, and authenticity of the data, for as long as needed
- Media must be:
  - Protected from unauthorized access, loss, tampering, destruction, theft, disaster, and be discoverable
  - Physically & logically migratable
  - Containing the right attributes:
    - Disk – Content-aware, WORM, or via hashing, digital signatures, etc.
    - Tape – WORM
    - Optical - WORM

A “Compliant” Infrastructure

- Begin with compliance-based apps & management tools
  - Email archive, Enterprise Content Management (ECM), Enterprise Databases & ERP/CRM apps, ILM management tools
- Make sure the storage infrastructure has the necessary retention & preservation attributes:
  - Security, confidentiality, discovery-ready, protection, privacy, integrity, authenticity, business continuity, permanent deletion
  - Self-healing storage systems (eliminate physical migration)
  - Plan for logical migration
  - Compliance is audited & monitored

Data Disposition & Sanitization

- Once the preservation and retention requirements are met, there will be a need to dispose of the data (disposition)
  - not necessarily data destruction
- If destruction of data is appropriate, data “destruction” is the process of removing information in a way that renders the data unreadable
- When disposing of data, there is often the need for media sanitization
  - *Sanitization* is one of various techniques to render access to data on storage media infeasible for a given level of effort

Note: For a detailed overview of “Sanitization”, read the Sanitization White Paper written by SNIA Security TWG – located at https://www.snia.org

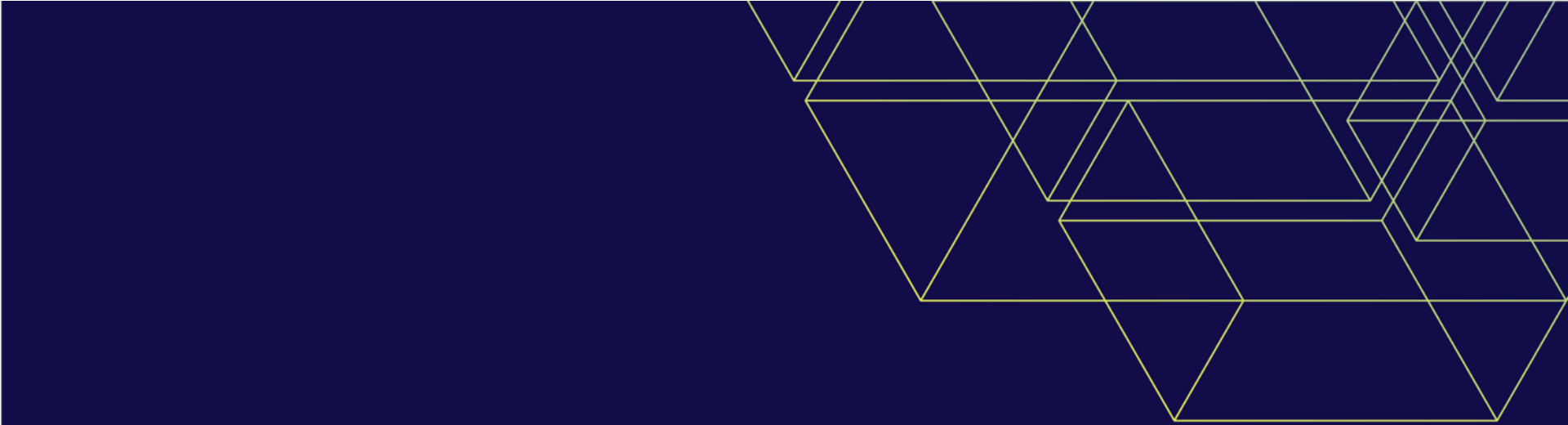
Key Takeaways

Key Takeaways

1. Only preserve and maintain what is required by your business & legal requirements ("Business Records")
2. Create, and then adhere to appropriate Best Practices:
   A. Collaborate
   B. Identify
   C. Classify
   D. Set Requirements
3. Update and Adapt to changing business and regulatory requirements

Please take a moment
to rate this session.

Your feedback matters to us!



Thank You for Attending this Session!