


Defensible Disposition
Understanding the 5Ws, How, and How Much

April 19, 2018




WASHINGTON DC | WESTVA VIRGINIA | CLEVELAND | CHICAGO | MINNEAPOLIS | SAN FRANCISCO

Agenda

- What is defensible disposition?
- Why is defensible disposition essential?
- When should defensible disposition begin?
- Where to look for defensible disposition opportunities?
- Who should be involved?
- What are the process steps?
- How are others doing it?
- How much is it going to cost?

Further Duplication Without Express Written Permission Prohibited
©2018 EdGrave, LLC All Rights Reserved



What is Defensible Disposition?

Further Duplication Without Express Written Permission Prohibited
©2018 EdGrave, LLC All Rights Reserved



The Faucet and Bathtub

Stop the unwarranted accumulation of unnecessary information by **turning the faucet off**

Further Duplication Without Express Written Permission Prohibited
©2018 RegisTech, LLC All Rights Reserved

The Faucet and Bathtub ... continued

Defensibly **drain the bathtub** by:

- Making **informed** decisions to retain or destroy
- Acting **timely** on the retain or destroy decisions

Further Duplication Without Express Written Permission Prohibited
©2018 RegisTech, LLC All Rights Reserved

The Intersection of Information Governance and Defensible Disposition

GOAL		STRATEGY
• Managing future growth	→	• Information Governance
• Reducing current accumulation	→	• Defensible Disposition
• Managing risks and costs associated with information	→	• Integration of Information Governance and Defensible Disposition

Further Duplication Without Express Written Permission Prohibited
©2018 RegisTech, LLC All Rights Reserved

Defensible Disposition

Identifies information no longer needed for any valid reason, thus enabling destruction

Is built around a solid understanding of regulatory, statutory, business, and litigation considerations applicable to the information at issue

Follows and documents a reasonable, consistent process

Addresses the unique circumstances of specific repositories

Secures input and buy-in from appropriate stakeholders before executing dispositions

Further Duplication Without Express Written Permission Prohibited
©2018 Regisys LLP. All Rights Reserved

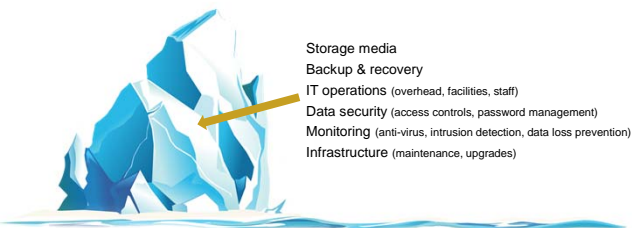


Why is Defensible Disposition Essential?

Further Duplication Without Express Written Permission Prohibited
©2018 Regisys LLP. All Rights Reserved



Costs of Keeping Too Much Information



Further Duplication Without Express Written Permission Prohibited
©2018 Regisys LLP. All Rights Reserved



Costs of Keeping Too Much Information ... continued

Storage media
Backup & recovery
IT operations
Data security
Monitoring
Infrastructure

Preservation
Discovery (cost to identify, collect, and review data for litigation)
Litigation (cost to defend against challenges when relevant data is lost)
Productivity (retaining too much information obscures valuable information with noise)
Data privacy

Further Duplication Without Express Written Permission Prohibited
© 2018 Regisys LLP All Rights Reserved

Costs of Keeping Too Much Information ... continued

Storage media
Backup & recovery
IT operations
Data security
Monitoring
Infrastructure

Preservation
Discovery
Litigation
Productivity
Data privacy

When There Is A Data Breach

- Reputational harm
- Lost sales
- Share prices tumble
- Earnings drop per share
- Profit declines
- Customer reimbursement
- Damage control
- Credit monitoring services
- Card reissuance
- Legal claims by consumers

Further Duplication Without Express Written Permission Prohibited
© 2018 Regisys LLP All Rights Reserved

Costs of Keeping Too Much Information ... continued

Storage media
Backup & recovery
IT operations
Data security
Monitoring
Infrastructure

Preservation
Discovery
Litigation
Productivity
Data privacy

When There Is A Data Breach

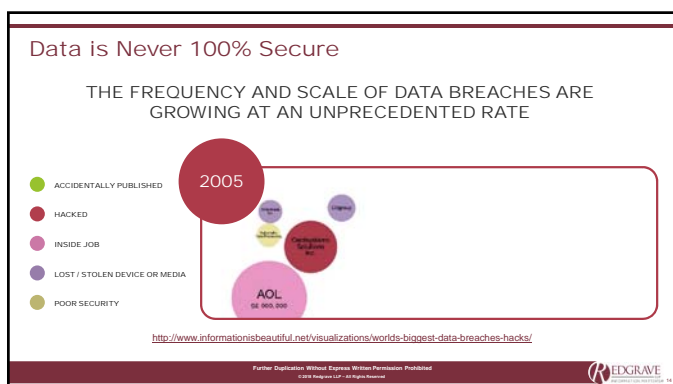
- Legal fees
- Consulting fees
- Administrative fees
- Personnel resignations or terminations
- Infrastructure changes
- Legal claims by employees
- Legal claims by financial institutions
- Legal claims by shareholders
- New ammunition for plaintiff's counsel
- Government investigations and fines

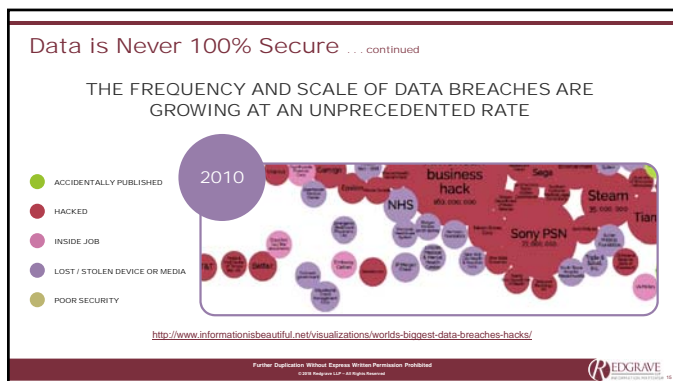
Reputational harm
Lost sales
Share prices tumble
Earnings drop per share
Profit declines

Customer reimbursement
Damage control
Credit monitoring services
Card reissuance
Legal claims by consumers

Further Duplication Without Express Written Permission Prohibited
© 2018 Regisys LLP All Rights Reserved







The Value of Defensible Disposition

- BUSINESS**: Improved access to accurate information increases productivity and supports decision-makers in ordinary course of business
- SECURITY**: Enhanced security of confidential, proprietary, and personal information
- LEGAL**: Increased efficiency and defensibility of litigation response

Further Duplication Without Express Written Permission Prohibited
©2018 Regisys LLP All Rights Reserved

Regulations Dictate Action

REGULATION	SIGNIFICANCE
General Data Protection Regulation (GDPR) (European privacy)	Applies to all organizations that collect, store, or process personal data of individuals residing in the EU, even if they are not EU citizens Mandates actions to protect and limit retention of personal data Violations result in fines up to €20 million, or 4% annual global turnover – whichever is higher
Fair and Accurate Credit Transactions Act of 2003 (FACTA) (consumer financial information)	Directed the FTC, Federal Reserve Board, OCC, FDIC, OTS, NCUA, and SEC to adopt rules to ensure the consistent and secure disposal of sensitive consumer report information
HIPAA Privacy and Security Rules (45 CFR 164.310(d)(2)(i)-(ii)) (personal health information)	Addresses policies and procedures that Covered Entities must implement to ensure safeguarding of Personal Health Information (PHI) through the disposition process

Further Duplication Without Express Written Permission Prohibited
©2018 Regisys LLP All Rights Reserved

Regulations Dictate Action ... continued

REGULATION	SIGNIFICANCE
PCI DSS Version 3.1, Req 3.1 (payment card information)	Applies to merchants, financial institutions, point-of-sale vendors, and hardware/software developers Mandates actions to protect and limit retention of cardholder data Violations result in fines from \$5,000 to \$100,000 per month
FTC Rule §2.14, 16 C.F.R. §2.14	Applies to FTC compulsory process subjects Relieves FTC compulsory process recipients of preservation obligations after passage of one year without written communication from the Commission The lifting of this preservation obligation does not apply to investigations by other government agencies or litigation
State Disposal Laws	More than 30 states have enacted laws related to the destruction and disposal process for personal information

Further Duplication Without Express Written Permission Prohibited
©2018 Regisys LLP All Rights Reserved

Rules Support Action

Proportionality was a major component of the 2015 Amendments to the Federal Rules of Civil Procedure

- Fed. R. Civ. P 26(b)(1): Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case

Proportionality is a tool that organizations can leverage to support the reasonable disposition of data

- Parties need not retain every file or scrap of paper, and perfection is not required
- Unilateral action to dispose of unique relevant information (i.e., action without consent or court order) carries some risk

Further Duplication Without Express Written Permission Prohibited
©2018 Regisys LLP. All Rights Reserved.



Reality Requires Action

Reducing discovery costs is a major justification for defensible disposition

- 75% of pretrial costs are related to discovery efforts
 - Much of that relates to costs of processing extraneous material
- Data volumes continue to increase exponentially
 - The digital universe (the data created and copied every year) will reach 180 zettabytes (180 followed by 21 zeros) in 2025
 - Many sources predict exponential data growth, generally agreeing that the size of the digital universe will double every two years, resulting in a 50-fold growth from 2010 to 2020
 - While unit costs of storage have decreased substantially, due to volume increases, total cost of owning data has increased substantially this century
- Advances in technology (e.g., TAR) can help sift through data in discovery, but are used in only a small percentage of cases

Further Duplication Without Express Written Permission Prohibited
©2018 Regisys LLP. All Rights Reserved.



Reality Requires Action

COMPANIES WILL CONTINUE TO SEE INCREASED PRESSURE TO MOVE FASTER IN LITIGATION

"I am hardly the first to urge that we must engineer a change in our legal culture that places a premium on the public's interest in speedy, fair, and efficient justice."
(Chief Justice Roberts, 2015 Year-End Report on the Federal Judiciary)

"The MIDP is premised on the idea that the goals of Rule 1 are promoted through the early sharing of information that normally would be provided only through more costly party-initiated discovery."
(Mandatory Initial Discovery Users' Manual for the Northern District of Illinois)

"Commonly known as the Rocket Docket, the EDVA [Eastern District of Virginia] boasts an average time of 11 months from 'file to trial.' Parties have only a short time to complete discovery...."
(Hunton & Williams)

Further Duplication Without Express Written Permission Prohibited
©2018 Regisys LLP. All Rights Reserved.



When Should Defensible Disposition Begin?

Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron, L.P. All Rights Reserved




Act Now or Pay Later

The cost of “doing nothing” is a lot!

The cost of deleting absent a defensible process may lead to discovery sanctions

Defensible disposition is the middle ground that enables organizations to delete data after taking reasonable care to identify and save that which the organization must keep

Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron, L.P. All Rights Reserved



Act Now or Pay Later


Early defensible disposition is less costly

- More is known about the history and purpose of the information and its repository during its useful life
- Avoid unnecessary future storage costs after deleting information eligible for destruction

Discovery risks and access costs may increase over time

- The more data there is, the more likely it is that some well-intentioned users will delete data just because it has not been accessed in years
- When the business is no longer actively using data, the costs of accessing and understanding the data increases as subject matter experts transition and technology ages

Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron, L.P. All Rights Reserved



Where to Look for Defensible Disposition Opportunities?


Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron LLC. All Rights Reserved



Natural Opportunities

- Mergers, acquisitions, and divestitures
- Reorganizations
- Data migrations (e.g., on-premise Microsoft to O365)
- Software/hardware overhauls
- Site closures/relocations
- Conclusion of large litigation


Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron LLC. All Rights Reserved



Containers that may Include Eligible Information

- Application and platform decommissioning
- Backup media
- Physical hardware assets (e.g., hard drives, mobile devices)
- Paper/boxes
- Legacy data sources (e.g., archives; systems/data associated with divestitures)
- Inherited data sources from mergers & acquisitions (i.e., not all inherited systems/data need to continue to live after the merger/acquisition)
- Redundant, Obsolete, or Trivial (ROT) data sources (e.g., file shares)
- Custodial data sources of former employees
- eDiscovery collections for completed matters
- Third-party data sources (e.g., IT service providers; discovery vendors; outside counsel)

Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron LLC. All Rights Reserved



Who Should be Involved in Defensible Disposition Efforts?

Further Duplication Without Express Written Permission Prohibited
©2017 Edgewise LLP. All Rights Reserved.

Groups Involved in Defensible Disposition

BUSINESS UNITS
INFORMATION TECHNOLOGY
COMPLIANCE
LEGAL COUNSEL
RECORDS & INFORMATION MANAGEMENT
INFORMATION SECURITY & PRIVACY
EXECUTIVE SPONSORSHIP

Further Duplication Without Express Written Permission Prohibited
©2017 Edgewise LLP. All Rights Reserved.

Session

See you in 30 minutes

Break

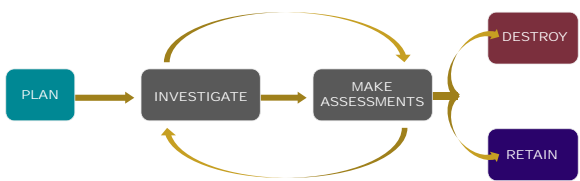
Further Duplication Without Express Written Permission Prohibited
©2017 Edgewise LLP. All Rights Reserved.

What are the process steps?


Further Duplication Without Express Written Permission Prohibited
©2018 Regency L.P. All Rights Reserved




Defensible Disposition Process




Further Duplication Without Express Written Permission Prohibited
©2018 Regency L.P. All Rights Reserved

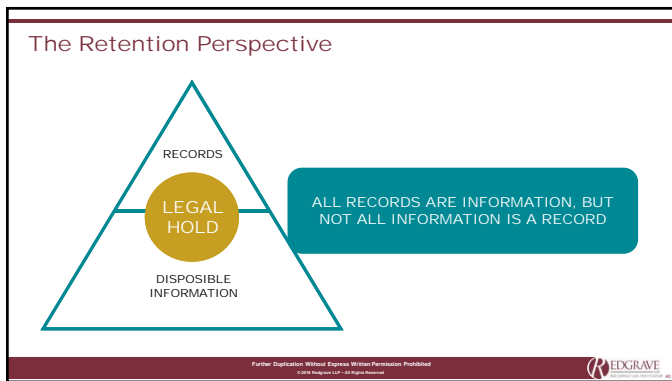


The Foundation for Assessments



Further Duplication Without Express Written Permission Prohibited
©2018 Regency L.P. All Rights Reserved





The Retention Perspective

Records should be destroyed when no longer required to be retained by the Retention Schedule

...and are not subject to a legal hold

Disposable information may be destroyed when it no longer has a useful purpose

...and is not subject to a legal hold

Therefore . . .

Before destroying, confirm that a record or disposable information is **not subject to legal hold**

Further Duplication Without Express Written Permission Prohibited ©2018 RegisTech, LLC All Rights Reserved

EDGRAVE

The Preservation Perspective

Litigation complicates defensible disposition projects, requiring additional analysis to identify and preserve relevant data

Failure to preserve/assess relevant data properly may lead to:

- Sanctions (monetary, or that impact case outcome)
- Loss of counsel's credibility in court's eye
- Reputational damage to client

Further Duplication Without Express Written Permission Prohibited ©2018 RegisTech, LLC All Rights Reserved

EDGRAVE

Legal Requirements for Defensible Disposition

- Process must be undertaken in good faith
- Process should account for applicable records retention policies, including relevant statutory requirements, regulations, and business drivers
- Process should involve assessments of the likelihood that the target population is subject to a legal duty to preserve information
- Process should tailor level of investigation and assessment to "reasonable steps"
- Standard is not perfection, but the process will be subject to post-hoc scrutiny
- Process should be memorialized to enable post-hoc explanations of reasonableness

Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron, L.P. All Rights Reserved



After Establishing the Foundation . . .

- Identify candidates for defensible disposition
- Assess candidates and opportunities
- Develop business cases, budgets, and plans for phases
- Execute defensible disposition plan

Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron, L.P. All Rights Reserved



Assessing Candidates

- Look for quick wins with large impact
- Determine which business units have relatively low-risk litigation profiles
 - Identify sources easier to isolate and separate into "keep" and "delete" groupings
 - Evaluate what information is the most costly to retain
- Consider candidates that may warrant extra due diligence
- Are there candidates where the organization may benefit from an independent legal opinion as to the reasonableness and defensibility of the disposition process?
 - Do any candidates involve ambiguous data sources?
 - Do any candidates likely contain sensitive information or personal data that will require heightened standards for destruction?

Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron, L.P. All Rights Reserved



Budgeting and Planning

Ensure that the following (often-overlooked) components are considered:

- Budget includes line item for actually deleting/destroying data that the organization determines is no longer needed (this can be a costly line item)
- Plan includes developing a comprehensive inventory of information that is eligible for disposition from each source
- Plan accounts for multiple iterations of analysis and decisions
- Plan includes a step to identify the documentation (e.g., inventory, workflow documentation, disposition documentation, and/or defensibility memorandum) that is required to close the project

Further Duplication Without Express Written Permission Prohibited
©2018 Progress L.P. All Rights Reserved



Executing the Plan

- 1 Determine everything known about the information eligible for disposition
- 2 Compare what is known against the organization's obligations to retain for record retention and/or legal hold
- 3 Assess risks associated with different categories of records
- 4 Evaluate, if necessary, the cost-benefit of doing further due diligence
- 5 Separate what must be retained from what may be destroyed

Further Duplication Without Express Written Permission Prohibited
©2018 Progress L.P. All Rights Reserved

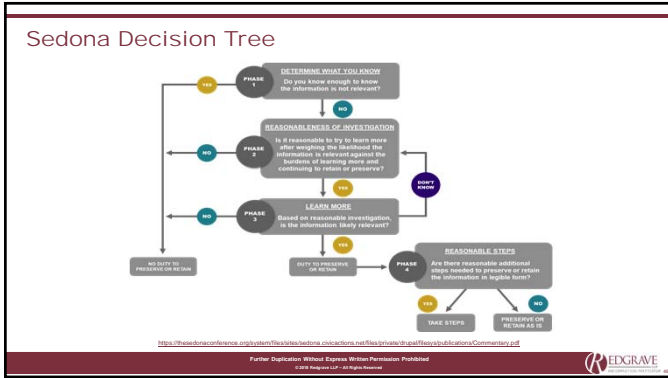


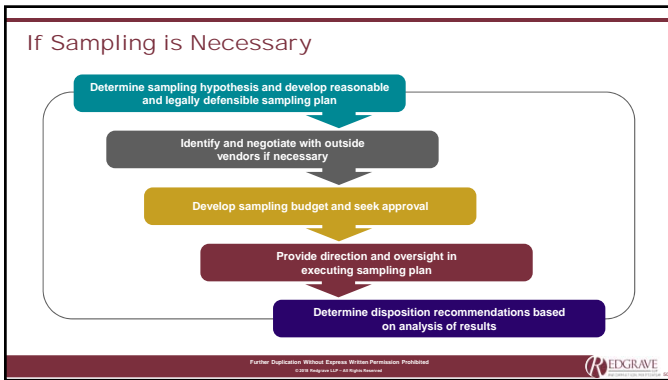
Executing the Plan

- 6 Document analyses, processes, and outcomes
- 7 Obtain appropriate approvals
- 8 Destroy eligible information
- 9 Identify solutions to stop unwarranted accumulation of data on a going-forward basis
- 10 Incorporate learnings from defensible disposition into a repeatable framework, and ensure that relevant learnings are incorporated into periodic records compliance training

Further Duplication Without Express Written Permission Prohibited
©2018 Progress L.P. All Rights Reserved









Case Study #1 - Email Archives



Fortune 1000 company with two legacy email archives (Legato and FileNet) and a new Autonomy email archive

Project goals included:

- Migrating over 300 million archived messages from the legacy archives to Autonomy
- Identifying and applying default retention periods using a tiering approach
- Identifying and applying legal holds in Autonomy
- Deleting messages past retention and clear of all legal holds

Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron, L.P. All Rights Reserved



Case Study #1 - Email Archives



Validated multiple stages of legacy Legato and legacy FileNet email migration into Autonomy

Determined rules for what to keep or delete

- Identified messages for hold using custodian and keyword criteria
- Deleted messages past retention and no longer on hold

Deletion required considering three locations:

- IDOL index
- Enterprise archive database
- Actual messages from Centera storage

Deletion required coordination with internal/vendor resources

Project required on-going collaboration and consultation

Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron, L.P. All Rights Reserved



Case Study #1 - Email Archives



Destroyed approximately 150 million messages (or 50% of the email archive)

Other significant highlights:

- Company developed, tested, and used a custom delete process because Autonomy's built-in delete process was incapable of efficiently handling deletes from an archive of over 300M messages
- DOJ investigation arose the same day deletes started, causing a temporary pause in delete processing
- It took about five months of actual processing time to delete the 150M messages

Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron, L.P. All Rights Reserved



Case Study #2 - Applications and Digital Assets



Fortune 50 pharmaceutical, medical device, and consumer products company seeking to reduce its technology footprint significantly

Project goals included:

- Decommissioning, consolidating, or migrating to SaaS (Software as a Service) 40% of its applications within three years
- Evaluating thousands of applications and digital assets (websites, social media, mobile applications) to determine if the related data was subject to record retention and/or legal hold
- Preserving data for record retention and/or legal hold purposes prior to decommissioning legacy applications and digital assets

Further Duplication Without Express Written Permission Prohibited
©2018 Regisys, LLC. All Rights Reserved



Case Study #2 - Applications and Digital Assets



Formed a cross-functional review team (IT, Records Management, Legal) and implemented a process for reviewing applications and digital assets for record retention and legal holds prior to decommissioning

Developed requirements for the preservation of data from applications and digital assets under legal hold

Introduced a "Legal Hold" flag in the company's asset management inventory

Worked collaboratively with the company's enterprise archive team to establish archive requirements and validation processes

Further Duplication Without Express Written Permission Prohibited
©2018 Regisys, LLC. All Rights Reserved



Case Study #2 - Applications and Digital Assets



Approximately 50% of over 2,000 applications and digital assets reviewed had no record retention and/or legal holds and were freely decommissioned

The remaining applications and digital assets were preserved via migration and/or archiving prior to decommissioning the technology infrastructure

Tiering approach reduced archiving costs from hundreds of thousands to less than \$5,000 to preserve applications with low likelihood of collection

Further Duplication Without Express Written Permission Prohibited
©2018 Regisys, LLC. All Rights Reserved



Case Study #3 - Backup Tapes



Global 500 company with over 60,000 legacy media items in one division

Mostly backup tapes of varying types and standards

Media assumed to contain emails, user files, application data, and other unknown content

Little to no inventory information available for a large subset of the media items

Desire to destroy information no longer needed to reduce legal risk and storage costs

Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron, L.P. All Rights Reserved



Case Study #3 - Backup Tapes



Synthesized information regarding media items and preservation obligations

Established sampling hypothesis and strategy

Restored, indexed, and filtered data based on legal hold keywords

Reviewed corpus for "responsiveness," and selected sample sets of emails and user files for validation by custodians and IT

Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron, L.P. All Rights Reserved



Case Study #3 - Backup Tapes



Destroyed approximately 80% of media items

Continued hold on the remaining media items

Other significant highlights:

- Complete process took about eight months — several months longer than originally planned
- Had to be flexible and adjust plan as issues were encountered and IT resources were limited
- End result was well-received within Legal and by IT

Further Duplication Without Express Written Permission Prohibited
©2018 Regeneron, L.P. All Rights Reserved



Defensible Disposition is Achievable

We know of companies that have defensibly:

- Deleted approximately 150 million messages (50%) from an email archive
- Destroyed all but a small subset of legacy backup media stored in a two-level "vault" room
- Deleted over 2.5 million archived legacy files from user home directories and over 18 million archived legacy files from departmental share directories
- Destroyed approximately 90% of targeted legacy backup media
- Discarded two-thirds of legacy paper documents

Further Duplication Without Express Written Permission Prohibited
©2017 Regisys LLP. All Rights Reserved.



Additional Takeaways

The business needs to appreciate relative risks of inaction vs. action

Once eligible for destruction (and not subject to legal hold), records and disposable information should be destroyed as soon as reasonably practical

Records and disposable information must be destroyed in a manner that preserves the confidentiality of the information contained therein and complies with applicable laws

Identify metrics that your organization can capture to help reinforce the benefits of defensible disposition while, at the same time, demonstrating that your organization took reasonable preservation efforts as it sought to reduce costs from the accumulation of unnecessary data

Further Duplication Without Express Written Permission Prohibited
©2017 Regisys LLP. All Rights Reserved.



**How Much is
Defensible Disposition
Going to Cost?**

Further Duplication Without Express Written Permission Prohibited
©2017 Regisys LLP. All Rights Reserved.



The Costs of Defensible Disposition Initiatives

Legal consulting costs for review, analysis, and opinion regarding the reasonableness and legal defensibility of the process

Internal resource costs to support the investigative and approval processes

Vendor costs may be incurred for use of enabling technologies, sampling, or similar

Destruction costs may be incurred when eligible information is destroyed

Further Duplication Without Express Written Permission Prohibited
© 2018 EDG RAVE LLP All Rights Reserved



?
QUESTIONS

WASHINGTON DC | NORTHERN VIRGINIA | CLEVELAND | CHICAGO | MINNEAPOLIS | SAN FRANCISCO
