DONOMA

DATA ARCHIVING & DATA PROTECTION FOR TODAY'S BUSINESS CONTINUITY CHALLENGES

Multi-Data Compliance Archiving, Information Governance, Data Protection Challenges & Best Practices

EXECUTIVE SUMMARY

Executive Summary

In the wake of accelerated adoption of new communication and collaboration tools, organizations have made a significant digital transformation. Powered by the cloud and supported by Software-as-a-Service solutions, many have rapidly new solutions to communicate and conduct business from anywhere, with anyone, at any time. This includes tools like Zoom, Microsoft Teams, Webex and more.

Data generated within these platforms is a vital component of an organization's intellectual capital. Managing and retaining it according to established EDRM processes continues to be critical to the recovery of relevant data and the enforcement of defensible holds during a legal proceeding.

However, considering the massive growth of Ransomware and its impact on Business Continuity planning, the value of an EDRM system spans beyond support for compliance and legal discovery.

This white paper outlines today's data protection challenges, best practices in information governance and how Donoma's OneVault Multi-Data Archiving Platform uniquely support organizations needing to manage both expanding data types and data threats.

About Donoma

Donoma Software specializes in data archiving, data protection and multi-vendor communications data integration. Donoma's solution stack helps organizations with information governance & compliance, streamline operations, gain insight into customer experiences and provides AI-powered audio transcription and translation.

DONOMA

TABLE OF CONTENTS

DONOMA

THE NEW RISK LANDSCAPE

REMOTE WORK IS DRIVING NEW COLLABORATION CULTURE

During the pandemic, businesses adopted cloud technology to support the Work-From-Home environment and increase communication between employees. Products like Microsoft Teams, Slack, Zoom and Webex were rapidly adopted. Since businesses were in a rush to turn on these services, they gave little thought to data retention. Now, many are learning that just because data is in a cloud system, it doesn't mean it is backed up or archived. These solutions rely on the **Shared Responsibility Model,** which means they take no responsibility for your data or its protection. Organizations must ensure their data is backed up, even if it is in the cloud.

"Organizations are facing an evolving archiving market that now covers multiple new content types, use cases and a predominantly cloud-based delivery model. The increased variety of use cases is as significant as the expanding number of content types. Archiving has moved beyond information storage optimization and retrieval to a focus that is oriented more toward risk management, information governance and related use cases, such as compliance supervision, e-Discovery and analysis."

-Gartner Research

Understandably, it does not make sense to bring data back on-premises to archive and protect it. That is why Donoma and others have pivoted archiving solutions into a cloud-based model. Cloud-based archiving combines Information Governance for compliance with cost-effective long term data protection. This prevents data loss and increases security.

There are several important drivers for communications and data archiving, although the impact of each depends on an organization's size, market vertical and associated operating regulations, its tolerance for risk, and other factors related to business continuity and intellectual property management.

THE NEW RISK LANDSCAPE

UPDATED RULES GOVERNING DISCOVERY FOR LITIGATION

Civil litigation in the United States is governed by a procedural framework called the **Federal Rules of Civil Procedure** or FRCP. The FRCP has been significantly updated twice in the last decade to codify the concept of electronic records that could now be used during litigation; and to shorten discovery periods. After all, with better technology, the expectation changed for the time it takes to gather information needed. This requires litigants to now be quickly prepared for e-Discovery quickly once the litigation process starts and requires a speeder resolution to e-Discovery proportionality issues.

FRCP Rule 26(a)(1) **obligates litigants to have a good understanding of their data assets**. Moreover, they must be able to discuss these issues in advance of the initial pre-trial discovery meeting. FRCP Rule 16(b) requires that this meeting occur within 99 days (often sooner) from the commencement of a legal action.

Time is an important factor, and today the expectation is that data can be quickly produced. It is therefore important that all parties have solid archiving and e-Discovery capabilities in place to be prepared for litigation that almost all organizations face.

ALL ORGANIZATIONS HAVE ONGOING RETENTION OBLIGATIONS

Any sound archiving & governance strategy must ensure that it can support an organization's litigation obligations and reduce the risk, exposure and cost associated with legal actions.

- **More data types must be archived and managed**

  Information Governance (and therefore archiving) requires more sophistication because of the explosion of new communication platforms and associated data.
- **Relevant data must be preserved**

  All organizations must preserve their relevant electronic communications records, even those outside heavily regulated verticals. These records include interactions with clients, communications pertaining to sales, contracts, employee records, policy statements and any other content that might be relevant for litigation, regulatory compliance, or any other information that management or legal deems necessary.

THE NEW RISK LANDSCAPE

- **Data is now decentralized**

  Due to the recent shift to the use of highly distributed systems, communication records may be generated and distributed across many different systems and devices, none of which may be under your organization's immediate or physical control.

- **Litigation holds are a critical requirement**

  A litigation hold requires that if an organization can reasonably expect legal action, they must immediately identify potential data impacts, identify the data/accounts, and suspend any content deletion processes for all related data. This must happen as soon as possible, ideally long before any legal action commences. Failure to react quickly and implement a legal hold can result in serious consequences such as sanctions on organizations that fail to implement proper litigation holds, including adverse inference instructions, fines, additional costs for third parties to review or search for data and, in some cases, criminal charges. ***At a minimum, an organization that deletes data improperly may suffer harm to its corporate reputation.***

THE RISE OF SAAS & CLOUD ARCHIVING

The cloud has significantly impacted archiving, governance & e-Discovery in two ways:

First, **a growing proportion of discoverable content is created and located in the cloud.** With the mass adoption of Microsoft Office 365; Teams, Zoom and other cloud-based communications platforms, the applications that power today's organizations originate in the cloud, having replaced on-premises solutions. While email used to be the only focus of archiving, now there is a rapid proliferation of communication and collaboration tools that contain information subject to e-Discovery. Organizations continue to move away from on-premises Archiving platforms as part of larger cloud strategies.[1]

Second, **there are a growing number of cloud-only vendors that offer e- discovery, archiving and other capabilities. These solutions are changing e-Discovery practices and expectations** by enabling easier access to discoverable information by a wider range of roles, most of whom are not overly technical.[2]

> ***"By 2023, 45% of enterprise organizations will adopt an Information Archiving solution, up from 5% in 2019."***
>
> ***-Gartner Research***

DEMOCRATIZING TECHNOLOGY DEPLOYMENT WITH CLOUD SAAS

As early as 2019, Gartner's advisory services have been advocating that organizations deploy Archiving as SaaS, if possible, due to its feature-rich offerings and ease of use; while satisfying requirements for an operating expenditure model.[3]

Cloud-based SaaS removes the burden of each organization purchasing, maintaining, and managing the infrastructure for applications. As such, the process to adopt solutions and start gaining measurable benefits has shortened significantly, requiring often only minimal involvement with the IT staff.

[1] Gartner Research, Critical Capabilities for Enterprise Information Archiving, December 2019
[2] Osterman Research
[3] Ibid

NEW DATA PROTECTION CHALLENGES

DATA ASSETS: ACCESS & PROTECTION

All organizations face the question of what to do with employee data that must be maintained and accessible long after their tenure. All employees leave behind huge amounts of potentially valuable data, as well as data that's subject to regulatory retention or e-Discovery requirements.

Data could be located on a shared drive, a smartphone, an employee computer or in their Office 365 account (which includes OneDrive, Teams and SharePoint). This can all be permanently lost when these assets are cleansed as part of the employee exit process.

It is common for companies to reassign software licenses to applications (Microsoft 365, Zoom, Webex, etc.) and quickly re-image workstations. While this is efficient and reclaims storage space, without an archive to maintain the prior employee's data, all data is lost.

Today there is greater awareness of the value of knowledge assets and the value of e-Discovery capabilities into the archive when facing legal disputes.

RETENTION POLICIES

Having an electronic records retention policy is vital to address several common issues:

- Meet federal and industry regulatory requirements.
- Support legal needs to retain and provide timely e-Discovery.
- Preserve institutional knowledge during normal employee turnover.
- Reduce IT server loads and storage consumption.
- Support business continuity.
- Provide immediate alternate access to data in the event of a downtime event.

Defining how long your company will retain data must be addressed with leadership and key department stakeholder involvement. Data protection is no longer a department level responsibility.

NEW DATA PROTECTION CHALLENGES

Data retention used to be the sole purview of IT. Now, executive leadership, usually with guidance from Legal, determines policy. Then it is IT's job to execute the corporate policy. Legal counsel, compliance, audit, and executive leadership work together to establish policies.

At a minimum, there needs to be a thorough review and understanding of regulatory requirements to form a retention baseline. Then there is often refinement to support the operational needs of various departments.

ESTABLISHING POLICY: BASELINE FIRST, THEN REFINEMENT

Begin with your regulatory requirements and involve the right stakeholders. Policy definition should involve Legal, IT, Operations/Audit and if applicable Compliance personnel. Legal will provide counsel based on the regulations. That advice will determine retention policies, data segmentation and retention groups.

It is extremely common for executives to expect to have access to historical data for longer time periods. Be prepared to apply layered policies based on (for example) data type, sender, recipient, or department.

For instance, a policy will designate email spam to never enter the archive. The remaining data will have a baseline retention policy of 5 years. Operations and HR will retain their data for 7 years. C-suite correspondence, invoices and sales records are often held for extended periods.

ENSURING MANAGEMENT THROUGH THE FULL LIFECYCLE

Finally, your policy needs to define strict guidelines regarding data disposal at the end of its retention period. With the volume of daily activity, this can no longer be a manual process. Instead, it's best to automate this process with a compliance archive. That way your retention policy is managed from start to finish with accountable, defendable data management.

NEW DATA PROTECTION CHALLENGES

IMPACT OF RANSOMWARE

Ransomware has created awareness of data protection vulnerabilities. It has even learned how to use traditional backup best practices as a weapon. How? Most ransomware attacks use a time delay to enable the malicious code to infiltrate everything, including access to full backups typically performed every 7 and 30 days. **By the time the ransomware executes, it has usually captured for ransom both the original data and the backups.**

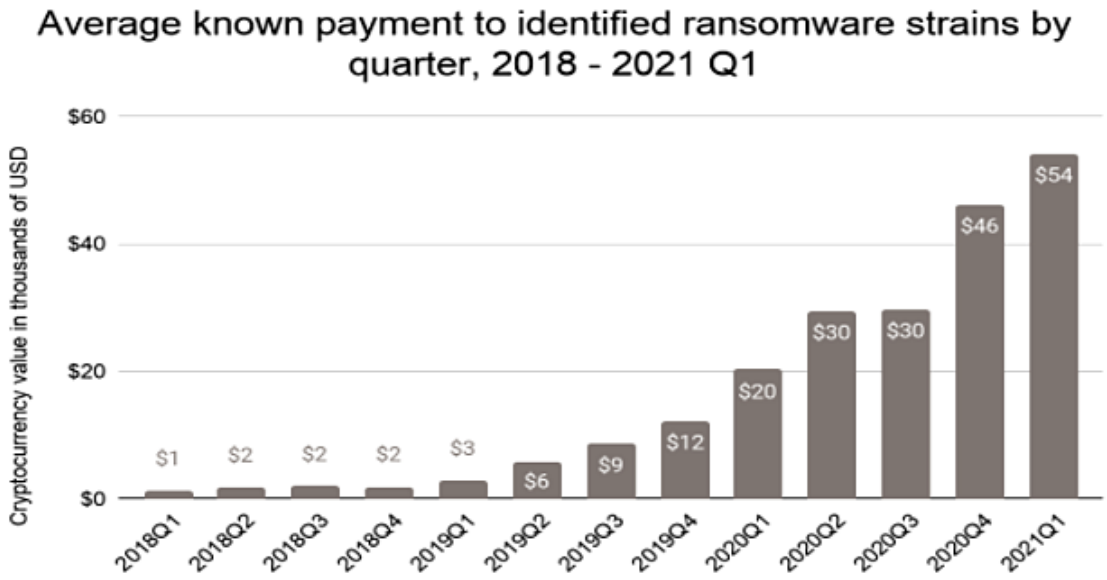
Some organizations adopt a move to a cloud-based cold storage repository. Sure, **it is cheap to push your data to that cloud repository, but when you need it back, you discover how expensive the retrieval fees, bandwidth consumption spikes and time can really cost** when each of these resources is already at a premium.

The distributed architecture of a cloud-based archiving platform supports business continuity strategies by the nature of its architecture, security control model and its real time encrypted retention. A backup and an archive do not replace each other in an ideal model, but, when necessary, your archive can provide a lot of interim benefits if your backup is compromised by ransomware or some other offline event. Given that the most attacked organizations are within verticals already subject to archiving requirements, the ability to leverage archives as part of a business continuity strategy cannot be overlooked.

NEW DATA PROTECTION CHALLENGES

BUSINESS CONTINUITY & THE C-SUITE

As ransomware has become a prolific business continuity threat; senior leaders have quickly come to understand the issues. Protecting data is part of their fiduciary duty to ensure the safety and continued operation of their organization. What used to be a concern for only the very largest organizations now plagues organizations of every size, vertical and type.



Ransomware 2021: Critical Mid-Year Update, Chainalysis

Organizations need and want the ability to quickly locate specific "conversations". Today, these may be in text form (email, Instant Message, Team Chats), audio (voicemails, audio recordings) or video (Zoom video meetings and saved audio & video recordings).

Data now must be automatically retained according to company policy, with provisions for extended legal holds management. Just as important, data needs to be automatically destroyed at the end of its lifecycle. **The volume of data and activity make it impossible to do this properly without an automated archiving solution.**

ONEVAULT: BUILT FOR TODAY'S ENVIRONMENT

PRODUCT PREMISE & VISION

Donoma OneVault is the product of over a decade of Donoma's experience building and maintaining communications archiving solutions.

OneVault brought together the security and ease of use of our prior stand-alone solutions to meet the market demand for managing a variety of different data types and move that process into secure clouds. provides an information governance solution that encompasses the entire lifecycle of communications data – from its initial capture through to its final disposition.

WHY MULTI-DATA?

Previously, email was the de-facto communication record within organizations. While certainly not official documentation at a contractual level, email provided knowledge continuity when there was turnover, and it enabled an understanding of the chain of communications that supported the operational dealings of an organization. Voicemail and some instant messaging were meaningful in certain industries, but when looking to review an organization's past activity, email was the repository of first choice.

Prior to the COVID-19 pandemic, the adoption of more holistic communication tools was starting. Video conferencing had moved out of the conference room and become a desktop/personal experience. Instant messaging technology moved from 1 to 1 conversation to persistent team chat spaces complete with documents. Communication tools proliferated to support greater agility with teams of people collaborating across organizations and around the globe.

These new communication tools exploded in popularity and adoption during the pandemic and show no signs of slowing. This means that organizations are facing the need to retain and manage data from a variety of communication systems. Email may still be in use, but it is no longer the only place where business is conducted. Ensuring that all these communications data records are properly retained and accessible for lookup (e-Discovery) has become a multi-data requirement.

ONEVAULT: BUILT FOR TODAY'S ENVIRONMENT

WHY CLOUD?

Since 2019, cloud has rapidly crossed the chasm and become a trusted delivery platform for applications as well as a trusted location for critical data. Several forced combined to make this culture change.

1. **Security.** The rampant ongoing proliferation of Ransomware proved that on-premises security practices were not being managed adequately enough to prevent network and data compromises of traditional on-premises network systems. The IT teams responsible for these systems were already being stretched thin in both skills and available time to focus on managing their data security. The argument that on-premises control was better and more secure was repeatedly and expensively exposed.
2. **Work From Home Agility.** As the global workforce was sent home during the pandemic, cloud-based solutions emerged as the path forward for business continuity. Cloud-based solutions were fast to provision, required much less staff IT support and were able to scale up and down very quickly. The value of this kind of agile scalability powered by the cloud became extremely apparent and organizations pivoted to support their business continuity with a workforce that was primarily now working from outside their office suites.
3. **Technology Budgets Moved.** Cloud democratized application selection and setup, thereby shifting the decision making on which applications were purchased and implemented. Because all the servers and supporting infrastructure were moved into the cloud and managed by the application vendors, IT no longer had as much authority or direct budget.
4. **Shifting CAPEX to OPEX**. Cloud enabled organizations to stop investing in as much IT servers and storage that were still often underutilized, hard to manage and secure consistently and required a continual refresh. Cloud led the way to delivering just the amount of technology needed at any given time and do so while freeing up CAPEX spend.

ONEVAULT: BUILT FOR TODAY'S ENVIRONMENT

ONEVAULT: ARCHIVING EXPRIENCE BROUGHT TO THE CLOUD

Donoma was already moving towards a unified cloud-based archiving model as early as 2018. Our prior single data solutions were requested as a multi-data option with a “single pane of glass” search experience for users, and a demand for centralized policy enforcement for data retention and governance.

OneVault was already well on its way in 2019 and our vision for cloud adoption accelerated by 5 years. We were positioned and ready to deliver the best of our prior archiving solutions, now combined with even more powerful search indexing and production, completely refreshed interfaces for each user role, now exclusively available as a cloud service. By doing so we know we can better secure and manage the platform and avoid the common problems we saw when archiving solutions were managed on-site by an overworked team who don’t specialize in this kind of data.

Our default data location is within our geo-diverse data centers within the United States, but we also provide options for government organizations needing specialized data handling, and our cloud management does provide options to handle data sovereignty requirements often seen in certain areas of the world.

DATA RETENTION & GOVERNANCE FOR THE ENTIRE LIFECYCLE

OneVault is a cloud- based archiving solution with advanced data management, search, and retrieval capabilities to manage multiple different data types from a single management screen. IT automatically captures all communications as they occur and stores them in. a secure, tamperproof, and centralized archive platform.

ONEVAULT: BUILT FOR TODAY'S ENVIRONMENT

As the single source of truth, OneVault provides:

- An indisputable record of 'who said what, when, to whom.
- Role-based access to data, so users can instantly search for and retrieve any message, even if the original has been deleted.
- Configurable retention policies to preserve data only for as long as it is relevant, valuable, or subject to legal requirements. Records cannot be deleted before the expiry of their applicable retention period or if it is subject to a legal hold. Once a legal hold is removed, OneVault will automatically compare the original retention schedule for that record and either resume its retention, or securely delete it if it would have normally been deleted by that time.
- Streamlined deployment and ongoing support with no software, hardware, or programming required. This saves on costly capital expenditures and alleviates IT from the concerns of data management, storage, and security.
- Tremendous scalability that enables organizations to easily provision and adjust their archiving needs over time. The aggregated allocations provide ample retention options that are much easier to manage.

MONITORING & AUTOMATED REVIEW WORKFLOWS

Every day, workers exchange millions of communications, which may include email, IM, Team chats and more. These communications document operations, understandings, agreements, and a variety of other business information of long-term value, necessitating their retention and ability to be quickly located when needed.

OneVault provides Keyword SmartActions ™ a real-time solution for automating the supervision of all the communications flowing through the archive platform. Understandably, these data volumes are beyond the scope of manual supervision. Instead OneVault monitors communications against a list of keywords – with matches triggering notifications and/or review workflows.

ONEVAULT: BUILT FOR TODAY'S ENVIRONMENT

OneVault's Keyword SmartActions provide:

- Adherence to corporate rules, including acceptable use, ethical standards, and privacy.
- Detection of a wide range of HR policy violations, from bullying and discrimination to sexual harassment and retaliation.
- Discovery of insider threats, corporate and customer data leaks, and intellectual property theft.
- Timely and appropriate notifications so that the organization may respond based on the keyword, its policy and related workflow. With timely insight, organizations can detect and address risks early, averting costly legal action or adverse publicity that can negatively impact and organization's reputation and brand.

E-DISCOVERY & LEGAL HOLD

Organizations of all sizes, in all industries, constantly deal with audits, investigations, and legal proceedings. In these situations, they typically need to produce evidentiary records to prove their case and protect their business.

Without an e-Discovery solution in place, organizations cannot access current and historical data in a timely fashion without incurring enormous costs.

OneVault's powerful indexing technology makes e-Discovery cost-effective and comprehensive with all the essential tools for data search, review, legal holds, and accountable data production.

DATA SEARCH & RETRIEVAL

OneVault continuously captures, processes, and preserves communications data – including original formatting and contextual metadata. Because all the data is indexed and continually optimized, individual records are easily available on demand without any special IT expertise. This enables the users and stakeholders to have confidence that the data they need is readily accessible to them.

ONEVAULT: BUILT FOR TODAY'S ENVIRONMENT

Because of OneVault's intuitive interface, Legal and e-Discovery personnel can immediately run their own e-Discovery searches to quickly find the records they need. Once found they can review and refine their data set for just the data (and contextual attachments and conversation threads), even if it involves people outside your organization. OneVault makes it easy to find the proverbial 'needle in a haystack' within a mountain of communications data.

With the archive's advanced proprietary technology, internal teams can conduct highly complex and targeted searches across petabytes of Slack, Microsoft Teams, and other business data – obtaining results in a matter of seconds, not hours or days.

RECORDS TAGGING FOR CASE MANAGEMENT

OneVault provides a framework for personal and organization-wide tagging that enables users to efficiently:

- Collect and organize data relevant to ongoing or potential legal cases or significant projects for easy production later.
- Classify data with configurable case- specific tags to support review workflows.
- Share case data and activity for secure, collaborative review.
- Document actions performed on archived data in unalterable audit trails and logs.

LEGAL HOLD

Organizations must preserve potentially responsive data when they anticipate litigation. Failure to do so can result in hefty fines and a weaker defense.

With OneVault, organizations can be confident their legal hold process will endure legal scrutiny, and the retention architecture prevents claims of data spoliation.

OneVault automates the application and management of defensible legal holds on archived data. Doing so overrides corporate retention schedules, protecting and preserving the data until such time that it is no longer subject to a legal hold. Given how lengthy these retention periods can be, and the complexity of managing overlapping data sets, trying to manage this process manually is no longer possible with any defensibility.

ONEVAULT: BUILT FOR TODAY'S ENVIRONMENT

Many different and potentially overlapping legal holds can exist simultaneously within OneVault. The system manages each individual record through as many legal holds as it may be subject to until all are expired. At that time, the system will assess the original retention policy of the record and manage or dispose of it accordingly. This ensures that data is not only securely retained, but proper sanitation practices are applied cradle to grave.

DATA SECURITY & INTEGRITY

With OneVault, organizations do not have to worry about the security, integrity, and availability of their archived data. OneVault services are hosted in multiple data centers. The systems are fully redundant within each data center and can withstand failures without interruption.

All archived data is replicated in near-real time to the secondary data center – with multiple copies of the data preserved in geographically dispersed locations. If the primary data center is lost, services fail over to the secondary data center, which functions as the data recovery site.

Our default data location is within our geo-diverse data centers within the United States, but we also provide options for government organizations needing specialized data handling, and our cloud management does provide options to handle data sovereignty requirements often seen in certain areas of the world.

ALTERNATIVES: WHAT WORKS, WHAT FAILS

THE PROBLEM WITH (ONLY USING) BACKUPS

It is essential to acknowledge that **backups and archives are not interchangeable solutions.** While both are important best practices for any organization to follow, backups are designed for tactical, short-term preservation of content to restore servers after a crash or system fault; while archives are strategic tools designed to preserve information for long periods.

Backups constitute unprocessed content and lack any sort of indexing. Moreover, the integrity of backup media is not guaranteed, and because backups capture a snapshot of data, information generated and deleted between backups will not be captured. Searching through backups for e-Discovery purposes can be extremely expensive. For example, in the case of Radian Asset Assurance, Inc. v. College of the Christian Brothers of New Mexico, the defendant estimated that the cost to search through 50.5 backup tapes would be $420,315, or an average of $8,323 per tape.[4]

THE PROBLEM WITH SINGLE DATA ARCHIVE SOLUTIONS

Many organizations are currently running a single archive solution, namely email archiving. When email was the de-facto method of communicating and documenting the day-to-day conduct or any organization, this was adequate. However, with the rapid adoption of so many additional communication systems while regulations and legal procedures were updated to recognize the fact that **communications must be retained from many different applications in addition to email.**

An email archive was built to archive only email. While some have attempted to forward other record types (such as voicemail) into an email archive, the shortcomings of that strategy are both procedural and technical.

From a technical perspective, the email archive does not index the meta-data of the forwarded content, and therefore it is very difficult to properly index and find data when it is needed.

[4] Osterman Research: Key Issues for e-Discovery & Legal Compliance

ALTERNATIVES: WHAT WORKS, WHAT FAILS

From a procedural perspective, this **"forwarding" causes data spoliation**. This means that when such data is used in a legal scenario, the **data from such a Discovery can be thrown out because it does not have an adequate chain of custody proving it has remained in a tamper-proof state.** By pushing one data type into another, the security of each data type is permanently compromised for legal purposes.

THE PROBLEM WITH SUBSCRIPTION RETENTION

When faced with the problem of retaining information, some organizations opt to maintain the subscription for the software, even though it may not be in active use. **This is a costly option, maintaining unnecessary software licensing merely to have access to the communications and emails created by former employees** or that were created within the system prior to a migration to a different software solution. This is being commonly seen where organizations may have adopted Slack, Teams, Zoom and Webex without centralized decision making during the pandemic; but now want to standardize on a particular platform.

When faced with the challenge of how to maintain data in the prior platforms, some organizations choose to maintain software subscriptions indefinitely. This creates additional problems of searching data, data access management and data lifecycle management.

By maintaining the data within the subscription, it may be backed up, but it is not archived an indexed. Therefore e-Discovery is not properly functional and requires all searchers to have login access to the account. **Data security becomes porous and there is no way to track who has accessed or even groomed the data.** Data maintained in this manner could be deleted at any time by anyone with account access with no way of telling it had happened. Furthermore, if any of the accounts are subject to a litigation hold, the subscription may have to be maintained for an indefinite period, usually spanning years.

Lastly, there will be no automatic application of an organization's retention policy. When records reach the end of their lifecycle, it will be a manual process to remove them. It becomes very easy for data to be forgotten until it turns up in Discovery, or data can be accidentally purged before its time. Both can be significantly problematic and avoided with the use of an archiving platform like OneVault that can ingest data from inactive employees and software platforms and address each of the challenges outline here.

ALTERNATIVES: WHAT WORKS, WHAT FAILS

THE PROBLEM WITH DATA LAKES

A data lake is a repository that houses data in its original, raw form. Data inside data lakes can vary widely in size and structure, and in not indexed or organized. **Data lakes are not built to handle archiving, governance, and e-Discovery**. They are built to collect data points for data analytics and workflow analysis. If you add on governance and security, there is much more management complexity and in return the information governance features will still fall short of a compliance archive.

In reality, data lakes often fall short of delivering on their promises, for several reasons:

1. **Data lakes are very expensive to implement and maintain**. Although some data lake platforms, like Hadoop, are open source and free of cost if you build and manage them yourself, doing so often takes months and requires expert staff. Managed data lake platforms like those that run in the cloud may be easier to deploy, but they are still very difficult to manage -- and they come with steep fees.
2. **Data is being created at a pace faster than the technology improvements needed to adequately host and manage the data lake**. This means, businesses end up paying more and more for the compute resources and still fall short on their information governance needs.

THE PROBLEM WITH COLD STORAGE

Cold data is data that is only occasionally accessed occasionally or do not actively use. There are several reasons why cold data is retained. Some companies automatically keep everything, some do so for regulatory compliance reasons, and some do so because of corporate mandates.

Defining active vs. cold data varies from business to business. In one, data that goes 30 days without getting used might be considered cold. In another, data have to remain untouched for up to 6 months before it's considered cold.

While cold storage often appears attractive for its opportunity to reduce the cost of data retention, there are several problems that can create real problems for organizations needing to retain data for longer terms.

ALTERNATIVES: WHAT WORKS, WHAT FAILS

Lack of Data Indexing. Cold storage is a backup, once removed. The data is maintained in an unstructured and un-indexed state. Any e-Discovery within that data will be even more challenging because of the lack of tools to find and appropriately handle data sets.

Speed of Access. Cold storage companies work from the assumption that, if you access the data, the speed of access won't prove important.

Management Complexity. Defining "cold" data for each organization is different and it can be very cumbersome to apply consistent retention and destruction policies on differing data sets.

Supported Data Types. Most data management still overlooks the seismic shift to the intellectual property and institutional knowledge that are accumulated via email and collaboration systems. Even when files are being managed, there is a massive amount of organizational documentation that is still unmanaged and unprotected.

Less Reliable Hardware. The data is often stored on servers that use traditional hard drives that are cheaper but have a greater possibility of failure. While such failure may not be common, it is a known tradeoff for the cheap price. If data is important enough to retain for lengthy periods of time, having confidence in the integrity of the media (and therefore the ability to access the data) is important to assess.

Limited/Fee-Based Access. Accessing the data in cold storage more than a certain number of times or above a certain amount of data incurs additional fees. Those fees can quickly add up and surpass any cost savings.

"While the majority of data is considered cold data that is seldom if ever accessed after 30 days, it still needs to be managed according to security, compliance, and corporate mandate requirements, all of which inject complexity into the process."

- Tim Bramble, Leonovu

GOVERNANCE & BUSINESS CONTINUITY

DATA SECURITY & PROTECTION

The volume of corporate lawsuits continues to rise, and this means the amount of data you need to collect in response to e-Discovery requests is also growing. Consequently, there's a lot of gigabytes (or even terabytes!) of potentially responsive data to search for in just one lawsuit collection phase. Then, once you've found it, you've got to place it on litigation hold and review it before you produce it to your opposing counsel. That's a lot of info to have sitting around unprotected.

Very often, corporate legal departments resort to storing these massive datasets on a shared drive, without any additional security. This means you're relying on your existing enterprise security technology, which might not always be able to protect your data repository as well as it protects the rest of your systems.

We know that you and your teams care about security. We also know that deadlines are ever present and looming over you, which is probably why you continue to store huge amounts of e-Discovery data on file sharing systems. What you might not realize is that **this security risk is made even worse when you provide your attorneys easy access and data portability,** meaning they can work from their mobile phones and laptops when not in the office. Obviously, everybody loves flexible working, but **when sensitive data is stored on unsecure file sharing systems, there's a big risk** to it. In fact, many industry pundits suggest that corporate legal department file sharing systems have experienced the same intrusions as law firms themselves.

So, you've got department file shares that are unsecured and potentially unmanaged, and you're relying on simple password access, with no audit or reporting capability. Chances are that most cyber-criminals would be able to gain access through a weak firewall and easily copy your entire file share. You probably wouldn't even notice.

GOVERNANCE & BUSINESS CONTINUITY

It's that frightening. What's worse is that these criminals can then review everything they've stolen and attempt to sell it to anyone who's interested, or even ransom it back to you. In many cases, you're unlikely to even know your datasets have been accessed and copied.

We're not denying the need for you to store your e-Discovery data for long periods of time, but if there was a more secure way to do it while keeping your budget as low as possible, wouldn't you want to know about it?

BACKUP & ARCHIVING: A CASE FOR EACH

Most organizations must be able to prove they are retaining documentation of business operations for future purposes. This could be for knowledge transfer as well as legal needs. However, a traditional backup is not sufficient for legal, compliance and other contractual needs because it was never designed for finding specific records within the backup. Think of the example of a photograph. It captures a moment in time, but you cannot easily examine a specific pixel within that image.

Backups only capture a moment in time and will miss a lot of information; including changes that occur in between backups. They don't index the data and are not tamper-proof. Backups are designed to quickly restore entire servers after a failure or outage event. Backups were never designed for electronic searches. Trying to find specific files inside a backup is difficult. That difficulty makes it time consuming and expensive. Locating emails, instant messages and other electronic communications is almost impossible.

Another challenge with on-premises backups is that ransomware attacks don't just lock down the servers and end user devices. They also ensure that the local backup is blocked.

Archiving and backup are both critical components of a solid data protection strategy. Even your backup should have a cloud component. For example, our **FLxStore Veeam-powered Backup-as-a-Service** provides a supportive hybrid-cloud backup-as-a-service to OneVault. A local backup appliance provides speed, replication offsite to the cloud provides more security in the event of a ransomware attack.

GOVERNANCE & BUSINESS CONTINUITY

DATA REPLICATION & FAILOVER

While data backup has been the most widely adopted form of data protection, **the usefulness of a backup is only valid if the network infrastructure itself is undamaged and accessible.** After all, there needs to be somewhere the data can be restored that is sized, configured and available to run the restored applications and data.

In the increasingly common event of a compromise by ransomware, backups are part of the ransomed data set, and the entire infrastructure can be unusable. Therefore, a data protection strategy must plan for automatic replication of the backup data to multiple secure locations and make provision for alternate data center facilities if onsite hardware is not able to quickly resume services.

This can happen not only because of equipment failure, but also during a ransom event, insurance providers will restrict the network until their forensic experts are satisfied as to the cause and entry point of the ransom attack. When security event & incident management (SEIM) tools are configured on the network, it significantly reduces the amount of time to find the breach point. However, it is not uncommon for organizations to suffer extended outages while lawyers, forensic and SECOPS specialists from the insurer review the network, the breach, and the damage.

Having parallel access to data (such as OneVault provides in the cloud) and using a DR/Failover option like **Donoma's FLxDR Data Replication & Disaster Readiness** ensures that organizations have a tested failover solution in the event that systems are offline for an extended outage.

KEY TAKEAWAYS

Cloud-based collaboration and communication systems like Microsoft 365, Teams, Zoom and Webex are now widely adopted in today's disperse work environments to drive engagement, efficiency, and productivity. With their increased use comes a responsibility to manage the messages they create – data constituting valuable intellectual capital.

Another influential change in Information Governance, is the expansion of e-Discovery to virtually all types of electronic communications. While many firms today are still not yet archiving email – the most commonly discoverable electronic content in litigation – they will be still be expected to produce under e-Discovery a wide range of data types, including text messages, social media posts, files, data in collaboration tools, voicemails, and other information. In short, any electronic information that contains a business record, regardless of the tool that was used to create it or the venue in which it is stored, will potentially be subject to e-Discovery.[6]

Donoma OneVault's multi-data archiving and information governance solution is essential to any organization requiring business continuity, risk reduction, and audit / litigation-readiness.

1. IMPLEMENT ARCHIVING FOR E-DISCOVERY

Litigation is clearly more efficient if the right solutions are in place for e-Discovery and litigation hold. This begins with good archiving technology that will capture, index, and retain business records for the appropriate length of time, ensure that these records cannot be deleted or modified after the fact, and that will enable the archives to be searched quickly, efficiently and at scale. E-Discovery tools will help define content that is and is not available and make the entire process much more efficient. Surprisingly, many organizations still rely on backup tapes as their litigation "archive", a role that backups were never intended to fulfill and one at which they fail miserably.

[6] Osterman Research

KEY TAKEAWAYS

2. BECOME PROACTIVE, NOT REACTIVE

It is essential for decision makers to acknowledge the importance of archiving in the context of all the information it manages and to give it the appropriate priority for budgeting, staffing, and planning purposes. E-Discovery must be a high priority for all managers within an organization and should be a key consideration for employees who are charged with creating, storing, and managing information. As a growing proportion of business records become discoverable, decision makers will need to implement capabilities to capture this information for long-term retention and retrieval.

3. IMPLEMENT LITIGATION HOLDS PROPERLY

A properly configured e-Discovery and data archiving solution will enable organizations to immediately place a hold on data when requested by a court or regulator or on the advice of legal counsel, suspend deletion policies and practices, and retain it for as long as necessary. One element of the litigation hold process that is commonly missed, and that creates spoliation concerns, is not tracking employee movements and protecting data on litigation hold from being accidentally deleted when an employee departs, changes roles, or when computers are automatically wiped by IT.

QUESTIONS?
READY FOR NEXT STEPS?
CONTACT US.

When you are ready to take the next step in your compliance archiving and data protection solutions, contact us or visit us on the web to schedule a demo.

DONOMA

www.donomasoftware.com
hello@donomasoftware.com
866-265-2770
(540) 443-3560