

Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **May 2021**
Sponsored by **Zix**

Why You Must Archive All of Your Business Records

Executive Summary

Organizations generate large volumes of electronic data, most of it unstructured. Content-generating sources include email, text messaging, telephony, collaboration systems like Microsoft Teams and Zoom, desktop productivity applications, CRM systems, social media and a wide range of other tools and capabilities.

Much of the content generated by an organization constitutes some form of business record: invoices, policy statements, client files, communications with members of a supply chain, orders, prospect inquiries, employee records, and the like. Organizations are obligated to retain these business records for varying lengths of time and for a variety of reasons: regulatory obligations, legal requirements, or best practice considerations.

Retaining records can be accomplished with simple backup, but this is an inefficient method of records retention that is fraught with problems: it normally retains an incomplete set of business records, data can easily be deleted or modified, and searching for and producing data is difficult, time-consuming and risky.

Instead, organizations should deploy an archiving solution that will do the following:

- Index all of the relevant content that an organization generates as close to real time as possible.
- Place this content into archival storage where it cannot be deleted before it is permissible to do so, and where it cannot be modified either intentionally or accidentally.
- Enable robust search capabilities so that legal counsel, senior managers, individual users and others can search for content in support of a variety of purposes for which the data might be needed.
- Enable archived data to be managed in such a way that analytics tools can extract insight and intelligence from the data.

ABOUT THIS WHITE PAPER

This white paper, in conjunction with a primary market research survey that was conducted specifically for it, was sponsored by Zix; information about the company is provided at the end of this document. A complete report of the survey results will be published following publication of this white paper.

Is it Important to Archive Business Records?

WHAT GETS ARCHIVED TODAY?

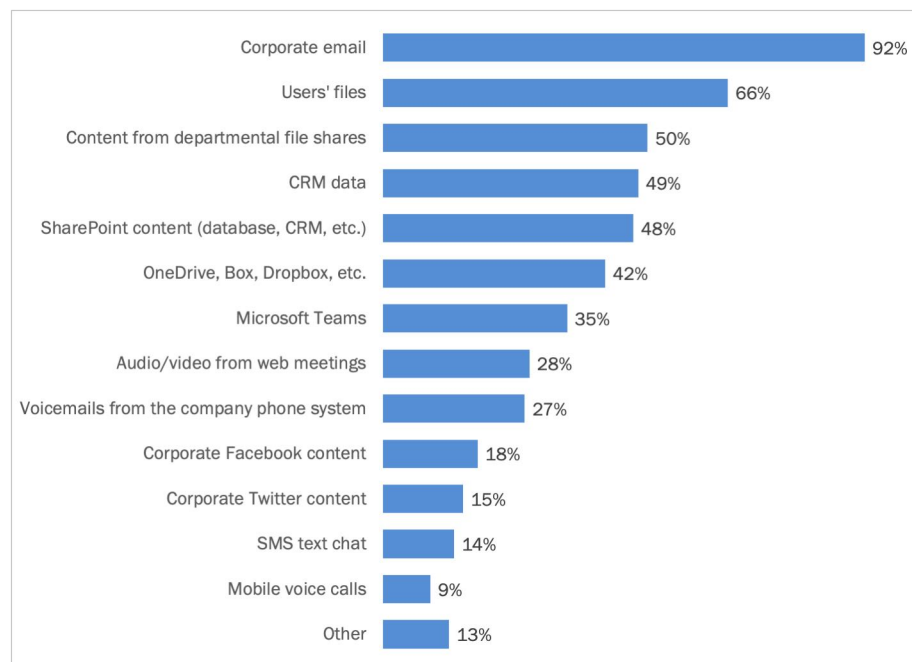
The vast majority of organizations are archiving corporate email, but significantly fewer are archiving other content types. Only two-thirds of organizations archive users' files, one-half archive content from departmental file shares, and slightly fewer archive their CRM data. See Figure 1.

The vast majority of organizations are archiving corporate email, but significantly fewer are archiving other content types.

Figure 1

Types of Electronic Content That are Archived

Percentage of Organizations



Source: Osterman Research (2021)

When asked about the types of content that they will archive by 2023 but that are not archiving today, 15% of decision makers responded that their organizations will be archiving content from Microsoft Teams, 12% will be archiving text messages, and 11% will be archiving files.

THERE ARE SEVERAL REASONS TO ARCHIVE CONTENT

The archiving of electronic content has been a best practice for many years despite the fact that many organizations still do not archive their content in a systematic, policy-based manner. While many organizations archive their content in response to strict regulatory obligations to do so, many more do so based on guidance from their legal counsel or their understanding about the benefits of retaining content for a variety of purposes.

A growing proportion of organizations are implementing information governance programs of which archiving is a key component. Information governance, in a nutshell, includes:

- Finding and properly classifying all of the information that exists across an organization.
- Determining what needs to be retained and for how long, and how best to store it. This includes the ability to “defensibly delete” information that is no longer required.
- Enabling appropriate access to information.
- Providing the ability to audit content for compliance purposes.

A growing proportion of organizations are implementing information governance programs of which archiving is a key component.

- Enabling robust search capabilities so that responsive data can be extracted for the right purposes, which can include regulatory compliance, legal discovery or analytics.

COMPLIANCE WITH PRIVACY REGULATIONS

While some industries, such as financial services and healthcare, are heavily regulated in the context of content retention, most organizations are now subject to compliance with a growing body of privacy regulations, such as the European Union's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). As a result, most organizations must now retain content in order to satisfy some of the key provisions that are contained within these regulations. For example, the CCPA includes a "Look Back" requirement that obligates companies with information on California residents to retain data for the previous 12 months so that it can provide these individuals with information on how their data was collected, used and shared. Under GDPR, organizations must establish a data retention policy to ensure that individuals' data is retained only for the appropriate length of time. Moreover, privacy regulations obligate data processors and controllers to produce a report of all of the information they have on individuals and, in most cases, to delete this information when asked to do so. Most other privacy regulations have similar provisions.

While the use of an archiving system per se is not specified in these regulations, there is no practical way to properly retain, produce and defensibly dispose of information in a satisfactory manner without the use of an archiving system that indexes content and enables robust search capabilities for archived content. As just one example, the GDPR includes a provision that enables individuals within the European Union to request of any organization the information it possesses on that individual – the so-called Subject Access Request (SAR). Without a properly configured and managed archiving solution, responding to an SAR is time-consuming and runs the risk of not being able to produce a complete set of the requested information.

COMPLIANCE WITH OTHER REGULATIONS

Various regulatory bodies impose data retention and production regulations on participants in specific industries, although some regulations cover virtually all industries. Given the nature of these regulations' requirements for retention and the ability to find relevant information quickly, an archiving capability is a key element in being able to satisfy them. Here are some examples of data retention regulations in the United States:

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA), obligates organizations to protect patients' electronic health records from unauthorized access and to retain these records for six years.
- Rules set forth by the Security and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) require broker-dealers, investment advisors and others to retain their transaction records, advertising, communications and other content for approximately six years, including the ability to recall and produce these records quickly when requested.
- A chemical manufacturer or processor must retain for five years any investigative reports about incidents in which the significant release of a regulated substance took place.

There is no practical way to properly retain, produce and defensibly dispose of information in a satisfactory manner without the use of an archiving system.

- The Federal Energy Regulatory Commission (FERC) requires the retention of records by energy and related companies for varying periods. For example, information on service contracts must be retained for four years, minutes of various corporate meetings must be retained for five years, and copies of the formal orders of regulatory commissions that have been served on natural gas companies must be retained for six years.
- The Equal Employment Opportunity Commission (EEOC) requires that employment records be retained for a minimum of one year, but for employees who are terminated involuntarily records must be retained for one year following their departure.
- Organizations that receive Federal Aviation Administration (FAA) Airport Improvement Program grants must retain a wide variety of documents – such as invoices, professional services contracts and purchase orders – for three years (or longer in some cases) following the date of final reimbursement.

Please note that these are but a few of the many thousands of data retention requirements that exist in the United States; other countries impose similar types of retention obligations for a wide variety of information types.

LEGAL REASONS

Every organization is subject to various legal obligations in the context of its business activities, whether they are contractual obligations or other legal requirements. Consequently, every organization must retain copies of its business records – and do so in manner that can demonstrate that the records are accurate and unmodified – in support of its potential role as a litigant in a legal proceeding.

The legal drivers for data archiving are somewhat less defined than those driven by regulatory obligations, but they are no less important. Legal drivers for retention and archiving are sometimes specified by statute, but often are based on legal precedent or advice from counsel. Among the legal reasons to archive data are the following:

- **Early case assessments**
An organization's management that suspects it might be the subject of a legal action can access its archived data to understand its position before legal action commences. For example, if management suspects a former employee might sue for wrongful termination, the archive can be accessed for all relevant information that might be relevant to the case. If the search of information reveals that the former employee has a strong case, the organization's legal counsel can pursue a quick settlement before the case can get to trial. Conversely, the archived data might prove that the employee's claims are groundless, offering senior management grounds for fighting the action.
- **Legal holds**
An organization that reasonably expects to be involved in litigation is legally obligated to place all relevant electronic content on legal hold so that this data will not be deleted until it is no longer necessary to retain. It is important to note that legal holds are required even if no formal legal action has been initiated. Implementing a legal hold without an archiving system is possible, but brings with it the risk of failing to retain all relevant evidence and incurring the consequences of not doing so, such as a charge of spoliation of evidence.

The legal drivers for data archiving are somewhat less defined than those driven by regulatory obligations, but they are no less important.

- **eDiscovery**

After a legal action commences, plaintiffs, defendants and third-parties may be required to produce relevant information in response to a court's order as it responds to each party's request for information from others. An organization so ordered to produce information must respond either with a complete set of the requested information or a satisfactory response as to why it cannot do so. In an era in which archiving capabilities are readily available, an organization that cannot produce the requested information runs the serious risk of sanctions or fines from the court or, in some cases, a pre-trial directed verdict or an adverse inference instruction at trial.

OTHER REASONS TO ARCHIVE

There are several other reasons that organizations should archive their electronic content:

- **Security**

Archiving can be an effective recovery mechanism if an organization is infected by ransomware, the victim of malicious or accidental destruction of data, or if data has been corrupted. While backups have been the traditional tool for protection against these potential causes of data loss, an archiving system has the key advantage of continual archival of data. For example, if the normal backup window is between 1:00am and 4:00am each day and an outgoing employee maliciously deletes data at 3:00pm, 11 hours of data will be lost if the previous night's backup must be used for recovery purposes. However, an archive of continually captured and indexed content will result in no or minimal data loss in this situation.

- **Self-service data recovery**

Eventually, most employees will find the need to search for old content that they have created: text documents, spreadsheets, presentations and the like. Moreover, new employees will often want to reference content generated by their predecessor in order to get up to speed in their new role. An archive is an important tool in enabling employees to find this information instead of spending time searching for or recreating it. An archiving solution that provides self-service not only increases employee productivity, it reduces the involvement of IT staff in helping to find this content. It is important to note that self-service data recovery is not a substitute for a backup solution, since both archiving and backup are important best practices.

- **Managing corporate knowledge**

Electronic content normally represents the bulk of an organizations' corporate knowledge. An archiving system enables the capture of the intellectual property and collective knowledge of an organization and enables senior managers, legal counsel, and others to search for and find relevant information when it's needed.

- **Storage management**

One of the primary benefits of an archiving solution used to be its ability to move data from "live", on-premises servers to less expensive archival storage. Because older data is accessed less frequently, it made sense to move this older data to an archive to reduce storage costs. However, in an era of 50- or 100-gigabyte mailboxes and other data repositories in the cloud, storage management is much less of a driver than it was in the past. However, even in

Archiving can be an effective recovery mechanism if an organization is infected by ransomware.

the cloud era, a key functional benefit of archiving is its ability to deduplicate and enable single-instance storage.

- **Extracting insight and intelligence from archived data**

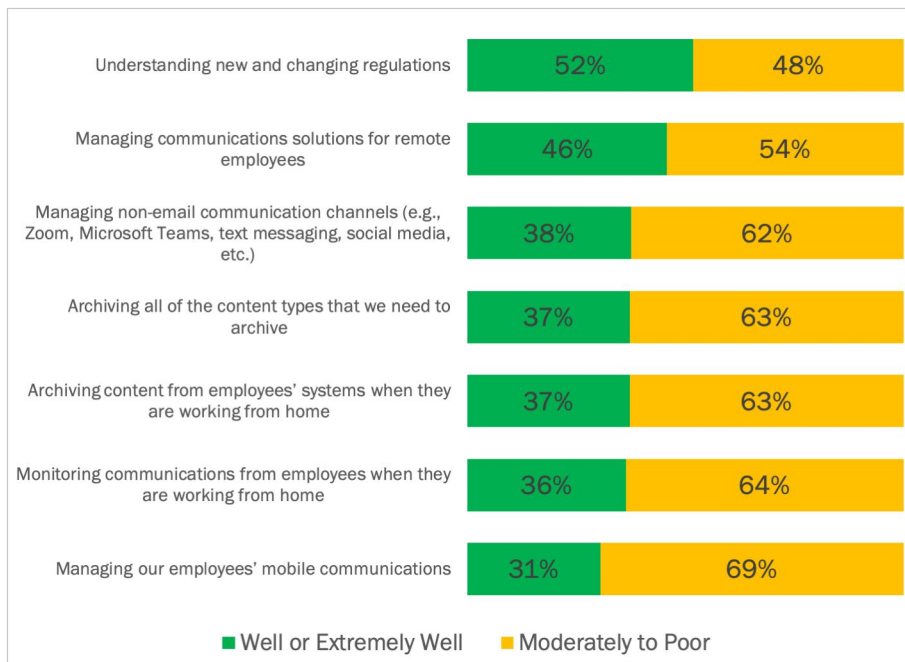
As will be discussed in the next section, an important benefit of archiving – and the fastest growing driver for deployment of archiving solutions – is the ability to extract insight and intelligence from archived data. More on that below.

MOST ORGANIZATIONS ARE FALLING SHORT

Clearly, organizations must archive their electronic content for a variety of reasons that vary by the industry(ies) they serve, their management's appetite for risk and other factors. However, the research conducted for this white paper discovered that most organizations are falling well short of what they consider to be best practice in the context of understanding regulations, archiving all of the content they need to archive, and managing communications outside of email. See Figure 2.

Figure 2

"How well is your organization meeting your corporate, regulatory, legal and other requirements for each of the following?"



Source: Osterman Research (2021)

What if analytics could be used on archived data and information could be gleaned from that data?

What Can You Do With Those Records?

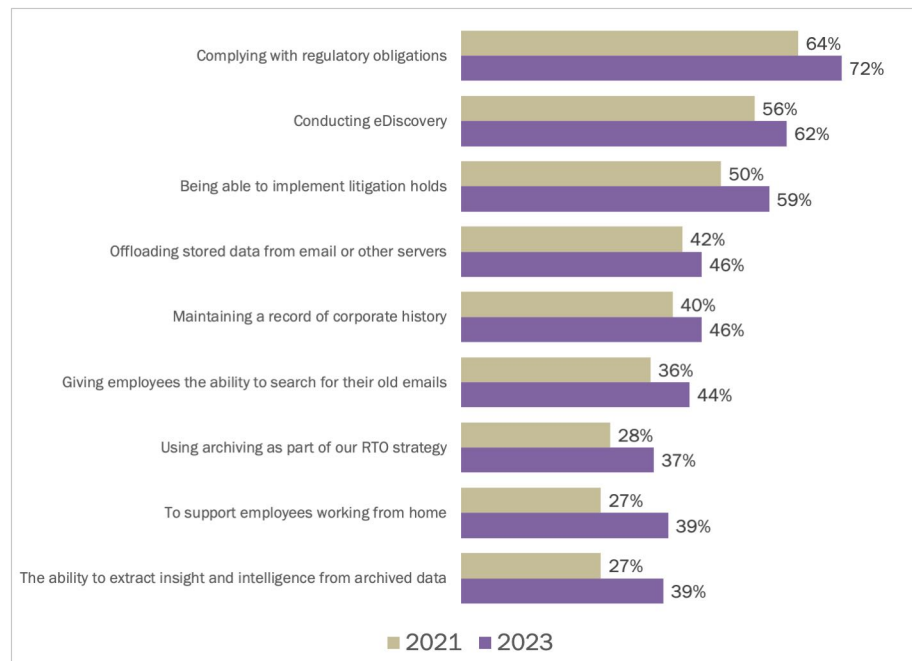
The most important role of an archiving solution has traditionally been defensive: retain business records so that if someone comes asking for them – a regulator, a court or an employee – the organization that has properly archived its content can easily and reliably respond to the request for information. That's a critically important reason for archiving electronic content and it will continue to be.

However, what if analytics could be used on archived data and information could be gleaned from that data so that it could be used for more than defensive purposes? What if data could be mined from archived data to gain insights, learn about undiscovered business processes, and discover if corporate HR, privacy and other

policies were really being followed? What if potential data breaches could be discovered before they occur?

All of the drivers for deploying an archiving solution – regulatory compliance, legal reasons, and the like – will continue to be important. But gathering insight and intelligence from archived data will be the fastest growing driver for deploying archiving solutions over the next couple of years, as shown in Figure 3.

Figure 3
Drivers for Archiving, 2021 and 2023
Percentage responding an important or major driver



Source: Osterman Research (2021)

WHAT DOES AN ARCHIVE CONTAIN?

An archive of electronic content contains business records and other information that an organization – or those requiring the organization to archive – deems important. As an example, let's consider what a well-managed email archive contains:

- The full text of all emails sent into, sent out of, and sent within an organization, including any attachments that they might contain. That includes emails that were sent and then deleted for whatever reason.
- A record of every email transaction, including every sender and recipient and when each email was sent and received.
- A record of if and when every incoming and outgoing email received a response.
- Whether or not sensitive or confidential information was sent via email and whether or not it was encrypted.

Gathering insight and intelligence from archived data will be the fastest growing driver for deploying archiving solutions over the next couple of years.

- A record of when employees are accessing the corporate email system and from where they are accessing it.
- A record of how employees are using the corporate email system: for business purposes and for personal reasons.
- In some cases, an archive will also provide a record of when employees use unapproved tools for conducting company business, such as when they use a personal email account to bypass the corporate security system or file-size limits. This can occur when a sender uses a personal email account, for example, and the recipient responds to the sender's corporate account.

Now, imagine that all of the generators of corporate content – things like email, SMS/text messaging, voicemail, Twitter, Facebook, file systems, collaboration tools like Teams and Zoom, chat tools, etc. – had their relevant content archived. And this archiving system enabled the search of content across data sources. This would enable a researcher, such as a paralegal, senior manager, or data analyst to understand how communications actually takes place in an organization. For example, a client might text his sales rep with a question about an upcoming renewal, she might respond via email, follow this up with a Zoom meeting, and then follow up with a contract sent from a Google Docs account. Archiving all of this information, and making it searchable from a single interface, enables researchers to better understand actual information flows within an organization and how people actually work.

SO, WHAT CAN YOU DO WITH LOTS OF ARCHIVED INFORMATION?

Once you have all of this archived information, what can you do with it? Here are some sample use cases, although there are far more such use cases possible than could be discussed in a paper of this type:

- **Detect policy violations**
If an employee uses her personal text messaging account or personal webmail to conduct corporate business, this could violate corporate policies and thereby create additional problems for an organization. These risks would include a potentially higher likelihood that content is not checked for malware, or sensitive content that is sent without encryption, thereby creating a regulatory or policy violation.
- **Find insider threats**
Disgruntled employees are more likely to steal data, commit sabotage, or cause other problems than their fellow workers who are happy with the company. This is particularly true for employees who are berated or otherwise treated badly by their supervisors. Searching an archive can reveal emails, social media posts, and text messages can not only help not to identify unhappy employees, but also their managers who are treating them badly. Understanding employee sentiment can go a long way toward addressing problems before they result in a data breach or worse.
- **Discover Code of Conduct violations**
A corporate Code of Conduct is a documented set of rules that sets out rules for appropriate employee behavior on a day-to-day basis. These behaviors might include fostering a safe work environment, refraining from corrupt business actions, not misusing company resources, and so forth. An archive can be used proactively to monitor for violations of the corporate Code of Conduct,

An archiving solution can be used to find disgruntled employees and search for patterns that might help ameliorate their concerns.

thereby enabling HR to provide confidence internally that the company treats good employee conduct and inclusive culture as top boardroom priorities. Moreover, using the archive in this way can encourage employees to want to report incidents because they will know that the organization can work to provide them with defensible information.

- **Find disgruntled employees**

Closely related to the point above is that an archiving solution can be used to find disgruntled employees and search for patterns that might help ameliorate their concerns. For example, archived data might reveal that employees who are not happy with their employer might be focused on a particular company policy, manager, or client.

- **Better manage customer relationships**

Customer relationship management (CRM) systems are important in managing the sales and client management process in most organizations, but they do not provide a complete picture of these processes. Using archived data, researchers can better understand these processes and use this information to improve them. For example, an examination of prospects' inquiries delivered via email might reveal that the length of time between an inquiry and a salesperson's response is inversely related to the likelihood of a sale – i.e., the shorter the period between the inquiry and a response the higher the likelihood that the prospect becomes a customer. Such an analysis might reveal that a voice call or voicemail responded to with an email is less likely to result in a sale than if a prospect's call is returned with a voice call.

- **Analyze use of profanity**

Some research has shown that using profanity in the workplace can reduce stress and improve employee moraleⁱ. Other research has found that the use of profanity at work can have serious consequences, such as losing out on promotionsⁱⁱ, losing a jobⁱⁱⁱ or claims of sexual harassment^{iv}. Wherever one stands on this issue, the use of archived data can help managers to understand who in their organization is using profanity and with whom, and it can help to identify the potential consequences of doing so. For example, an analysis of archived data might reveal that managers who use profanity in email or text messages have a higher level of turnover among their female employees, or it might reveal that employee morale is lower among male employees who are subject to it.

- **Deal with inappropriate messages**

Analyzing archived data can reveal not only profanity, but also racist or sexually offensive jokes, memes and other content that are sent via email, social media, text messages, etc. This kind of content can create significant problems for organizations that do nothing to stop them. For example, a management company for an adult community in Delaware was sued for racial discrimination because a resident of one of their properties sent offensive jokes via email^v. The former police chief and government of St. Charles County, Missouri are being sued by two female employees for sexually harassing text messages that were sent to them by the chief^{vi}. Using analytics to search for this kind of content allows organizations to deal appropriately and promptly with employees who send it.

- **Understand how employees communicate**

A good archiving solution that retains all of the content and communications

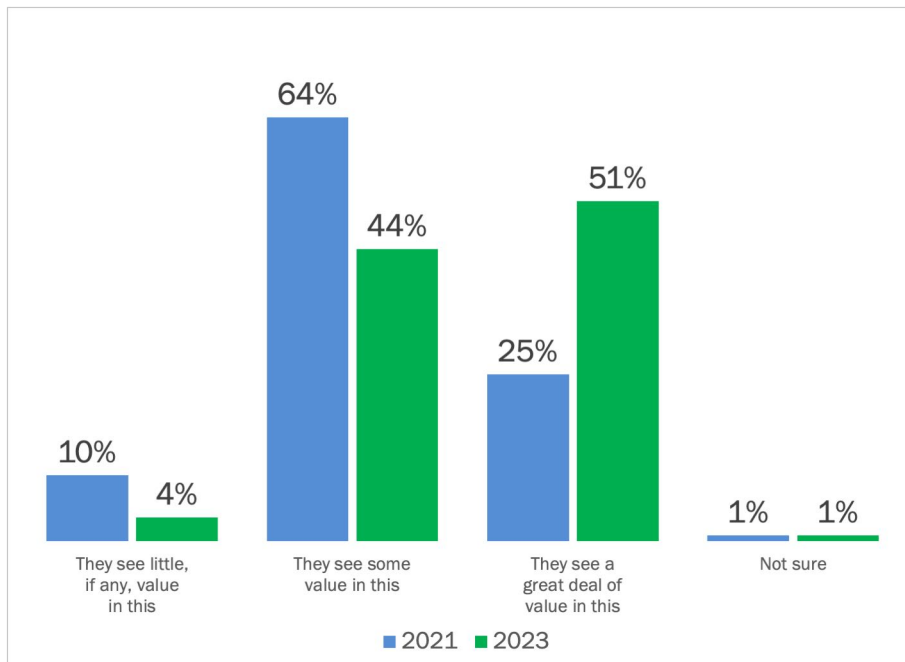
Analyzing archived data can reveal not only profanity, but also racist or sexually offensive jokes, memes and other content.

from employees is useful in helping to identify and track how communications really takes place within an organization. For example, a sales rep may send a text message to a client to request a meeting, then send an invitation for a Microsoft Teams call, and then send an attachment using their personal webmail account when working from home. Archiving all of these channels will capture all of the messages in context and help decision makers to understand how their employees actually communicate.

GROWING INTEREST IN ANALYTICS

The research conducted for this white paper found that there is growing interest in the application of analytics to extract insight and intelligence from archived data. When asked the extent to which senior business decision makers in the organizations surveyed see value in using analytics to extract data from their electronic archives, only 25% feel their senior managers see “a great deal value” in this practice today. However, they anticipate this will increase to 51% by 2023. See Figure 4.

Figure 4
Perceived Value From Being Able to Perform Analytics on Archived Data
 Percentage of Senior Business Decision Maker



Source: Osterman Research (2021)

There are several problems to address in archiving and information governance.

Finding the Right Archiving Solution

Some archiving solutions, particularly those focused solely on email archiving, were designed with an emphasis on storage management and retaining email primarily for defensive purposes – namely, regulatory and legal compliance. Storage management was more relevant when email inboxes were limited in size, but more modern solutions like Microsoft 365 offer practically unlimited email inboxes and so that issue is not as critical as it once was. Similarly, while archiving for regulatory and legal compliance continue to be critical best practices, they are no longer the only considerations in the choice of an email archiving solution.

Organizations that are choosing an archiving solution should continue to focus on key drivers like regulatory and legal compliance when evaluating their options. But they also must focus on other issues, such as new content types that their organization is using and will be using over the next several years, how these content types will be archived, the speed with which searches can be performed, how analytics can be used to search for content, and so forth. Moreover, decision makers need to evaluate specific features and capabilities of these archiving solutions, such as their ability to archive content like emojis that might be used in social media or in collaboration tools.

DEALING WITH PROBLEMATIC ISSUES

There are several problems to address in archiving and information governance. For example, information is increasingly distributed and disconnected because of the large number of tools used to create, send and store it. This makes it difficult to search across siloes and synthesize this data when conducting search or performing analytics on the data. Those who are trying to make sense of information must visit multiple data siloes individually, learn a different interface for each one, and extract what they need. In many cases, data just cannot be shared between siloes.

Moreover, the increase in the number of corporate applications that are in use, especially those in the cloud, and IT's acceptance of (acquiescence to?) the "Bring Your Own" phenomenon, means that information governance is now more fragmented and distributed. This is particularly true after the experience of 2020 in which most information workers were forced to work from home. These issues make formalized data access more difficult. Even simple data queries, such as when employees look for old files, are more difficult if an organization is storing a variety of data types in various, standalone siloes. Decision makers either cannot find what they want, or they resort to recreating what they cannot find.

Complicating things still further is that many archiving solutions were not designed with analytics in mind. While they were designed for indexing, storing and searching for information, they were not designed to be analytics tools to help decision makers gain a deep understanding of what their archives really contain.

Some Recommendations

Osterman Research offers the following recommendations as organizations pursue their archiving and information governance strategies.

ARCHIVE YOUR BUSINESS RECORDS

Many organizations do not archive their business records, even for defensive purposes like legal actions or regulatory obligations, but they should do so. Some organizations have an archiving policy, but often this involves just letting users decide what to archive and what to discard. Instead, decision makers should identify all of the stakeholders within an organization and develop a comprehensive data retention and archiving plan that will satisfy the needs of all stakeholders, whatever statutes might apply, and the anticipated long-term needs of the organization.

FOCUS ON THE FUTURE

Organizational decision makers should understand the value of the information that their organization has available to them if they archive their data and use the right analytics tools for extracting data from their data. The information stored in an archive can reveal valuable insights about the organization that are not available

Establishing a good information governance program is an essential best practice for any organization.

elsewhere. Plus, given that few organizations today have taken this next-generation approach to archiving, early adopters will gain significant competitive advantage by understanding their business more thoroughly than their competitors understand their business.

FOCUS ON INFORMATION GOVERNANCE

Establishing a good information governance program is an essential best practice for any organization. Decision makers need to understand what data they have, where it is located, how they can access it and gain control of it, and then manage it across its entire lifecycle. Proper information governance can offer significant benefits in reducing corporate risk, reducing compliance costs, reducing storage costs, improving employee productivity, and reducing overall risk. The return-on-investment associated with good information governance is significant for most organizations and should be considered as high a priority as possible. Because archiving is a key element of any organization's information governance program, the choice of an archiving solution needs to be made along with other information governance decisions.

DEPLOY THE RIGHT TECHNOLOGIES

It's important to deploy the right archiving solution. Decision makers should focus on:

- The archiving solution's ability to archive all current data types and those that reasonably can be anticipated will be used over the next several years. That means email at a bare minimum, but also data from text messages, collaboration solutions, voicemail, social media, and the like.
- The ability to archive non-email content in its native format, not merely as snippets of text that might be stored in an email archive, for example. Stripping the context and metadata out of non-email content diminishes its value for analytics purposes.
- Scalability, since large volumes of data must be searched as quickly as possible, both for traditional purposes like searches in support of a legal action or regulatory audit and for analytics purposes. Some archiving solutions are not well-suited to high-performance search or dealing with very large volumes of data.
- The ability to manage data residency, since some cloud solutions do not enable customers to determine where their data will be stored.
- Finally, decision makers need to understand that not all archiving solutions are suitable to their requirements. For example, many organizations rely on Microsoft's native archiving technology within Microsoft 365 to address their archiving requirements. While Microsoft offers many useful archiving features and functions within the platform, there are requirements that it does not satisfy and for which third-party solutions are superior.

Decision makers need to understand that not all archiving solutions are suitable to their requirements.

Summary

Archiving of electronic content is an essential best practice for virtually every organization. While the traditional drivers for archiving will continue to be important – regulatory and legal compliance being chief among them – other drivers are also becoming important. These include the ability to enable employee

self-service to archived content, as well as the ability to extract meaningful data from archives so that insights and intelligence can be gleaned. In choosing an archiving solution, decision makers must consider all of the sources that will generate business records and choose the archiving solution that will best meet all of their requirements.

Sponsor of This White Paper

To better meet your company's security, data protection and compliance needs, Zix can enhance your Office 365 environment with advanced threat protection, archiving and email encryption. Zix delivers a superior experience and easy-to-use solutions that have earned the trust of more than 19,000 organizations including the nation's most influential institutions in healthcare, finance and government.

To defend your company from malware, ransomware, phishing and other email threats, ZixProtect combines a multi-layer email security approach with automated traffic analysis, machine learning and real-time threat analysts. In addition, ZixProtect's business continuity feature ensures that your organization can continue to communicate if your email experiences a disruption.

ZixArchive eases email archiving and eDiscovery with automatic email collection and storage in a secure cloud. Its automatic indexing and multiple search criteria gives you and your employees convenient and rapid access to archived emails. ZixArchive also enables you to share an email hold with outside legal counsel and auditors and revoke privileges when access is no longer needed, keeping your data within your control.

To ease email encryption for you, your employees and your recipients, leverage the industry's leading solution ZixEncrypt. Automatic transparent delivery between customers and robust delivery methods for other recipients enables easy access to encrypted email for anyone, anywhere and on any device, making the user experience exceptional and compliance simpler. Proven policies and advanced reporting provide peace of mind, while customizable branding and security capabilities make email encryption fit your unique company needs.

Leveraging our more than 15 years of hosted experience, you can have confidence that Zix email security solutions integrate seamlessly with Office 365. You also benefit from the support of the ZixData Center, a state-of-the-art facility with PCI DSS 3.2 certification, SOC2 accreditation and SOC3 certification. Staffed 24/7/365, ZixData Center has a track record of consistent 99.999% availability. In addition, Zix delivers exceptional customer support 24/7/365 no matter your questions or concerns.

With reliability, experience and superior support, Zix improves email security for your Office 365 environment. To learn more about our solutions for Office 365, visit www.zixcorp.com/office365.



www.zixcorp.com

[@ZixCorp](https://twitter.com/ZixCorp)

+1 866 257 4949

sales@zixcorp.com

© 2021 Osterman Research. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, nor may it be resold or distributed by any entity other than Osterman Research, without prior written authorization of Osterman Research.

Osterman Research does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

- ⁱ <https://www.emerald.com/insight/content/doi/10.1108/01437730710780958/full/html>
- ⁱⁱ <https://oregonbusinessreport.com/2012/08/survey-examines-profanity-at-the-workplace/>
- ⁱⁱⁱ <https://www.shrm.org/resourcesandtools/hr-topics/employee-relations/pages/profanity-at-work.aspx>
- ^{iv} <https://www.akinlaws.com/practice-areas/sexual-harassment/hostile-work-environment-sexual-harassment/curses-vulgar-and-offensive-language-hostile-work-environment/>
- ^v <https://www.delawareonline.com/story/news/local/2015/01/25/racial-joke-email-focus-lawsuit/22320135/>
- ^{vi} <https://www.msn.com/en-us/news/us/i-see-breasts-in-your-future-among-text-messages-cited-in-sexual-harassment-lawsuit-against-former-st-charles-county-police-chief/ar-BB19mjeC>