

Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **July 2019**
Sponsored by **TeleMessage**

Why Archiving All Electronic Content is Critical

Executive Summary

Electronic content archiving – the process of capturing, indexing and placing data into long-term storage for later search and retrieval – has been a best practice for many years, particularly in industries that are more heavily regulated, such as financial services, energy, life sciences, healthcare and government.

The primary role of archiving has traditionally mostly about defense, such as retaining copies of business records and other important documents that might be needed as part of a legal action, or to have the ability to respond to a regulator’s request for information. However, archived data in email, text messages, social media posts, files and other content contains a wealth of information about an organization that is rarely, if ever, available from other sources. For example, a properly managed, next-generation archive that combines data capture with good analytics can be used for a variety of proactive purposes:

- It can show how quickly salespeople respond to inquiries from prospects and customers and if there is a relationship between the speed of response and the likelihood of orders or renewals.
- It can help to gauge customer sentiment and provide indicators of problems before they have a chance to manifest themselves as a problem, such as a customer switching to a competitor.
- It can determine which employees are being treated poorly by their managers and so are more likely to commit fraud or a breach of data.
- It can determine how information actually flows in an organization that might be at odds with the way that things are supposed to happen.
- It can find communications that are sexually harassing, racially insensitive or indicative of other types of employee misbehavior.

In short, an archiving solution can be used for both defensive purposes and as a proactive tool to glean insight and intelligence about an organization’s operations, and to detect problems before they turn into big problems.

It’s important to note, however, that realizing the benefits of next-generation archiving requires the use of an archiving solution, whether on-premises or in the cloud, that captures all of an organization’s relevant business records in email, files, text messages, social media platforms, collaboration platforms, mobile devices, voicemails and anywhere else these records might be found. It requires the establishment of good information policies, processes and practices. It requires a highly scalable archiving solution that includes robust analytics to enable the extraction of insight and intelligence from the archived data.

ABOUT THIS WHITE PAPER

This white paper was sponsored by TeleMessage; information about the company is provided at the end of this paper.

Why Organizations Should Archive Electronic Content

ARCHIVING AS A GOOD DEFENSE

Archiving’s traditional role mostly been defensive: organizations need to retain business records in the event they are requested by a regulator in support of an audit, by a court in the case of an eDiscovery order, or by senior management or

An archiving solution can be used for both defensive purposes and as a proactive tool to glean insight and intelligence about an organization’s operations.

legal counsel for early case assessments, among other reasons. We discuss these below.

REGULATORY COMPLIANCE

A significant proportion of the electronic records related to an organization's activities are subject to a number of regulatory compliance obligations, particularly in highly regulated organizations like financial services, healthcare, energy and life sciences. It's important for decision makers to understand that almost every organization and industry faces some level of regulatory compliance obligation to retain records, and that these obligations are not limited just to specific types of organizations or industries. For example:

- In the United States, various rules from the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) obligate members of national securities exchanges, brokers and dealers to retain securities transaction records for approximately six years. In Canada, the records of securities purchase and sell orders must be retained for seven years according as required by the Investment Industry Regulatory Organization of Canada. In the United Kingdom, investment service and transaction records must be retained for at least five years as required by the Financial Conduct Authority. The European Union has similar requirements under the Markets in Financial Instruments Directive. A failure to comply with these obligations can result in sanctions, fines and various other penalties.
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA), requires organizations to protect patients' electronic health records from unauthorized users and to retain this information for six years. Non-compliance with HIPAA requirements can result in fines of up to \$50,000 per violation, or criminal penalties of \$250,000 and up to 10 years in prison for the most serious violations.
- Organizations in the chemicals industry must retain investigation reports for five years about incidents in which a catastrophic release of a regulated substance occurred or might have occurred.
- Oil and gas companies that do commodity trading and insurance companies that sell life insurance through brokers are regulated under the financial industry regulations, such as those from FINRA and the SEC.
- Facilities and entities that store and move various types of nuclear materials must retain records for three years about authorized individuals, visitors, vendors and others; routine security tours and inspections; alarm events; shipments; procedures and other information.
- Manufacturers or importers of charcoal lighter materials must maintain records of charcoal lighter material compliance test information for five years.
- Any air transportation company offering passenger services operating to, from or within the United States with at least one aircraft that has 30 or more seats must maintain records for two years about tarmac delays that last more than three hours, including the length of the delay, the reason for the delay, the actions taken to minimize hardships for passengers, the disposition of the delayed flight, and an explanation for any delay in excess of three hours.

PRIVACY REGULATIONS

Privacy regulations are becoming the norm worldwide. The European Union's General Data Protection Regulation (GDPR) is the most significant of these regulations, but others have been implemented or will be soon in California, Colorado, Australia, Brazil, Japan and many other nations.

Almost every organization and industry faces some level of regulatory compliance obligation to retain records.

Here's why archiving is an essential component in maintaining compliance with privacy regulations:

- Article 30 of the GDPR obligates data controllers to maintain records of their data processing activities, with a list of specific information to be retained for each record. A good archiving solution is essential to ensure that all such records are captured and later accessible.
- The GDPR's Article 15 enables data subjects to ask any entity that possesses or processes his or her personal data to produce their data on demand. Without an archiving solution that enables a search across all of the information that a data controller controls or processes, compliance with this kind of request would be very time-consuming, if even possible.
- The California Consumer Privacy Act (CCPA) includes a "look back" provision that requires data holders on California residents to be able to produce data going back one year. That means that even though the CCPA goes into effect on January 1, 2020, the look back requirement went into effect on January 1, 2019.
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) requires holders of personal information to provide complete details of any personal information they hold if an individual requests it, typically within 30 days.

LEGAL CONSIDERATIONS

All organizations are subject to various legal and contractual obligations. Consequently, they must retain various types of electronic content in case this content is needed to support their role as a plaintiff, defendant or third-party participant in a legal proceeding.

The requirement to retain and manage data is imposed by statutes (specifically defining the retention and production obligations for certain types of data), legal precedent (courts will establish standards for the length of time that data must be retained), and internal best practices. Moreover, organizations that reasonably expect upcoming litigation must place relevant electronic content on legal hold that may be different from their standard policies. An archiving solution can facilitate that process in a way that traditional backup solutions cannot.

Managing eDiscovery capabilities using a robust archiving solution is a much better practice than relying on backups to do so. Information is easier and faster to find, the data set that is captured is more complete (which reduces the risk of problems like spoliation), and it's normally much less expensive because less work is required to assemble and produce the data. Plus, having an archive with proper eDiscovery functionality also helps organizations to bring a big chunk of eDiscovery back in house and allows them much faster early case assessment, especially around smaller cases.

ARCHIVING AS A SECURITY TOOL

The primary defense against ransomware, malicious or accidental destruction of data, corrupted data, and the like has traditionally been backups. A good backup will enable administrators to restore data back to a server or workstation to the last known good state before the problem occurred. The problem with a backup, however, is that a significant proportion of work can be lost if the data loss does not occur immediately after the backup. For example, if a backup ends at 4:00am and a ransomware infection renders data unavailable at 4:00pm later that day, 12 hours' worth of email, files and other content can be lost. An archiving solution that continually captures, indexes and places content into archival storage is a better option for data protection and more complete recovery of data.

An archiving solution that continually captures, indexes and places content into archival storage is a better option for data protection and more complete recovery of data.

END-USER SELF SERVICE

Most employees will need to search for old documents, spreadsheet, presentations and the like in the normal process of doing their work; and new employees will often want to refer to communications and other content generated by their predecessor. An archive is an essential tool in enabling employees to search rapidly for and find this information instead of spending inordinate amounts of time searching for it, or worse, recreating it. Good archiving enables enhanced user productivity by allowing employees and others to spend less time looking for content.

STORAGE MANAGEMENT

Although not nearly as important today as it was when storage was much more expensive, one of the benefits of an archiving solution is its ability to improve system performance by reducing the amount of active data that must be stored. Older data is still necessary to retain – sometimes for many years – but as it ages it is used less frequently, and so does not need to be maintained on active servers. Moving this data to an archive will improve system performance, and will also speed the process of backing up and restoring servers and workstations after system problems. Another important benefit of archiving in the context of storage management is the ability to deduplicate and provide single-instance storage, which offers the potential to dramatically reduce storage requirements.

KNOWLEDGE MANAGEMENT

Emails, files, text messages and other electronic content normally constitute the core of an organization's corporate knowledge base – some have suggested that the bulk of an organization's intellectual property is housed in its communications systems. The ability to retain and easily find this information is essential to maintain an organization's critical data assets.

Extracting Insight and Intelligence From Your Archives

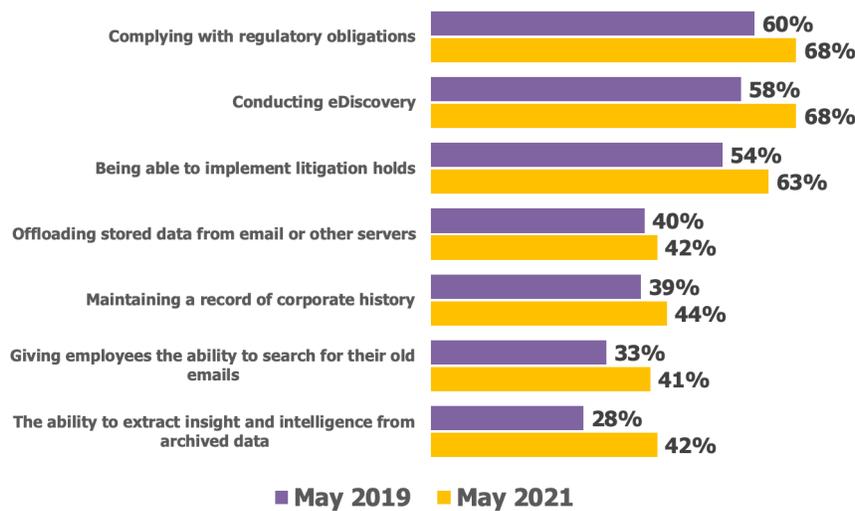
As noted earlier, the primary role of an archiving solution has been mostly defensive in nature: keep records in the event they are needed as a defense for a court order, a regulatory audit, or to determine early on if an organization is liable in a potential lawsuit.

But what if organizations retained data not only to defend themselves, but to take a more proactive approach and glean insights and intelligence about their organization? What if they performed analytics on their data to understand the timeliness with which they respond to customer inquiries and how this translates to sales? Or if certain types of employee behavior correlate with a greater likelihood of data theft? Or if employee sentiment could be better understood so that problems could be addressed before they get out of hand? Or if monitoring of ethics and internal compliance rules, such as HR policies, could lead to catching violators early on and thereby avoiding bigger problems later?

As shown in Figure 1, all of the drivers for deploying an archiving solution will become more important over the next two years, but the ability to extract insight and intelligence from archived data – while today the least important reason for an archiving solution – is the fastest growing.

What if organizations retained data not only to defend themselves, but to take a more proactive approach and glean insights and intelligence about their organization?

Figure 1
Drivers for Deploying an Archiving Solution, 2019 and 2021
 Percentage of Respondents Indicating a “Driver” or “Major Driver”



Source: Osterman Research, Inc.

Our research found that additional information types will be archived in the future. We asked survey respondents about the types of electronic content that they are not archiving today, but will be archiving in two years. The most commonly mentioned content that will be added to the mix of archived content will be corporate social media posts (mentioned by 20 percent of respondents), text messages/SMS (19 percent), and content from mobile devices. It’s important to note that non-email content, which typically is not archived today, already should be archived. For example, a recent case involving the estate of the deceased entertainer Prince included spoliation sanctions for the defendants’ failure to preserve text messages relevant to the caseⁱ. It’s important to note that some entities, such as FINRA, do not distinguish between content types, but are instead focused on business records, regardless of the system that created them.

THE KEY ELEMENTS OF AN ARCHIVE

Email archiving is the most common approach to archiving and one that many organizations will address first given the importance of email to their operations. While an archive of electronic content, including email, contains indexed content, it also contains a wealth of other information that can be mined for insight. For example, a properly managed email archive contains:

- A time-stamped copy of every communication and attachment sent by everyone with access to the corporate email system, including the senders and recipients of these emails.
- Full audit reports showing who has access what information, when they accessed it, etc.
- The wording and tone of every email that has been sent and received.
- A record of how quickly recipients respond to emails that call for some kind of response, such as a customer or prospect inquiry.
- Whether or not sensitive or confidential information was sent encrypted in compliance with corporate policies.
- A record of when employees are conducting company business.

An archiving solution that retains all relevant data types...can be used to gain even more insight about how the organization runs.

- A record of employees or contractors using corporate email resources for personal uses.
- Employees' commentaries on clients, prospects, business partners, fellow employees, their managers, senior corporate leadership and others; including employees' use of profanity, racially or sexually offensive content, and potential instances of fraud.

An archiving solution that retains all relevant data types, such as text messages, tweets, Facebook posts, instant messages, content from collaboration systems, and other data can be used to gain even more insight about how the organization runs.

AN ARCHIVE CAN YIELD ENORMOUS BENEFITS

A properly configured, scaled and managed archiving solution can yield tremendous benefits when used solely for defensive purposes by allowing timely response to legal inquiries, regulators' requests for information, and the like. However, the proactive ability to conduct in-depth investigations is also enabled by use of a robust archiving solution. These investigations require gaining understanding of what took place and when. Because individuals often do not have a clear recollection of what took place or what might have been said, having access to archived email, text messages, voicemail messages, instant messages and other content provides clear evidence of what was said. Consider the following, proactive applications for an archiving solution:

- **The ability to find possible insider threats**
Managers who criticize and ridicule their employees are more likely to create fertile ground for data breaches among those whom they manage, since disgruntled employees are more likely to steal data, send sensitive information to competitors, and the like. Analyzing archived content can help to highlight these managers and address their abusive behavior before employees reach the point of wrongdoing.
- **Managing customer relationships**
While CRM systems are useful, they don't provide a complete picture of the sales and prospecting process in most organizations. Analyzing prospect and customer inquiries, their tone, the time it takes for them to receive a response, the tone of those responses, and so forth, can yield valuable insight. For example, decision makers could find a correlation between the length of time it takes to respond to a customer inquiry and renewal rates for those customers. They could find that customers report different types of problems via email than they do using text messaging, necessitating a different type of response depending on their customers' choice of communications channel. They might find useful differences in their sales staff performance that wouldn't show up by analyzing CRM data.
- **Analyzing the use of profanity can yield important insights**
Employees' use of profanity can create problems for an organization. In the case of *Griffin v. City of Portland*ⁱ, for example, an employee filed a hostile workplace claim against her employer for fellow employees' use of profanity. IBM has found that traders in the United States who reduce their use of profanity may be guilty of nefarious activity, while just the opposite is true in the UKⁱⁱⁱ. Applying good analytics to archived emails, text messages, social media posts and the like can help decision makers to understand changes in employee behavior and to find employees who create more risk for an organization.
- **The ability to detect policy violations**
If an employee uses personal webmail to conduct company business, this can violate corporate policies and can create additional security risks because corporate archiving, security and encryption capabilities are being bypassed.
- **The ability to detect employee sentiment and behavior**
Good archiving and analytics can help to identify problems so that violations of

Good archiving and analytics can help to identify problems so that violations...can be addressed proactively before they result in a more serious problem.

the law, corporate policy, or industry best practice can be addressed proactively before they result in a more serious problem. For example, a compliance officer can use the corporate archiving system to search for evidence of illegal music downloads, sharing of racist or sexist jokes, employee complaints, or angry employees, so that these situations can be dealt with as quickly as possible.

- **Dealing with inappropriate messages**

Some employees will use email, text messaging and other communication channels inappropriately, while others will falsely claim harm. For example:

- In the case of *Enriquez v. U.S. Cellular Corp.*^{iv}, an employee filed a sexual harassment lawsuit based on what she claimed were inappropriate text messages from her supervisor. However, the employer's archive of text messages demonstrated that the plaintiff had actually forwarded the messages along with her claim that she did not find the messages to be offensive.
- An employee of a car dealership posted disparaging comments on Facebook about an event held by his employer and was fired. However, the National Labor Relations Board found that the firing was illegal because the comments were considered protected speech^v.
- An employee of UBS was fired after years of being sexually harassed by her manager via email, phone calls and personal comments. She sued her former employer and won \$8.4 million in damages^{vi}.

In each of these situations, analyzing archived content could have revealed the problems early on, potentially helping the employers to address the problems before they were allowed to continue.

- **Understanding how employees and others really communicate**

A properly configured and managed archiving solution that retains email, social media, text messaging and other communications is useful in identifying and tracking how communications actually take place. For example, a field salesperson may send a text message to a client asking for a meeting, follow it up with an email with the meeting details, and then send an attachment using personal webmail 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.

Corporate data is often locked away in content siloes.

Many Solutions Were Not Designed for the Next Generation of Archiving

Early generation archiving solutions – most of which focused on email archiving – were designed with an emphasis on a) managing mailbox size and b) retaining email primarily for regulatory and legal purposes. Because mailbox size was limited to only tens or hundreds of megabytes, early archiving solutions were focused on removing email and attachments that were consuming storage, replacing them with a small “pointer” or “stub” to the archive. This enables users to keep months’ worth of email in their inbox while allowing email administrators to keep mailbox sizes small.

Modern email solutions developed in an era of cheap storage, such as Office 365, support multi-gigabyte mailboxes, which can hold orders of magnitude more data than their earlier counterparts. As a result, mailbox size management is much less of a driver for email archiving than it used to be and its importance in the context of archiving will continue to decline. That doesn't mean that users no longer need archiving to address their mailbox management, since some users continue to run into limitations, but the ability to store enormous quantities of data in a mailbox

negates much of the advantage of archiving this content solely for storage management purposes.

Moreover, some believe that in an era of Office 365 and other cloud-based applications, on-premises archives should be replaced with cloud-based archiving solutions. On-premises archiving solutions can be more difficult to maintain and update, and much of the innovation occurring in the archiving space is taking place in the cloud.

PROBLEMS IN INFORMATION MANAGEMENT

Included among the problems with many legacy archiving solutions – and information management in general – are the following issues:

- **Data is locked away in siloes**
Corporate data is often locked away in content siloes – email systems, CRM systems, ERP systems, corporate databases, cloud storage, mobile carrier databases, and the like. The rapid increase in the number of corporate applications, especially those in the cloud, and IT's acceptance of the "Bring Your Own" phenomenon, means that information management is becoming ever more fragmented and distributed. This makes formalized data access more difficult – even ad hoc data queries, such as those that employees might make to look for their older emails or files, are more difficult if an organization is storing a variety of data types in disconnected siloes. The result is that decision makers and others either can't find what they need, or they resort to recreating content.
- **Data is difficult to access**
Because data is increasingly distributed and disconnected, this leads to a situation in which it's difficult to search across siloes and synthesize this data to satisfy regulatory or legal considerations, let alone analytics requirements to understand what the data really means. Those charged with assembling a story from the data must visit multiple data siloes individually, navigating a unique interface, and pulling out what they need. In many cases, data simply cannot be connected between siloes.
- **Most solutions just weren't designed for analytics**
Most legacy archiving solutions were never designed for robust analytics – and it shows. While most of these solutions are adequate for capturing, indexing and retaining data – and many can do so at the scale that even large organizations require – they were not designed to provide the type of in-depth analytics that next-generation archiving requires.

Most legacy archiving solutions were never designed for robust analytics.

Next Steps

Osterman Research recommends that every organization consider the following steps for moving forward with the next generation of archiving:

- **Understand the value of archiving's traditional roles**
Osterman Research surveys have found that many organizations do not have a coordinated plan for retaining data, either leaving retention up to individual users, purging data stores on a regular schedule without regard to the content stored within them, or relying solely on backups to serve as the "archive" of corporate business records. However, the traditional roles of archiving – retaining business records for the appropriate length of time for regulatory and legal compliance, managing storage effectively, reducing backup and restore times, and enabling users to access their own data – continue to be best practices. In short, every organization in every industry should implement appropriate and granular retention schedules and archiving capabilities to ensure they are maintaining the appropriate defensive and functional posture for good data management.

- **Understand the value of next-generation archiving**

Decision makers need to appreciate the wealth of information that their organization has available to them if they properly archive their data and implement the appropriate analytics for understanding this data. The data stored in an archive of email, files, text messages, social media posts and other content stores can reveal insights about the organization that simply are not available from any other source. Moreover, given that relatively few organizations today have taken a next-generation approach to archiving, there will be a period in which the early adopters will gain significant competitive advantage by understanding their business better than their competitors understand theirs.

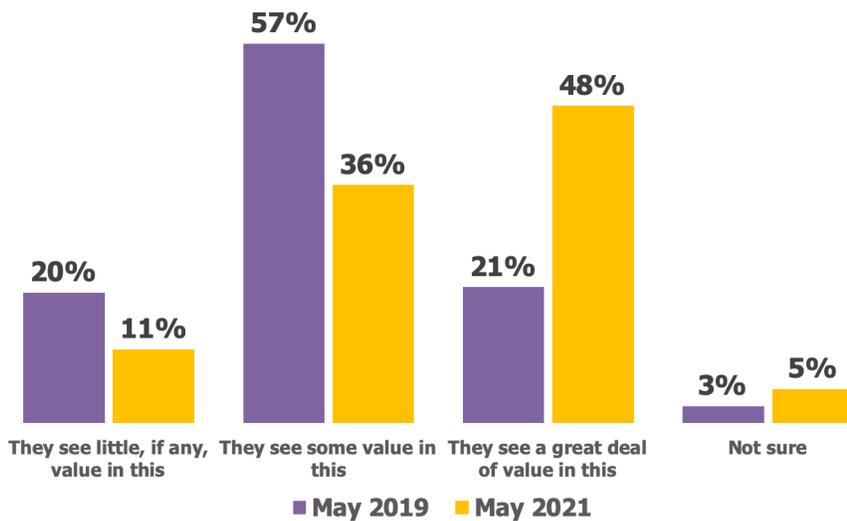
Our research bears out the notion that, over time, decision makers are becoming increasingly interested in using their data archives as sources of insight and intelligence. As shown in Figure 2 on the next page, while today only 21 percent of senior business decision makers see significant value in this application of archived data, nearly one-half of these decision makers will see this level of value in just two years' time.

- **Implement a good information governance program**

Good data is the lifeblood of most organizations, and so proper governance of this data must be an essential element of any organization's information management approach. Good information governance can offer huge benefits in reducing corporate risk, reducing the costs associated with legal and regulatory compliance, can reduce storage costs, and can make employees more productive. The return-on-investment associated with good information governance is substantial for most organizations and should be considered a high priority. Next-generation archiving is an essential element of any organization's information governance and should be considered holistically as a key element of it.

It is essential to establish policies that describe how all of an organization's data should be retained and managed.

Figure 2
Senior Business Decision Makers' Views on Using Analytics to Extract Intelligence from Archived Data, 2019 and 2021



Source: Osterman Research, Inc.

- **Implement the right policies**

It is essential to establish policies that describe how all of an organization's data should be retained and managed. Decision makers could establish a policy that will collect copies of archived data into a central repository and maintain it under

IT control in a single archive. This can be a viable solution in many cases, but it can cause problems, such as duplication of data across the organization, and data in the central archive being temporarily or permanently out of sync with data in the original archives as changes are made to the latter between replication cycles. Another option would be to implement a solution that will enable “in-place” retention and analysis of content instead of moving it into a centralized archive.

Have the right policies also means creating specific policies around other content, such as social media and chat, and including setting rules around not allowing the use of specific applications if the organization isn’t going to capture data from them.

- **Deploy the right archiving technologies**

Finally, it is essential to deploy the appropriate archiving technologies. Among the key considerations for an archiving solution are:

- Its ability to archive all of the data types that an organization needs to retain, manage and analyze, including email, text messages, social media content, files, content from collaboration systems, voicemail, etc. This includes all of the data types that should be retained today and that can reasonably be expected to be necessary to archive over the next several years.
- Its ability to archive content in context, not translating it into other, non-native forms that strip the original content of its context and metadata.
- The ability of the solution to be scalable, including the ability to store and quickly search potentially hundreds of millions or even billions of data elements. A key point here is that archiving solutions should offer fast, reliable and unrestricted export of content. Many archiving products are slow to get data out and, in some cases, will charge for data export.
- The ability to store data in a holistic way rather than in independent siloes of content that must be knitted together manually by those seeking information and insight.
- The ability to control data residency – that is, where the archived data will be stored – since, some jurisdictions have specific requirements around the physical location of personally identifiable and other types of information.

It’s important to note that not all archiving solutions are created equal. With the move to Office 365, many organizations are relying on Microsoft’s native archiving technology within the platform to address their archiving requirements. It’s important for decision makers to perform due diligence on these capabilities to determine if Office 365 – or whatever other platforms are in use in the organization – will meet their next-generation archiving needs, or if a third-party platform will be required.

It’s important to note that not all archiving solutions are created equal.

Summary

A high-performance and scalable archiving solution is essential to enable an organization to defend itself in legal matters, for regulatory purposes, and to provide a way for users to become more productive by searching more efficiently for older information. But next-generation archiving solutions can be used proactively to gather insight and intelligence from the vast quantity of archived data that they maintain, yielding important benefits and reducing risk.

Sponsor of This White Paper

TeleMessage is transforming business mobile messaging and mobile archiving with its mission-critical solutions: Managed, Secure, Reliable and IT Ready.

The TeleMessage Mobile Archiver effectively addresses mobile phone text and call archiving for compliance, regulatory and eDiscovery response requirements. It reduces risk across a variety of industries, capturing mobile content from BYOD and corporate phones.

TeleMessage is providing secure enterprise chat for co-workers and customers by using Android/iOS mobile apps, Web portal, Email to Mobile, and a range of APIs that connect to any operational IT system.

We provide tools to deliver multi-channel bulk messaging across: SMS, MMS, Voice calls, Faxes, Email and Mobile Apps.

TeleMessage has been providing state-of-the-art messaging solutions On-premises and in the Cloud for over 19 years. Our software has been successfully deployed and used by thousands of enterprises, trusted by dozens of telecom operators, reaching hundreds of millions of users and powering billions of messages through customers' networks. We support an ever growing number of enterprises, including telecom carriers, government agencies and leading brands across a range of industries such as healthcare, finance, manufacturing and retail, among others.

Our messaging solutions portfolio includes: [Mobile Archiver](#), [Secure Enterprise Messaging](#), and [Mass Messaging](#) product lines.



www.telemessage.com

sales@telemessage.com

#1 978 263 1015

© 2019 Osterman Research, Inc. 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, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. 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, Inc. 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.exterro.com/case-law-library/reasonableness/paisley-park-enterprises-boxill-ediscovery-case-law/#.XQgkT-IdEgQ.twitter>
- ⁱⁱ https://chippewa.com/business/businessreport/columns/legally-speaking-i-swear-it-can-be-harassment-workplace-profanity/article_29641235-6a2d-5603-89f2-a857a1aa648b.html
- ⁱⁱⁱ <https://www.ibtimes.com/wells-fargo-scandal-banks-tap-watson-monitor-employee-activity-2586425>
- ^{iv} <https://www.qsr magazine.com/human-resources/don-t-let-employees-texting-hurt-you>
- ^v <https://www.accountingweb.com/aa/standards/when-employees-rant-online-the-nlr-weighs-in-on-workers-rights>
- ^{vi} <https://www.eandblaw.com/employment-discrimination-blog/2015/10/08/can-a-single-employee-win-a-discrimination-claim-against-a-fortune-500-company/>