The Critical Need for Messaging Intelligence

An Osterman Research White Paper

Published January 2014

SPONSORED BY

TrustSphere
EXECUTIVE SUMMARY

Messaging Intelligence lies at the intersection of Big Data and Social Network Analytics. Messaging Intelligence takes the essence of data and makes relevant, real-time analytics available to key staff members within an organization at the point at which they need to make decisions. In short, Messaging Intelligence provides decision makers with situational awareness at the point of decision-making.

Some refer to this as either “fast data” or “little data”. However, it is more about relevant and essential data that is continuously synthesized and made available to staff members and management so that they can generate instant answers or conduct immediate discovery regarding a question, problem or situation that must be addressed quickly and efficiently. The context provided by this data is akin to a roadmap that enables decision makers to know where to look next for detailed answers to their queries.

KEY TAKEAWAYS

• Email continues to be the primary method of communication, collaboration and content sharing in the vast majority of organizations. Despite the growing use of other tools like social media or real-time communications, email will continue to dominate corporate communications for several years to come.

• As a result, email represents the “social fabric” of an organization – the primary and highly detailed source about how information flows within a company, as well as between companies and their business partners, customers and others.

• Organizations need to generate better insight into what is happening within their companies. Many decision makers do not have the information they need to ask the right questions or make the right decisions when investigating matters of importance to their organizations.

• Messaging intelligence, essentially a thin layer of analytics applied to content that organizations already possess in their messaging infrastructure, can be used to enable decision makers to ask the right questions and make the right decisions. This will help them to conduct formal and informal investigations more quickly, more efficiently and at lower cost.

WHAT IS THE VALUE OF ELECTRONIC CONTENT?

THE PRIMARY VALUE OF EMAIL

Despite the growth of social media, real-time communications, collaboration platforms, document management systems and other tools that many believe will displace email as the dominant communications and collaboration tool used in the workplace, the reality – as demonstrated by the survey data presented in Figure 1 – simply does not bear this out. Email continues to be the primary method by which users in the workplace communicate and the primary tool that they employ to collaborate with others inside and outside the organization.

It is also important to note that the same survey found 42% of respondents using email more today than they were 12 months earlier, with only 10% using it less. Consequently, Osterman Research sees no evidence that email’s dominant role in communications or collaboration will be usurped during the next several years.
Moreover, email continues to be the primary method by which users share content – files, contact information, task assignments and other information. For example, Osterman Research found in the survey noted above that 25% of emails contain attachments, and that the typical user sends and receives a median of 110 emails during a typical workday. This means that during a typical 260-day workyear, the typical information worker will send or receive 28,600 emails and 7,150 files. An organization of just 2,000 users, therefore, will generate traffic of more than 57 million emails and more than 14 million files each year.

In addition to the dominance of email communications, Figure 1 indicates that telephony – i.e., voice content – is also a key mode for communications and collaboration in most organizations, and one that must be taken into consideration in the context of how users communicate and collaborate. Moreover, as discussed later in this white paper, voice information is an important consideration for content management purposes.

EMAIL UNDERPINS THE SOCIAL FABRIC OF AN ORGANIZATION

Because email is used so extensively for purposes of communication, collaboration and content management by information workers and the organizations that employ them, it represents the primary source about how information flows within a company, and between companies and their business partners. For example, email data stores contain:

- Data on what information workers are doing during working hours. This information includes data on emails sent and received, to whom and from whom they are sent and received, files sent and received, how employees responded or did not respond to various communications, the tasks they assign to themselves or to others, the appointments they set, where they will be at specific times, requests that they make of others, etc. Moreover, because social media, real time communications, voicemail and other content types are often integrated with email, email archives often contain a wealth of information on other modes of communications used by employees.
• Information about how they collaborate with fellow employees, customers, business partners and others.

• Information about how employees support internal workflows and key business processes across the organization.

• Information on when employees work.

• Information on how employees work, such as sharing content with others or sending content to their personal accounts.

• Information about whether or not employees are complying with corporate policies, such as appropriate use or data leakage policies.

In short, email contains a wealth of information – most of which is largely untapped – about what transpires in the typical organization. Consequently, decision makers that do not tap this rich source of content are operating their organizations without much of the insight and business intelligence they need to be more effective.

THE NEED FOR IMPROVED INTELLIGENCE

DECISION MAKERS NEED BETTER INSIGHT

Clearly, email contains the primary source of information about content flows within an organization. Because decision makers rarely have the tools available to extract meaningful data from this rich content source, they lack much of the insight into their organizations that would help them to ask better questions, make better decisions about how to manage their companies, respond more effectively to customers, or satisfy their compliance obligations – just a few examples of how this information might be used. In short, decision makers need three fundamental capabilities:

• Insight about what is being said and transmitted via email; who is generating, receiving and responding to this information and content; and where this information is being sent and from whom it is being received.

• The ability to prioritize investigations based on these content flows.

• The ability to perform triage on email content at the beginning of an investigation in order to minimize the effort and intrusiveness required to completely it fully.

It is important to note that by "investigations", we are not referring to the invasion of individuals' privacy, nor are we talking about monitoring user behavior for the purpose of unreasonable or excessive control. While some may be sensitive to a misapplied notion of monitoring or investigating corporate email, particularly in light of the early June 2013 revelations about US government activities focused on widespread information gathering from email and other sources, what we are discussing here is much more about understanding how information flows through an organization’s email system and how decision makers can use this insight and intelligence more effectively to meet their legal, regulatory and best practice obligations. The goal of improving insight through the appropriate application of Messaging Intelligence is to enable better decision-making and to understand the context about the activity of the organization without invading privacy.

SUPPLEMENTAL TOOLS ARE NEEDED

Osterman Research has discovered that the vast majority of organizations believe they are reasonably well prepared to deal with searching for, finding and producing live email – i.e., content on email servers – in the context of eDiscovery (although Osterman Research believes that many decision makers overestimate their ability to do so). However, decision makers are much less prepared to satisfy various
eDiscovery requirements for other types of content, particularly social media and cloud-based content repositories, as shown in Figure 2.

Our research also revealed that internal legal counsel and corporate management believe that eDiscovery activities – and, by extension, eDiscovery-related activities like regulatory audits – are important, but they are not as prepared for them as they need to be. For example, nearly three-quarters of internal legal counsel believes that eDiscovery is important or extremely important for their organizations, yet only about one-half of them are prepared or very well prepared to deal with the issues presented by eDiscovery. Similarly, a significant proportion of both IT management and senior, non-IT managers place great importance on eDiscovery, but a much smaller percentage believes they are well prepared to address the issue.

What this means is that many organizations are relatively unprepared for the fairly well understood practice of conducting eDiscovery and related types of detailed and formal investigations. How much less prepared are they to use Messaging Intelligence to conduct faster and more efficient investigations?

In short, supplemental tools are needed to conduct not only eDiscovery and related activities, but also for formal investigations, informal investigations, regulatory compliance and other activities that require insight into the operations of an organization.
The Critical Need for Messaging Intelligence

Drivers for Better Insight and Better Tools

Osterman Research believes that there are five primary drivers for organizations to improve their insight into email-related and other types of information flows:

- To improve decision makers’ ability to ask the right questions before an investigation has begun, and to cull the appropriate information from the email system and other relevant sources to answer these questions.

- To streamline and shorten the investigation process. This is important not only for the sake of efficiency and minimizing the time required for an investigation, but also to minimize the actual and perceived intrusion into individual employees’ or functions’ email and related content.

- To minimize external legal costs by culling only the right information and by shortening the investigation process.

- To minimize storage requirements as well as retrieval and reconstruction costs.

- To proactively improve corporate governance.

Why is a Better Approach Needed?

The fundamental problem with current approaches to information management and investigations are several:

- First, those who manage email systems, collaboration tools and other systems that manage corporate records tend to operate independently from those who must investigate issues within an organization. This separation between those who manage corporate records and those who conduct investigations into them introduces delays into the investigation process, adds a quasi-bureaucratic layer to the investigation process that impedes it, and creates interdepartmental tensions that tend to slow the investigation process.

- Second, systems that manage records – email, document management, social media, voice, etc. – tend to be designed and managed as siloes of information...
and so are not capable of identifying or sharing the context of communications with one another. This not only impairs the process of investigation, but also drives up its cost and the length of time required to investigate even relatively insignificant matters.

- Finally, more formal systems of record, such as CRM systems, may not contain all of the information that an organization might need to manage customer accounts, conduct informal investigations and perform other tasks. For example, a customer that sends an email to a salesperson inquiring about a new product, or an existing client that leaves a voicemail with a complaint, might have their information lost if someone does not take the time to record the information. What is needed is a way to capture this information, integrate it with other relevant content, and make its existence readily discoverable so it can be retrieved from the appropriate systems of record during an investigation.

It is essential to note that what companies need is not a radically new approach to the way that they manage data, nor do they need to rip-and-replace their current infrastructure to overcome these problems. On the contrary, most organizations already have in place the systems of record that they need to understand their business. What they need is a better way to understand this information by extracting relevant content from the variety of information stores they already possess, and then integrating it to understand how their business really operates.

**COST AND ROI CONSIDERATIONS**

One of the key advantages to this better approach to information management is that it can reduce the cost and time required for an investigation, resulting in significant cost savings to an organization. For example, let’s say Customer ABC has indicated they are unhappy with XYZ Company, a supplier of a key component in ABC’s product. In fact, ABC may eventually be the target of a product liability suit because of a possible failure in the component that XYZ supplied. Using traditional eDiscovery tools, XYZ’s management might conduct an early case assessment and engage its internal and/or external legal counsel to pore through its email archives and other records stores, identifying every employee and third party that was involved in the relationship with ABC before, during and after the component was supplied to the company. They would extract a large amount of information that might or might not potentially be relevant to the investigation. Attorneys, paralegals, XYZ internal staff and others would be used to analyze the information, possibly travel to remote locations to secure individuals’ laptops or hard drives for further analysis of locally held data stores, analyze the information on these devices, and so forth.

A much better approach would be one focused on Messaging Intelligence that would identify only the relevant parties that were involved in XYZ’s supply of the component to ABC. It would enable investigators to rapidly identify only those specific time periods during which relevant email communication might have occurred between these parties, and then to hone in on only the involved individuals and specific time periods. The result would be not only a dramatic reduction in the amount of content generated for further analysis, but also significant cost reductions because less attorney time would be involved, XYZ staff might have fewer remote devices to collect and analyze, travel could be reduced, and XYZ management would know about their potential liability – or lack of it – much sooner and more cost effectively. This would provide not only lower direct costs, but also less potential liability and consequently less disruption to the business as a whole.

**NEXT STEPS**

Osterman Research recommends a three-step approach to addressing the issues raised above:

1. **Understand the data already available**
   The critical first step is to understand the enormous wealth of data already
locked away in the messaging activity that organizations have recorded. For example, most larger companies have deployed email archiving systems that contain records of emails and the metadata surrounding them. This means, that with the right tools, organizations can understand the "social graph" that exists within their organization: the frequency of email traffic between individuals, the velocity of email traffic, the context of communications, how communications changes over time, the relationships that might exist between third parties and internal staff members, any discrepancies between an individual’s .PST file or entries into a CRM system and their actual activity, etc.

Decision makers must understand that if they capture this information, which most already do in email archiving systems, they already have the core of the information they need to understand their business more thoroughly and conduct investigations more efficiently. What they lack is the ability to identify and extract the relevant information they need. This is where Messaging Intelligence tools can prove very beneficial.

2. **Understand the cost of conducting investigations**

The next step is to understand the current cost of investigations. For example, how much does a typical formal investigation cost using outside attorneys, internal legal counsel, paralegals, forensics specialists and others? By contrast, what would the cost of an investigation be if internal teams could conduct less formal investigations that resulted in narrowing their scope so that less, but more relevant information was generated for use with eDiscovery and other analysis tools?

It is essential to understand that what we are talking about is not the ability for business managers, legal counsel and others to peer into the communications of individual employees, third parties and others. Appropriately deployed tools of the type we are discussing in this white paper will not permit business managers or others to see sensitive data – instead, these tools will simply permit appropriately authorize officers of an organization to understand information flows for the purpose of improving the efficiency and lowering the cost of the investigation process.

3. **Evaluate the options that are available**

Finally, decision makers must evaluate their options:

- They can opt for the status quo and do nothing, resulting in the same level of (in)efficiency that most organizations experience in their investigation process and living with the same lack of insight into how their organizations truly operate.

- They can use full-featured eDiscovery or similar tools that generate large amounts of information and are useful for formal investigations. It is important to note that these tools are quite valuable when used for the large-scale tasks for which they are intended.

- They can use technology that applies a thin layer of analytics as an initial step. These tools will enable decision makers to ask the right questions and extract the right data immediately at the initiation phase of any investigation and provide the relevant clues for investigations that may otherwise remain obscured in the detail.

The critical first step is to understand the enormous wealth of data already locked away in the messaging activity that organizations have recorded.
ABOUT TRUSTSPHERE

TrustSphere is the recognized market leader in Messaging Intelligence, having pioneered a next-generation approach to analyzing both internal and external email communication patterns across an organization. TrustSphere’s clients use this intelligence to reduce and investigate internal fraud, improve their sales force effectiveness as well as improve network security applications.

Messaging Intelligence is a missing source of critical data within an organization, despite the fact that it truly represents the pulse of how an organization operates. Moreover, most organizations already possess the building blocks of Messaging Intelligence through the various stores of the critical content needed to implement it, such as email archiving systems, voicemail systems and the like.

TrustSphere’s Messaging Intelligence solutions integrate with most email systems (including Microsoft Exchange, IBM’s Domino, MS Office 365, Google Apps for Business) and an increasing number of advanced archiving and eDiscovery technologies.