Practical Email Governance Now:
Meeting the Minimum Threshold to Regain Email Control

By Robert Pease,
VP of Product Strategy
MessageGate, Inc.

Companies face quite a dilemma when it comes to what to "do" about email. Email growth has been organic both in terms of system design as well as usage, becoming today's corporate workflow tool, records management system, file sharing platform, and critical communications vehicle all in one. Faced with both pressing security concerns as well as pressures to ensure proper record keeping, companies must take practical and meaningful steps to meet the minimum threshold to regain control over email. This document discusses the challenges facing enterprises today, and examines steps to consider when formulating a strategy.

MESSAGEGATE
Enterprise Email Governance

Email is, unfortunately, a core part of everyone's working day. It is used for both work-related activities like planning meetings, negotiating contracts, and sharing information as well as less work-related purposes like gossip and social planning. Although various communications technologies continue to emerge - from text messaging to instant messaging - the corporate world of electronic communications is defined by email.

Companies face quite a dilemma when it comes to what to "do" about email. Email growth has been organic both in terms of system design as well as usage. Make no mistake, email is used as a corporate workflow tool, records management system, file sharing platform, and critical communications vehicle. Your other enterprise systems dedicated to these functions play catch up to the information contained in your employees' inboxes.

Faced with both pressing security concerns as well as pressures to ensure proper record keeping steps are being taken, companies must take practical and meaningful steps to meet the minimum threshold in order to regain control over email.

Email Challenges Facing Enterprises Today

Topics such as risk management, compliance, and governance are at the top of the corporate agenda these days and email is there to document every bit of non-compliant or questionable activity.

As absurd as it may be, companies are beginning to question the rationale for having email at all. After spending so much money on infrastructure, storage, employee time, and litigation, many leading companies are asking "what if we turned it off?" Once the nervous laughter dies down and companies begin to get a real grasp on just how much they depend on email, several telling trends become visible.

Lack of Security Awareness

CISOs and other professionals responsible for information safeguards consistently cite security awareness among end-users as the number one issue with which they must grapple. Every user makes mistakes, either through carelessness or by not understanding the implications of their actions.

The notion of the "insider threat" is certainly valid and there could be a nefarious employee lurking in the corridors of your company, scheming on how to steal information from you. Odds are you can quickly isolate these rogues out of the population either by examining previous disciplinary actions or by examining gaps in the employee screening and hiring processes.

The much larger issue is that 99%+ of breaches that occur are not based on malicious intent, but due to accidental, well meaning, or ignorant behaviors. People trying to get their jobs done will take short cuts to get it done quickly such as sending sensitive documents to their Gmail account to circumvent the corporate VPN or releasing customer information to an applicant get a loan closed sooner.

Contents

Looming Litigation

Electronic discovery of email is an unfortunate (and expensive) business reality in today's business climate. Companies can plan on spending between $1 and $3 per email recovered and reviewed during the course of litigation. Regardless if claims are frivolous or unfounded, companies must be in a position to defend themselves as well as respond efficiently.

Converging Content & Security Needs

Not so many years ago, security problems were the responsibility of security people and content needs were the domain of records managers. Given that email is the de facto corporate workflow tool, it is also the number one generator of business records. On top of this, the free form nature and minimal oversight applied to email communications makes it a huge security concern in terms of what is said, what is sent where, and what could possibly come back to haunt the organization due to one employee's actions.

There is more and more focus on making this a cross-functional issue where traditional IT security stakeholders and business-side content stakeholders are coming together to form committees or groups to tackle the issues and problems with email. Companies are quickly realizing that email is both a business record and a source of risk and exposure.

Balancing Security & Privacy Concerns

Sending an email is a very individual and personal pursuit. Although regulations vary globally, in the US email is a corporate asset and the company not only owns email but is responsible for what is in it - thus the focus on email discovery during litigation.

The issue that rapidly emerges when discussing what to "do" about email is how to balance the overriding security needs of the company with the employee expectation of privacy – in spite of whether or not that expectation is correct.

Regardless of your job function, the role of company police officer is not high on anyone's list. Again, since email usage has grown organically, the line between acceptable and unacceptable use has become more difficult to define. As we heard one CISO lament "how do you define appropriate use?" The core challenge is how to find the right level of oversight aligned with an expected level of employee privacy.

Achieving the Minimum Threshold

Understanding the major trends and issues driving corporate email usage is a necessary first step. However, even consistent agreement that email is, quite possibly, the greatest single source of business risk to the enterprise leaves those responsible with solving the problem with few, if any, practical and realistic steps to take.

The minimum threshold is defined as implementing those processes and technologies that satisfy the requirement to take best and reasonable efforts to avert email incidents and properly retain email records. As an officer or executive of a company, whether public or private, not meeting the minimum threshold creates significant exposure should a lawsuit or incident occur and could possibly be construed as negligent behavior. The following table illustrates the practical four step approach to achieving the minimum threshold.

Electronic discovery of email is an unfortunate (and expensive) business reality in today's business climate. Companies can plan on spending between $1 and $3 per email recovered and reviewed during the course of litigation.

The minimum threshold is defined as implementing those processes and technologies that satisfy the requirement to take best and reasonable efforts to avert email incidents and properly retain email records.

Achieving the Minimum Threshold

- Get buy-in from stake holders; form a group to address the issues
- Include Legal, Compliance, HR, Internal Audit, InfoSec, IT, and anyone else whose job is risk management
- Can't "boil the ocean" all at once; the problem is too dynamic for "silver bullet" solutions
- Emphasize practical actions to achieve the minimum threshold

- Take a historical snap shot of email activity
- Get a true picture of email usage including efficiency, hidden processes, and potential misuse
- Remember... 99%+ of improper use is not malicious
- Inform cross-functional initiatives to address the email dilemma

- Segmenting business & non-business email does not require a complex retention policy... get started now!
- All email is not created equally - identify high-value correspondence
- Classify email for retention - start with the "low hanging fruit": non-business, legal hold, Attorney/Client privileged, department/division codes

- Fix the problem you can solve quickly
- Increase security awareness, educate users, and change behaviors
- Respect end-user privacy while proactively mitigating risk
- Automated rules scan all outbound email

Getting Started - Make Email a Priority

As a ubiquitous communications tool, email touches every part and everyone in an organization. The step is to make email a priority and establish a working group to look at the problem holistically.

Members of this group vary, but at a minimum should include representation from Legal, Compliance, Internal Audit, HR, Information Security, and IT. The group should also include the executive designated as the risk officer or risk executive. These groups are generally chaired by someone from Legal who is responsible for getting buy-in from stakeholders and driving the decision-making process.

Crucial to this step is to emphasize the practical actions that can be taken to put the company on the path to meeting the minimum threshold while delivering the maximum impact. The problem can easily become too big to solve and is far too dynamic to believe in single, "silver bullet" solutions. Instead focus on informing the process and taking meaningful actions.

Inform the Process - Audit Your Email Usage

Often companies spend an extraordinary amount of money on email infrastructure, reporting, and staff, but still don't have any real understanding of how email is used and what it is used for enterprise-wide. So before buying another product or hiring someone else, conduct an audit of email usage.

An audit takes a historical snapshot of email activity and then analyzes it against established benchmarks, metrics, and best practices. The result is an eye-opening, true picture of email usage including all the inefficiencies, hidden processes, and potential misuse that lurks in the volume of daily activity.

The results will reinforce that 99%+ of improper email use is not malicious and that there are many quick and meaningful things that can be done to improve email performance. Start by examining who sends and receives the most email on any given day. If this is a system alert or mail delivery failure notice, turn it off because no one is reading it.

An audit takes a historical snap shot of email activity and then analyzes it against established benchmarks, metrics, and best practices. The result is an eye-opening, true picture of email usage including all the inefficiencies, hidden processes, and potential misuse that lurks in the volume of daily activity.

99%+ of improper email use is not malicious.

The results produced inform the cross-functional initiatives established to address the email question with company-specific and relevant information. Operational cost savings are easily identified and possible areas of risk are highlighted.

Retain Email Efficiently - Deploy Email Classification to Support Retention

Companies struggle with what to save and for how long. Physical records management programs have file plans which specify which documents to put where and how long to save them. The challenge is to translate a physical world file plan to an electronic world file plan and then extend that to records created by email. Most electronic documents end up as attachments to emails and to properly classify both the email and attachment according to a retention plan can prove difficult based on the sheer volume of email created in any given day.

With classification, less is more and all email is not created equally. Identify high-value correspondence and start by focusing on the "low hanging fruit" like segmenting business and non-business email and retaining it (or not) based on that segmentation. Non-business email can be anywhere from 20-40% of what a company sends and receives daily. Newsletters, alerts, and notifications are easily identified with 100% accuracy and with proper classification can be segmented or removed from the archival process to greatly reduce load and cost.

Beyond non-business email, are categories such as legal hold, Attorney/Client privileged, and adding department/division codes to the meta-data of an email as it is archived. Tagging email records with value-added information prior to ingestion by an archive improves downstream retrieval processes by focusing on the way you ***want*** to retrieve records. Also, having a streamlined and efficient method to enforce legal hold orders increases overall litigation preparation and confidence in responses to requests and inquiries.

Recent changes to the Federal Rules of Civil Procedure (FRCP) make classifying email a priority for all companies. Companies are required to have their houses in order as litigation begins and can no longer hide behind the "mountain of data in various places" defense.

Properly classified emails improve search and retrieval processes by adding greater context to email records in the archive. Discovery costs are also reduced due to proactively segmenting archived email records prior to review and production activities. Storage costs can also be reduced by differentiating and separating high-value, business critical email from low-value, non-business related traffic.

Companies must apply classification to archived emails going forward as well as the massive amounts (terabytes) of archived emails that exist in archives, tapes, and other types of storage. There is no delineation among messages in terms of those that should be retained and those that shouldn't as well as no way to quickly access and retrieve emails for internal or external review.

Sender Makes the Decision - Pre-Send, User Self-Review

There is very little appetite in any organization to disrupt email flow or put someone in the position to read suspect emails. There is no one you will find that wants to read more email, let alone someone else's. Outside of the brokerage firms, there is a reluctance to implement full-scale monitoring due to staffing, privacy, or culture concerns

The easiest and most direct way to address the risk created by employee-generated email is to implement a system that supports pre-send, user self-review. There is no way for every employee to understand all the prevailing corporate, legal, and regulatory rules and policies each time they hit the "Send" button.

Recent changes to the Federal Rules of Civil Procedure (FRCP) make classifying email a priority for all companies.

"Classifying emails as they enter archives helps to minimize the cost and time for identifying and retrieving emails containing discoverable information in a lawsuit."

-- Mark Levitt, VP for Collaborative Computing and the Enterprise Workplace, IDC

With more than 99% of breaches the results of unintentional or non-malicious motivation, you can increase security awareness, educate users, and actually change behaviors by implementing an automated scan of outbound email.

The focus here is to fix the problem you can solve quickly. With more than 99% of breaches being the result of unintentional or non-malicious motivation, you can increase security awareness, educate users, and actually change behaviors by implementing an automated scan of outbound email. Much the same way "spell check" works in a word processor, user self-review uses automated rules to identify emails that are more risky than others not by keywords alone, but by examining the context of an email.

Is there ever a good reason to forward an internal email outside the company? The answer is "maybe" and underscores the difficulty in accurately policing what is sent and received. If there is a good reason, an employee will confirm and, if not, they will abandon the activity. Where there is a desire for additional oversight, a confirmed email can be routed for review prior to release or exception reports generated. The key here is to respect end-user privacy while proactively mitigating risk.

Evolving Business Needs

To summarize, you can achieve the minimum threshold by:

1. Making email a priority
2. Auditing email usage
3. Classifying email
4. Deploying self-review

As needs evolve, expand technology use by creating new email retention categories or by increasing oversight and review where practical. However, keep in mind, meeting the minimum threshold is as much about people and process as it is about technology. The technology provides the tools and audit trail to demonstrate that you are taking best and reasonable efforts, but the employees are the ones using it to get their jobs done on a daily basis.

Depending on your business activities, you may have certain users who are not supposed to be sending external email, but you have no way to control external email sends. A simple technology addition will give you the flexibility to enforce this rule as well as modify it as business needs dictate. Some companies are exploring intelligent sampling of employee email to ensure both internal and external do not contain inappropriate material. Again, rather than thumb through a mountain of email, implement a technology that not only automatically samples users, but uses rules to identify those emails that are the most suspicious or of interest. Purely random sampling will quickly lead to frustration and erode the effectiveness of any program as reviewers lose interest due to the sheer volume of irrelevant email to review. Additional needs around information boundaries or dynamic disclaimer management are examples of business needs above and beyond the required minimum threshold, but essential to doing business. These requirements will materialize as you go through the process of meeting the minimum threshold and you must ensure you have the proper technology capabilities to address them.

Best in class companies conduct regular and routine audits to track progress, changing behaviors as well as demonstrating good business controls over email. Taken in measured and practical steps, regaining control over corporate email is not only possible but imperative for every company.

Keep in mind, meeting the minimum threshold is as much about people and process as it is about technology. The technology provides the tools and audit trail that you are taking best and reasonable efforts, but the employees are the ones using it to get their jobs done on a daily basis.

Best in class companies conduct regular and routine audits to track progress, changing behaviors as well as demonstrating good business controls over email. Taken in measured and practical steps, regaining control over corporate email is not only possible but imperative for every company.

To view a sample email audit report, visit
http://www.messagegate.com/auditreport/

For more information
email: info@messagegate.com
or
call: 877.544.8500

MessageGate, Inc., 10900 NE 8th Street, Suite 1300, Bellevue, WA 98004, Phone 877.544.8500, Fax 425.460.5061, www.messagegate.com