Streamline Email Governance with a Midsummer Fitness Check

Many organizations have a love/hate relationship with email. On the one hand, email remains the cornerstone of business communication. On the other, without diligent oversight, it can quickly become not only a time sink, but also a security and compliance liability. Spending some quality time on email governance can make the difference.

Automate Email Policies

A midsummer IT fitness checkup provides the perfect opportunity to review and update email policies. A well-crafted email policy both improves regulatory compliance and streamlines the archive to ease the eDiscovery process down the road. But policies require periodic adjustments to keep up with regulatory changes and evolving business practices.

Realistically, depending on users to remember and incorporate written policies almost certainly leads to problems. Thus, using archiving system controls and tools like Microsoft 365 retention policies and labels proves invaluable. These tools allow companies to automate email policies for retention and size limits, as well as those for attachments and proper sharing of documents.

For example, an archive full of redundant messages, large attachments and ancient reminders about the company holiday party brings the eDiscovery process to a crawl. With the right controls in place, the archiving system can categorize emails and automatically retain or delete them accordingly.

Update Email Security

Email continues to top the list of favorite targets for hackers. Consequently, an effective cyber security strategy must include a focus on email. Two key elements involve email filters and email encryption.

Basic email filters identify spam messages and automatically move them to a junk folder. More advanced filtering systems provide organizations the ability to whitelist or blacklist certain senders. They can also protect against new and emerging viruses by blocking certain file attachments and analyzing message content.

Email encryption prevents unauthorized access of sensitive emails. If you have not reviewed your email encryption in a while, do it now. A good encryption service will provide end-to-end encryption and allow admins to define pre-set rules. For instance, certain keywords will indicate sensitive information and flag an email for automatic encryption.

Educate Email Users

As businesses incorporate more communication options, end users need to understand how to use them efficiently and properly. For instance, while email works well for detailed or official communication, it should not become a file cabinet for documents. Instead, users should use document libraries like SharePoint for collaboration and file storage.

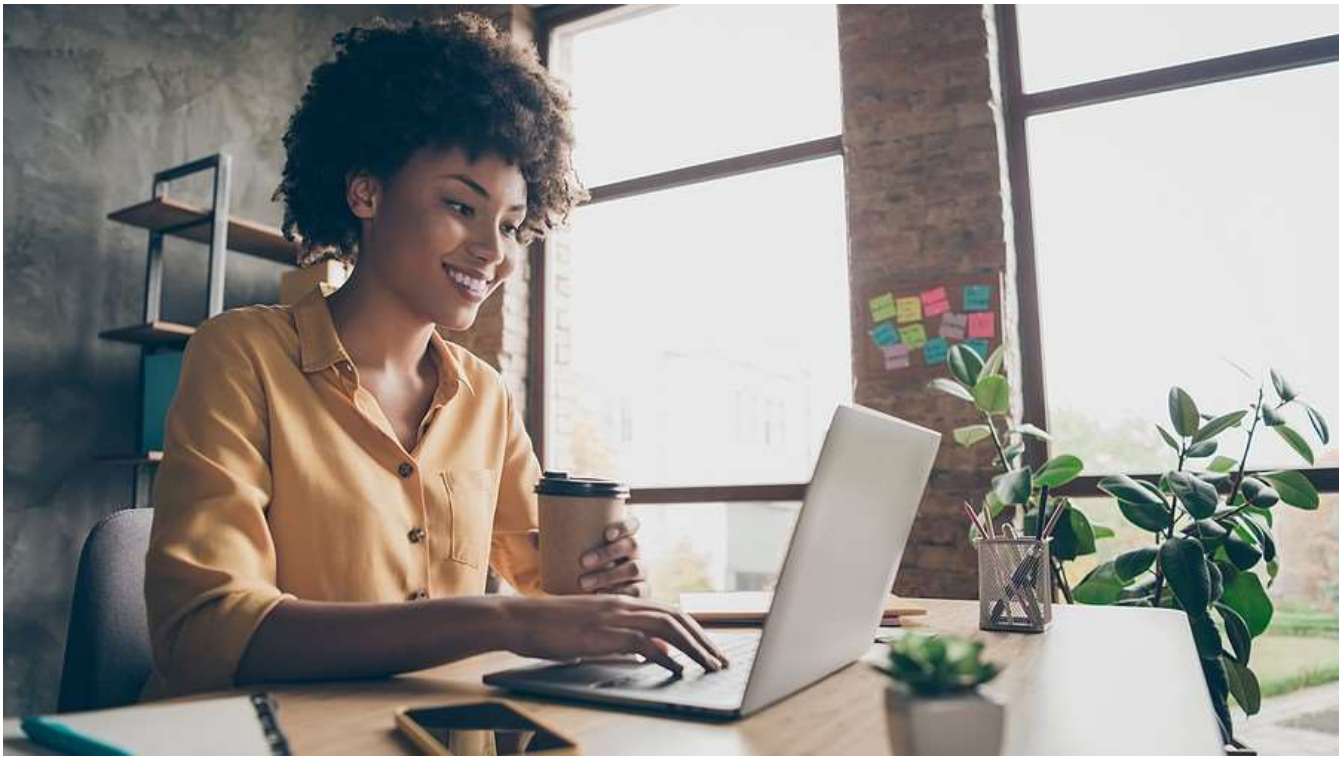
Additionally, users need to understand what information they can and cannot legally share via email. And they need to internalize safe email practices for avoiding phishing schemes and other email-born cyber threats.

Regular end-user phishing awareness training reduces successful phishing attacks and helps employees incorporate email management best practices.

Your summer email governance fitness check is also a good time to ferret out potential timebombs hiding in your email. Credit Card numbers, patient healthcare information, Social Security numbers, etc., all of which could prove detrimental to your organization if released, accessed, or used inappropriately.

Determine the Right Time to Migrate Away from Legacy System

Finally, organizations still limping along with outdated email systems should consider the right time to update to a modern solution. Legacy archiving systems may no longer provide the features needed to ensure security and compliance. They can also make eDiscovery cumbersome. And they often lack adequate technical support and sufficient storage space.



Incorporate Email Governance Best Practices

Effective email management involves utilizing data governance best practices such as effectively categorizing and organizing data, updating information security and monitoring for regulatory compliance. The email experts at Messaging Architects can help.

For instance, we provide consulting services to review and improve ePolicies surrounding electronic documents and email. We also tailor email security strategies to meet your business needs. And after years of conducting successful email migrations for clients of all sizes, we confidently ensure a smooth migration process when the time comes.

In addition, eGovernance solutions, provide not only email archiving and eDisovery but also an assessment of your exposure to PII, PCI, or PHI. If infractions are found, eGovernance is the right tool to manage that content by quarantining or eradicating it from your email system. Let the experts from Messaging Architects provide an exposure analysis of your current system.