WHITE PAPER:

Manage Your Email Before It Manages You

Is your email system helping or hindering your business? Effective email management is a requirement for protecting your business. Improper management can be costly in terms of lost productivity, including the time required to search for files and the hours required to reproduce any lost documents or information. The penalties from noncompliance with federal or state laws can be even more devastating. Employing best practices of email management can help companies be better prepared to deal with potential threats and other issues.

TeamLogicIT®
Your Technology Advisor

More Than a Communications Method

Though it only existed for 18 months in the 1860s, the Pony Express set the original bar for fast (and typically reliable) messaging. That standard eventually passed to the United States Post Office, followed years later by UPS and FedEx. It took approximately 100 years to streamline the mail delivery services from more than a week to overnight thanks to scores of drivers, pilots, and sorters.

Of course, the process and time required to move messages around the world changed significantly with the arrival of the Internet which is the most reliable and cost-effective way to move documents and messages between businesses and their customers and other associates.

Thanks to the growth of mobile devices, and a bevy of cloud computing options, accessing your email is now easier than ever. And the flexibility these latest solutions bring to the business community is invaluable. Employees can receive and respond to messages from almost anywhere. Your company's email system is more than a communications method; it's a file containing much of your business critical information and a record that must be protected to ensure business continuity and compliance.

One inherent issue with email is the network by which it's delivered. The vast quantities of emails held in a business' inboxes, sent folders, and deleted item folders can negatively impact network performance. While networks are increasingly efficient at moving data, they also have made it easier to transport malware and spam. The number of malicious attacks continues to climb. That's why it's so important for businesses to not only have the proper systems and safeguards in place, but to monitor and test them regularly.

The Real Cost of Spam

Unsolicited email messages make up a vast majority of electronic communications that businesses receive, adding significantly to network and data storage infrastructure and administration costs. Despite the implementation of various filters and protocols to restrict spam, you can't stop every unwanted message from getting through. Creative spammers understand the verbiage and protocols and continually devise new ways to fool the systems. That means your business must be diligent in maintaining and updating the latest spam controls.

The largest costs associated with spam are not related to the technology. According to a recent National Technology Readiness Survey, the time employees spend managing spam messages equals approximately $21.6 billion per year. That figure is truly staggering when you consider the number of tools that have been put in place to eliminate it. The overall battle for email control seems to be at a standstill, but businesses that implement the latest proactive procedures to thwart malicious attacks typically gain the advantage over their competition.

Meet Compliance Requirements

Corporate improprieties over the past few years have led to a number of new state and federal laws designed to increase the transparency of organizational practices. That means increased business requirements for document and message retention and higher costs for the technology needed to ensure compliance.

This myriad of regulations still isn't easy to comprehend, but hosted email management systems can simplify and streamline the required processes for most organizations. These solutions regulate the capture, classification, storage, preservation, management, and destruction of email messages based on the particular rules or regulations your business must follow. It would require many pages to list each law that involves email management, but here are some of the key regulations:

- **The Sarbanes-Oxley Act of 2002** (commonly referred to as SOX) requires records management and retention policies for all public companies as well as private firms that may be acquired by a public company. Penalties for noncompliance include substantial fines and up to 20 years in prison for those responsible.

- **The Federal Rules of Civil Procedure** applies to any organization that could be involved in litigation in the U.S. federal court system and mandates that each be prepared for electronic discovery. Failure to have a system in place that can store, search, and retrieve email data as needed could lead to substantial fines or loss of the lawsuit.

- **The Gramm-Leach-Bliley Act** applies to the protection of emails in financial institutions.

- **The Health Insurance Portability and Accountability Act** requires organizations to protect the security and confidentiality of patient healthcare information, including email messages containing records or data.

Reduce Your Litigation Risk

Many companies believe they have an effective email management system in place since they capture every inbound and outbound email, but that is only half of it. When called into court by a customer or former employee, retrieving all the relevant electronic messages and attachments can be a nightmare without the proper archiving and retrieval tools.

A hosted email system with central archival storage can save a substantial number of employee hours and reduce the frustration associated with locating the files needed to defend lawsuits. For a thriving business with a large number of emails and other data to sort through manually, the efforts could be substantial. Search functionality built into the archive helps ensure the process will be much less painful and costly.

Reduce Email and Network Security Threats

Viruses delivered via email can expose important company assets, including intellectual property and confidential customer information. The financial losses from a single breach can be devastating—from lost revenue and the cost of litigation to fines and penalties for noncompliance with state and federal statutes. While these liabilities may not concern every business, losing customer data or company secrets can significantly damage reputations and customer relationships.

Ensuring proper antivirus and antispyware software is implemented is essential to prevent the compromise of your business networks. Isolating email messages that contain potential threats is a key first step in stopping security threats. Employees also play a significant role, reviewing and disposing of suspicious messages and alerting the IT support team when they have questions or concerns about something they received. Due diligence is the best threat prevention method.

Improve Disaster Recovery Capabilities

The starting point for post-disaster recovery is to ensure necessary business information is being backed up. A well-defined email archiving system will help identify and categorize the messages to keep and eliminate spam from being saved. This will reduce the time required to perform backup activities and make it easier to restore the files during a disaster recovery process.

A good email archiving system will also identify the employee workstation or file server where the information originated, making the restoration process much easier. Consider the challenges facing a company after a fire, hurricane, or system failure. An effective email restoration process will get the business back online faster and provide greater assurance to customers and prospects.

Quick Tips for Managing Business Email

- **Establish email policies for all employees**—Create and enforce policies, from time management rules to security precautions.
- **Communicate and publish policies**—Include electronic messaging rules in employee handbook and communicate specifics on a regular basis.
- **Implement spam filters**—Reduce the time spent reviewing email and related security issues by removing unwanted messages.
- **Establish email archiving needs**—Understand your company's compliance and business needs and set goals for storage and retrieval methodologies.
- **Regulate employee use of alternate email**—Security procedures must also be followed when opening email attachments and filtering spam in Gmail, Yahoo and other accounts.
- **Consult an experienced email professional**—Engaging an expert is the fastest and least frustrating way to ensure your compliance and business needs are being addressed.
- **Ensure continued support**—Email management requires constant focus and continual enhancements from network specialists.

Email Management Protects Your Business

With email as the standard for business communications, its continued growth presents major information management challenges for many organizations. Just like any type of business data or record, email must be included in the company's long-term technology and operations plans. The addition of legal and regulatory requirements makes it imperative to follow a prescribed list of industry standard procedures. This includes the capture, classification, storage, preservation, management, and destruction of email messages.

Hosted email management systems capture inbound and outbound messages of all employees and use a classification scheme to manage the content, retention rules, and who can access it. The information associated with each communication is also captured using the same methods. Archiving is one of the most critical components of an email management system, copying any required information and deleting the spam or unnecessary material.

Effective email management requires the support of an experienced and trained professional. Whether you hire an individual or contract with a managed services provider to implement and manage the ongoing development of the systems, the complex laws and specific needs of each company necessitate the advice an expert can provide.

For help with your technology, contact your local TeamLogic IT office.

TeamLogic IT is a national provider of advanced IT management services for businesses. With locations across the U.S. and Canada, TeamLogic IT provides managed services, computer consulting and support services focused on helping companies minimize downtime and improve productivity. TeamLogic IT helps businesses compete better through the effective use of information technology.

©2023 TeamLogic, Inc. All rights reserved.