INTRODUCTION

It’s easier for someone to view email in transit than it is to eavesdrop on a phone conversation. And despite the immense popularity of Web-based messaging tools, email remains the primary means of online communication. Its widespread use as a business tool and potential for exploitation, along with a growing list of regulations, makes email compliance a major issue for organizations worldwide.

Is regulatory compliance daunting? Yes. Is non-compliance costly? Sometimes. Does it have to be difficult? No. This paper details how organizations are affected by government and industry regulations and explains how to simplify compliance management through well-controlled policy, thoughtful planning and flexible email security solutions.
EMAIL IS STILL THE “MASTER APP”

With so many instantaneous or mass messaging vehicles such as Facebook, Skype and Twitter, email often seems less relevant to organizations today, especially in a security context. But realistically, email is still the “master app”, with 78% of employees stating that their email usage has increased significantly in the last five years.¹ This is supported by a Radicati Group report which predicted that there will be 1.9 billion email users by 2013, which breaks down to 247 billion messages per day and 2.8 million messages per second.²

Along with ubiquitous email usage comes an increased capacity for its exploitation. For example:

- Approximately 80% of these high volumes of email are unwanted (spam or viruses).³
- Email is commonly used as a conduit for malware, a scenario where unsuspecting users click a link or download a document within an email which takes them to an infected Web page.
- Data loss via email, whether intentional or accidental, can result in non-compliance with a variety of regulations, which often leads to costly consequences.

These issues portend the need for businesses to secure inbound, outbound and internal email and set flexible, easy-to-manage policies that ensure regulatory compliance.

There will be 1.9 billion email users by 2013, which breaks down to 247 billion messages per day and 2.8 million messages per second.²

Email as a Form of Online ID

Email has become the online equivalent of a driver’s license—a unique identifier. As a rule, any online account, registration or subscription requires a user email address, making email essential for all users and businesses.

Email as a Vital Business Tool

Most businesses communicate with their customers via email to announce new products and promotions, confirm orders or provide support services. As a matter of fact, Forrester estimates that $2 billion USD will be spent on email marketing in 2014⁴, while $1.8 billion will be spent by an average 1,000-user organization for spam management—not including anti-virus, data loss prevention and malware protection. This validates email as a significant investment which merits earnest efforts to secure and control what enters and leaves an organization.

Email has become the online equivalent of a driver’s license—a unique identifier.

HOW REGULATORY REQUIREMENTS AFFECT ORGANIZATIONS

Organizations must work within a growing, disparate and constantly changing framework of regulations. Often these regulations overlap—sometimes even conflict—complicating an organization’s attempts to enforce compliance efficiently. For example, a business with multiple locations across the U.S. contends with various state requirements in addition to federal mandates. Add industry-specific regulations to the mix, and compliance can become complicated and difficult to manage across the organization. Moreover, for global organizations, regulations need to be addressed on a country-by-country basis. And lack of compliance carries serious consequences, so there’s no room for error.
Examples of just a few of the regulations affecting today’s organizations include:

**Privacy-based Legislation for Government Agencies**

- **Privacy Act of 1974**
  This legislation mandates that U.S. federal government organizations protect data related to private individuals.

  “No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.”

**Privacy-based Legislation for Private Organizations (Mandated by Government)**

- **PII (Personally Identifiable Information) protection laws**
  Already in place for several state governments, these laws protect PII such as social security numbers. Examples of legislation include:

  - California Online Privacy Protection Act (OPPA) of 2003
  - Nevada Revised Statutes 603A: Security of Personal Information
  - Massachusetts 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth
  - Proposed Federal Trade Commission (FTC) legislation
    In December 2010, the FTC proposed new legislation to tighten regulations that protect personal information.

**Industry-specific Regulations**

Organizations in industries such as healthcare, finance and legal services manage large volumes of sensitive personal information and are required to adhere to stringent regulations, including:

- **Health Insurance Portability and Accountability Act (HIPAA)**
  Sets requirements for healthcare organizations regarding the electronic communication of patient information, including names, birth dates, admission dates, telephone/fax numbers, social security numbers, medical record numbers, health plan beneficiary numbers, and biometric identifiers.

- **The Health Information Technology for Economic and Clinical Health (HITECH) Act**
  Contains changes to HIPAA legislation that enforces its Security Rule and Privacy Rule. Specifically, notification of an unsecured data breach must occur within 60 days, and violations to privacy breaches are subject to civil and criminal prosecution.

- **Sarbanes–Oxley Act of 2002 (SOX)**
  Provides criminal penalties, including prison sentences, for corporate executives who destroy documents and business information. It also specifies a records retention period of seven years and defines record types, such as physical and electronic documents and correspondence.

- **Gramm–Leach–Bliley Act (GLB)**
  Contains several provisions relating to the privacy of consumer financial data, including a definition of privacy and information disclosure policies.

- **Payment Card Industry Data Security Standard (PCI-DSS)**
  Provides guidelines for the protection of credit card holder information, including the use of encryption, the storage of secure data, and access control methods.

Although the previously-listed regulations are U.S.-based, they have global impact and repercussions. Other regulations that affect organizations worldwide include, but are not limited to:

- **Basel II Accord – European Union**
  Basel II is a global standard for risk management in financial institutions. Part of this accord ensures the privacy of financial information when transferred across international borders. It also provides guidelines on disclosing private information.
• **International Organization for Standardization (ISO) 15489 – Worldwide**
  The ISO 15489 standard offers guidelines on the classification, conversion, destruction, disposition, migration, preservation, tracking and transfer of records.

• **Personal Information Protection and Electronic Documents Act (PIPEDA) – Canada**
  PIPEDA protects personal information from being disclosed during commercial transactions, federal activities and business dealings within Canada and internationally. It also provides guidelines for gathering, using and storing data.

• **Data Protection Act 1998 – U.K.**
  This legislation specifies that electronic personal information must be secured and retained for defined periods, after which it must be destroyed. It also includes rules on the transfer of personal data.

  RIPA addresses the interception of electronic communications as part of an investigative action and describes circumstance under which this information would be disclosed.

• **Spam Act 2003 – Australia**
  Restricts unsolicited commercial electronic messages (spam), prevents individuals and organizations from harvesting addresses, and requires that all commercial messages contain an unsubscribe option.

**Business Contracts and Agreements**

Many businesses need to implement policies that account for agreements with vendors, contractors and partners, in addition to government and industry regulations. So email solutions that offer specific levels of customization and flexibility help organizations set and control their business-specific policies.

**CONSEQUENCES OF NON-COMPLIANCE**

**Reputation**

According to Warren Buffet, it takes years to build a credible reputation but only a few minutes to ruin one. Loss of credibility translates directly to an organization’s bottom line. For example, when consumers lose confidence, they switch to other services or brands, resulting in profit loss. And public relations efforts to restore trust can be costly and time consuming.

**Financial Cost**

According to the Ponemon Institute, organizations were charged $214 per compromised record in 2010, and the average organizational cost of a data breach increased to $7.2 million\(^7\). This trend has increased steadily over the last five years, and per-record costs add up appreciably in instances where mass data is compromised. Furthermore, expenses associated with public notification and any applicable compensation further burden organizations.

**Legal Repercussions**

Email is subject to libel laws in addition to other requirements. Employees who communicate false stories about other employees via email subject themselves and/or their organization to libel lawsuits. More egregious instances of non-compliance can result in imprisonment for those involved.

*According to the Ponemon Institute, organizations were charged $214 per compromised record in 2010, and the average organizational cost of a data breach increased to $7.2 million.*\(^7\)
Examples of Compliance Breaches

**Cignet Health Fined $4.3M**

The federal government fined Cignet Health of Prince George’s County, Md., $4.3 million for violating 41 patients’ privacy rights by denying them access to their medical records, violating HIPAA law.⁴

---

**California Department of Consumer Affairs**

In June 2008, a Microsoft Word document containing names, salaries, social security number and titles of 5,000 people was emailed outside of the department.⁵

---

**Blue Cross Blue Shield of Louisiana**

In Sept. 2008, a document containing the personal data (social security numbers, birth dates, phone numbers and addresses) of 1,700 brokers was compromised via email which was meant to notify agents of a software upgrade.⁶

---

**Epsilon Data Breach**

On March 30, 2011, Epsilon, a company that manages email communications for several large companies, experienced “unauthorized entry into [its] email system” that exposed customer names and email addresses.⁷
FUNCTIONALITY MATTERS: WHAT YOU NEED TO SIMPLIFY EMAIL COMPLIANCE

Message Retention

Email is subject to the same laws as paper-based communications: it needs to be securely archived and quickly produced when required. eDiscovery pertains to the retrieval of Electronically Stored Information (ESI) for legal evidentiary use. Organizations need solutions that store high volumes of email and make them easy to retrieve within specific, mandated time limits.

Data Loss Prevention (DLP)

As previously discussed, data protection is essential for compliance. An effective DLP solution, which should include encryption, will prevent many data breaches from occurring in the first place. To accomplish this, organizations need content-aware solutions that provide full control of all data shared among employees and sent outside the gateway.

Built-in content inspection capabilities such as email monitoring and filtering; deep content inspection of attachments; fingerprint technology; and lexical dictionaries all manage distribution of sensitive content to prevent data loss.

• Data in Motion
  Data at rest (stored) is one thing. Data in motion is yet another. Information transferred over the network or Internet is at high risk, but it can be secured effectively using solutions that offer precise, flexible policy controls. These controls should address who can send what data, where that data can go, and what data needs to be secured.

Security

Many regulations require the presence of basic security such as anti-virus protection or access control. However, as blended threats increase, it would be prudent for organizations to deploy solutions that protect from advanced, data-stealing malware that originates in email and then executes when the user clicks on a link within the email message. To successfully prevent breaches that impact compliance, it’s becoming important to proactively protect against malware, regardless of the entry point.

User Education

Successful compliance policy begins with education and many regulations require ways to advise users on behaviors that could potentially breach policy. When users understand proper workplace email usage and the consequences of non-compliance, they will be less likely to err. One of the most common breach methods is unintentional human error, making unsuspecting or poorly-trained staff a popular target for attackers.

Organizations need solutions that store high volumes of email and make them easy to retrieve within specific, mandated time limits.

WHY GATEWAY OR CLOUD SOLUTIONS ALONE MAY NOT BE SUFFICIENT

Compliance requirements stipulate the rules, not how or where they are enforced. Nowhere is it stated that the need to secure data ends at the gateway. And while controlling what goes in and out of an organization is critical, many organizations underestimate the effects internal email traffic (between users on the same network) can have on compliance.

Securing Internal Emails

Compliance-based legislation was enacted to prevent data from falling into the wrong hands. Obviously, this applies to information sent outside the organization. But what about an email sent to the wrong internal employee? Often, proprietary data is limited to specific users or even clearance levels. A document appropriate for a senior human resources director might not be so appropriate for someone on the sales team. Or confidential R&D specs may be restricted to engineers or legal staff.

Accidents Happen Inside the Gateway

Most internal email breaches are inadvertent, but that doesn’t necessarily make them any less damaging. User-friendly email features such as “auto-complete” addresses and pre-set distribution lists make it extremely easy to mistakenly send the wrong email to the wrong people. And with one click, someone can erroneously send a confidential attachment to one or more users.
Cloud-based Data

Is data that resides in or is transmitted via the cloud as secure as on-premises data? To ensure full compliance, an effective email solution must be capable of setting and enforcing policies as well as providing encryption and security for cloud-based data.

Management of Encrypted Content

Encryption is critical for securing sensitive emailed data from prying eyes. However, it can be used illicitly to conceal information from an email security product. For example, an employee could use desktop encryption to hide confidential data from the gateway security email server. This makes it important to establish who, if anyone, is allowed to send encrypted messages that cannot be scanned for content.

Most internal email breaches are inadvertent, but that doesn’t necessarily make them any less damaging.

FIVE STEPS FOR IMPROVING COMPLIANCE AND REDUCING LEGAL RISKS

An effective compliance policy typically focuses on data protection with additional attention to retention and security. To improve compliance, organize a team with representatives from the relevant locations and affected business units to work through the following steps.

STEP 1: Plan a Compliance Policy

a. Keep it simple
   • Devise a realistic, phased approach for outlining your policy.
   • Begin with the most critical components of your plan. What are your most vulnerable areas in terms of email compliance?
   • Plan, implement, test and refine over time.

b. Understand how regulations impact your data protection policies
   • Which regulations apply to your organization?
   • What is required for compliance with these regulations?
   • If specific rules conflict, determine which ones supersede others.
   • Determine whether policies will need to be set for different regulations in different locations.

c. Identify what data requires protection and set policies accordingly
   • Who? Sender or receiver, specific user groups, etc.
   • What? Keywords, message size, files, patterns, credit card numbers, social security numbers, etc.
   • Encrypt based on content that matches the criteria.
   • Block, delete, archive or notify if content matches the criteria.

c. Determine how data is being lost
   • Do most email breaches occur through one user or a group of users?
   • Is email the primary source of breach or do most DLP incidents occur via Web 2.0 applications?
   • Is data commonly leaked through email attachments? If so, is your current email solution able to scan content within attachments, versus only blocking by attachment type?
   • Are most data loss incidents internal (among employees) or external (sent outside the network)?
STEP 2: Enforce the Compliance Policy

a. Implement a few well-targeted rules and enforce them

Technical policy enforcement:

- Removes the burden from users and administrators.
- Allows organizations to set flexible policy controls.
- Enables organizations to automatically preempt activities that could lead to noncompliance.

b. Educate users

- Inform all users about the company’s email policy and provide initial training via video, face-to-face or Web-based trainings or other communications.
- Automatically remind users about the policy at set intervals of time or whenever they mistakenly violate a policy.

c. Update your policy periodically

- Promptly inform users of any changes to existing email policies.

d. Include robust reporting

- Implement easy-to-use, centralized reporting with features like pre-set templates, automatic delivery and the ability to schedule reports automatically.

STEP 3: Implement the Policy Thoughtfully

a. Take an incremental approach

- Implement the policy in phases and with monitoring, rather than all at once, to prevent wasted effort and ensure that each phase works well.

b. Ensure the policy is enabling

- Although the policy must be compliant, it shouldn’t impede the ability to do business. The goal is to set smart policy that protects data, yet enables access to appropriate information.

STEP 4: Accept Limitations

a. Demonstrate a serious effort

- No plan is 100% effective. Compliance means that a true effort is in place, but it is understood that even with the best controls, every policy infringement cannot be stopped every time.

STEP 5: Incorporate Security Benefits

a. Protect users and the network

- Integrate protection from malware, blended threats, phishing, spam and inappropriate content where possible. In addition to providing corporate protection from libel and data loss, it will prevent costly attacks that begin in an email, proliferate via the Web and infiltrate the whole network.
USING THE RIGHT TOOL IN THE RIGHT PLACE

The good news for organizations requiring email compliance is that various solutions are available to fit their compliance needs, number of users and budgets. The best solutions offer flexible policy administration, scalability and centralized management in a variety of deployment options.

Once an email compliance policy plan is created, technical enforcement can be accomplished using one or a combination of the following types of email security solutions.

- **Email Gateway Security**
  Secure email gateway products provide strong anti-spam and anti-malware protection for inbound email as well as data loss prevention for outbound email. Robust reporting is another feature that assists with overall security, productivity and compliance.

- **Cloud-based Email Security**
  Typically, cloud email solutions provide solid security, blocking viruses and eliminating the 80% of spam and unwanted emails coming in before they reach the network. In addition to being cost effective, these solutions are scalable and store volumes of email.

- **Internal Email Security**
  An internal email security solution should provide organizations with centralized security that simplifies email compliance and management. It should also provide visibility into email traffic flowing between users on the same network as well as traffic entering or leaving the organization. These types of solutions incorporate anti-virus, DLP features and regulatory compliance capabilities in a single on-premises solution.

M86 Security Solutions for Email Compliance

The M86 MailMarshal Secure Email Gateway and M86 MailMarshal Email Content Manager can be configured to detect content within data streams, including internal email traffic, using techniques such as pattern matching, which inspects messages and attachments to identify credit card numbers, social security numbers, sensitive data and other restricted or controlled email content. These solutions enable administrators to create rules quickly and easily, ensuring that any content containing specified data will be managed, blocked or quarantined, and the appropriate notifications will be sent. In addition, M86 MailMarshal SEG protects against malicious code, phishing attacks, dangerous file types and other threats that occur at the email gateway.

M86 MailMarshal Secure Email Server and M86 MailMarshal SendSecure can be used in conjunction with M86 MailMarshal SEG to ensure that all personal information allowed to leave the email gateway will be encrypted.

Key Solutions

- The **M86 MailMarshal Secure Email Gateway (SEG)** protects against spam and malware while managing complex compliance policies and preventing confidential data loss.

- The **M86 MailMarshal Email Content Manager (ECM)** simplifies compliance by ensuring inbound, outbound and internal email—including text, images and file attachments—adhere to data loss prevention and policy requirements.

REFERENCES

2. Radicati Group report, May 2009
3. Forrester report, July 2009
5. InfoSecurityAnalysis.com, Data Breach Statistics 2008 Summary
6. ID Theft News, Blue Cross Blue Shield Louisiana
7. Epsilon.com, “Epsilon Notifies Clients of Unauthorized Entry into Email System,” April 1, 2011
ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry’s leading Secure Web Gateway provider. The company’s appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 25,000 customers and 26 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information, and ensure regulatory compliance. The company is based in Irvine, California with international headquarters in London and development centers in California, Israel, and New Zealand. For more information about M86 Security, please visit: www.m86security.com.