

...EMAIL COMPLIANCE

Chief Information Officers and IT managers in the highly regulated health and financial industries or in large, publicly traded organizations are usually well aware of what is required for email compliance. For privately held or smaller companies and non-regulated industries, email compliance is often unclear and the apparent complexity and serious consequences for violators can make the task of complying seem daunting.

The concern is largely unjustified. According to the definition of compliance opposite, for most organizations, compliance is achieved by operating under a formal set of clearly defined guidelines that ensure adherence both to formal legislation and to accepted ethical standards and best practices. These guidelines should also cover how to handle deviations, accidental or otherwise. In the absence of guidelines it becomes extremely difficult to respond positively and effectively to an audit (or “eDiscovery), or worse, a legal inquiry.

This document looks at compliance in relation to email, giving clear and simple guidance for managing your email infrastructure*.

COMPLIANCE DEFINED

“Compliance” is the state of being in accordance with established guidelines, specifications, or legislation – or being in the process of becoming so.

1 Establish clear rules about email usage

Email is the quintessential communications tool with much of an organization’s day-to-day life dependent on it for both internal and external communication. Email can contain as much as 80% of a company’s business records so setting out the rules for how it should be used is essential.

The starting point is to define a clear and transparent framework for behavior, setting down what’s acceptable and what isn’t when it comes to using email. An explicit, organization-wide Acceptable Use Policy (AUP), accompanied by the ability to audit its use and enforce its rules is a simple first step in demonstrating the intention to meet regulations and goes a long way toward avoiding liability. As an example, typical clauses might be:

- don’t forward or send email containing pornographic images
- do limit attachment sizes to 5MB.

With the AUP in place, you can then focus on ensuring that your practices are compliant with the wide range of local, regional, national and international laws that extend into email communications.

A wide range of online examples is available from industry analysts such as Forrester, IDC and Gartner.

2 Prevent data loss via email

The data that you hold in your systems is valuable business information. It must be guarded carefully from accidental or deliberate disclosure of confidential information to parties outside and, on occasion, within your organization. Some of the processes will be covered by your AUP, but new employees, leaving employees, distracted employees and disgruntled employees can all inadvertently (or maliciously) threaten the security of your data.

It is essential to put in place an automated, centrally managed mechanism to prevent data loss regardless of intention or the goodwill of your employees. This solution should be able to:

- block emails by the filetypes of their attachments
- scan messages for keywords
- add disclaimers and banners to mail in all directions
- encrypt messages so that only the intended recipient can read them
- ensure that your email system is not being abused by unknown and/or malicious users.

3 Maintain visibility over and access to current and past traffic

You need to make sure that you are aware of – and can account for – the email coming into, going out of and circulating around your organization. This means you must:

- Retain accessible records of relevant email communications, including log information that can show who sent what to whom and when.
- Copy and/or archive sensitive messages, both internal and external.
- Be able to intercept and re-route violating messages to those responsible for enforcement so that potentially damaging incidents can be avoided and remedial efforts can take place.

It is important to recognize that not every email contains sensitive data, so not everything needs to be archived and/or encrypted. Depending on your jurisdiction, there are also limits on how long you must retain copies of email communication.

In fact, the cost of storing and accessing large volumes of email requires you to be deterministic when it comes to what needs archiving or encryption, and how long you should be storing.

4 Eliminate spam, phishing and malware

One of the main ways that virus writers get malware onto your users' computers and into your systems is through email. Spam campaigns that rapidly change in order to attempt to evade detection use a variety of methods – such as dropping keylogging Trojans or linking to malicious websites – to steal confidential business and personal information.

You must ensure, and be able to demonstrate, that your email infrastructure is protected against malware, viruses, spyware and other threats to system and data integrity. For this you need a solution that blocks malware, spam, Denial of Service attacks, and harvesting of email addresses.

By blocking threats at the perimeter right through to your internal mail servers and desktops, you will eliminate most of the external risk associated with data loss. Your AUP will go a long way toward covering the remaining internal risk.

ANALYST VIEW

“Because successful messaging strategies must encompass malware blocking, content filtering, compliance, eDiscovery and archiving, an integrated product set is needed that reduces administrative overhead, satisfies customer needs, and minimizes disruption from new vulnerabilities and changing regulations.”

Christian Christiansen, Vice-President, Security Products and Services, IDC

Sophos Email Security and Control provides a range of hardware and software solutions to protect your entire email infrastructure from threats and enable you to comply with regulatory requirements. It works in tandem with Sophos Endpoint Security and Control and Sophos Web Security and Control to provide complete network protection that enables good compliance practices. To find out more about these products and how to evaluate them, please visit www.sophos.com.

Sophos is a world leader in IT security and control. We offer complete protection and control to business, education and government organizations – defending against known and unknown malware, spyware, intrusions, unwanted applications, spam, and policy abuse, and providing comprehensive network access control (NAC). Our reliably engineered, easy-to-operate products protect over 100 million users in more than 150 countries. With over 20 years' experience and a global network of threat analysis centers, the company responds rapidly to emerging threats and achieves the highest levels of customer satisfaction in the industry. Sophos is a global company with headquarters in Boston, MA., and Oxford, UK.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Copyright 2007. Sophos Plc. All rights reserved. All trademarks are the property of their respective owners.

**Disclaimer: this is not intended to replace professional/legal guidance on compliance issues that your organization may face. We strongly suggest that you seek advice from recognized compliance experts to determine your needs.*