clearswift
A HelpSystems Company

# Six-Step Guide to Email Security Best Practices

**Modern business is reliant on email. Think how difficult it would be to collaborate with colleagues, customers and trading partners without it. Research group Radicati predicts that in 2020 the number of emails sent and received per day will exceed 306 billion. The sheer volumes of traffic and the ever-increasing threat from email-based cyber-attacks, present significant challenges for IT teams to overcome. All organizations using email need to:**

- Detect and stop exploitation from phishing attacks
- Control spam volumes without the risk of trapping genuine business emails
- Prevent infections from email-borne viruses such as ransomware and malware
- Stop employees from leaking confidential information
- Prevent accidental data loss or acquisition that may result in a fine
- Block inappropriate content from being circulated

With the right email security solution in place these risks can be minimized without it impacting on an organization's ability to conduct business. To help determine what's required from a solution, we've put together a six-step guide to email security best practice.

STEP 1

# Determine What Data Needs to be Protected

Since the GDPR regulation came into force, the Information Commissioner's Office (ICO) has issued numerous fines for data breaches including significant penalties for high profile companies such as British Airways, Marriott Hotels and Google. These fines serve as a warning to organizations to take their data protection seriously. Rules to mitigate the risk of regulatory non-compliance (and the damage to reputation that goes with it), must be defined and enforced. The first step in this process is to look at what data needs protecting. This might include, but is not limited to:

- Personal identifiable information (PII) about employees and customers (or patients if a healthcare organization)
- Information such as customer bank or credit card details (PCI)
- Corporate financial information
- Product designs and intellectual property
- Top secret or classified information

Email security solutions with the ability to automatically detect and redact sensitive data from incoming and outgoing communications will allow organizations to collaborate without disclosing sensitive information such as customer credit card details. Employees are protected when accidents occur and so is the organization if unwanted sensitive data is received. A solution that offers encryption is another way to protect sensitive data – where emails containing PII or PCI data, for example, are automatically encrypted (see step 5 for more details).

STEP 2

# Be Clear About the Dangers

An organization must have a clear understanding of the threats it's up against before determining what email security strategy is needed. Knowing what needs to be prevented, allows organizations to ask the right questions when looking for a suitable email security solution. An email security solution that doesn't defend against the following is no solution at all:

- Malware/Spyware/Ransomware
- Business email compromise (phishing)
- Regulatory breaches (GDPR, PCI, HIPAA, etc.)
- Unwanted data acquisition
- Unnecessary file types
- Hate mail and pornography


In the first half of 2019, **4.1 billion records** were publicly reported as compromised as part of more than 3,800 data breaches – a **54% increase over the first half of 2018**. (Norton). Email (contained in 70% of exposed records) and passwords (contained in 60% of records exposed) were at the top of the pile. (Forbes)

The average pay-out for cybercriminals targeting individuals and businesses increased to over **$41,000 in Q3 of 2019**, a growth of 13.1% over the previous quarter. (Data Breach Today)

STEP 3

# Establish a Robust and Sustainable Email Security Policy

An email security policy should set the parameters within which employees can, should and do use data and email within the organization. The policy should be:

- **Seen** – an effective policy is seen at induction, and visible on bulletin boards, in cafeterias, company newsletters etc.
- **Clear** – easy to understand, with very little room for interpretation
- **Consistent** – applied over all messaging traffic, including internal, inbound, and outbound emails
- **Appropriate** – recognize that different users, departments, and locations use email differently (while sharing common ground)
- **Reviewed regularly** – reflecting continuous feedback from all areas of the business
- **Flexible** – with the ability to evolve as the business changes or as threats emerge

An email security solution that's easy to deploy, monitor and manage will help support and enforce the policy in a way that doesn't over burden the IT department, email administrators or messaging teams. Features such as the ability to handle all threats from a single interface and have employees manage their own quarantine list will help increase the efficiency of the solution and ultimately free up time for IT teams to spend on other projects.

STEP 4

# Close the Zero-Day Window

Anti-malware solutions are great for defending against known dangers. But what happens if a brand-new virus tries to enter a network before security loopholes have been identified?

This 'zero-day' window is one of the most glaring vulnerabilities in many organizational email strategies. And there's only one way to defend against it: content filtering with intelligent rules.

Email security solutions that can filter and analyse the content of messages and attachments to identify the characteristics of malicious content will go a long way to achieve this. Even seemingly benign files such as Microsoft Word and Adobe PDFs can carry harmful macros and scripts. A robust filtering engine will analyse content down to its smallest parts. If active content or executable files are identified, the solution applies the relevant policy created to deal with the problem in real time. This might be to remove the offending active content (through structural sanitization) and allow the communication to go on its way, or to block it, delete it, or report it – or a combination of these approaches. It must not be allowed to get through untouched.

STEP 5

# Encrypt Sensitive Data

As a last line of defense to protect employees from accidentally sending important information to unauthorized parties, and to ensure continued compliance with strict regulations, organizations should automatically encrypt email messages that contain sensitive data. Many email security solutions offer proprietary encryption methods that are complex to use and expensive. Others provide a range of easy-to-use policy-based encryption options including TLS, PKI technologies such as S/MIME or PGP, Web-portal or password protected messages.

Organizations looking to control access to corporate data once it has left the organization should consider an email security solution that offers eDRM (Enterprise Digital Rights Management) capability. eDRM defines what the recipient can do with the data (i.e. edit, print, or copy, etc.) and how long they have access to it. It is commonly used in industries such as banking, financial services, manufacturing, pharmaceutical and legal that regularly share high value information in their supply chains.

STEP 6

# Monitor Traffic Behaviour and Performance

The saying 'you can't secure what you can't see' is very true when it comes to email security, which is why reporting is such a vital part of the process. If email behaviour and performance issues are flagged, swift action can be taken. For example, behavioural reports can be used to monitor employees that send and receive large numbers of emails, along with the type and size of the files sent. This information might prove invaluable when identifying problem areas, allowing the organization to shape policy and reallocate resources if necessary. Blocking the number of attachments or files of a certain size, will also protect storage and bandwidth resources. Set a policy to either strip out large files or park them for later delivery.

Email security solutions that provide detailed audit trails help IT teams investigate potential breaches. Those that export data to SIEM systems allow organizations to get a 360-degree view of the data flowing in and out of the organization.

# Summary

These steps summarize a simple approach to best practice in email security. While the technologies to defend against emerging threats and data loss may have changed, the basics have not: define a clear email security policy and enforce it with the right technology.

**Why Clearswift?**

Clearswift has helped organizations protect and secure data for over 25 years. Using award-winning adaptive redaction technology, its email and web security solutions offer organizations the ultimate protection against cyber threats and data loss, without compromising day-to-day collaboration.

**www.clearswift.com**

## Next Steps

**The Clearswift Secure Email Gateway offers:**

- Integrated malware and spam protection
- Zero-hour active code detection
- Adaptive data loss prevention, including data redaction, document & structural sanitization
- Automated encryption

Contact us for help defining your email security policy or to find out more about our Secure Email Gateway.

LEARN MORE

clearswift

A HelpSystems Company

## About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.



DB04CSGD20