DataMotion / Email Security Policies That Work

By Brian Wood, CISSP

Best Practices for Defining, Developing & Implementing Outbound Email Security Policy

Security policies protect your company, your clients, your data and your staff from noncompliance nightmares. With so much at stake, you want to implement best-in-class practices when developing, defining and implementing your security policies.

In this white paper we will outline the best practice steps that will keep the information you transfer internally and externally safe and encrypted. We'll also introduce you to automatic filtering of outbound email messages and file attachments by using content filtering technology, including "exact matching" - a cutting edge best-practice that minimizes outbound security risks.

Understanding the regulatory requirements that impact your business will help you understand what kind of data to protect. Follow the links below to identify which federal mandates apply to you and what data each set of rules requires that you protect:

- ***HIPAA***
- ***GLBA***
- ***PCI***
- ***FERPA***

Best Practice Tip 1: Know What's Driving Your Policy

In order to implement effective policies you need to know what factors, internal and external, are driving the need to secure your data.

Depending on your industry and business you might be impacted by government and industry regulations like HIPAA, PCI, GLBA and FERPA. If that is the case, then fear of noncompliance may be what's driving your need to develop policies.

Another reason companies and organizations lay out security policies is to protect themselves from a cyber-attack or security breach. According to Ponemon Institute, these events can be costly with average breaches costing around $244M in cleanup funds. They also come at the expense of a tarnished reputation and loss of customer confidence.

Best Practice Tip 2: Assemble Your Troops

Best-in-class companies know that security policy isn't the job of one person. They involve all of the necessary positions and departments from the beginning.

To determine who in your organization should be a part of these discussions ask yourself these questions:

+ Who can lend valuable knowledge about defining our policies?
+ Who would be responsible for enforcing our policies?
+ Who touches the data we need to secure on a regular basis?

Involving everyone up-front means that you won't have to backtrack and make unnecessary changes down the road. Be sure to consider people from your legal, compliance, HR, IT and even marketing departments. Marketers can help translate policies into layman's terms for your end users and help "sell" them on policy compliance.

Best Practice Tip 3: Identify Your Data

With your team of experts assembled, identify the data that needs protecting. This step will be driven by the reasons you outlined for needing policies, which are discussed in step one.

Some data sets, like social security numbers, are obviously sensitive and apply to most organizations. Other sensitive data may be specific to the organization, such as an account number or an entire department whose communications need to be protected and encrypted.

In this step identify and understand what data it is that you do not want others to see and why.

Best Practice Tip 4: Forget About Patterns, Match Sensitive Data Exactly

Filters search for patterns in outbound messages and secure the content when those patterns are found. The problem with this functionality is that one keystroke can unbreak a pattern and then private information gets sent unsecured.

Best-in-class companies strive to match your own data and not a pattern of what the data should look like. For example, you may know that an account number has 2 letters followed by 6 numbers. But instead of writing a pattern match to look for that, set your filters to look explicitly for your account numbers in the messages and KNOW that they are secure.

Best Practice Tip 5: Know Your User

In order to ensure that your policies are adhered to, you need to understand the end user experience and know who your end users are. This can have a huge impact on whether or not your policies are followed. To keep it simple, make sure policies integrate and work within your existing business processes. Making the user change behaviors to add security means the user has a harder time getting their job done, and is then resistant (and resentful) about the change.

Best Practice Tip 6: Combine Protection & Policy

Whenever possible, try to layer your protection in the policy creation. For example, providing your users a way to explicitly mark an outgoing message to be sent securely benefits you in terms of message load (those tend to be very quick filter checks) and also by providing a first pass security checkpoint.

Users can serve as the first step to identify what outgoing data needs security. Often times they know that some data should be sent securely even if it doesn't conform to filtering rules (ie, an improperly formatted SSN). This increases your success rate of sending the right data securely by combining user knowledge and company policy.

Best Practice Tip 7: Remember to Keep It Simple

Regardless of how bulletproof you develop your policy plan, your rules won't be followed if they are too complex. For maximum policy compliance, keep your policies clear, concise and short. To make sure they are understood start by outlining why you have the policies and what the dangers and risks are if they are not followed. And make sure they adhere to your business processes and do not interrupt the daily flow of work for your end user.

CONTACT US WITH QUESTIONS:
Toll-Free: 1.800.672.7233 Tel: 1.973.455.1245 Fax: 1.973.455.0750
Email: info@datamotion.com www.datamotion.com
DataMotion, Inc. 35 Airport Road Morristown New Jersey 07960

Best Practices for Writing Filter Policies

- Do not make policies that are broad or very general. It will cause a lot of false positives and make diagnosis difficult.
- Try to minimize the number of messages your filters apply to. Some users have different requirements and may not need every filter applied to their email, or they may have specific needs that are unique to them and not necessary to apply across the board.
- The fewer filters you have the better. False positives mean extra hassles for your recipients, so you don't necessarily want to turn on every possible rule. Also, every rule that is not relevant but must be scanned adds to the time it takes to move an email through the system. For example, a financial institution likely has no reason to search for ICD-9 codes.
- Start small and move up/out. Scanning takes CPU time, and the more effort you need to put into the scan, the fewer scans you can do or the longer they take. Do the simplest rules that are very specific first to minimize the load as matches are made.
- Exit immediately on a match. Once a match is made, there is no reason to continue scanning the message. You have already determined it needs to go secure. One match or 100 matches in the same message lead to the same result of needing to go secure, so don't waste time continuing scans once you have a positive match.
- Use Subject line tagging when possible. Users generally know when things need to go secure (and sometimes do even when a filter will not). Subject line tags are easy to implement (such as by an email client add-in, manually typing the tag or by macros or other built-in tools), and finding the tag is a very quick, low power search since the content filter does not need to search anything past the subject line (such as the message body or attachments).
- Make sure you consider attachments. Attachments can have a lot of sensitive information that is not readily viewable within the message. It is important to be able to scan attachments as well as the message body to ensure matches.
- Consider the email clients sending the messages. Especially when using tagging, you should consider how a sender can easily tag an outbound email as needing to go secure when on their iPhone.
- Leave users an OUT when necessary. Sometimes users understand that something in their message is likely to get caught by a filter and be sent secure when it shouldn't be for some reason. Leave the users with a way to explicitly send an unsecure message, and then monitor the usage (say by keeping a copy of any message using this out and letting you know it was done) to ensure proper usage and compliance.
- Use exact matching when possible. If it is possible to create a filter that matches your data exactly, instead of a matching pattern, the results will always be much better. A list that can be dynamically updated as the information changes is ideal.

About DataMotion

DataMotion enables organizations to dramatically reduce the cost and complexity of delivering electronic information to employees, customers and partners in a secure and compliant way. The company's core DataMotion Platform solves a broad range of business issues by providing a secure data delivery hub. The company's easy-to-use solutions for secure email, file transfers, forms processing and customer contact leverage the DataMotion Platform for unified data delivery. Millions of users worldwide rely on DataMotion to transparently improve business processes and reduce costs, while mitigating security and compliance risk. DataMotion is privately held and based in Morristown, N.J.

ABOUT DATAMOTION

DataMotion provides secure information delivery solutions that enable organizations to easily transact with partners and customers over the internet. Our solution helps customers achieve regulatory compliance through visibility, security and reporting of data in motion. Core applications include encrypted e-mail, file transfer and electronic forms.

CONTACT US WITH QUESTIONS:
Toll-Free: 1.800.672.7233 Tel: 1.973.455.1245 Fax: 1.973.455.0750
Email: info@datamotion.com www.datamotion.com
DataMotion, Inc. 35 Airport Road Morristown New Jersey 07960