SilverSky
SECURITY FROM THE CLOUD

White Paper

Five Strategies for Email Data Loss Prevention

Andy Jaquith is the CTO and Senior Vice President of Cloud Strategy at SilverSky. Prior to his work at SilverSky Andy was the lead data security analyst at Forrester Research focusing on data security topics including DLP. At Forrester Andy conferred with hundreds of customers annually on how to best manage their data security policies. Andy is also the author of "Security Metrics" which focuses on best practices for measuring your security policy. Andy has been featured in several publications including but not limited to CSO, Forbes, Business Week and Information Week.

Summary

Email is the primary source of communication for most organizations and their employees. Everyone has email, everyone uses email and it not only serves as a method of communication but can act as a de facto knowledge management system as well. Keeping both personal and organizational information secure should be a top priority for IT staff.

The average employee sends and receives about 110 emails each day or 29,000 emails per year . One in every 20 of those emails contains "risky" data – from sensitive attachments to social security numbers to protected health information to valuable corporate secrets that set your organization apart. All of this risky data can become toxic to your company if it's hacked or suffers a breach – causing reputational damage, customer loss, heavy fines and decreased competitive edge.

For a 1,000-employee company, that means at least 1.5 million risky emails per year must be reviewed, blocked, encrypted or archived. SilverSky's Email Protection Suite and Email Data Loss Prevention (DLP) capabilities can help relieve some of the pressure on your employees and IT staff.

Here are five simple steps from SilverSky CTO Andy Jaquith on best practices you can take today to help prevent sensitive information leakage, while keeping up with the rapidly evolving regulatory environment:

1. **Measure Violations and Set Targets**
2. **Filter Toxins Out of Your Email**
3. **Let Employees be Your Eyes and Ears**
4. **When In Doubt, Encrypt and Notify**
5. **Communicate your policy**

1. Measure Violations and Set Targets

You have to be able to measure something in order to manage it. Email DLP can be used to help track and report on violations over time, while monitoring progress across individual units. To properly measure violations you should view your reports based on business units, regions, or another identifier. Tracking metrics across different parts of the organization creates a virtuous cycle of friendly competition, and over time you'll begin to see that your each business unit within the organization is nearing or reaching their target metric. Using SilverSky's Email DLP solution you can tag specific violations in your policy, for example the inclusion of a Social Security Number in an outbound email, and track those violations across your organization over time. Even if the competitive approach is not the right approach for your organization, tracking violations and viewing monthly reports is helpful in determining the ongoing success of your policy.

How to know when you are successful: To avoid drawing in data, it is recommended that you measure violations on a monthly basis. As your staff becomes more comfortable with your policy, violations should decrease.

2. Filter Toxins Out of Email

Many companies spend too much time concerned with incoming traffic and protecting themselves against viruses, worms and botnets. While those things are important, it's the critical information flowing out of their organizations that represent the greatest risk – first/last names combined with social security numbers, protected health information, financial account numbers, credit card numbers and other government identifiers. Increasingly stringent state, federal and contractual mandates also underscore the importance of securing outbound communications.

Outbound content filtering or email DLP solutions can help block, quarantine, redact, or automatically encrypt inappropriate and risky messages using the highly tunable policy-driven rules engine. SilverSky's Email DLP solution makes building and enforcing granular policies a breeze. The basic content control allows customers to block critical outbound information such as credit cards and social security numbers, while our leading DLP technology, with features like content-aware fingerprinting and proximity checking, full redaction capabilities and the ability to test policies before deploying them allows for fine-grained actions that ensure the industry's highest level of data protection.

How to know when you are successful: In order to accurately gauge how well your email filters are working you should also utilize the tip number one, "Measure Violations and Set Targets." At the time your organization implements its outbound content filtering policy you may see an increase in violations as employees need to adjust to the new policy. Over time these violations should decrease and employees and admins will spend less time grooming their quarantines to release or delete messages.

3. Let Employees be Your Eyes & Ears

Your email administrators or compliance officers cannot possibly be all-seeing, all-knowing content censors. You need your employees to be an extension of your IT staff. When creating rules for your policy you can allow employees to justify or self-release any outbound emails that fall into gray areas – when the intent of an email is not a direct violation of your policy. Allowing your employees to justify the release of a message is a good practice because employees know best what is legitimate and what is not legitimate. If you require them to justify their actions, you policy is less restrictive and you have something that's logged for posterity. This has the added benefit of not impacting productivity.

How to know when you are successful: When the email administrator or compliance officer and your employees can be spend less time managing their quarantines. Also, employees will begin to self-police the content of their own emails, over time justifications should also decrease.

Creating the Right Policy: When creating a new policy it can be a challenge to prioritize exactly what needs to be deleted, blocked, quarantined or logged to satisfy the increasingly stringent regulatory environment. A good baseline is to block Social Security Number's and PCI (Payment Card Information)– this will comply with multiple regulations. HIPPAA requires that you block out insurance numbers, first and last names, etc. Each organization has Federal, State and Local regulations to follow and we recommend that you create policy in that order. By meeting requirements for Federal regulations you will likely satisfy requirements for State and Local regulations as well. Keep in mind that there is no law or regulation that requires you to protect industry trade secrets, but it is a good practice to do so. As mentioned in section 5 on communicating your policy you want to keep your policies clear and concise. A potential web security policy might read, "We don't block the sites you visit – but we log and regularly review all web activity."

4. When in Doubt, Encrypt and Notify

Often times, it's simpler to encrypt an outbound message that may go against policy and notify the sender than it would be to involve the message in quarantine activity. This allows employees to send email without spending unnecessary time in the quarantine. By notifying the sender, they are aware of how they have violated the policy and you create more incentive for employees to self-police their content. SilverSky recommends that when creating your encryption rule you add multiple actions: notify the administrator and sender of the message and encrypt the message. With this rule in place employees will recognize the importance of vigilance, and will think twice before sending sensitive information outside of the company.

How to know when you are successful: With this rule in place, both the admin and employees should spend less time in the quarantine. You will know that this policy is really working when the employees begin to self-police and the number of encrypted emails being sent due to rule violations decreases.

5. Communicate Your Policy

This is critical for every organization looking to get started with a DLP program. If your staff does not understand the policy they cannot be expected to follow it correctly. A good starting point is partnering with a member of your HR staff to write a simple, concise memo explaining the policy. Creating your policy can be a delicate process as you want to create a policy that is brief and concise, without being too vague. You need to cover all required areas effectively without boxing yourself in. Effective communication smooths the road to acceptance and promotes your security program within the organization. Employees who fully understand the policy goals will more readily accept the policy.

How to know when you are successful: Instituting a new policy will be an adjustment for your entire organization. By effectively communicating your policy there should be quicker turnaround within the organization on what is acceptable and policy violations should decrease quickly.

Takeaway

We hope that the tips above have been informative and will help you with the challenge of protecting your customers and employees' sensitive information and that by using these tips you will enhance security and regulatory compliance without having to add staff.

SilverSky's Email Protection Suite and Email DLP solutions can help your organization implement new policies quickly and efficiently.

Compliance: Whether an internal company standard or a regulatory requirement, compliance is about knowing your email and data are protected to a specified standard—and having proof. The external requirements can be tricky, and you don't want to run afoul of them. If you can't comply with regulations, fines and bad press could be in your future. But, ultimately, the biggest loss could come to your business. SilverSky can help your company comply with strict regulations, including but not limited to:

- **Federal Financial Institution Examination Council (FFIEC)**
- **Federal Rules of Civil Procedure (FRCP)**
- **The Health Insurance Portability and Accountability Act (HIPAA)**
- **Securities and Exchange Commission (SEC)**
- **Gramm-Leach Bliley Act (GLBA)**
- **Family Educational Rights and Privacy Act (FERPA)**

About SilverSky

SilverSky is the expert cloud provider of information security solutions. We deliver the industry's only advanced Security-as-a-Service platform that's simple to deploy and transformational to use. For years, SilverSky has been recognized as a leading managed service provider of business email and network security services (2012 Top Player for Hosted Email and Collaboration (Radicatti Group), 2012 Top Player for Microsoft Hosted Exchange (Radicatti Group), 2013 Emerging MSSP Leader with top marks for strategy and strength of offering (Forrester), Scored 5/5 for 2012 and 2013 R&D Investments (Forrester), supervised by FFIEC). We have hosted, secured and monitored the information assets of thousands of large enterprises and regulated businesses utilizing our proprietary security software. By tirelessly safeguarding our customers' most important information, we enable growth-minded leaders to pursue their business ambitions without security worry.

If you would like to learn more, please do not hesitate to call at 800.234.2175 Option #2 or visit our web site at silversky.com