Cisco Email Security Image Analysis: Protecting the Network from Explicit Images

Challenge

Eighty percent of the world's business communication takes place on email, making it the primary communication method for organizations of all sizes.[1] Along with the business advantages email provides, however, are significant risks from email being used intentionally or otherwise as a form of sexual harassment.

Employees sending and receiving sexually explicit content via a corporate email system is a serious concern and a security threat. Unchecked, such email can damage a company's culture and contribute to the creation of a hostile working environment, exposing the business to legal liability.

"The proliferation of pornography and demeaning comments, if sufficiently continuous and pervasive, may be found to create a hostile working environment."

– U.S. Equal Employment Opportunity Commission

Most employers have a legal duty to protect their employees from sexual harassment. They can be held liable for the actions of their employees and may face adverse financial consequences. To avoid liability, an employer must demonstrate they have taken all reasonable steps to prevent a hostile work environment.

At a minimum, an employer is expected to have an email acceptable use policy that is effectively **enforced, monitored,** and **communicated**. A written policy on its own, however, is insufficient. A policy that is not implemented through communication, education, and enforcement will be of little or no use in discharging liability.

*"An effective preventive program should include an explicit **policy** against sexual harassment that is clearly and regularly **communicated** to employees and effectively **implemented**."*

– U.S. Equal Employment Opportunity Commission

Lack of awareness that harassment was occurring is not in itself a defense for employers. Ignoring the issue can have repercussions that, in addition to damaging the company's bottom line, could even extend to criminal charges against the employer if illegal imagery is involved. By taking proactive measures to monitor, educate, and enforce policy, the employer can significantly mitigate the risks of:

- Damage to the company reputation and brand
- Fostering a hostile work environment
- Reduced productivity
- Sexual harassment lawsuits
- Criminal lawsuits

[1] Source: Radicati, 2011

Solution

The Cisco® Email Security Image Analysis solution filters sexually explicit image attachments and can be licensed for use on the award-winning Cisco X-Series and C-Series Email Security Appliances or via the Cisco Cloud Email Security service. The technology assists businesses with demonstrating duty of care by allowing employers to:

- **Identify** emails containing high-risk image attachments
- **Monitor** users that are misusing the email system
- **Educate** users on the company's email usage policy
- **Enforce** the policy as and when required

Figure 1. Cisco Email Security Image Analysis uses 12 different detection layers to identify explicit content in both incoming and outgoing email.

Features

Cisco Email Security Image Analysis delivers the control to identify, monitor, educate, and enforce email image policy.

Identify

Multilayered detection engine. Cisco Email Security Image Analysis uses 12 different detection methods to identify explicit images hidden within the mass of legitimate business images traveling through the email gateway.

First-generation image analysis technologies were overly reliant upon inaccurate "skin tone" analysis techniques. A common complaint about such solutions was the high number of false positives. Cisco Email Security Image Analysis has relegated this element to a minor part of a more sophisticated decision making process that delivers accurate detection with very low false positives.

Embedded image scanning. Cisco Email Security Image Analysis allows inspection of the following types of attached and embedded files: JPEG, BMP, PNG, TIFF, GIF, TGA, and PCX. If the image is embedded in another file, Cisco's content scanning engine extracts the file. The content scanning engine can extract images from more than 400 file types, including Word, Excel, and PowerPoint documents.

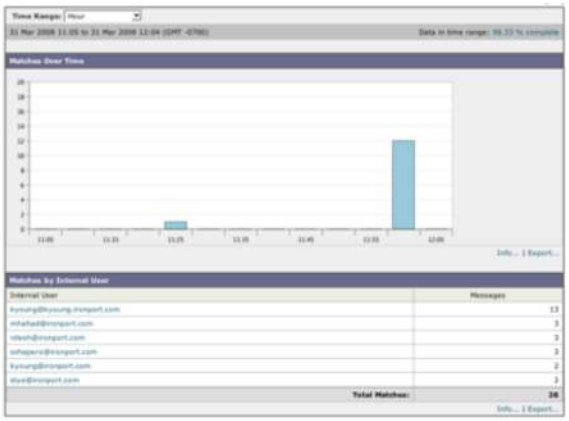
Adjustable sensitivity. The sensitivity setting allows the administrator to adjust the aggressiveness of the engine to suit their unique requirements.

Monitor

Management reports. Many network administrators admit that they do not know if or when inappropriate image content is flowing across the network. Cisco Email Security Image Analysis allows administrators to generate management reports that provide visibility into any misuse in both incoming and outgoing email traffic. Based on filter matches, administrators can use the existing reporting functionality and create easy-to-use reports in both PDF and CSV formats. These reports can be generated “on demand” or scheduled for automatic generation and distribution to other departments, such as human resources.

Figure 2. Content filter reports show inappropriate or suspect images caught in incoming and outgoing messages by specific user.

Cisco Email Security Image Analysis gives administrators visibility into inbound and outbound message content.



Quickly zero in on users with the highest match on the policy filter.

Educate

Email notifications. Cisco Email Security Image Analysis gives administrators the option to send users a customized email notification when they breach the policy. These notifications ensure the company’s acceptable use policy is clearly and regularly communicated to users and acts as a powerful tool for discouraging misuse in the future.

Enforce

Policy integration. Cisco Email Security Image Analysis integrates with message and content filters to enable policy-based filtering on a per-recipient or per-sender basis. The existing filtering infrastructure allows for multiple actions to be combined based on a single filter match. For example, if the engine detects an explicit image in an email, multiple actions (quarantining or stripping the attachment, stamping the image with a company policy message, etc.) can be performed.

Benefits

Gain peace of mind. Many companies have limited visibility into the type of images being exchanged via the corporate email system. Cisco Email Security Image Analysis gives companies peace of mind that their email system is compliant and being used appropriately.

Avoid legal liability. In cases involving a hostile working environment, U.S. Supreme Court rulings have held employers liable for actions of employees. Based on data collected by the U.S. Equal Employment Opportunity Commission, the average sexual harassment verdict against employers has been more than $250,000. Even in cases where employers have successfully defended themselves from such claims, the legal costs have averaged about $100,000. However, court rulings and laws have indicated that an employer may be able to avoid liability or limit damages if it has taken best efforts in exercising reasonable care to prevent and promptly correct any harassing behavior. Cisco Email Security Image Analysis provides various detection, reporting, and policy enforcement features that can help employers defend themselves in such situations.

"In fiscal year 2010 the EEOC obtained a record $404 million in compensation from employers."

– The U.S. Equal Employment Opportunity Commission

Preserve brand image. Companies spend millions of dollars to develop a brand identity and project that image worldwide. In financial, government, and medical establishments, the image is conservative, professional, and, in the case of local government, publicly funded. For large retailers, a "family friendly" image is important. The effect of negative publicity upon these carefully crafted brand images can be serious, potentially leading to adverse publicity and lost revenue. Cisco Email Security Image Analysis enables employers to proactively thwart such threats by constantly monitoring corporate email messaging and taking necessary remediation steps.

Protect employees. Companies need to take proactive measures to protect their employees from their own behavior and preserve their company culture from the damaging effects of inappropriate email content. Cisco Email Security Image Analysis gives companies the tools to proactively eliminate threats before they become pervasive throughout their organization.

Improve productivity. Proactively managing explicit image content in a workplace encourages a compliant and safe working environment for all, removing the temptation to indulge in non-work-related activities on company time, positively impacting productivity.

International Laws and Regulations

The following may count as sexual harassment; the display of pornography or the circulation of obscene material by email. – United Kingdom Equality and Human Right Commission

Sexual harassment can take many different forms and may include sending sexually explicit emails.
– Australian Human Rights Commission

You may have been sexually harassed if you are shown sexually offensive pictures in the workplace.
– New Zealand Human Rights Commission

Conclusion

The distribution of pornographic and inappropriate images in corporate networks represents a significant business risk to employers. Identification of offending users and enforcement of company policies are important steps in protecting organizations against the legal liabilities and brand degradation that can arise from such offenses. Cisco Email Security Image Analysis is an easy-to-use solution that detects and controls explicit content before it enters or leaves your organization.

For More Information

Through a global sales force and reseller network, Cisco offers a “Try Before You Buy” program. The 30-day free trial of Cisco Email Security Image Analysis with Cisco Email Security will give management complete visibility into any misuse of the corporate email system. Visit http://www.cisco.com/go/emailsecurity for more information.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C22-719504-00 10/12