Cisco Provides Analysis and Management for a Leading Financial Institution

EXECUTIVE SUMMARY

EBS BUILDING SOCIETY AT A GLANCE

Headquarters: Dublin, Ireland

Employees: 665

Members: 450,000

Business: Mutually held financial institution that provides mortgages, insurance, personal lending, savings, investments, credit card services, and more

Total Assets (2007): €19.5 billion

THE CISCO IRONPORT ADVANTAGE

- Accurate detection and classification of illicit images and content
- Minimized exposure to legal liability as well as loss of brand image and reputation
- Easy management with maximum visibility into acceptable-use policy violations
- Complete integration with content filtering and reporting infrastructure
- Nonintrusive, reliable results for superior user satisfaction

Overview

Serving 450,000 members, EBS Building Society provides a comprehensive range of financial services, including mortgages, savings and investments, pensions, personal loans, credit cards and insurance. The Dublin-based organization operates through a network of offices across Ireland.

EBS places a premium on the trust it has earned through its many years in business. It has also been recognized as one of Ireland's top places to work. With an eye on sustaining its market appeal and the loyalty of its more than 600 employees, the company turned to Cisco® to provide it with robust protection against a rising tide of illicit images and content.

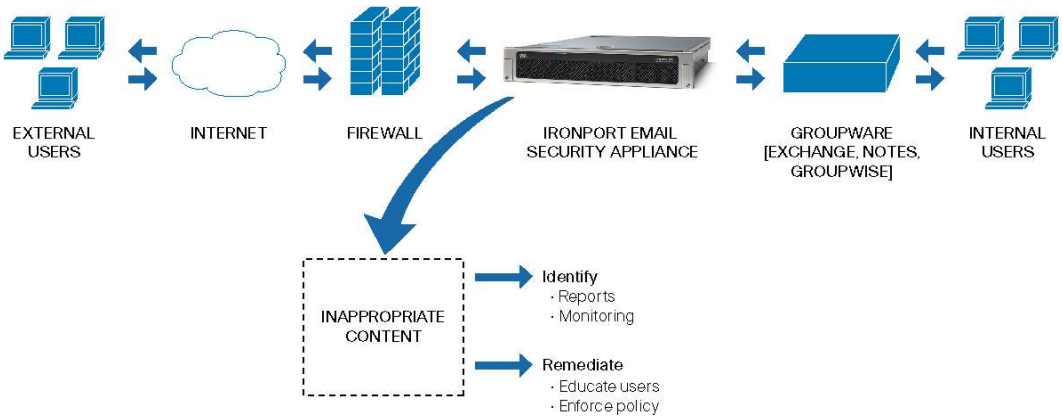
The Situation

With a trusted brand built on a long history of providing quality products and service, EBS Building Society is one of Ireland's most respected financial organizations. However, in recent years, the email-based proliferation of illicit images posed a serious threat to its hard-earned market stature as well as the safety and security of its employees and members. Based on its satisfaction with its existing Cisco IronPort® C-Series Email Security Appliance, the organization looked to Cisco for a new means to combat these increasingly complex threats.

Technical Challenges

With roughly 1200 users on its system, EBS realized that manual detection of suspect images was an unsustainable task given the drain on productivity and probability of human error (which continually posed the risk of allowing inappropriate content to infiltrate its network). The company needed a more efficient means to analyze the threats posed by external users who create, upload, and share inappropriate images. Employers are required to provide a safe work environment for their employees, and block message content that can compromise their brand identity or reputation in the market. With that in mind, EBS sought a powerful resource that would accurately identify inappropriate content at the gateway, and maintain it in quarantine until its risk could be evaluated. After a rigorous two-month trial, EBS selected Cisco IronPort Image Analysis (Figure 1).

Figure 1. Cisco IronPort Image Analysis—Advanced Technology for Monitoring Incoming and Outgoing Email



"Overall, Cisco IronPort Image Analysis has been a very useful product. Prior to deployment, we relied on manual detection of unwanted attachments. This was a major drain on productivity and continually posed the risk of allowing inappropriate content to breach the internal network. Cisco has enabled a significantly more robust monitoring process."

— David Cahill, Information Security Specialist, EBS Building Society

The Cisco IronPort Advantage

The distribution of problematic images via email, particularly offensive graphics, jeopardizes organizations worldwide. Cisco IronPort Image Analysis has emerged to help ensure enterprises' enforcement of acceptable-use policies and ultimately to preserve the integrity of their reputation in the marketplace.

Integrated into the award-winning Cisco IronPort C-Series Email Security Appliance, the Cisco IronPort Image Analysis solution has enabled EBS to prevent illicit images from entering its network. EBS has been able to identify traffickers and dramatically reduce the amount of time spent protecting the network from such threats.

The system draws on 11 different detection methods to render a verdict on suspect attachments. It has easily configurable settings that give administrators full control to determine what actions to take on a particular message. Additionally, embedded image scanning enables a rigorous inspection of attached and embedded files, including JPEG, BMP, PNG, TIFF, GIF, TGA, ICO and PCX Files. The Cisco IronPort scanning engine can extract images from more than 400 file types, including Microsoft Word, Excel, and PowerPoint.

Cisco IronPort Image Analysis is easily aligned with message and content filters to allow policy-based filtering and reporting on senders and recipients. When an illicit image is detected within email, a variety of actions can be taken, including stripping the attachment from the message or stamping it with a company policy message. EBS was particularly pleased with the technology's ability to remove a suspect image from a message, while still allowing the message's text to be delivered to its intended recipient.

EBS estimates that approximately 40 percent of all email traffic attempting to enter its network contains inappropriate image content. Since deploying Cisco IronPort Image Analysis, the company reports that 99 percent of that bad content has been blocked. The management time allocated to combat this problem has also been dramatically reduced from several days per week to only a few hours. Cisco enables EBS to protect its users and itself.

This document was originally published in 07/08, and is being republished with limited, non-substantive updates in 08/10.

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 C36-599573-00 08/10