



Case Study



Version 1.1: February 9, 2011

Presented by: Adam Veriker & Lianne Pitcher

Case Study – Ironshore & MessageLabs

Client Company Profile

Ironshore is a relatively new insurance company, incorporated in late 2006. Following a successful first year, achieving \$317 million in Gross Written Premium (GWP), expansion and partnerships occurred quickly in different fields of insurance such as health, environment, energy, construction, property, casualty and professional liability. Ironshore has offices located in the United States, Canada, United Kingdom and Bermuda with approximately 800 employees worldwide.

Ironshore has become one of the fastest growing companies in the insurance industry, with an excellent rating in the industry classification. With over a billion in capital and over 26 years of collective experience, Ironshore is quickly emerging as a recognized leader in the reinsurance marketplace.

MessageLabs Partner Profile

Computer City became the local MessageLabs partner in 2007. MessageLabs leads the industry in managed cloud-based email security with more than 11 million end-users worldwide. MessageLabs recently merged with Symantec, expanding their portfolio to include new services such as hosted internet security in addition to their traditional email protection, archiving and encryption services.

Business Situation #1

Ironshore's rapid growth in employees, combined with the often sensitive client financial information being exchanged, caused the technology team to re-evaluate their approach to email protection. Ironshore recognized the consistent, continuous and increasingly sophisticated threats that malware, spyware and phishing attacks represented to their business. Spam (unsolicited email) volume had also increased to the point where Exchange policies and Junk Mail folders alone were unable to contain it. Ironshore needed a robust, secure and customizable email protection solution that would be transparent to users, avoid burdening their systems and network, and flexible enough in deployment and pricing to meet their consistent user growth.

Business Situation #2

Ironshore later identified further need for certain very sensitive information to be protected even beyond the boundaries of their corporate network. They wanted a way to encrypt the content of these emails to ensure it could only be seen by the intended recipients. However, they did not want the responsibility of encrypting emails left solely to the user and did not want to encrypt all emails, so they needed a solution that would intelligently and automatically encrypt emails containing specific sensitive info, like account numbers, while still allowing users to manually encrypt other sensitive emails if needed. Similarly, this solution needed to be almost transparent to users and avoid burdening their systems and network, and obviously needed to be compatible with their email protection service.

Solution #1

MessageLabs Email Protection Suite was implemented throughout Ironshore's offices in 2008.

The Email Protection Suite protects against all types of malware, spyware, phishing and spam. MessageLabs protects from outside the network, hosted in 'cloud' server clusters strategically located worldwide to increase service redundancy. Protecting from outside the network also removes the need for software to be installed on servers or clients.

Since the time Ironshore implemented MessageLabs Email Protection, all their spam has been quarantined offsite. Other features like Traffic Management and SMTP Heuristics have also eliminated the strain that was placed on their network bandwidth. Therefore, any illegitimate email traffic is immediately detected and rejected before it even reaches their network. Furthermore, the MessageLabs Spam Manager interface allows each of their individual users to govern their own quarantine protection. This personalized feature has significantly cut down on the number of support calls received by their technicians. Now that these reliable systems are in place to protect their network, Ironshore can continue with greater ease of mind to deliver top quality insurance services.

Solution #2

MessageLabs Encryption was implemented to an initial select group of Ironshore users in 2010.

The Encryption service automatically safeguards the security and privacy of sensitive emailed data.

MessageLabs Encryption enables the creation and enforcement of flexible rules in accordance with company policies and provides additional boundary protection to ensure against human error. This service also eliminates the hassles of managing keys or digital certificates required for traditional encryption. For end users, encryption is transparent and email can be delivered decrypted directly to their inbox, and replied to directly from their inbox with minimum assistance from technical staff.

Ironshore is now meeting and exceeding their compliance obligations and can communicate securely, easily and efficiently with clients and trusted partners.

Return on Investment

By implementing MessageLabs Email Protection Service and Encryption Service, Ironshore has recognized a reduction of up to 50% in time utilized by technical staff responding and managing email issues and updating servers with security software. There is a noticeable increase of approximately 20% in performance of servers and their network due to redirection of email bandwidth increasing the effectiveness of communication of employees and overall operations. The added security of encrypting and protecting sensitive financial and legal information increases the client's confidence in Ironshore thus increasing their business portfolio, in turn raising quarterly revenue.