

Jelf Introduces Webroot Email Security and Business Continuity Services

For Jelf Group Plc, a UK insurance broker and financial services consultancy with 55,000 corporate clients and 70,000 individual clients, protecting the confidential content of its emails to ensure that they can not be read by anyone other than the intended recipient is a key commercial and regulatory priority.

Business drivers

David Jones, Group IT Director, has seen the company grow from just 83 employees in two offices five years ago to more than 1,000 employees at 33 offices across England and South Wales. Managing an IT team of just 11 people, Jones recognises the importance of having a centrally controlled email security system that can apply the same rigorous policies across the company regardless of the office location.

“Our type of business sends information that is subject to the Data Protection Act, such as salary details, health reports, financial advice or insurance records. It is critical that we send this information securely,” says Jones.

The UK Data Protection Act requires that companies protect personal data, use it only for its intended purpose, keep it accurate and comply with several other data protection principles. Violators are subject to criminal prosecution.

“As a financial services provider we are governed by the Financial Services Authority (FSA), which states that we must ensure that the information we send is transmitted securely, reaches the intended recipient, and that there is a preserved audit trail.”

“Additionally, we have to protect the company from data leakage, such as commercially sensitive information being sent outside the company by an employee,” adds Jones.

Data security is taken extremely seriously by Jelf. A Data Security Committee comprising senior management meets quarterly, and minutes taken at these sessions are audited by the FSA.

Finding a solution

Jelf has relied on Webroot® Email Security Service for virus management and spam elimination since 2004. “As a hosted service, Webroot acts as a central repository for all our email, stopping 91% of incoming emails which equates to about 2.7 million emails a month. This means that we are not wasting bandwidth receiving and filtering out the 300,000 legitimate emails on-site,” explains Jones.

To meet the FSA guidelines on data security and to comply with the Data Protection Act, Jelf decided to choose a solution that allows all of its employees to encrypt emails, and which offers an archive of encrypted email that can be read by the administrator. Jones says: “As everyone within the organisation has the need to send confidential information, we needed a solution that could be used company-wide rather than restricting it to a few senior individuals.”

The Webroot Email Security Service offers policy-based encryption which automatically encrypts email messages based on company email policy as well as allowing users to also encrypt communications on an as-needed basis.

Where Jelf benefited

- Confidence that Policy-Based Encryption means information is not intercepted and read by a third party but reaches the intended recipient and can only be read by them.
- Email archiving. Meets requirements for complete audit trail including encrypted emails.
- Spam elimination. The system identifies and removes all the spam sent in. The company receives 100,000 emails per day on average but this can peak at 400,000. 91% of emails received are spam equating to about 2.7 million emails per month.
- Great support. A two-way relationship with Webroot staff offering advice.

"We wanted a system that could be easily integrated into our network. We only needed to make some simple DNS server changes before Webroot's service could be quickly activated."

Another important factor was the ability to design and apply rules within the Webroot platform. "With Webroot Email Security Service we can set rules to determine what type of email is automatically encrypted. For example, we may want to encrypt all email that has an attachment. It is also easy for an individual to encrypt a message by simply putting (*encrypt*) in the subject header."

"The FSA requires that the same standards are set and can be audited across the whole company, not just main offices. This is regardless of whether they are on our computer network or not. One of the attractions of the encryption service is the ease with which we have added all our users on to the service. All the offices are now migrated to the network, but as the company makes further acquisitions new offices will be added and it is good to know that we can deploy encryption quickly and easily."

Reducing risk

Failure to comply with the FSA guidelines can have devastating affects. The regulator has the power to fine companies hundreds of thousands of pounds. However, the report which the FSA publishes when it implements the fine can be much more damaging to the long term reputation of a company with its customers and partners.

"Though primarily we are concerned about our responsibilities and legal obligations as the sender of confidential information; our clients also have the option of replying to our encrypted email using our portal to encrypt their responses."



Webroot acts as a central repository for all our email, stopping 91% of incoming emails which equates to about 2.7 million emails a month. This means that we are not wasting bandwidth receiving and filtering out the 300,000 legitimate emails on-site

David Jones, Group IT Director



As probably one of the first financial services companies to become compliant, with Webroot's help, we are at the leading edge of maintaining data security

David Jones, Group IT Director



Preventing commercially sensitive information leaving the company is another issue for Jelf which is managed by the Webroot platform. "We have put in place rules which help us to trap data leakages preventing staff from sending out unauthorised information under encryption. Our employees sign up to our email policy allowing us to monitor email. If, for example, an email is going to a home address, a rule will be triggered which allows us to check that email."

In addition to the service's spam elimination and policy-based encryption capabilities, Jelf is also using image filtering to support its strict internal email policy. The company sets very high thresholds for embedded and attached images and video not only to protect staff from inappropriate material but also to safeguard the organisation from any potential liability.

Expert advice

"I am happy to say that we rarely need to approach Webroot Customer Support with a problem. Instead, we tend to go to them for advice about how we can best design a new rule, for example. They have been very open to hearing our thoughts on how the services could develop and I see our relationship with Webroot as very much two-way."

Leading the way

The FSA and Data Protection Act are clear about the financial and legal consequences of not securing email communications. "As probably one of the first financial services companies to become compliant, with Webroot's help, we are at the leading edge of maintaining data security," says Jones.

Webroot Software, Inc. – World Headquarters
2560 55th Street
Boulder CO 80301 USA
www.webroot.com • 800.870.8102

Webroot Limited – EMEA Enterprise Headquarters
Venture House, Arlington Square, Downshire Way,
Bracknell, Berks RG12 1WA, UK
www.webroot.com/europe • +44 (0) 870 141 7070

Webroot Software Pty Ltd. – APAC Headquarters
Level 20, Tower A, 821 Pacific Highway
Chatswood NSW 2067 Australia
www.webroot.com.au • +61 (0)2 8448 8144 • 1.800.029.234

© 2010 All rights reserved. Webroot Software, Inc. Webroot, the Webroot icon and the Webroot tagline are trademarks or registered trademarks of Webroot Software, Inc. in the United States and other countries. All other trademarks are properties of their respective owners.