

Email 999

NHS organisations across the United Kingdom increasingly rely on email as a primary communications method. While a significant proportion of IT budgets are spent annually on email security to protect employees, patients and the NHS healthcare infrastructure, current solutions cannot keep up with the rising amount and complexity of inbound threats such as spam and viruses.

Not only do NHS organisations need to consider the escalating cost and complexity of maintaining 'point products' for spam and viruses, but they must also ensure the security, integrity and confidentiality of communications outside the NHS.

Failure to secure email involves both direct and indirect costs. The inadequate protection against 'inbound threats' can lead to the collapse of an email infrastructure, or worse, a virus can bring down an entire network. But indirect costs are also taking their toll, including lost productivity and low employee morale from sorting through unwanted, offensive and even pornographic spam, not to mention additional capital expenditures to keep pace with the exponential growth of email volume.

In addition, as compliance and privacy regulations gain momentum, inadequate protection of outbound email communications can be costly and devastating.

Could you be liable?

Email has streamlined and improved the ability to communicate sensitive, time-critical information such as patient diagnoses, research activities and drug treatment programmes with other NHS organisations, hospitals, doctors, specialists, pharmacists and others. However, all of this information is highly confidential and, as a public authority

that holds records and information, NHS organisations are subject to the Data Protection Act and the Freedom of Information Act. This means that strict records management and controls are required for email because they represent an important part of an NHS organisation's corporate memory. Emails are subject to the same rules as other forms of recorded information, and are therefore subject to the NHS policies and procedures about how private information is managed and stored, ensuring that only the proper individuals or systems have access to private information.

Freedom of Information and Protection Act at-a-glance

What	Protect personal and confidential information held about individuals in any form
Who	All NHS organisations
How	Access control, authentication, message encryption, anti-virus
When	Freedom of Information Act was passed in Nov 2000 and full access granted in Jan 2005; Data Protection Act came into effect March 2000
Penalties	Contempt of Court and maximum sentence punishable is two years, imprisonment for the accountable officer

According to IDC Europe, by 2008, 80% of all security solutions will be delivered via a dedicated security appliance. The reasons for this include easier installation and administration, centralised policy enforcement, reduced total cost of ownership and enhanced performance, availability and security of the email infrastructure.

An emergency call to the NHS to enhance email security...

Top 10 capabilities an NHS organisation needs for end-to-end email security

NHS organisations need to look at the problem of email threats, but also compliance and content control, not as individual silos of independent issues, but as a broader comprehensive mandate. Essential capabilities are required for total email security, privacy and compliance; they include:

- Monitor all messages – inbound, outbound and internal. All three requirements must be integrated in a single solution;
- Protect against all inbound threats in a single solution;
- Meet regulatory requirements – granular policies and content controls to protect and secure all outbound information while enforcing regulatory and organisational compliance requirements;
- Real-time and after-the-fact content scanning – prevention, not merely detection, is paramount for both inbound and outbound email security;
- Scanning attachments – To ensure compliance, you must be able to detect potential violations in traditional email attachments, as well as within the message itself;
- Tight integration with existing email systems – to deliver any measure of internal email monitoring, there must be integration with an existing email system. This will reduce administration, training and support costs;

- Flexibility in defining the actions you can take upon messages – flexibility and choice of how to handle harmful emails (delete, quarantine, strip attachments, redirect, etc.). Look for this functionality so that you are able to block the delivery of potentially non-compliant, or offensive, content. You may also want to instantly notify your HR manager, or put controls in place for specific users or groups;
- Quickly and easily define or modify content policies – look for a solution that efficiently creates, modifies and manages compliance policies that reflect internally defined rules that are re-usable and hierarchical;
- Reporting for quick checks – you can't manage what you can't monitor so look for a solution that includes reports that allow you to track and confirm the delivery or receipt of any message that enters or leaves your organisation, plus the status of how that message was handled;
- Contingency in case of system failure – 'Our email system will never go down' – never say never. In the event that your email server fails, look for a solution that can automatically 'failover', ensuring that no message is ever lost in case the primary system becomes unusable.

MXtreme™ Mail Firewall for the NHS

MXtreme is a comprehensive email security, privacy and compliance solution that enables NHS organisations to prevent inbound threats, control outbound content and centrally manage the email infrastructure.

MXtreme takes a new multi-layered approach to email security to proactively detect and prevent all email threats, and offers an integrated approach that is a complete solution for email,

by consolidating disparate point solutions in one system. MXtreme provides unprecedented granular content management that is integrated with secure content delivery to ensure information is secure and regulatory requirements are met.

MXtreme is the only email security appliance on the market to have passed the Common Criteria EAL4+ certification. This level of certification is recommended for perimeter security devices connecting to the NHSnet and will greatly assist in satisfying the code of connection. MXtreme shares many components, including a proven hardened operating system, with the BorderWare Firewall server, a general purpose Firewall that is currently deployed widely in NHS organisations.

By controlling both inbound and outbound messages, MXtreme enables organisations to enforce policies whilst maximising the protection, confidentiality and integrity of information required by corporate and regulatory requirements. MXtreme provides the capabilities that the NHS needs to secure, examine, determine, deliver and report on their email messaging systems, reduce costs and take a major step towards meeting compliance requirements.

Rising to the challenge

NHS organisations must take steps now to prevent, control and manage email holistically with a comprehensive email security solution that:

- Prevents all email threats before they impact internal resources;
- Controls internal information and outbound communications to ensure that integrity and confidentiality guidelines are enforced;
- Manages email centrally, and ensures that systems are always available and no messages are ever lost.

As Graeme Robinson, Network Systems and Servers Administrator at North

East Wales NHS Trust, explains: "We were looking to overcome a number of problems: firstly, to reduce the volume of spam email we received, and thereby increase staff productivity and save money; secondly, to reduce the load on our servers; and thirdly, to improve staff morale by removing offensive spam emails. During the tender process, we reviewed a number of alternatives, most of which were software-based. MXtreme Mail Firewall was the only hardware solution, and it met all of our requirements and more by offering a stand-alone box that was upgradeable, scalable and very cost-effective. Now in place, it is – without doubt – a vital piece of our equipment."

Conclusion

To successfully secure email, NHS organisations need to carefully assess their current and future email compliance and security needs, and make strategic planning and purchasing decisions.

By taking a proactive approach to email security, NHS organisations will be ready for not only inbound email threats, but also ready to take the next step in the evolution of email compliance and control requirements.

BorderWare Technologies is the preferred email security provider for the NHS. Visit the link below for the White Paper, 'When pressing the send button leads to legal liability'.



BorderWare Technologies
Heathrow Boulevard III
282 Bath Road
West Drayton
Middlesex UB7 0DQ

Tel: 020 8759 1999
Fax: 020 8759 1998

nhssecurity@borderware.com
www.borderware.com/nhs