

Email as Intellectual Property

The need for suitable management

Contacts:

Clive Longbottom
Quocirca Ltd
Tel +44 118 948 3360
Clive.longbottom@quocirca.com

Email is now more important to companies than ever – sensitive information is committed to email both inside and outside of the organisation. However, growth in overall email volume, driven by more sophisticated spamming attacks, as well the need to filter out malware and to ensure content is suitable for purpose means that we now must re-address how we view email within the organisation.

MAIN POINTS

- **Email's importance continues to grow**
The use of email has moved from simple interpersonal communications through to widespread financial and other sensitive information exchanges.
- **Email volumes continue to grow**
Spam email continues to evolve, and volumes are growing strongly. Tools to manage the amount of email entering the company will provide benefits to users in having fewer emails to read, less security issues around malware, and multiple storage benefits.
- **Although storage is cheap, storage management is not**
Governance is moving towards a view that once information hits an organisation's network, it must be stored for audit purposes. Therefore, spam and other content filtering tools must be utilised to minimise the storage of non-required (and possibly harmful) content.
- **Email downtime is no longer an option**
Email is now a mission critical service within the organisation. Issues with system patching, upgrades and migration means that a company suffers. Having the capability to manage upgrades and migrations successfully can keep users connected – and therefore working.
- **Information must be secured**
leakage of information to outside parties needs to be controlled. Here, we are not only looking at employees wilfully sending intellectual property to competitors, but the accidental sending of information to the wrong email address, and the sending of inappropriate content to people both inside and outside of the organisation.
- **New tools are required to manage today's email services**
The base offerings from the main email systems do not meet the needs of today's businesses. Therefore, companies must look to other vendors to ensure that they have the correct means of managing their communication and collaboration needs.
- **Mobility is now a key driver of email usage**
A large proportion of most organisations are now mobile – and email availability and accessibility for those on the road is a critical factor in many companies' success in the market. The creation of a suitably scalable and resilient communications platform has to be high up on any organisation's priority list.

REPORT NOTE:

This report has been written independently by Quocirca Ltd to address certain issues found in today's organisations. The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

CONCLUSIONS

Most companies started utilising email over 10 years ago, and many have let its usage evolve in a relatively uncontrolled manner. The workloads being put on today's messaging backbones means that organisations need to review how their email systems are managed – and look for tools to increase stability, resilience and response, while filtering out malware and inappropriate content. Also, where email is being utilised for the exchange of sensitive information internally or externally to the organisation, the use of secure systems must be looked at.



An independent report by Quocirca Ltd.
www.quocirca.com

Commissioned by Symantec Corporation
www.symantec.com

quocirca

Contents

It's time to revisit email	3
Email stability and resilience	3
Email accessibility.....	4
Controlling email growth	4
Email storage and archiving	4
Email security	5
Email migration	5
Conclusions and Recommendations	6
About Symantec	7
About Quocirca	8

It's time to revisit email

email has rapidly evolved from a useful tool for interpersonal ad-hoc communication, through being a more formalised means of exchanging information to an integral part of an organisation's informational intellectual property.

During this evolution, we have also seen a massive change in the volumes of email being sent and received – and also in the types of email: we now receive emails with viruses, spyware and Trojans in the attachments and with messages trying to ascertain specific private information from us. This spam has grown to a point where around 80% of email being sent is spam – and so we are looking at massive volumes of rubbish going backwards and forwards on the network.

But, we are more dependent now on email than we ever have been – we are utilising email as a means of transacting business between our customers and ourselves, and between ourselves and our suppliers. A company email could well be the first thing a supplier or customer sees from the organisation – if the content is wrong, inappropriate or just badly worded, the impact on the company's brand and profile could be high. These emails often include financial transaction data – tracking this information is becoming increasingly important as we look to local, regional and global governance and audit requirements. We are increasingly committing highly sensitive information to email – it is fast, it is relatively dependable, and it is easily available.

We still use email as a communication tool, but the collaborative side of email has also grown. After trying many different tools such as document management, team rooms, portals and shared intranets, the majority of people still use email to send around work in progress for comment by their peers and review by their bosses. This has been forced through the remaining high price of formalised workflow tools – and that email can be easily called from within any application, or can easily accept output from any application as an attachment in a manner that is acceptable to the vast majority of people. Indeed, we also see that many users utilise email as a disaster recovery repository – if any of their systems goes down, another system will probably hold a good proportion of their work as attachments in email.

So, we now have a new problem with email – it is no longer a nice-to-have tool used by the few to impart information of low or dubious nature to others. It is now a business critical service carrying and holding information where loss could heavily impact the business. Therefore, for many email users, it is now time to review how we look at email, and how we put in place tools to manage the possible problems that we have with the rapid growth of email volumes, with the ever-present dangers of spam, of the need for content security and for centralised management of email systems, to be able to search across this information repository and to provide a more stable and scalable solution to the individual users and the organisation as a whole.

Email stability and resilience

With email now being a business critical tool, the issues around data store corruption have to be addressed. Although fixing most problems found with Microsoft .pst files is technically relatively simple, it is not something that the ordinary user can be expected to do – and the time taken to fix these issues rapidly builds up. Therefore, any tool which helps to stop .pst corruption will create a more stable environment.

Further, the continued growth of email volumes means that we need better means of monitoring and managing mailbox sizes – not only to improve the resilience of the mailboxes themselves, but also to improve responsiveness for the users concerned.

A major focus for many large enterprises is to look at server rationalisation – the minimising of the number of servers involved with carrying out a specific function. Email is one of the main areas where multiple servers have grown to service the numbers of users and the number of departments involved, and companies and vendors alike are pushing for email to be

consolidated down to as few a number of servers as possible. Although this makes good sense, we are then looking at consolidating at what has become an inherently unstable platform into fewer instances – and taking more users out if there is a problem with that instance. Again, by utilising tools that manage the email environment more optimally by providing better data store management, storage offloading and rapid information restore capabilities, such server rationalisation can be carried out with the knowledge that the solution will be more resilient, more accessible and more resilient.

Email accessibility

In general, we can look at between 20-40% of a typical organisation being mobile in one sense or another – whether this be in having multiple desks, working from home and the office, being field-based or spending a lot of time travelling between the office and other environments. This can lead to problems with accessibility to email systems, and of redundancy in content storage.

Tools which manage centralised email data stores, rather than proliferating multiple stores, reduce issues with information accessibility, with the storage of the same information in multiple different areas, and with data synchronisation needs.

Through negating the need for local stores for anyone who has a network connection, issues with support at a local level are minimised. Through centralising information stores for the “road warrior” (those who spend a large proportion of their time outside the office), information synchronisation can be optimised, minimising the time required to download new information, while maintaining a local store for off-line usage where appropriate.

Controlling email growth

The people responsible for spam and malware (“Blackhats”) continue to try new ways of getting past existing filters. With 80% of internet email traffic now being spam, organisations need to ensure that as much of this data traffic is filtered from the incoming email stream as possible. Not only does this remove issues for users looking at an inbox stuffed with spam, it also lowers storage requirements and alleviates the possibilities of having to manage useless and possibly harmful data within a governance/audit requirement.

By trapping suspect traffic before it enters the corporate network proper, companies can delete definite malware before it becomes an issue. However, with the way governance requirements are building on a worldwide basis, the deletion of information once it has entered a user’s in-box may become an issue – how do you prove that you only deleted harmful and/or useless content, and that you did not delete content that had a material impact on another person?

Email storage and archiving

The Sunday Times estimates that over 10 Trillion emails were sent over the last 12 months. Even though 80% of these are estimated to be spam, this still leaves 2 Trillion messages that are not – and so may need to be stored. If we also consider that not all spam is being filtered, we also have a proportion of the 8 Trillion messages that will also be stored. Further, if we are using multiple email stores for each device we have, we need to have storage for each of these instances. Therefore, it’s fairly safe to say that email storage is now a major issue.

Although the costs of raw storage are at an all time low and will continue to fall, the main issues become the speed of response on information searches, and on the windows of time available for carrying out full and incremental backups of the information. Alongside this is the real-estate needed for large storage farms, the power that is required for powering the disks, the cooling requirements, the back-up systems and skills to manage such environments.

If the right tools are utilised to minimise the amount of information that is required to be stored – through solutions such as anti-spam/virus/adware tools, content filtering and centralised

mail file storage, it is possible to minimise the volumes concerned. Further, by tightly controlling the data stores, it is then possible to ensure that backup can be optimised, with functionality generally found more in the main data centre, such as snapshots, staged backup and incremental backups.

Once such storage technologies are in place, then other best practices become possible, such as hierarchical archiving, data restore from near-line stores, data recovery from cold stores if the need for disaster recovery is there, and higher levels of resiliency based on having better data policies in place.

Email security

Information “leakage” – where sensitive content is sent via email inappropriately – is a growing problem for companies. With the immediacy of email, once a message has been sent, it is all too often too late to recall it.

Users can find that they have sent a sensitive email to an email address in error (the use of type-ahead address finding often provides a valid email address against a mis-typed name), and dissident employees often utilise email as a means of sending information to competitors or to their personal email account for future usage.

Through the use of content filtering tools working against company content policies, this activity can be minimised. Email messages and attachments can be searched for specific types of information, and can be blocked and isolated if any problem is found.

A further benefit of content filtering is the removal of inappropriate content – this may not be seen as being as damaging as sensitive information being sent to the wrong person, but with the legal situation around racist, sexist and other content, companies need to ensure that content remains appropriate at all times. In many cases, jokes that have been forwarded on to a distribution list have caused brand and profile damage for the companies concerned – and content filtering could have saved this from happening.

Lastly, content filtering enables certain types of attachments to be directly filtered - executable files of all sorts are often dressed up as documents or pictures with a reader being duped into opening this Trojan or other malware payload. Through the use of granular policies, certain file types can be blocked in and out for the majority of users, while enabling those who may need to send and receive these attachment types to continue working.

Email migration

Email systems continue to evolve, and companies need to be able to migrate from one email system version to another with the minimum amount of user impact. In most cases, a direct migration from one email system version to another is difficult, and roll-back on migration error is almost impossible.

Again, by utilising the correct types of tools, email migration can be made far more facile – the use of centralised data store systems means that you have control over where users’ emails are, that you can have dual data stores during the migration, enabling users to continue working and to roll back if needs be.

Conclusions and Recommendations

Email is now far too core to a business' needs to just leave to natural evolution. Server consolidation is required to create a more cost effective and manageable environment, but resiliency and accessibility need to be addressed at the same time.

Email volumes continue to rise, and managing the content that reaches the reader is increasingly important. Spam, malware and inappropriate content needs to be stopped – both incoming and outgoing, and email content needs to be secured against leakage to recipients who are not meant to see the content.

Storage needs to be controlled – both because storage management in itself is not cheap, but also due to the increasing needs for governance and audit. Correct storage policies can then lead to greater email system availability and for the capability to manage backup and restore needs in an appropriate manner.

Finally, a company's communication and collaboration needs will continue to evolve, and tools will be required to manage this evolution while maintaining accessibility to function.

Quocirca's belief is that companies should be looking at what tools are required to make their communication and collaboration solutions more fit for purpose, as existing systems tend to have too many holes in their base offerings.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. Symantec provides a comprehensive solution to ensure the security and availability of email information and systems. Unique and sophisticated technologies combine to reduce the risk and potential downtime posed by security threats and spam, help satisfy email policy and regulatory compliance needs, enable data migration to less expensive storage, facilitate email server migration, and optimize the availability and resiliency of the email infrastructure.

Contact:

Symantec United Kingdom

300 Brook Drive
Green Park
Reading
RG2 6UH
United Kingdom

Tel: +44 (0) 870 243 1080



About Quocirca

Quocirca is a company that carries out world-wide perceptual research and analysis covering the business impact of information technology and communications (ITC). Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry in the following key areas:

- Business Process Evolution and Enablement
- Enterprise Applications and Integration
- Communications, Collaboration and Mobility
- Infrastructure and IT Systems Management
- Utility Computing and Delivery of IT as a Service
- IT Delivery Channels and Practices
- IT Investment Activity, Behaviour and Planning
- Public sector technology adoption and issues

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of a company's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly polling users, purchasers and resellers of ITC products and services on the issues of the day. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, Dell, T-Mobile, Vodafone, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Sponsorship of specific studies by such organisations allows much of Quocirca's research to be placed into the public domain.

Quocirca's independent culture and the real-world experience of Quocirca's analysts, however, ensure that our research and analysis is always objective, accurate, actionable and challenging.

Quocirca reports are freely available to everyone and may be requested via www.quocirca.com.

Contact:

Quocirca Ltd
Mountbatten House
Fairacres
Windsor
Berkshire
SL4 4LE
United Kingdom
Tel +44 1753 754 838