

iQ Insights:

email archiving
and security

FEATURE

Alpha mail fairytales

With email having quietly matured into one of today's most mission critical applications, is it time to start taking its management, maintenance, and security rather more seriously?

As cultural phenomena go, the story of email's emergence as the world's undisputed champion of personal and business communication is about as impressive as any.

It's hard to believe, for instance, that there was a time not all that long ago, when deploying email was still considered a pretty big deal; when email meant specialist employee training; when half a dozen messages a day was a lot; when only the most senior management in a business could expect their own dedicated email accounts. How times change.

Driven by all manner of market factors – server, storage, and software costs falling, the rise of always-on connectivity, teleworking, webmail, and mobile email to name just a handful – a robust, reliable, secure email solution is now nothing short of absolutely business critical.

Indeed, issues such as email management, archiving, storage, and security now affect – or should affect – every company from SME to Enterprise, says Neil Hammerton, former CEO and founder of Email Systems, and currently VP of SaaS Development at Webroot. [↪](#)

iQ : INSIGHTS / EMAIL ARCHIVING & SECURITY 7

Vital email security and archiving questions

- How does your solution provide Compliance, Search, Exchange management, PST file ingress, Offline client?
- Where's your support team based? Is it 24 hour?
- Administration overhead, will our IT people be able to manage this solution?
- How easy is it to make updates/upgrades? How easy was the upgrade process between previous versions?
- How easy is it to back-up the archive data?
- Does functionality require any add-on components in Outlook or on the mail server?
- What technology are you using for integration with third party apps? Open as in API technology or proprietary SDK?

- Product roadmap – what's your vision for the solution over the next 3 years?
- Vendor stability and market consolidation – will you still be around in 3 years time?
- Can the solution prove email is authentic and unaltered (and that it is therefore legally admissible?)
- How is access protected with reference to laws such as the Data Protection Act?
- Does it have any safeguards to prevent abuse of privileged user searches?
- How much time and consulting is needed for the install?

Sources: Quest Software & Trend Micro

“...confidential data mustn't be kept in archives accessible to supervisory bodies, and personal emails cannot be stored without the agreement of both sender and recipient.”

There are many drivers for this, he says. The need for information to be easily accessible where and whenever it's required; Sarbanes Oxley and Basel II, which are driving archiving from a regulatory compliance perspective and which, in turn, are having a filter-down effect to businesses that don't necessarily need to be compliant, but wish to employ best practice.

The threat of data loss is a further key factor, with industry reports indicating that 85% or more of a company's intellectual property now passes through its email, according to Hammerton.

“Businesses are conducting more and more legal transactions including quotes, orders, confirmations, and agreements via email”, confirms Duncan Ash, EMEA Business Development Manager with Sybase. “To protect both the organisation and its customers, these emails have to meet stringent statutory requirements governing document authenticity, confidentiality, and availability.”

Worryingly though, it appears that a disturbingly low number of UK businesses can be confident as regards the integrity of their email systems currently.

In a recent study conducted by Vanson Bourne on behalf of Forensic & Compliance Systems (FCS), nearly half the businesses surveyed (44%) couldn't prove email hadn't been changed or tampered with, and more than a third (35%) were unsure whether any changes had taken place or not; results that suggest that three in four UK businesses have millions of emails floating around their synapses that would enjoy no legal standing.

It uncovers a worrying reality, said Ralph Harvey, CEO at FCS. Specifically that many firms simply don't “understand the consequences of not having a tighter control over their emails...”

It's a problem businesses simply have to address, counsels Steve Tongish, marketing director EMEA at Plasmon. “European regulations are

now developing teeth. There have been recent court cases in both the UK and Germany where steep fines have been imposed when the process controlling records and the integrity of data was found to be inadequate.”

This shift in risk exposure, he says, is forcing a rethink in digital archive requirements.

Malcolm Etchells is VP Europe for Waterford Technologies – a provider of solutions that allow the visualisation of email usage, data pattern analysis, and policy improvement and enforcement. He also bangs the compliance drum, citing several costly cases.

“Some of the world's largest, most IT savvy organisations – UBS Warburg, Fidelity, Morgan Stanley – have fallen foul”, he says. “(Businesses) must begin to think more proactively about how to archive, retrieve, and produce emails and related content in the event of a request from a regulatory or government body.”

“... the issue is not storing the emails – that's relatively easy – but finding and retrieving (them). Many organisations can show authorities the email in the system but can't retrieve it. A well-publicised example is Morgan Stanley which has been fined repeatedly because of its inability to retrieve emails, with two fines of \$15 million and \$2.5 million respectively.”

Ash warns, that there is a “conflict” between the need for strong record maintenance and data privacy law however. For example, he explains, confidential data mustn't be kept in archives accessible to supervisory bodies, and personal emails cannot be stored without the agreement of both sender and recipient.

There are pressing productivity concerns too. First, says Ash, if email is filed in an unstructured way, it's impossible to fully exploit the information contained within it. Second, with knowledge increasingly available only within emails, companies need a way to store, access, and analyse this precious data efficiently.

And a ‘save all emails’ strategy is clearly not the answer, he says. Separating what can and can't be stored calls for increasingly sophisticated technologies.

“Most specialised email archiving solutions are based on file-oriented data management systems.

EMAIL ARCHIVING & SECURITY

LA Fitness

When health club group LA Fitness discovered that 40 per cent of the emails it was sending were non-work related, it deployed an intelligent email management solution to get an insight into employee productivity and performance. It now helps ensure the company's email policy is adhered to across 88 clubs nationwide.

Policies include running reports drilling down into email usage to ensure employees aren't using inappropriate language and tracking monitoring levels of personal email *to prevent it impacting productivity levels.

Personal email usage has fallen from 40% to just two; inappropriate emails have been eliminated; extra bandwidth has been freed up; and storage costs have been cut by half.

These are neither audit-secure, nor able to conduct a combined analysis of structured and unstructured information."

Etchells cites further productivity concerns. According to the Office of National Statistics, he says, employees spend an average of two hours a day assessing, managing, and responding to email, which equates to 55 days a year or 11 working weeks for every email user. Translated into costs, the figures are alarming.

Based on an organisation with 1,000 employees earning an average of £25,000p.a., for instance, each spending 1 minute per inbound email on an average of 40 messages per day, and a further 4 minutes creating and sending each of around 20 emails every day, the estimated cost to the business over the course of a year would be £7.5million. And that's without the cost of email misuse and storage.

So what's the answer? Says Etchells: "Productivity is very much seen as an issue for the IT department but it cannot be held responsible for reducing the volume of email sent by, or within, an organisation. Even with adequate storage in place, creating a culture of efficient and responsible email use needs to be driven by the business, not IT."

Urs Raas, Senior Product Manager at enterprise content management (ECM) software vendor, Tower Software offers some practical first steps.

"First you need a system that can automatically move mail into an archive that uses cheap storage and is easy to maintain from a back-up and disaster recovery point of view. Second you need a system that allows the easy capture of emails into the context of the business process, alongside any other records documenting it. This is where email archiving meets compliance."

Michael Brooke, Archive Manager Product specialist at Quest Software argues that a solution must also reduce the total volume of information stored, and not simply move the problem from a mail store to another media. "80% of email volume is attachment data and in most organisations the duplication rate of attachment data is close to 50%, i.e. 50% of the attachment storage used by a Mail server is duplicate data!"

He cites easy administration and cultural ignorance as other growing issues. "IT staff are busy people and an archiving solution that requires significant management time becomes a liability."

Key archiving and storage requirements:

- ✓ Archival of all email and attachments
- ✓ Mail server data offload
- ✓ The capture of recipients including distribution lists and blind copies
- ✓ Full content indexing for search
- ✓ Compression of email data during storage
- ✓ Stubbing support – to replace large attachments in user in-boxes with shortcuts
- ✓ Secure, tamper-proof storage
- ✓ Encryption during storage
- ✓ Time and date stamping
- ✓ Separate Administrator and Privileged User access levels
- ✓ Easy user access and search where authorised

Source: Trend Micro

"IT staff know that storage is not unlimited but the business doesn't, so the IT manager is often left explaining to senior management why the legal department can't have a 10GB mailbox. They aren't interested in the back-ups and recovery, what if a disputed contract they sent 2 years ago is no longer retrievable?"

Implemented properly, says Etchells, the benefits can be huge. "Having an intelligent email management solution in place will provide (an) insight into email usage, especially the patterns that cause waste." It can also help identify and eliminate non-work related email, he says, and even change the way employees create, manage, and think about email. ■