

Corporate messaging services in the crucible



By Javier Ribas,
Partner Landwell - PwC
IT Risks Manager at PwC
March, 2009



E-mail has become as essential to companies as rivers are to the ecosystem. Just as is the case with rivers, the contents of messages must be clean and transparent, but without filtration. You must be able to capitalize on the content when necessary, yet garbage and other polluting materials must be removed. It is also essential to avoid logjams that might slow everything down or cause serious overflowing. And, of course, the more navigable the river, the better. Making rivers meet these conditions is one of the great challenges of ecological policy. Achieving a fluid electronic mail system with those same characteristics represents a challenge that IT administrators cannot fail to meet.

Saturation and loss of efficiency

In the 21st Century, e-mail is competing with the telephone to become the most commonly used communication service by companies. This service has become essential over the years, but now it is in danger of being killed by its own success. This is mostly due to the fact that the volume of e-mail increases by an astounding 25-30% per year. Employees feel obligated to dedicate a growing portion of their working hours to going through their e-mail, and in some companies, this portion has reached one hour per day. Administrators are also spending more time and resources to confront a workload issue that is both threatening and insatiable. The lack of discipline in reading e-mail generates the expected lapses in productivity, but real-time attention to messages as they come in also provokes distraction, stress, and burnout for users.

More resources needed

To address this problem, we need strong and measurable management and storage systems that, in a perfect world, have the virtualization technologies necessary to optimize workloads. It is also vital to remember the needs for messaging created by corporate mobility. E-mail, which was born in 1971 in large computer-based environments, became popular with the advent of desktop computers. However, its most natural ecosystem may be the mobile phone, where it has entered in earnest thanks to “push” technology. Naturally, mobile phone mail demands proper servers and services, which translates into more resources.

Tests and electronic transactions

Electronic mail messages can contain contracts, budget proposal acceptances, transactions, architecture plans, engineering plans, and administrative forms. These are especially valuable and delicate documents that can be used in international transactions and with official organisms. Digital certification enters into the picture here, requiring its own technology, servers, and custom processes. The challenge facing companies and their lawyers is to try and preserve electronic mail in such a way as to be able to use it as proof in a trial if they ever have to defend themselves against a legal claim or file suit against another party.

Recommendations for companies

1. Establish norms for the use of electronic mail that are oriented towards efficient and responsible use of this corporate resource.
2. Publish these norms and create evidence of their dissemination, if possible, by having users expressly accept these norms.
3. Include in these norms the users’ obligations regarding confidential information, protection of intellectual property and the use of personal data.
4. Alert users to the possibility that e-mail may be monitored, stored and, in case of infractions, used as proof in eventual claims.
5. Alert users to the possibility that their messages may be used as proof by clients or providers in a court case involving breach of contract.
6. Offer training to users about the correct and efficient uses of electronic mail.
7. Establish an action protocol that explains the steps to be taken in the case that a possible infraction is detected.

Compliance to regulations

To ensure that e-mail fulfills its role as the backbone of corporate and institutional information, it is also necessary to comply with increasingly demanding legislation. It is important to bear in mind the fact that some messages will hold private content and, yet, must comply with a series of requirements for its management and control. The European Union's EuroSox regulation has been in vigor since July of 2008. In short, this regulation demands a transparent corporate policy. In the near future, it will perhaps be necessary to consider initiatives that are being passed in other countries. One such initiative involves Finland's so-called "Nokia Law", approved at the insistence of Nokia because it wanted to be able to control the destination (not the content) of its employees' e-mail in order to avoid information leakage and industrial espionage.

Spam

As if all of this were not enough, a legion of spammers continues to succeed in making even the most expert administrators constantly divert much of their attention from more important objectives in order to deal with millions of unsolicited messages. E-mail has shown its capacity in marketing and publicity campaigns, but unfortunately this is also true for unwanted mail. According to the *Study on the situation, nature and socio-economic impact of unwanted e-mail: spam* conducted by INTECO (Instituto Nacional de Tecnologías de la Comunicación), 84.6% of e-mails sent to companies are spam, and employees at those companies take between two and four minutes daily to delete unwanted mail. This represents a cost of 179 euros without considering the costs of possible fraud. The problem grows quantitatively due to the increase in infected computers (zombies) that forward these e-mails without their owners' knowledge. It also grows qualitatively due to the increasing technological capacity of cyber-delinquents, who are gearing spam mail towards identity theft or sending Trojan horse programs. According to BitDefender, the latter activity grew no less than 400% during last year's second quarter.

The immediate future

Electronic mail is a young technology. It was born in 1971 and introduced to Spain in and around 1985. Therefore, there are still many bugs to be worked out. It is true that ambitious plans are afoot to turn this service into something “as secure as certified postal letters”, at least as far as De-Mail is concerned. This company’s new project is so promising that it is being backed by Germany’s Ministry of the Interior. However, while these and other similar initiatives are taking shape, it is necessary to confront the challenges that exist right here and now. IT managers must optimize the necessary technological resources, reduce costs, and guarantee compliance with regulations and security. In order for the floodwaters not to overflow, it is necessary to implicate all the actors that make up the messaging system in the best practices available. Among these practices, a few stand out as essential. Nobody should use corporate e-mail without being covered by fully updated security tools. Employees should be taught how to use common sense to increase efficiency. They should never open attached files or click on Web links that come from an unknown sender, and they should use extreme caution when confronted with suspicious contents, even when these appear to be coming from a person they know. This is a short list of common-sense measures that their companies rely on to ensure speed, flexibility, and the ability to be competitive.