Latest industry statistics reveal that over 183 billion emails are sent each day. The incredible growth in email communications over recent years has transformed the way we do business and how we socialise. It has become an essential tool to support our need for increasingly efficient ways of communicating. But all this does come with an increased security risk as Jim Black, Marketing manager at Bloxx, explains.

Email has replaced the need to telephone colleagues who work on another site or even to get up and talk to a colleague just a few feet away. We arrange to meet up with friends via email rather than picking up the phone to talk. We use our email application to manage a calendar, as a reminder for tasks, meetings and appointments, and to maintain a current address book. This is all done quickly and easily, which is in contrast to the time-consuming nature of more traditional communication media.

Immediate response
With the almost instant delivery of email messages, there is an expectation by the sender of a near immediate response, much like the short message service (SMS) used by mobile phone subscribers. It is a well documented fact that email recipients tend to answer email messages as they arrive or when they are back at their desk whereas phone and voice mails are often easier to ignore. Also email is associated with having very little cost to the sender or recipient whereas phoning and other forms of communications carry a direct monetary cost.

With most email clients constantly running and often configured to instantly notify the recipient when new email arrives, each new email received constitutes an interruption. While a quick glance at the email may take only a few seconds, the actual impact is much longer as the recipient then needs to get back into the train of thought or activity. As a consequence of this speedy reaction to emails, it’s likely that there is a reduction of an individual’s overall productivity. It is estimated that over 50 per cent of emails received by corporate email servers – after the removal of spam, virus and malware email – are deemed non-business-related, meaning the cost in impacted productivity for an organisation could be huge.

Productivity impact
Organisations therefore need to determine how much personal email is coming into a business email account and the impact that it has on productivity, i.e. the amount of time taken in reading, analysing and responding to such email in business hours and the impact it has in performing tasks that contribute to the delivery of the goods or services the business provides.

Email threats
Traditional email filtering solutions are now mission-critical providing functionality that enables organisations to detect and eliminate the following threats:

- spam – unsolicited bulk commercial emails, designed to entice recipients into purchasing some goods or service;
- phishing – unsolicited bulk emails, designed to entice recipients into disclosing private or business information with a view to using that data to commit fraudulent acts;
- malware – viruses, trojans, worms and any other sort of executable content designed to cause damage to a recipient’s computing infrastructure.

SURVIVING THE EMAIL TSUNAMI
These solutions are deployed in the network on the route inbound from the internet and remove infected email. These traditional solutions can also protect recipients from inappropriate content with keyword-based filtering on the title and content of emails. With the volume of spam and malicious email continuing to grow, these types of solutions are still required by businesses today, alongside a solution that maximises performance and throughput while processing large volumes of emails.

Once email is filtered to remove the above threats it will then be delivered to the recipient. When you add in the number of non-business-related emails sent to business email accounts and the interaction required by the recipient, you can start to understand how personal email can detract the recipient from the duties they are employed to carry out. This major problem could potentially rank alongside the traditional email threats previously mentioned.

Hidden cost of email
For example, can your organisation easily determine:

- Who is receiving and sending personal email?
- How many personal emails do they send and receive each day and week?
- What type of emails are they sending or receiving – shopping, dating etc?
- Are the emails legitimate based on the user’s job function?

Do you have a social networker?
The social networker has lots of friends on the social networking site Facebook and receives emails whenever someone writes on their wall or comments on their photos. On average they might receive around 25 emails a day and send 50 emails a day.

Or do you have a share dealer?
The share dealer has a big portfolio and is constantly looking to buy shares. They receive emails when a share’s value changes by one per cent and when a shares tracked fall below a buy threshold. They might receive on average around 64 emails a day and send 50 emails a day.

Or maybe you have an auction buyer?
The auction buyer makes money from buying and selling on auction sites and receives emails whenever they are outbid for an item, a new item has been listed or someone has placed a bid. They might receive on average around 150 emails a day and send 200 emails a day.

So what can be done?
New research evidence suggests that there might very well be a case for a need to address the delivery of personal email to users’ and to either stop or limit delivery. Some email users are becoming stressed by email, which can have an adverse impact on the health of employees and a resulting effect on the organisation. Companies are legally obliged to deal with any problem that affects employee health. Others might use email as a form of displacement activity; a way of legitimately engaging with their work, whilst avoiding the less attractive tasks they need to carry out.

Stay in control
A typical email appliance can be deployed on the network behind the main firewall in which all email traffic is checked for spam and malware to determine if any email is spam or contains a security threat. Assuming the email passes these checks, it can then pass through a content categorisation tool as part of email analysis. Real-time categorisation provides an additional layer of spam and virus detection that further reduces the risk of bad email being delivered to email accounts.

Categorisation can also provide another dimension to traditional email filtering by easily identifying non-work related emails. Each email is categorised in real-time, which together with an optimised URL database accurately determines which category the email belongs in, i.e. auctions, dating, property and so on. With this categorisation functionality IT managers can perform analysis and management of personal email usage that provides insight into patterns and levels of personal email use across the organisation with the ability to drill down for deeper analysis. The addition of a high level dashboard delivers an understanding of email usage and more in-depth business analytics is delivered through comprehensive reports, which can be customised and made available instantly. The addition of this real-time categorisation and analysis of emails allows organisations to quickly implement and manage a flexible and effective acceptable use policy for personal use of a corporate email account.

Policies can be created for a specific department or job function or for an individual user. A policy specifies how each category should be treated. For example, a policy could be created that delays the delivery of emails that come under the shopping category until lunch time. Other categories that might contain more inappropriate content can be blocked completely. In addition, rules can be configured so that an alert is automatically sent when thresholds showing excessive numbers of personal emails for an employee are breached.

Now IT managers can truly understand how much personal email is coming into their business enabling them to more effectively defend the network, manage network resources and understand the impact that reading, analysing and responding to non-work related email has on staff productivity. Only with an email filtering solution that contains spam and virus protection, as well as the ability to categorise email, can they reduce the headaches and costs of email security management by delivering better manageability and protection.

References
1. Radicati Group, ‘Corporate Email User Habits’, 2005
2. Radicati Group, ‘Corporate Email User Habits’, 2005