

## the newsletter of Tarragon Solutions

### Tarragon Solutions

#### Head Office

First Floor  
Victor House  
Barnet Road  
London Colney  
AL2 1BJ

#### Accounts

Accounts Dept  
Tarragon Solutions Ltd  
PO Box 528  
Huntingdon  
PE29 9AQ

#### Phone:

0800 0199 925

#### Fax:

0845 1305 807

#### E-mail:

info@tarragon.co.uk

#### Web:

www.tarragon.co.uk

### Solutions!

#### Editor:

Steve Booth

#### Email:

solutions@  
tarragon.co.uk

## Email Archiving - it's your responsibility!

As you well know, the law places many obligations on companies. These include a growing number of regulations regarding the length of time business-oriented information must be retained, depending on your industry. For example, for regulated financial institutions, the UK Financial Services Commission mandates that members must retain all pertinent client records – paper and electronic – for a period of 10 years.

Pertinent records includes emails and this particular aspect is beginning to cause real headaches for many companies; how long would it take you to search your email archives (you *do* keep email archives, don't you?) for all messages containing a particular fact (or opinion) about a specific deal or person?

Luckily, sophisticated solutions to this problem are becoming more available and we're pleased to highlight two that are available now, from Tarragon: **Exclaimer Email Archiver** and **Barracuda Message Archiver**.

### Why is email archiving needed?

With the exponential growth of email and the legal requirement to retain it for a long time, organizations are faced with two major problems:

- How do we physically store more and more email data?
- How do we search effectively for particular emails when required?

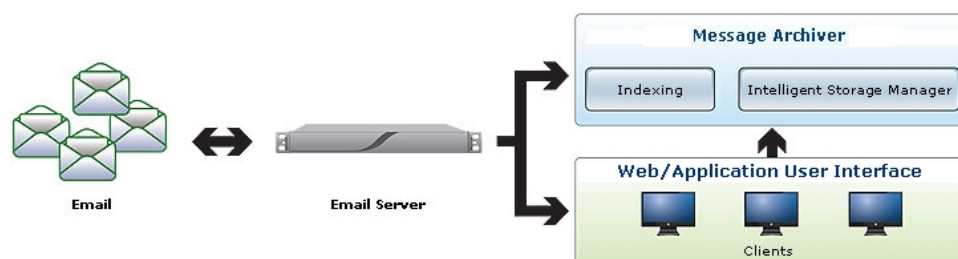
Of course, it is possible just to use the facilities of Outlook, Exchange Server or another email server. Many have tried and most have decided upon another approach. There are limits to the overall size of the information you can store in most email servers, they tend to slow down rapidly as the amount of data increases and, most damning for legal compliance, emails may be deleted or modified.

The most useful solution is to ensure that all emails are logged in a single place when they are sent or received, in such a way that security, space and searching are managed effectively and efficiently. And that is what email archivers set out to give you.

### How do email archivers work?

The better products "intercept" email messages as they are read or sent and each one, together with any attachment, is then stored in a relational database such as Microsoft SQL Server. The advantages of using a relational database is that they can be made very secure and far more sophisticated searching techniques can be used. Indexes are used to provide rapid lookup on all sorts of criteria.

Access to the archive can be controlled very closely so that privacy laws are satisfied; once messages are stored they may not be removed or altered and the storage potential is such that it is feasible to retain many years of data online, thus fulfilling other legal requirements.



Both the Exclaimer and Barracuda products provide all the features needed to implement an effective email archiving system. The main design difference between them is that Exclaimer Email Archiver is a software-only solution whereas Barracuda Message Archiver is designed around its own hardware—a small computer with a very large disk capacity. We will be pleased to discuss with you your archiving requirements and which of the solutions would best suit your needs.

Remember, failure to fulfil legal obligations in record keeping could result in severe penalties, possibly even custodial sentences, so it is in your interests to check the requirements for your own industry—and ensure your systems support them.

# IPv6 – the **Unprotected** Gateway

IPv6? It probably means nothing to you but, before long, it will be the standard for addressing the Internet. In the meantime, though, it is a potential open door for unauthorized access to your network.

IP (Internet Protocol) is the addressing system used to uniquely identify each site in the internet. The current version of the protocol is IPv4; when you use your Internet browser to visit, say, [www.tarragon.co.uk](http://www.tarragon.co.uk), that easy to remember name is converted into its IP address, which is 83.70.124.3

IPv4 was introduced in 1981 in the sure belief that it would provide more than enough addresses (some 4.2 billion) to satisfy requirements for ever. By current estimates, the addresses will actually run out early in 2011.

IPv6 has been developed as a replacement for IPv4 with the same belief although with a possible  $2^{128}$  addresses it really should see us through a few decades.

IPv6 will gradually come into general use (for instance, it's being used by China to provide coverage of the Beijing Olympics) although most modern operating systems have support built in already – and this is where the problems arise.

Because IPv6 traffic isn't common at the moment, many protection systems aren't set up to guard against malicious IPv6 traffic yet some operating systems (Microsoft Vista, the current version of Macintosh OS/X and some mobile telephone OSs for example) switch on IPv6 by default.

The problem isn't confined to attacks from inbound IPv6 traffic; security analysts found—by accident—their “honeypot” systems\* compromised when an intruder entered the network by “traditional” means, turned on IPv6 from within the system then used it to send information to another computer, completely undetected by the usual controls.

Clearly, it is important to check whether the computers in your network are IPv6 enabled and to ensure the protocol is managed by your firewall if necessary. It's easy to check whether your desktop or laptop (or phone!) is IPv6 enabled – see the “Tip of the Month” below. If you require help to disable IPv6 or to determine whether your firewall package is protecting you from undesirable IPv6 traffic, please do get in touch with us.

\*A Honeypot system is a computer deliberately left weakly protected in order to attract attacks by hackers. In this way, security companies can analyse novel attacks and find ways of protecting against them.



## Tip of the Month — does your PC have IPv6 enabled?

To determine whether your desktop, laptop or mobile phone has IPv6 enabled simply visit the website <http://ipv4.whatismyv6.com/> and click on the hyperlink “IPv6 only Test” at the right of the page.

If you successfully reach a page then IPv6 is enabled on your computer; if you receive an error message, it is *not* enabled.

Please let us know what you think of **Solutions!** - email [solutions@tarragon.co.uk](mailto:solutions@tarragon.co.uk)