

## The Danger inside your Firewall

Mark Altman  
Altman Technologies

Who cares if British Gas Customers can see each other's invoice details?

Well I suppose the people concerned probably do but the seriousness in terms of financial loss is er ... ZERO. Security has always been important in all walks of life, but it's taken the internet to bring the issue to some people's attention in terms of how computers and networks are used, abused and the need for protection.

Privacy is one thing and it has certainly heated a few collars recently and given a springboard for lots of "Internet Security" products to stake their claim on a potentially massive but still gullible market. Many internet users are still novices and whilst many are seduced by the trend-setting and dynamism of the internet, few over the age of 30 are capable of change and actually understanding how to use it and the issues around it.

Even business owners and stakeholders who actually carry the can for "security" (whether they realise this or not) often do not understand what is needed. To know what to do, the risks have to be understood. In computer terms, this does require some degree of knowledge about the technology being used - at this point, another few heads bury themselves in the nearest bucket of sand, probably still there in the corner of the office as a remnant of the company's outdated fire policy. Law firms, accountants and most financial institutions have carefully, and probably expensively, worded legally correct and compliant disclaimers on their emails and sometimes even the acknowledgements they send automatically. But amazingly, the people who send emails are often unaccountable when it comes to the access they have to the information they can send, the content they use and the recipients of the information they are sending. A case of damage limitation instead of damage prevention surely?

Financial loss and fraud is a far more serious issue than that of privacy. OK, that's subjective but commercially it is true. Privacy is generally a fashionable issue for the do-gooders in Brussels; the sorts who will try their best to ensure we can't find out about child molesters living next door by or to ensure murderers get a second or third chance at rehabilitation.

It may not be headline making but the truth is that the most significant threats in the context of computer network security are INSIDE an organisation's Firewall.

Trusted employees ... in general, can't be. Everyone should be accountable, whoever they are and whatever they do.

Auditors now expect organisations to be able to track who has been on the network, when they were on, what they did, when they did it, where they did it. The pressure is on IT Security Officers (do you know who yours is?) to be able to comply with their company's security policy and meet their Auditor's requirements.

Whilst there are software tools available that help, a culture change should be the first item on the agenda which probably explains why it is so difficult. A good example is the use of passwords. Everyone uses them and probably everyone has abused them. Passwords are still a very effective, low cost, easy to deploy method of authentication but not if users still insist on writing down a variety of their passwords on post-its stuck to their desks or monitors - the really security conscious users at least hide the post-its in a drawer!

continued

If you strengthen your authentication process your network is more secure - it's that simple. Once you are *sure* of who is on the network, then it is possible to focus on monitoring for inappropriate or exception type activity amongst your "trusted users". The most trusted are typically System Administrators and IT Consultants/Analysts. This is out of necessity rather than choice and is often an area hard to reconcile with a company's security policy. Auditors would love to be able to hold this unruly bunch to account and re-establish themselves as the rightful custodians of their organisation's electronic assets ... in the good old days before computers, wasn't life a lot easier?

---

*The writer:*

Mark Altman is a Director of Altman Technologies Ltd, a software company specialising in auditing and surveillance tools for Novell and Microsoft environments - more information [www.altman.co.uk](http://www.altman.co.uk).