



Knowing what is necessary.

Paolo Marini
May 2003

One of the many obstacles to achieving good security is knowing what is necessary.

Its easy enough to install firewalls, anti-virus software, intrusion detection systems (IDS) and require everyone to change their passwords once a month. But is it good security?

Are passwords being shared because job function, privileges and user roles don't match? Are they being written on 'Post-It' notes because they are too hard to remember? No doubt the firewall is blocking unauthorised incoming connections, what is being allowed out? Is the IDS and anti-virus software up to date? Are the IDS and system logs being discarded or overlooked?

A common misconception about Security, especially Information Systems Security, is that its all about prevention and that it is solely achieved by deploying technology. This is a counterproductive view, it stifles business and encourages workarounds or attacks. It is better to consider Security as an enabler.

Building and maintaining trust is fundamental to social and commercial relationships. Knowing what to protect, how much or what kind of protection is necessary and sharing these criteria with correspondents helps build a trusted environment which enhances relationships. Therefore, the considered application of security can enable new channels and enhance existing ones between correspondents, partners, suppliers and customers.

This knowledge is typically encapsulated in a Security Policy. A good Security Policy should be a pragmatic protocol taking into account, the assets to be protected, any threats affecting them and the nature and aspirations of the business. A good Security Policy will reflect the consensus of what is necessary, will be supported throughout the enterprise and will be reviewed regularly for appropriateness and adequacy.

Paolo Marini is an Independent
Consultant at Muckle.Org

e-mail: info@muckle.org

web: <http://www.muckle.org>