Netintelligence
OPINION SHEET

"What you cannot enforce, do not command"

How policy enforcement is driving up the demand for end point security solutions

The man credited with the headline quotation was not a high flying business guru, he was not an analyst or even a highly paid management consult. He was Sophocles, a Greek tragic dramatist and he was born in 496 BC. Some 2500 years later as businesses battle with trojans, viruses and identity theft, his words still ring true. Many companies hit by Slammer, NetSky and Blaster worms - and any of last year's main viruses- learned the hard way about what worked when it came to their security defences. According to the latest DTI information security surveys, 74% of all UK businesses have suffered a security breach with each one costing companies an average of £7K - £14K. Amongst the hardest hit were the smaller companies without the resources - manpower, financially and technically - to devote to adequately protecting their systems. And with the widespread adoption of always on/broadband connections within businesses, the problem is set to worsen.

In a recent report 'Always On, Always Vulnerable', the Yankee Group showed that only 45% of small businesses - 20-99 employees - had purchased security services, and alarmingly this figure fell to 20% for companies with between 2 and 19 employees.

Most organisations are aware of the issues surrounding internet and eCommerce, after all 87% of UK businesses are now dependant on IT in some form, and many will admit to having some form of security policy in place and yet the bare facts suggest they are not working. Designing and implementing a security policy is the easy bit.

The stark lessons from last year highlight that there is no real value in designing security policies and investing in protective technologies - if you can't ensure that they're enforced at all times. To do this, three things need to happen. The first task is to determine the actual policies that the business requires to function, both securely and operationally, the second is to obtain the buy in from those affected by those policies, and the third is to effectively enforce the policy on a day to day basis. Apart from the deployment of the physical elements of security e.g. firewalls, anti virus, web filtering etc a major 'must' is the education of employees. It is misleading to suggest that all Internet security issues arise because of technology vulnerabilities. Many breaches (over 70%, according to Gartner) originate from staff within the organisation.

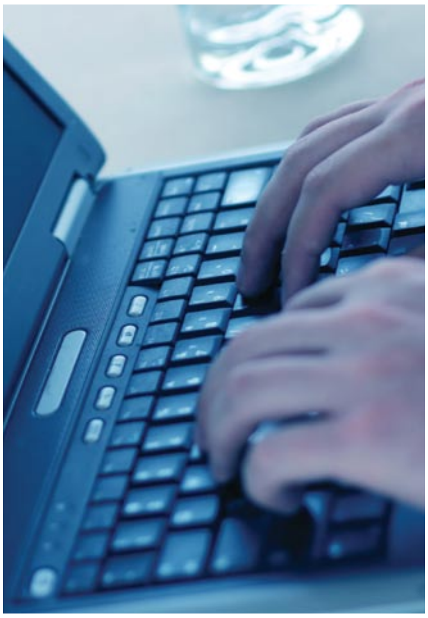
Senior management from all Lines of Business must take ownership for determining policy rather than the usual approach of offloading the responsibility to IT & HR. To get employees to agree with polices and support them through their actions, an organisation's leaders must be seen to actively be involved in the process. Far too often the IT department is viewed as 'anti business' by employees. Much of the time this is a largely unwarranted distortion of the truth - but as with most things in life, perception is everything. An Acceptable Use policy should be devised which clearly explains what employees must do and what they should not do when accessing the company's systems, regardless of where they physically connect. This involvement will ultimately result in a culture which accepts info security into the overall organisational
bloodstream.

The security policy must stack up with the business' overall objectives e.g. what are the key risks to the organisation - not the imagined, not the nice to have - but the real risks and what tools are available to ensure that end users are reminded of their responsibilities under the terms of the policy. The late Indian Prime Minister and orator, Jawaharlal Nehru, once stated that "The policy of being too cautious is the greatest risk of all" and whilst he might not have been specifically referring to security policy, his sentiments still apply. For example a virus is a real risk to an organisation but is the use of the Google tool bar as big a risk? Quite simply, many organisations resort to "management by vulnerability as opposed to management by policy".

Allied to risk is the issue of trust. A stand alone blanket policy 'designed to prevent everything and anything' will fail; it will be circumvented and most harmful of all it will create an environment where employees do not feel trusted. Once an Acceptable Usage policy is in place which is logical, acceptable, easily understood and can be modified effectively, the organisation can then seek to find technical solutions to enforce it.

The selection of the tools to enforce the policy is the final challenge. With the rise in mobile working the perimeter has changed and has become more fluid. Mandating and enforcing policy across a wide and disperse user base is causing no end of heartache. Consideration must now be given to a total security system by realising that end points, laptops, computers etc, are core network components. An end point solution enables the organisation to take the policy and apply it at an individual level whilst focusing and protecting the network as a single unified whole.

The end point solution can provide the ideal combination of effective compliance tools with individual policy. Without the blending of both, an organisation's policies will never be totally effective. End point security is now considered the new frontier for the business and end point solutions should be considered by IT resellers. The security industry is responding with multiple layers of products because of the inability of single product solutions to secure against all threats. This market is being attacked from traditional networking vendors, security vendors, and broadband service providers.



Organisations now have a choice, they can treat the enforcement of policy seriously or they can follow the advice of the ancient Italian proverb "Better no law than laws not enforced".

For further details:
Netintelligence.
www.netintelligence.com
or email:info@netintelligence.com.
Tel: 44 (0) 870 050 0121