“It’s Probably in the Filing Cabinet”

Michael Barwise

When did you last review your information security policies? When did you last look at them? Have you ever tested them? Where are they anyway?

For most SMEs and a surprising number of larger companies, security policies are documents which are written by the IT department, filed somewhere and largely forgotten about. For these enterprises, the reality of day-to-day information security is handled by technical people who are left by Management to fly by the seat of their pants through the fog, often without adequate resources, training or authority to successfully take command of the situation. As a result, nobody is really in control, so when a problem arises it is usually dealt with piecemeal on a technical level without reference to the bigger picture. This is to a great extent why, in spite of advances in defensive technologies, attacks are on the increase and the bad guys seem to be winning. I believe this situation exists because the majority of corporate information security policies just don’t work.

Let’s look at a simple example. Most policy documents contain a blanket clause such as *“no software shall be installed by any user without the authorisation of IT Support”*. Sounds very conscientious, but I have a couple of questions before I’m convinced. Firstly, what is this policy trying to achieve? Licensing control? Protection against Trojans? Control of private computing? IT Support would have to take a different course of action in each case, so without an appropriately defined intent and action plan, this policy statement is non-functional. Secondly, how is this single policy supposed to cater for everyone in the company from accounts clerks who don’t generally need to install software to engineers who do (possibly at short notice in the field)? Thirdly, if everyone were to follow the policy rigorously, would IT Support have the resources to properly handle all the requests? Finally, has anyone trained the end users so they realise a screen saver is software, and has anyone noted that some dangerous Trojans masquerade as screen savers?

What generally happens as a result of this vagueness is that *nobody* follows the policy as a rule, but it may be wheeled out occasionally after the fact to bludgeon some unfortunate whose software installation caused an identified problem.

Good policies should protect against threats, not just specify punishments to be inflicted after disaster has struck. They are an expression of rules and restrictions that maximise the security of corporate information while minimising the impact on the business. They must be tested and proved to be functional in the business context. And, given the rate at which the hazards are evolving, good policies soon go out of date. Obsolete or unworkable policies can be more dangerous than none at all, as they can engender a false sense of security, and policies that do not mesh with your business needs can be a constant brake on performance.

So, what’s the way to create good policies?

First and foremost, ask yourself what you are trying to achieve: Identify the problem you are trying to solve, and involve business decision-makers, IT support staff and even HR, rather than leaving policy definition to one or other group alone.

Take professional advice where appropriate, but never hand over your policy definition to outsiders, and never use off-the-shelf policies, however big the apparent cost savings.

Include a regular formal update mechanism in your policies, and also amend them immediately in the light of any incident and whenever a major new threat is announced. That means you *must* investigate all incidents, however trivial, and you *must* keep up to date with new threats. Both these duties should feature in your policies, and HR and Management need to ensure that appropriately qualified staff are given the time and resources to fulfil them.

Consult with your IT users, explain what your policies mean and why you have implemented them. Listen to their responses and adjust your policies if necessary. Train them in security basics, so they understand when you have to impose restrictions on them.

Allow no exceptions: make a policy for every explicit case.

Contemplate simplifying your policies by eliminating unnecessary hazards. Imposing minimum privilege can do wonders for security: instead of giving everyone full Internet access at their desktop, consider opening a “cybercafe” in the canteen, completely isolated from the corporate network. You might give everyone a private e-mail address as well as their corporate one, with explicit, monitored, rules on usage.

But above all, update and test your policies regularly to ensure they actually *work*.

Originally appeared in Computer Weekly, August 2001