Depends what you mean by "policies"

Michael Barwise

When people are discussing security policies, I regularly come across comments about "HR" and "getting fired". That's a common position but it is doomed to failure because:

- the kind of policy that is just a set of "thou shalt nots" for front line staff is an indication of lousy security management - devolving responsibilities that should be borne elsewhere onto people who can't be expected to bear them effectively. From that frame of reference, more than just the policies is doomed to fail;
- threats never stick unless you make them stick _every time_, and if you do that you necessarily operate in a conflict zone where everyone hates you and finds ways to bypass or subvert your controls. Witness the speed camera problems faced in the UK. Initially, people vandalised them until the government bowed to pressure and painted them bright yellow. Now, drivers slam on the brakes just before they come to them and storm away again after they're past. Result - no reduction in speeding. The only way to be secure is to get everyone on the same side, working together willingly. That means you need to encourage co-operation, not conflict - and strangely enough threats don't do that.

I generally find that what are called "policies" are scrappy mixtures of policy and procedures - what I call "polcedures" - that fail to explain background or reasons but seek to impose often complex apparently arbitrary rule sets on people who have not had the basics explained to them so they find them hard to remember and follow (lack of compliance).

Often, even the procedures are poorly defined - obviously written by people who don't really understand the problem they are trying to solve or the underlying principles of a robust solution (see most "password policies") - and can't fulfil their ostensible objectives even if followed to the letter (lack of efficacy).

So effective user policies need to be created by people who actually understand not only the technical problem but also the underlying principles, the business processes affected and the psychology of the people the policy is aimed at. And user policies are only part of the policy set you will need. Every activity and implementation (both technological and non-technological) should be governed by a policy that specifies at least

- what the policy sets out to achieve
- why it matters
- how the process should be conducted
- how compliance should be monitored
- how efficacy should be monitored
- how breaches should be dealt with
- how failures of efficacy should be dealt with

The policy should be developed in consultation with all stakeholders, and tested before it is formally put in place. ISO 27001 is no help here as it offers zero guidance on how to achieve any of these aims - it only points out the need to do so, which is obvious. There is practically no standard guidance on "how" anywhere - it's all about "what", which leave the door open to having policies and processes that don't actually work and still passing audit. I've seen that all too often.

This means that policies are not the domain of the Information Security team, or even of the IT department - they're a collaborative team effort that will include input from those, but also from other stakeholders.

Finally, just a reminder - security depends on trust. The greatest threat to corporate infosec is people who just don't care, and that's a cultural issue. In a don't care culture, sacking someone for a policy breach will serve no useful purpose - another person who doesn't care will step smoothly into their shoes because it's the corporate culture.

Originally appeared on LinkedIn, January 2010