How do you render your digital security policy â€œoperationalâ€•?

When it comes to managing security policy, name your poison: do you keep it via wiki, knowledge management system, or CMS? Or, is that all important document still paper-based this many years into the digital evolution?

A related question: How do you render your policy operational? By this I mean, how do you motivate employees with all those theoretical security ideas and make sane, safe practice something that’s part of the daily routine? From what experts have told me, a digital security policy can be a first step of a bigger process (including training) in getting this important work done.

What does the digital policy element bring? Well, easy access can mean that the parts of the policy that pertain to a given department or activity can be viewed, perhaps FAQ style. Sure, many companies think of having a policy ‘on tap’ as simply a matter of compliance, but it can be more. It can be a source of awareness for new behavior.

After all, in the busy world of office work, content in all forms floats out the door on laptops or in email, or on USB flash drives and similar devices. Now, most of flow through the front (and side) doors is both necessary and routine. It’s the exceptions that can be the problem.

I mention all of this because digital security—and how best to manage security policy—has been top of mind for me lately.

One reason for this, purely personal, has to do with the act, in recent months, of setting up a home office. Beyond the typical media storage devices, back-up options from Google and other cloud dwellers are possibilities. Naturally, I want to make the right decisions just in case an event strikes. (My Mac is good, but nothing is permanently invincible.)

The other reason for the security policy focus, though, has to do with what’s making broader news regarding emerging standards of protecting healthcare records—and security policy is implicated. I familiarized myself with a Houston-based company, Information Shield, which is a leading developer of information security policy products. It recently announced the availability of a solution for for the Health Information Technology for Economic and Clinical Health Act. (The product goes by the name of the HITECH Security Solution Bundle.)

As the press release indicates: [The HITECH Security Solution Bundle] allows organizations responsible for protecting the nation's electronic health records to address key security policy and security awareness provisions of the newly modified standards... . So this product is a way to get compliant and also serves that key educational role. And, it can be a way to inch security awareness up. We’re all busy, but it’s important to understand why certain habits need to change.

Of course, when it comes to forging that security policy at your company in the first place, there are a few ways to go. I ask about wikis and CMS right up front, assuming you run with an internally developed plan. So I’d like to hear how you approach it.

Again, as a leader of the technology organization, I’m sure you do what you can. I understand that you could give me a first class lecture about security matters, with all your staff experts offering their input and advice. Your security budget is probably “up there.” You likely test your disaster recovery and general continuity plan with strict regularity and enhance when necessary, for instance. (In that regard you may have hot sites and all method of failover planned.)

You understand the risk, but...
And yet, when it comes to content, and lock down of IT assets or even physical security, I wonder if the rigor in the process is all that it could be, given all the distractions in the workplace. Getting that work done is more than a matter of policy, but again, it starts with policy.

Because while system configuration is important, it’s also about worker habit, to repeat myself.

In closing, it has always amazed me, over the years, of the little tales of less-than-perfect deployment that I hear, usually on background. Often enough, I was also told that the financial services industry was—for regulatory and cultural reasons—one of the stronger adopters of the leading edge tools and techniques. So it was a mixed message indeed. And it always had me wondering.

Because, in the spirit of short cuts, and just-this-once exceptions, and so on, well, mistakes have been made and events have occurred with our regrets and things slipped through...down the slippery slope. Now, I am aware that a little fear

mongering can be good for business, too. Somewhere in between is the actual truth. Just make sure you’re not on the wrong side of it, okay?