2007-10
Measuring Compliance

Introduction:

You will comply! Resistance is futile... For Star Trek fans, the compliance gurus sound like the Borg – an alien race that assimilates other races and cultures by force, turning them into drones doing the bidding of others. But in the real world, compliance is... something that an seemingly alien race forces all of us to do. Since we, more or less, have no choice about many compliance issues, once we resign ourselves to having to do it, how do we figure out how much we have done and how much is left to do? That's what measuring compliance is all about.

What are we really asked to do?

The first task in measuring compliance is to figure out what constitutes compliance. I get a substantial number of consulting gigs where the main benefit I bring is an understanding what the words in the standards mean. For example, in ISO-27001, an increasingly popular standard used in and between businesses exchanging content, one of the requirements states (section 4.3.3:

> "The ISMS takes account of any relevant legal or regulatory requirements and contractual obligations."

Beyond the obvious questions associated with what an Information Security Management System is (which is the most common question), does this really mean that my management system has to know about any and all legal or regulatory requirements around the whole world that might be relevant to anything we do within our company? Do we really have to track every contract we have at a detailed level? Of course the answer is – yes and no...

Do they really mean it?

Not really. They don't mean that the ISMS has to track every law and regulation in the world and map them all into everything that anyone does within the enterprise that seeks to comply with ISO-27001. If a city ordinance somewhere in Zimbabwe changes and your company sells through a reseller in Zimbabwe, this does not mean that you are responsible to identify all of the impacts of that change and deal with them. On the other hand, you really do have to have a system of tracking legal and contractual issues. As these requirements change, you do need to make suitable changes. When making contracts your legal department should be able to check to make certain that the new contract doesn't have terms that you cannot fulfill. When asked, you should be able to show compliance to a level of due diligence and avoid gross negligence in fulfilling your legal and regulatory duties.

Most standards are this way, just as most laws are this way. There is a letter and a spirit that need to be fulfilled.

How do I measure this?

Understanding what they mean is at least half the battle. The other half is finding ways to measure how well you do what they mean for you to do. This really calls for two different sorts of things working together. You need people doing the measurement task that understand the needs of the standards well enough to interpret facts and words in light of those standards, and you need some way to count things relative to the requirements of compliance.

While many people look at security metrics in terms of technical details, like what percentage of my systems have installed patch number 3457, relatively few use sound management metrics or measure the things that are directly related to compliance issues. Measuring compliance means counting things that people do. That either means going to a work flow system that automates the tracking and documentation of all relevant actions taken by all affected people within the organization so that they can be measured by examining the work flow system without talking to the people, or talking to the people involved to see what they do, how they do it, and to get and assess their documentation relative to the standard.

Since few organizations have such workflow systems in place, this means that measuring compliance and using those measurements to make management decisions, requires a substantial amount of manual effort by knowledgeable people – read costs.

Having done this many times with and for clients, we developed increasingly systematic methods for measuring compliance. They are far from perfect in that the numbers they give are only percentages of lines of the standard fulfilled in each of a set of areas with roll-up figures presented in a color scheme that looks like traffic lights. One line of the standard (like the one shown above) might be a lot more work than another line, so 98% done may not mean that only 2% of the work is left. But it's a start, and one that customers seem to think is helpful.

Conclusions:

At the end of the day, this combination of people who understand the issues and automation to reduce time and effort is the most efficient and effective way we have found to do sound measurements of compliance.

It means that people who know what things mean have to show up and evaluate statement after statement in light of the present situation. For large enterprises this has to be done again and again. Tools help to make it more efficient and clearer to all, and they automate counting, adding, and dividing to give presentations that look reasonable. But there is no hope at this time that such tools will be fully automated unless all of the work of the enterprise is also fully automated. And I don't see all contracts fully negotiated, signed, and fulfilled by computer quite yet.

Fraud of the month

Every month, we take an example from "*Frauds Spies and Lies and How to Defeat Them*" and describe a recent example. From page 138:

"Because"

> "... "because" ...works, because it generates nearly automated responses indicating that whatever was said seems like a good reason to follow through on the request"

Actually, that description is an example because it uses the "because" thing to make you believe that the word "because" generates nearly automated responses... Hmm. Actually, even though the word "because" works AND people tend to respond to it almost automatically ignoring whether or not the statement is in fact true, the automated response is not the cause of the effectiveness of the the use of the word "because". The response is a result of the use of the word "because", not its cause.

The cure to these problems is listening carefully when people use the word "because" and figuring out whether they are telling you the truth or not. People don't really seem to like to think a lot about what other people are saying, and most of the time, if it sounds plausible they will just go along with it unless they have a strong view that disagrees. That's why:

> *"You should buy my product because it helps with compliance"*

should be examined carefully. In looking at the market over the last several years, we have found that a very large percentage of security companies sell what they sold before under the false claim that it helps with compliance. Watch out for the "because" - and it's many relatives. Think before you believe.

Chet's Corner

Ah yes... compliance. The thing of the day. Another way to sell the same old stuff – under a new name. Need to comply with SOX? Buy my CD and be free! To me, it's really no different than what we have been trying to help people do for years, only now, instead of doing it because it's good for them, they do it because someone else tells them they have to. On the other hand, it makes it easier to explain why. Instead of actually understanding why it's good for them all we have to say is that it's required.

"Always look on the bright side of life"!

Service Summary

Every month we feature one of our services and give an example of how it benefited one of our clients. This month it's actually about some of the tools we use in our services and the evolution they are going through.

Over the years, we have developed internal tools to help us do our job more efficiently and effectively. Lately, our clients have started to ask us if they could license the tools they see us use. The ones that seems most popular these days are the decision support tools (*Decider* and *Security Decisions*) and our compliance metrics tool (*Metrics*). We aren't all that cleaver about coming up with fancy names because we aren't in the retail software business. But we have started to license our tools to our clients for their internal use.

It turns out that we of the many tools that we have developed and use, only a few of them are of interest to our clients. This week we finally think we figured out why they are popular. It's because they offer instant gratification. Within the first minute or two of use they produce results. We have spent many years creating and using tools that take hours of effort to start produce results, including really useful things like risk management, work flow, simulation, and other similar tools. But the ones that customers want to know about and get for themselves are the few that the users "get" right away.

As a service to ourselves as much as to our clients, we maintain and enhance our tools over time, and for those who license them, the upgrades and fixes are, of course, part of what they license. So in a round about way, our software tools are as much a service to our customers as our consulting services.

Mollie gets the last word in

Compliance. They teach it to you from the day you start going to school and you are done with it the day you die – when it is taken over by whoever's left alive that cared about you. Sit in the assigned seat, fill out this form, wait in line, redo the whole form because you made this mistake, You used the wrong number, here is the right number, now fill out the form again using the right number and send it to me so I can check the number again and then process your form. I think that the computer geeks think that they are somehow different from the rest of us. We have always had to comply, now it's their turn.