2007-11
Covert Awareness

Introduction:

Covert awareness must surely be an oxymoron if ever there was one. Any yet it is not. Covert awareness programs are awareness programs designed to create the social environment that supports sound and sensible security behaviors by creating social norms. They are covert because they seek to influence norms by presenting the proper behaviors as if they came from a friend and colleague and not from on high.

Why should we even consider this?

The sad truth is that most security organizations are viewed by most workers as the grim reaper coming to force them to do things they don't want to do. No matter how many times we may tell them we are from security and here to help them, it won't wash.

This approach takes the approach of using well known social influence factors to improve security-related behaviors. By having people that workers relate to, like, and feel similar to hold out views that are supportive of the security function, all workers benefit and will show improved behaviors.

Is this legal? What if they find out?

Like anything, if done in excess or too harshly, it may run into legal impediments, but there is no legal restriction on the use of one worker to influence another. But it may be more problematic if workers believe that they are being tricked into things by covert means.

The best approach to dealing with the issue of worker awareness of the covert program (another oxymoron?) is to make the existence of the program overt and part of the expectation of workers that they will participate in the security program. Try something like this:

> *Every year, select workers in each organization will be internal security awareness advocates. They will advocate for security on a day-to-day basis, but they will not otherwise be identified in that role. Everyone will act as an advocate at one time or another, and we encourage all of you to be advocates for security every day.*

Select workers are then taken aside and given security advocacy training to help them advocate for security on a daily basis without offending others or being pushy about their role. The program is not covert, but the current advocate is, in the sense that they don't perform a formal role for security, but rather an informal one. They can also help security get a better handle on why the things being called for are not being done and how to do them better.

How do I manage and measure this?

We are advocates of being able to measure security programs and their effectiveness. Like any other security program, we think that covert awareness programs should be measured, monitored, and properly managed.

Managing covert security programs involves creating controls over the behavior of those in the program designed to influence others, measuring the effectiveness of those behaviors, and making changes to improve or retain a desired performance level.

In the case of a covert security awareness program, this means training the workers in issues related to influence strategies and giving them specific strategies and goals. For example, one goal would be that every day, the identify a different co-worker, pick one security related issue from a list of key issues, and find a way to bring that issue up in interactions with that co-worker. Suppose the issue of the day is proper use of encryption. A suggested approach might be to bring up a recent news story about how some company had 100,000 social security numbers stolen when somebody had the information on a laptop that got stolen. The comment by the covert advocate might be:

> *"Who in their right mind would keep all that sensitive information on an laptop and not even encrypt it?"*

The covert advocate then reports what issue was brought up with which co-workers each day (they might bring it up at lunch or in a morning meeting and get many co-workers with one comment), and the security awareness program includes testing on the specific subjects in periodic security awareness verification processes. Workers exposed to different issues are measured for knowledge, awareness, and compliance and the results are be correlated to the covert awareness program. If there is a correlation between the program and worker behaviors on tests and compliance, then the program is associated with those successes.

Conclusions:

Covert awareness is not an oxymoron. It's workable and sensible, can have measurable results, and helps keep security issues fresh in the minds of workers on a day-to-day basis. It can be inexpensive and may be highly effective, but it must be used with proper precautions and controls or it may turn into a security debacle.

Developing covert awareness strategies and programs should be undertaken cautiously and on a step by step basis, with test runs and ongoing evaluation and measurement. As the program develops, eventually all of your workers will have a chance to advocate for security, and that's the best awareness program of all.

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 102:

"We interpret based on how others interpret"

> "Laugh tracks work even when we know they are in use..."

Social proof replaces scientific proof when there is uncertainty, and as a result, creating the [proper social environment can cause people to lean toward desired behaviors. Whether you are perpetrating a fraud or trying to generate the proper behaviors for your security program, the mechanisms are present and operating.

There is no avoiding the nature of people in the security arena, so rather than trying to ignore or suppress the human issues, it's usually a better idea to embrace them.

Chet's Corner

It gets cold in the winter in Nebraska, and the icy feel of snow flakes on your nose, makes everyone who lives here stop and ask ya, if you still have any feeling in your toes...

One of the most enjoyable things we do as security folks is to teach others what we think we know about it. One of the least enjoyable is when we find out that what we taught folks last week wasn't really right. It sometimes seems like we never really know what we think we know in security because things keep changing.

But then I talk to old timers. And I keep finding out that the things we keep on learning are the things that we already knew, and lack the systematic means to carry on from generation to generation.

I rarely rally for standards because they are usually used to codify the least common denominator. They are sometimes called "best practices" when in fact they are "minimally acceptable practices" at best. But I think we need to create the legacy of knowledge through education in our field that is necessary to grow beyond where we are today. I think we need a standard for Masters and Doctorate level expertise in our field, and the sooner the better. Now all I have to do ifs find a University that will accept my application.

"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 is our expert witness services.

Most companies don't allow their workers to act as experts in legal matters other than on the behalf of their companies in cases involving their companies. This means that there are far fewer real experts available to resolve legal matters than are needed, and that many of the experts that make it to court cases are not as expert as they may, at first, seem.

Our expert witness services provide true technical experts with extensive relevant experience to anyone that has a legitimate legal need. We are not experts in everything, but on the other hand, it's very hard to detail everything that our folks know on a sheet of paper or two. A good example was a case involving a 15-year old file in an old document format.

> *How old was the format? It was old 15 years ago when the document was created, but it was not so old that we couldn't find a vintage copy of the software. We created an emulation of an old computer with an old version of DOS so we could run the old software in a native environment. When we did, we established authorship by a combination of internal data fields and file content. All of this was done on an emergency basis for a long-time client over a 24 hour period, resulting in a completely different theory of the case than was previously held.*

Every legal matter is unique, and standard forensics like running a disk imaging and analysis package simply don't do the things that our legal clients need done. They need real experts who can do what it takes to get the right answer and clarify how certain they are that they are right for legal purposes.

Mollie gets the last word in

I don't think that I would want a covert awareness program where I work. The idea that my co-workers are acting as covert operatives for my employer is just too spy-vs.spy for me. And I wouldn't want to do something this underhanded for my employer. I would feel like I was betraying my relationships with my co-workers.

Just because we can, doesn't mean we should!