All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Question everything

In recent months, I have been to a number of conferences, and as usual, I ask about things I don't think are quite right. I have included some examples below, but the fundamental theme seems to me to be one of the direction of our society. The question is “Will we go down the path of (1) hierarchical obedience and loyalty with the rewards of advancement and punishments of shunning, (2) disrespect for authority unless backed up with sound reasoning and facts with the punishment of tearing down those who fail to meet our standards of quality and the rewards of those who excel at getting it right being given more to do, or (3) will it be somewhere in between?”

Some recent examples

At the 2012 IEEE Security and Privacy conference, there was a paper with a title claiming, in essence, to be able to identify individuals responsible for content from all of the individuals using the Internet. Of course that was just baloney. It was 100,000 users, not the billion or more (is that really the number) Internet users. And it wasn't really identifying the individual responsible. Rather, 50% of the time, there was an 80% chance that the individual was in the top 10 ranked as possibly responsible. Which is to say, half the time, there was an 8% chance that the top ranked identified individual was the responsible party. The other half the time, it was less than an 80% chance of being in the top ten. And there is no way to tell which half of the cases any particular attempted attribution is. And this means it's more like a 6% chance on average – or correct only 1 time in 18. But still, that is stunning indeed. Except of course that this only covered certain types of “blogs” and excluded cases where there were too few postings to come to these statistics, and assumed there was no deception, and assumed that authorship was original and not copied from elsewhere, and ignored changes in style or word usage over time, and failed to provide any description of why the particular methods worked, and failed to address the fact that the same methods might perform far worse anywhere else. Of course the paper was accepted at a peer reviewed conference, and only questioned in writing to date here. Which is to say, someone else might actually believe it.

I saw another presentation recently about using anomaly detection for detection of insiders. Actually, I have seen quite of few of them, and I will see another later this week... look out presenters – here is your chance to fix it before I ask you embarrassing questions. Of course the notion of “insiders threats” is sensible, except that all insiders are threats – as are all outsiders. But this wasn't what bothered me in this particular case. One of the key things of note in the attempts to detect insiders behaving badly (my words, not theirs) is the recognition that the high performance insiders vary substantially from the norm. That is to say, if we simply look for behaviors that are different from the average, we will detect all of the high performers. We may or may not detect the bad actors, but we will almost certainly catch the folks we most want to keep working for us. The ones that have different social patterns than the average user, the ones that work longer hours once in a while, the ones who try something different, the ones who all of a sudden start doing research into areas they weren't looking into before, and so forth. And we will start the witch hunts. As we have.

A third example will fill out the trio. The rules surrounding passwords keep getting stranger and stranger. In effect, for many claiming “security” as the goal, they are actually reducing security by forcing users to comply to more and more foolishness. And increasingly, the security professionals are coming to state openly that they know it is foolishness, but that they will continue to do it. The classic examples are the 14-24 letter passwords that must have several upper and lower case letters, numbers, special characters, no two in order up or down alphabetically, numerically, or co-located on the keyboard, and they have to be changed every 60 days, and you can't reuse a password for 2 years. So the natural response is that after the 30 or so tries it takes to get one that works, the users put it in a file on their computer along with the URL, and when time comes to change it, they change the last character by one (a → b → c, etc.). Every 52 months it repeats (26 characters at 2 month change rate). We all know it is just so much baloney, but we are forced to do it and those forcing it continue to do so without real basis, and when challenged, they fail to seriously consider that the policies may be doing more harm than good. It's a cultural thing.

So what if we just take it

Many think it's better to get along by going along. Dale Carnegie said so, and if you do this, you are more likely to get promoted and be liked – that's the theory. And of course as we do this over time, the results is weaker and weaker institutions, with the leaders weakened by years and years of kissing up to move up. Such institutions ultimately start to lean on power and money to force success rather than using innovation, efficiency, and similar practices that improve the world while strengthening our understanding of it. And that is what we see more and more of today. But such things cannot work forever. They burn out, as we see much of modern society burning out. The rich get richer and many will go along with them for the rewards of being better off than their peers, and we may get back to fiefdoms or similar societies with large numbers of the great unwashed being controlled and having their views of the world managed by the rich and information controlling. The news media is supposed to compensate, but it is increasingly a propaganda branch, often supporting one side or the other and not recognizing that both sides are engaged in different versions of the same game, or at least not paying attention to the truth and questioning authority when it isn't backed up by facts.

And the saddest part of it all is that we look at others and recognize this, but fail to see it in ourselves. We are all flawed, and we all need someone standing against us to point out our mistakes. The peer review process of professional societies seems like the place we might best make a start at this, at least from a standpoint of the scientific, technical, and academic fields. But this too is flawed – and studies have shown how flawed it is, at least to a limited extent. And the problem comes in at least two forms; (1) not accepting views dissimilar to or competitive with our own and (2) accepting views from those who should be questioned more deeply.

Conclusions:

I don't have the solution to all of this, but I have a prescription that might help out. Question everything, especially yourself. Look to become a better scholar and do your research carefully. Assume things are wrong instead of accepting them as right just because of the source. If you don't know, say so. But do it politely, so they will hear you, and perhaps listen.