BUSINESS AND TECHNICAL

Recently I was lucky enough to get to go to an IT security conference, and while there I was able to listen to some seriously bright people speak. But while I was there I noticed three reoccurring and alarming -at least for me- trends coming through from the people speaking.

Number 1 - Mind the Gap
There was lots of talk about bridging the gap between the IT department and the business. The idea was that a CIO or Technical Manager must be able to explain the IT issues to the CEO in such a way that the CEO can understand it. I have a problem with this. One of the fundamentals of any logical discussion is a concept called "Burden-of-Proof", simply put it means that each party must give supporting evidence for their respective viewpoint. If I apply this to the CEO and CIO example, the CIO seems to be doing all the "proving". Now I do agree that the CIO should learn some business-speak, but the CEO -and the rest of the board- should learn some IT-speak as well. There should be effort put in from both sides. Why should the CEO bother? Simple, they are responsible for the company after all. Business needs to take responsibility for the business goal choices, while the technical crowd take the responsibility for realizing these goals.

Number 2 - Accepting the Holes
I also heard lots of talking about how we could only achieve 80% security in our companies. Again I have a problem with this. I am aware that there is no silver bullet for IT security and that each component can only be so effective, but who says you should only put that one component in? If your anti-virus software does not detect spyware, do not just shrug your shoulders. Install an anti-spyware program. This "80% coverage is acceptable" mindset is an unfortunate influence from traditional business, which is applied to IT security. When you place a advert in a paper, you do not expect 100% response, in fact 80% is a very good response. It is here that traditional business people learn this mindset. But it does not work in IT security. Imagine this, an outsource company comes to you and says "Hire us, we can make your network 80% secure" Will you hire them? I sure wouldn't. Business needs to understand the damage that even one incident can cause, then any reasonable person will want to aim for 100%. Don't take stupid risks, an attacker looks for any hole. Your IT security person needs to cover all your security holes, an attacker only needs to find one.

Number 3 - Who needs Geeks?
The last trend is just as disturbing, I heard a lot of disparaging remarks about the "geeks in the basement", those "strange IT guys", even "those guys with no suntan". The same people who make these remarks say that the "geeks" time has passed and that they are outdated. As you might guess, I have a problem with that. It never ceases to amaze me that people insult the people they need to keep their businesses running and secure. I agree that if all you employ are "geeks" you will struggle to relate to them or to align your business goals with IT. But if you have no technical people, you will suffer. The single biggest reason I can say this is simply due to the technical expertise of the hacker themselves. You can only protect against what you know after all. If you do not have access to the good-guy counterpart of these people, then you are up that famous creek without the much needed paddle.

You see whether or not people like it, those of us who practice IT security are doing it for the good of society as a whole. If you are in charge of a banks database, and someone hacks in and steals information, then not only is the bank impacted but also every single person whose information was stolen. We cannot afford to fool ourselves into thinking that our responsibility is limited to the company we work for, to quote Dennis Longley of Queensland, Australia;

"Information security is to protect society, not to provide an alibi to senior management"