WHY WE ARE STILL SITTING DUCKS

You know what I find strange? That we still have so many information security problems. No, I mean it, there are no real new threats. Yes, the threats are being used in new and different ways, but fundamentally there is nothing really new, so I have to ask myself why the problem seems to get worse each week. Let me try to answer this by drawing an analogy between IT security practitioners and medical doctors, and as such I mean the people in each profession who know what they are doing. The reason I do this is because there are great similarities between the human body reacting to and dealing with threats, and the way a network does.

Lets start with a basic problem. when you think you are sick, you go to a doctor, and he tells you what to do to get better. When you follow his directions you get better. If you do not, you get worse. If he says "Do not eat apples or you will be sick", and you go and eat apples, then guess what? You will get sick, and anyone you complain to would tell you that you should have listened. And you know what else? The doctor does not care whether you like apples or not, or whether you have eaten them your whole life, he will still tell you to give them up. So why when an IT security person tells a company to do something, why do they think it is open to negotiation? Why do they think just because they have done something for a long time that that means that the recommendation does not apply to them? And why when they do not listen, and something goes wrong -as it will-, do they try to blame people other then themselves? This is the first problem then, that the people who are responsible for making security happen, think that they know better than the "doctor".

Next lets look at another problem. I don't know about you, but if I am getting ready to go into surgery, I do not tell the doctor "Listen up you quack, I expect you to do good job and to do it quickly. I am not paying for more than one hour and you better not use too many medical supplies because I will not pay for it. now hurry up four-eyes." I think that something like that would be ... shall we say ... sheer bloody stupidity. But yet there are companies where the IT staff are openly mocked or spoken down too. Recognize any of them .. "Geek", "Nerd", "Button pusher", "Propeller Head" and I am not even going into the rude or vulgar ones. Now I am sure that there are companies where IT is treated properly, unfortunately I have yet to see one or hear of one. So what you ask. I believe that there is no such thing as a marketing company, or a sales company, or any other type of company. They are all IT companies that do something else, such as an IT company that does marketing. How can I say this you ask, simple. Take any modern business, rip out the cables and machines and see how long that business lasts. So why do companies so reliant on this infrastructure belittle those who maintain it? Especially when much like a doctor again, a company's IT staff does not need to actually do anything wrong to cause damage, they just have to not do the best job they can. This then is the second problem, that the people who need the "treatment" think they do not need to treat the "doctor" with any normal respect.

Lets stick with the treatment idea to discuss the next problem. If I need brain surgery, I am not going to go to the local vet and ask him to operate because he is cheaper, in fact I am not even going to ask a recent medical graduate. I happen to be rather partial to my grey matter functioning properly. So, I am going to find a brain surgeon who does what I need done, and who does it well. I do not care if he is more expensive then the vet, I would rather pay a bit more, then end up with an involuntary lobotomy. Again I ask, why then do businesses decide on using the cheapest possible labour. Either they think that any IT person can do any IT job equally well, or they do not value their IT infrastructure. You know what, I am not sure which is worst. But more then that, lets turn it round, say a company has a good IT resource, one who is performing the required duties well, why then do many companies feel the need to pay them the lowest possible salary, very often justified with "I can get <insert name of graduate/cousin/mechanic here> to do this job for half your salary"? Strange as it may seem, you get what you pay for. If my brain surgeon says "If you want I can use a second hand scalpel for the operation if you want to save some money", I will very politely tell him to go right ahead and use a new one. To quote Jon "Maddog" Hall, I am not paying the surgeon for the amount of time he spends on the operation, but rather because he knows where to cut. This is the third problem, the people who need the "treatment" want the "back-street" price.

These are the reasons I think why we still have IT security problems. Simply because businesses refuse to listen to the professionals. Because the business always thinks it knows better, because IT security professionals have to compromise. We are told we must play nice, not rock the boat. We are told to play the game, or that we do not

understand the company. And as long as this carries on we will never have secure networks. As long as untrained people can call the shots, we will always have problems. And the cost of this situation is getting higher, for while the threats haven't changed, the stakes are higher. More and more attacks are motivated by criminal intent. We can no longer afford to bandage the problems, we need corrective surgery.

Harsh? Undeserved? Try this, find a company that has a draconian firewall and anti-virus policy, and see how many information security problems they have as opposed to a company that has less restrictive policies. I will guarantee that there will be a visible difference. I have personally worked in both types of environment, and can testify to the difference. Like it or not the net is not a friendly place, and a company's network is not some magical island of peace and calm. Peace and calm like that can only come with work and vigilance. Much like our bodies, when it is cold we dress warm so as not to catch a cold, it's common sense after all. No-one likes eating veggies but we do it because we know it is good for us. I find it strange we do not apply such common sense in the business world.

What do we do to fix it? Just listen to the experts, but how to fix the business's attitude? I do not know, really I do not. But I am about to say something that I am sure lots of people will disagree with and if you want to try and convince me otherwise please contact me and try. Until I change my mind though, let me go out on a limb here and say this. If the company you work for..

- thinks they know better than you in your area of expertise
- treat you with less then normal decent respect
- always want the quick and cheap fix

Then you will never be able to properly secure their network or do your job. You will be constantly fighting and compromising your suggestions and sometimes even your ethics. You will always be a sitting duck. So try your best, do your work to the best of your ability and if you get the chance to go to a business not suffering from these three aliments, then move. Trust me your work and life will get a lot more fulfilling.