THE MISUNDERSTOOD MYTH

Let me get flamed here, there will never be total security. How can I say this when elsewhere I have slammed others for saying this (see here)? Simple, I stand by both statements as I believe both are true. You see, I do not think that we should ever settle for or be happy with less then 100% security, but the chances of us getting to that level without hard work are slim. Note that I did not say impossible, but slim. And note that I said that we should all aim for that slim possibility. So what stops us from getting there?

Ghosts in the machines
It may help if you relate your network to the idea of a biological entity. Think of any living creature (what you choose is up to you ... and the operating systems you run). Seriously though, think of a person. Why do people carry on catching colds? Why has this virus had such a hold on mankind?

- *The arms race*
  One reason is that the cold virus mutates. Mankind beats it in one form, but it changes in order to beat our new defenses, and thus the cycle repeats. You see in a static environment, once a threat has been conquered, it stays conquered. But in an environment which is subject to change, the threats can attempt to change to effect their version of survival. Look at computer viruses, anyone who has been around computers for a couple of years has seen how viruses have evolved, and can see that they also have not finished. We fight a continual arms race to prevent outbreaks and to stop viruses, just as they exploit new attack vectors in order to spread

- *Human stupidity*
  Another reason humans always suffer with the cold is that we put ourselves in the situations which are conducive to contracting the virus. We go out in the cold, we do not take proper preventative measures (vitamins, etc), we hang out with people who are sick, and it carries on. Is it any wonder than that we get sick. The same goes for networks, if users (at all levels) disregard proper processes (open cute email attachments from people they do not know), make uninformed choices (switch off the anti-virus because it slows their PC down) or download those cool tools to speed up your bandwidth (.. always off those very questionable sites). If the users on your network do this, you will always have problems.

- *Ultimate authority*
  What also contributes, is when those who know best do not have the final say. If your doctor says that playing rugby in the rain will cause you to catch a cold, but your coach says that you will play or else, guess what.. you will probably catch a cold. Relate this to a previous example, you tell your users do not switch your anti-virus off, but the CEO tells the company to do it in order to try and up productivity by making the machines faster. Then guess what.. you have no defense when a virus enters your network

- *Progress*
  Also a reason is the changing world, this is different to the "arms race" in that it is not the threat that adapts, but the environment changes making an old threat more dangerous. Take for example a city, if you have one person with a cold, going to work in a large company, getting on a bus, etc. This person could infect hundreds of people, whereas in more primitive times, the same person would not have had as much contact with other people. In the IT world think of wireless, the explosion of wireless networks have made many old threats (which many professionals had almost written off) take on a whole new life (clear text protocols, traffic sniffing, etc). As long as technology progresses and as long as the progress is driven by the need for "cooler" features, we will always find old threats growing new teeth.

Give up now?
I suppose I can make it seem rather hopeless. That is not my intent, rather I just want people to understand that a 100% secure network today, can be rendered vulnerable by tomorrows exploit, that we must never rest on our laurels because things change, they mutate, they grow, and all this change means we have to adapt our countermeasures. We can make our networks secure, we just have to work a lot harder at doing it then most people think or are comfortable with. So be realistic. Let me end with this quote..

"The price of freedom is eternal vigilance" -- Thomas Jefferson

"The price of freedom is eternal vigilance" -- Thomas Jefferson