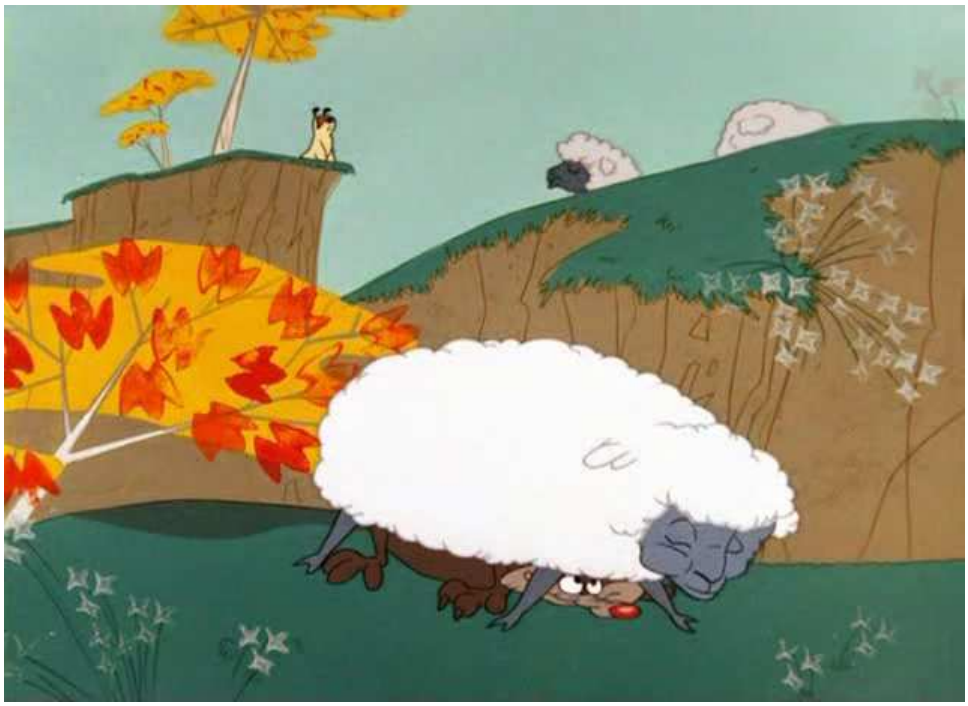
CISO - Or Profit Prevention Officer?

Or No Opinion? – Never mind, Just borrow one from the first person you meet at the coffee machine !!

My boss has just come back from one of those round-table forum things – they're always trouble. Twelve IT directors seeking enlightenment set against one CTO – unfair odds? Too bloody right!! *Cat in the hen house? No…. Wolf in Sheep's Clothing* comes to mind with graphic imagery of the cartoons of my youth.



And that's all well and good until it causes me extra work – and this is the extra work I speak of. He now wants to know why security always gets in the way, cos its obviously my fault.

He has a point; I have to reluctantly admit that security is often the excuse people give for not doing things. Sometimes this inertia is completely appropriate and sometimes it isn't - But in most cases the decision hasn't been based on any qualified analysis, it will have been driven by hearsay and rhetoric picked-up from various chats at the coffee machine and a google search. Guessing! And business decisions based on guessing are always bad!!!!!

My personal belief is that in most organisations, many managers are not properly managed. Sales is treated as an art and not managed as a science, with only a basic metric of "How much sold" applied at end of each quarter, rather than a more continuous multi-metric approach that really successful organisations use. But to be fair a "job sold" = "Money In" which must relate to the overall organisations objective somehow. Leave sales and go into the accounting department, say, and managers objectives will in no way relate to making money or business survival. And so it is with security.

There are just too few security professionals around who are tasked with getting the job done (of course safely, but with mission accomplished as the objective). That's why our Managed Security services are booming – organisations give their security issues to me to worry about.

Everyone has an opinion about security. You could say security opinions are like the proverbial backside, everyone has one but it isn't advisable to listen to the sounds they make. The truth is managing security risk is not easy and not understood, especially by CTOs. The problem comes from "wrong thinking" - It is not my job to tell the business that their needs have to go unfulfilled. But similarly I do not believe the business in a rational organisation should be telling me "how to fulfil their needs". The wrong questions are being asked – " the auditor NEEDS full admin privileges to so he can run some scripts", "the sales team NEED direct wireless access without a firewall to demonstrate the product" or the "Voice solution doesn't work from behind the firewall". Wrong demands !!! They have a need; they should express it but let me fulfil the best way I can.

Used correctly your security expert should be there to help you fulfil the business need with minimum risk to the organisation – By arranging for the administrator to run the auditor's scripts or providing wireless access through the firewall so the product can be correctly demonstrated. And where your security officer advises against, he should able to point to a methodical analysis that holds water under scrutiny and allows the CIO/CEO to make a judgement call. And this analysis should take into account your environment, your business and your risk profile – after all not all organisations hold military secrets or deal in derivatives. So you need a security officer and you need to involve him early enough in projects to get the best from him.

So the solution is more TRAINED security officers not less – before you employee him, ask the candidate to explain exactly how he has personally implemented a firewall, VPN or virus solution. Even if it is ten year ago, it will demonstrate applied knowledge. If he can't, the applicant is an administrator not a leader. Then ask him about Michael Porters' "first mover advantage" – if he doesn't understand, he is not business focussed enough to help, university of life stuff is fine but not if it didn't involve at least some reading. Lastly, ask him a question that would offend a job applicant looking for his first job – if doesn't get up full of righteous indignation, he'll never be able to face off the CEO

So if, in the analogy in first paragraph, the CTO is Sylvester the Cat, Ralph Wolf or Tom from Tom & Gerry, what animated figure gets the job of Security officer? FogHorn-Leghorn or is Spike-the-Dog. I'll have to figure that out later.