Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Inventory Revisited – How to reduce security losses by 70%?

According to recently described but not yet officially published results of one of the largest firms in the world that investigates information security breeches related to Internet uses, about 70% of losses were either of content that was not known to exist by the target or from systems that were not known to exist by the target. It seems that the content or systems not protected adequately were not protected adequately because they were not known to the owner. This smacks of a lack of adequate inventory,.

Inadequate inventory systems, processes, and mechanisms is a subject that I have been discussing and giving recent talks about, writing about, putting up Web sites about, and that is not exactly at the leading edge of emerging high technology. Inventory has existed from the beginning of commercial business, and inventory control was one of the first applications of computers. Identity Management deals largely with inventory of people, systems, roles, and authorizations, and inventory of systems and content has been long required for businesses to do financial reporting and to keep track of what is going on.

Is the solution mandatory valuation of information for taxation purposes? That would require inventories to be generated, kept, tracked, and properly so, subject the inventories to audit under GAAP, provide legal penalties for understating or overstating inventory, and force companies to place values on information, systems containing it, and to generally track inventory. It would apparently have the pleasant side effect of reducing loss incidents by 70% in the Internet realm as well, because the knowledge of the inventory items would allow enterprises to apply the controls they normally use to those items.

Surely this cannot be so difficult that it is unattainable. Indeed, I have seen plenty of cases where it has been attained and, in many enterprises, this sort of document control system has been in place for many years. Older folks will recall that document control was commonly used in the era of paper documents. Copies were tracked, signed in and out, numbered, and ... I almost forgot. That is still done today. For classified systems, for manufacturing operations, for trade secrets and other similar intellectual property subject to controls, for many government documents, and... did I say that the government does something better than industry? Good gracious! It's true!! Government is better than industry at limiting this 70% of losses associated with inadequate inventory. Maybe industry can learn something from government?

Sorry – I just woke up from what seemed like a nightmare. I thought I heard myself saying that industry has gotten so bad that it can't even keep track of its valuables as well as government can. It's not true. If it was really valuable to industry, they would keep track of it – that's how the optimization of economics works – isn't it? Well... actually, it isn't. Evolution – despite the claim to fame of having created us, does not do a very good job of optimizing anything on a global basis. It's all local optimizations in the niches that happen to be there.

The fact is, most of those in industry who make the key decisions relating to these issues

don't care about your private information or mine except as it gets them more money. They don't care about a computer on their network unless it disrupts the network or causes liability for them – or performs a valued (not necessarily valuable) service for them. That's why they don't keep track of it all that well or particularly optimize for that purpose. The only way to change that would be to make it brutally punishing to lose track of things. Which is apparently what the bad guys are doing. If it's true that 70% of incidents producing losses involve assets that are not in inventory, then either industry just doesn't care about those losses or they will start to adapt once they know that this is the source of 70% of their problems. Now, at least those who read this analyst report, will know.

Which brings me to the other point. How do we make them care? California seems to have figured it out to some extent with SB1386. That's the legislation that forces companies to disclose breeches of private data to the public (or all affected individuals) if the breeches involve a California person. State after state have now created similar laws and, while a national law is likely to weaken all of them, at least it will create a standard for diligence. The Sarbanes Oxley Act apparently made CEOs and CFOs care – something about the potential for going to jail does that. Although – I hear rumors that “orange is the new black” and “stripes are slimming”. Apparently, the threat of jail for executives causes them to care.

This brings me to the conclusion that the threat of punishment works and the threat of harsher punishment works better. It seems that all of the attempts to provide rewards of one form or another, standards passed and agreed to by international bodies, logical long-term reasons that it is in the enlightened self interest of the enterprise to do the right thing, and so forth, have failed miserably. But the threat of severe and brutal punishment, public embarrassment, and these sorts of things have worked.

So how do we create the proper feedback for doing a better job of inventory while helping to solve the global financial crisis and eliminating most of the most rampant digital crime? How about is we have governments around the World declare information assets to be inventory that has to be properly accounted for? OK – maybe that's a bridge too far – all of the benefits claimed. But still – think of the benefits for a moment. The big CPA firms that have been hurting so badly lately will have a huge new arena to delve into. The accountants and lawyers will have work for centuries just defining how to value information. I personally want to be able to set the price for my information to any value I desire and generate royalties on each use with the legal owner being responsible for all illegal use that occurs through attacks on their inventory. I think I will charge $100 per bit for each copy of any of my personal information. Each backup of my address alone will earn me thousands of dollars! Identity theft will be something those of us who charge for our information will be cheering on. Hey, for that much in fees, take my identity – please!

OK – that's enough silliness for now. My point is that enterprises have to get their act together in terms of doing a diligent job of simply knowing what's present if they are to have any hope of protecting it – and there is great hope that we can reduce the incidents of loss by 70% by simply finding out what is there that we don't know about today and handling it as we do what we already know is there. Now, if I could only find that password, I could upload this file and ...

