All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The security squeeze

Consider the human aspects of security in terms of cognitive load. People can only handle so many things to do before they become unable to do them all. When you put too much burden on their mental processes, they start to perform less well in some, many, or all of the things they have to do. So what happens when we increase the security burden?

A theory

I have a theory – as yet untested in scientific terms – that people can only take so much security. When you have people over the edge of what they can take, which I think is widely the case today, every new burden you add forces something else to fail to be done well if at all. If you have a 14 character password that has to change every month and must be composed of a hard to remember symbol sequence, it will be written down. If you make a rule that it cannot be written down, the help desk load will increase. If you punish people for help desk calls of this sort, they will break the rule about writing it down. And if you somehow force them to follow all of these rules, you will get malicious compliance with these rules and breaking of other rules. That's the theory.

Suppose it's right

Of course I have little evidence and no proof of this theory at this time. But suppose it's right. That means that almost every security “improvement” that involves things that people have to do will result in a compensating loss of control elsewhere. The problem is that the control that is not properly operated may be far more consequential than the control that forced it out. If I don't write down my password, I may instead take an hour or more each month to memorize it and worry about it over a period of days. My work efficiency will go down, costing potentially thousands of dollars per month. For more than the value of the ever changing password. If I am forced to account for every action I do by writing down a description of that action, I will likely get less done per unit time, and if you force me to work extra hours without pay to compensate for it, I will likely not be as diligent at my work as you wish. If you require me to track more and more in bookkeeping so you can detect potential minor frauds, I may end up charging a lot more for actual work performed, even though you may force me to charge less per hour of effort expended.

An officious proposal

I propose that all of you with undue security burden – in your own mind – undertake to fully and sincerely comply with full rigor to every security-related requirement, and to accurately and fully document all such activities in your reporting process. After all, we cannot manage what we cannot measure. Let's start measuring security fully to see how it grinds us down.

Summary

Consider very seriously work you impose for “security”. The tolerance for such work, once exceeded, may yield enormous negative returns in protection achieved and cost incurred.

