All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

How to justify (security) metrics and what to measure

I have seen many folks in the security community ask about how to justify security metrics, and I've seen lots of answers that were, shall I say, uninformative? So I figured I'd provide my answer(s) in the hopes that others will find them informative.

Justification

Justification should be easy. Presumably you decided to measure things for a reason. Tell us the reason. If we agree that it's a good reason and worth the cost, we will agree and pay for it (or support someone else doing so). Otherwise we will disagree.

Some of you want something more? Perhaps a standard reason? The reasoning I use for business decisions is typically something like this:[1]

- There are specific decisions we need to make (list the decisions and their alternatives).
- The basis for the decision (between the alternatives) is (identify the decision process).
- To make these decisions (between the alternatives) we need to know (list the differentiating elements of the decision process).
- We already know (list the things you know).
- We don't yet know (list the things you don't know that are required).
- The more we know the better our decision – but information isn't free (state the cost).
- Your decision is whether to spend (the cost) to get a better decision or to chose based on (whoever's) best guess.

There are of course other reasons to measure things. Intellectual curiosity – we hope to gain insight – we want to be first and best – whatever. Go for it. Plenty of people favor those things and I generally support getting smarter. But if you ask me to pay for it...

What to measure

I think I have already answered that in producing the justification. But I will reiterate it. There is a reason you decided to measure things. Find a reasonably effort/cost/convenience way to measure what you need to make the decision (and nothing more) and do so.

Alternatively, if you have to measure a lot of things, instead of finding satisficing ways to measure each, there may be synergies between measuring for different purposes, and if that's the case, you might want to measure some things adequately for multiple use. For example, if I need to know the cost of a door, window, and installation of same, I might want to also price them together to see if I get a discount.

Summary

Business measurement justification is, or should be, easy. As a decision-maker, my point of view on what to tell me is this. Stop trying to convince me with elaborate BS. Just tell me what you need to measure and why. Make a reasoned case, avoid waste, and let me decide.

[1] See http://all.net/ICSSec/index.html for lots of examples of such decisions in context.