Security Metric of the Week #18: information security expenditure

Authors:
Krag Brotby, CISM, CGEIT
Gary Hinson, PhD, MBA, CISSP

At first glance, this metric looks like it would be ideal for those managers who are obsessed with costs. "Just how much are we spending on security?" they ask, followed shortly no doubt by "Do we really need to spend that much?"

OK, let's go with the flow and try to get them the figures they crave.

Our first challenge is to define what counts as security spend, or more precisely information security expenditure. It's pretty obvious that the salaries for full-time dedicated information security professionals go in that particular bucket, but what about the security guards, or the network analysts and systems managers, or the architects and programmers spending some variable proportion of their time developing security functions? Oh and don't forget managers and staff 'wasting their valuable time' constantly logging back in or changing their passwords or whatever: does that count as security spend? If so, how much, exactly?

Then there's the security hardware and software - the antivirus and firewall systems, and backups ... and what about the additional incremental costs of finding and purchasing secure as opposed to insecure systems?

Next, security incidents: these are 'clearly' security costs, aren't they? Well, no, it could be argued that incidents result from the lack of security, the very opposite.

Issues of this nature fall into the realm of cost accounting, allocating the organization's costs rationally across the appropriate accounting categories. Given sufficient interest and effort, costs can be allocated although the figures will inevitably be highly subjective depending on exactly what proportion of various costs is labeled 'information security'. Due to the arbitrary decisions, this is likely to be a significant source of error when trying to compare the figures across successive periods, even if some of the cost allocation decisions are captured in a cost accounting system. Consequently, the Accuracy rating for the metric is quite low, and the Time and Costs incurred in measuring it are also low-scoring factors on the PRAGMATIC score:

P	R	A	G	M	A	T	I	C	Score
82	94	60	60	89	29	33	49	59	62%

The high scores for Predictiveness, Relevance and Meaning might be worth building upon, in other words would it be possible to alter the metric's definition to improve the lackluster PRAGMATIC score? Knowing the total expenditure on information security would be fascinating, but unfortunately that's still only half of the value equation. What about the benefits of information security? This is where things get really tricky. The primary benefit of security is a reduction in risks, in other words a secure organization suffers fewer and/or smaller incidents. Measuring the value of the risk reduction is difficult, involving various assumptions and estimations based on the predicted occurrence and severity of incidents if there was no security in place. Further benefits are associated with the assurance element of security - the confidence for the organization to be able to do business that would otherwise be too risky. Again, hard but not impossible to value.