Security Metric of the Week #21: proportion of information assets not marked with the correct classification

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

There are three key assumptions underlying this week's Security Metric of the Week:

1. The meaning of "information asset" is clear to all involved;
2. There are suitable policies and procedures in place concerning how to risk-assess and classify information assets correctly;
3. The metricator (person gathering/analyzing the data for the metric) is able to tell whether or not a given information asset is (a) correctly classified and (b) correctly marked.

Part of the concern about the meaning of "information asset" is the determination of what should be assessed and marked: should we classify the filing cabinet, the drawers, the files, the documents or the individual pages? In some cases, it may be appropriate to classify them all, but there are practical limits in both the micro and macro directions. The wording of the policies, procedures, examples etc. can make a big difference.

Whereas classification policies are fairly common, the related procedures plus the associated awareness/training and compliance/enforcement activities, are not universal. This metric could be used to determine the need for additional procedures etc., and with a bit more detail it could help direct resources at the business units, departments, teams or people who evidently need more support.

However, the metric's poor PRAGMATIC score raises concerns:

P	R	A	G	M	A	T	I	C	Score
52	53	63	44	62	13	17	87	44	48%

Low ratings for Accuracy and Genuineness arise from the way the metric would have to be measured. The third assumption above is the main fly in the ointment, since it is necessary for someone to review a sample of information assets to determine what their classifications should be, and confirm whether they are indeed correctly marked. This is a tedious process that can result in disagreements regarding the correct classifications and the nature of marking required.

We marked it down on Timeliness since the measurement process would inevitably take days or weeks, during which time incorrectly classified and/or marked information assets would probably remain vulnerable to being mishandled. Once the final numbers are available, management can take the decisions about additional procedures, awareness and compliance activities, but these will also take time to put into effect. All in all, there are likely to be significant lags between taking, acting on and adjusting the measurements.

The relatively high Cost of assigning one or more suitable metricators to the job could be offset by reducing the frequency of measurement, perhaps measuring and reporting this metric just once or twice a year ... but of course that makes the metric less useful as a management tool - it's a trade-off.

The bottom line is that although there are circumstances in which this metric might be worth using, its low score suggests that there are many more PRAGMATIC metrics that should probably take priority.