Security Metric of the Week #25: proportion of critical information assets residing on fully compliant systems

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

In order to measure this metric, someone has to:

1. Identify the organization's critical information assets unambiguously;
2. Determine or clarify the compliance obligations;
3. Assess the compliance of systems containing critical information assets.

All three activities are easier said than done. In our experience, the concepts behind this metric tend to make most sense in those military and governmental organizations that make extensive use of information classification, but even there the complexities involved in measuring compliance with a useful amount of accuracy would make it slow and expensive. Consequently, the low Accuracy, Cost and Timeliness scores all take their toll on the metric's PRAGMATIC score:

P	R	A	G	M	A	T	I	C	Score
48	26	36	41	56	13	19	46	12	33%

Thus far, we have considered and scored this and other example metrics from the perspective of management within the organization. The situation is somewhat different from the perspective of the authorities that typically impose or mandate security compliance obligations on others. We are not going to elaborate further ourselves but leave it to you as an exercise to re-score the metric on behalf of, say, a government agency responsible for privacy. Imagine yourself inside such a body, discussing information security metrics with management. What would they make of its Predictability, Relevance to information security, Actionability, Genuinness, Meaningfulness to the intended audience, Accuracy, Timeliness, Independence or integrity, and Cost-effectiveness? Go ahead, try out the PRAGMATIC method and tell us what you make of it ...