Security Metric of the Week #17: number and severity of audit findings

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

Our latest 'security metric of the week' builds on the following premises.

Firstly, the number and severity of audit findings bears some relationship to the state or maturity of the organization's governance, risk, compliance and security arrangements, along with the number, quality, scope and depth of the audits.

Secondly, since audits are invariably independent and formal, the number of audit findings is an objective, cheap and easy-to-obtain measure, as is the 'severity' (or gravity or importance) provided findings are routinely rated/classified by the auditors, which they usually are. The severity of audit findings also helps focus management attention on the issues that really matter.

[We are of course assuming that "audit finding" is a recognized term. Most if not all audit functions generate reports that identify and discuss discrete findings. Many also explicitly identify "audit recommendations", again as discrete items in the reports, so counting them is also a possibility.

This metric may be presented in purely numeric form (e.g. as graphs or pie charts or whatever), as text (e.g. a tabular report outlining each of the findings along with other relevant information such as when it was raised, when it should be actioned and closed, and who is responsible for the action) or both (annotated numbers or graphics).

When designing and specifying the metric, management probably ought to decide whether it takes account of the findings from internal, external and certification audits, management reviews and/or risk assessments etc., although it may not be necessary to define this formally: it could perhaps be managed dynamically according to the nature and number of issues to be reported (e.g. ignoring the less important findings/recommendations to concentrate on the biggies, whatever their source).

The metric may be a useful high-level/strategic metric, particularly as it is highly Independent and hence a Genuine measure, unlikely to be substantially manipulated by someone gaming the system.

P	R	A	G	M	A	T	I	C	Score
79	89	87	96	92	84	30	96	36	77%

Notice that, as worded above, the metric is not about information security findings specifically: all findings are counted. You may think it better to distinguish those audit findings that specifically relate to security, but doing so begs questions about how findings are categorized. Perhaps the auditors can be persuaded to categorize their own findings? It could be argued that practically everything in audit reports relates to information security in some fashion, and at the end of the day, management is not solely concerned with information security so does it really matter anyway?

With hindsight, the PRAGMATIC score of 77% that we calculated for the metric is probably on the low side: it looks as if we were rather pessimistic on the cost factor, especially if audit already creates and uses/reports the raw data for other purposes i.e. on their reports and in their databases used to track audit findings and recommendations. [By the way, there are probably other sexy numbers and information in audit's databases that could be used for further security metrics, provided they are not so confidential that they cannot be shared!]