Security Metric of the Week #23: Business Continuity Management (BCM) Maturity

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

The high PRAGMATIC score for this week's metric shows that we consider it a valuable measure of an organization's business continuity management practices:

P	R	A	G	M	A	T	I	C	Score
90	95	70	80	90	85	90	87	90	86%

This metric is designed on exactly the same lines as the HR security maturity metric, SMotW #15, using a maturity scoring table with predefined criteria for various aspects of business continuity management indicating various levels of maturity.

We are not going to give you the entire maturity scoring table now (you will have to continue waiting patiently for the book, I'm afraid) but here are two rows demonstrating the approach:

No business continuity management	Basic business continuity management	Good business continuity management	Excellent business continuity management
Nothing even vaguely approximating a policy towards business continuity	Something vaguely approximating a policy towards business continuity, though not very well documented, hard to locate and probably out of date	A clear strategy towards business continuity, supported by a firm policy owned and authorized by management and actively maintained	A coherent and comprehensive business continuity strategy, supported by suitable policies, procedures, guidelines and practices; strong coordination with other relevant parties
Business	Major business	Business impact	Business

No business continuity management	Basic business continuity management	Good business continuity management	Excellent business continuity management
continuity requirements completely unknown	continuity requirements identified, but typically just those mandated on the organization by law; limited documentation	analysis used systematically from time to time to identify, characterize and document business continuity requirements, both internal and external	continuity requirements thoroughly analyzed, documented and constantly maintained through business impact analysis, compliance assessments, business analysis, disaster analysis etc.

The table's four columns correspond to maturity scores of 0%, 33%, 67% and 100% respectively. Each row in the table considers a different aspect or element of the measured area, in this case business continuity management, laying out four markers or sets of criteria for the four scores.

If your management decides to adopt security maturity metrics like this, you could either take the scoring tables directly from the book (when available!), or use them as a starting point for customization. Adapt them according to your experience in each area, integrating good practices recommended by various standards such as ISO27k and NIST's SP800-series, and organizations such as ISACA and the Business Continuity Institute. Adjust the wording of the criteria to be more objective if you wish. Include specific criteria or conditions. Reference your policies, legal and regulatory obligations, whatever.

You may for instance feel that certain aspects of business continuity management are far more important than others, in which case you could weight the scores from each row accordingly ... but doing so would further complicate the scoring process and might lead to interminable discussions about the weightings, rather than about the organization's business continuity management maturity.

Similarly, you may prefer further or fewer columns, giving you more or less granularity in the criteria. Knock yourself out.

The percentage scoring scale lets us score things "towards the lower edge of the category" if appropriate, and to fine-tune the scores to represent a range of situations (e.g. if two businesses, departments or business units both qualify for the 3rd column on a certain criterion but one is a bit stronger than the other, its score might be a few percent higher than the other).

The flexible design of this style of metric, coupled with its high PRAGMATIC score, is why we find it so useful in practice. It is a particularly good way of measuring relatively subjective matters in a relatively objective and repeatable manner.