SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Metrics for Success: Assess the Probability of Business Loss

George Campbell

Originally Published in SecurityInfoWatch.com

October 2008

Assess the Probability of Business Loss

Objective: To estimate the probability of loss in areas of concern, given known vulnerabilities.

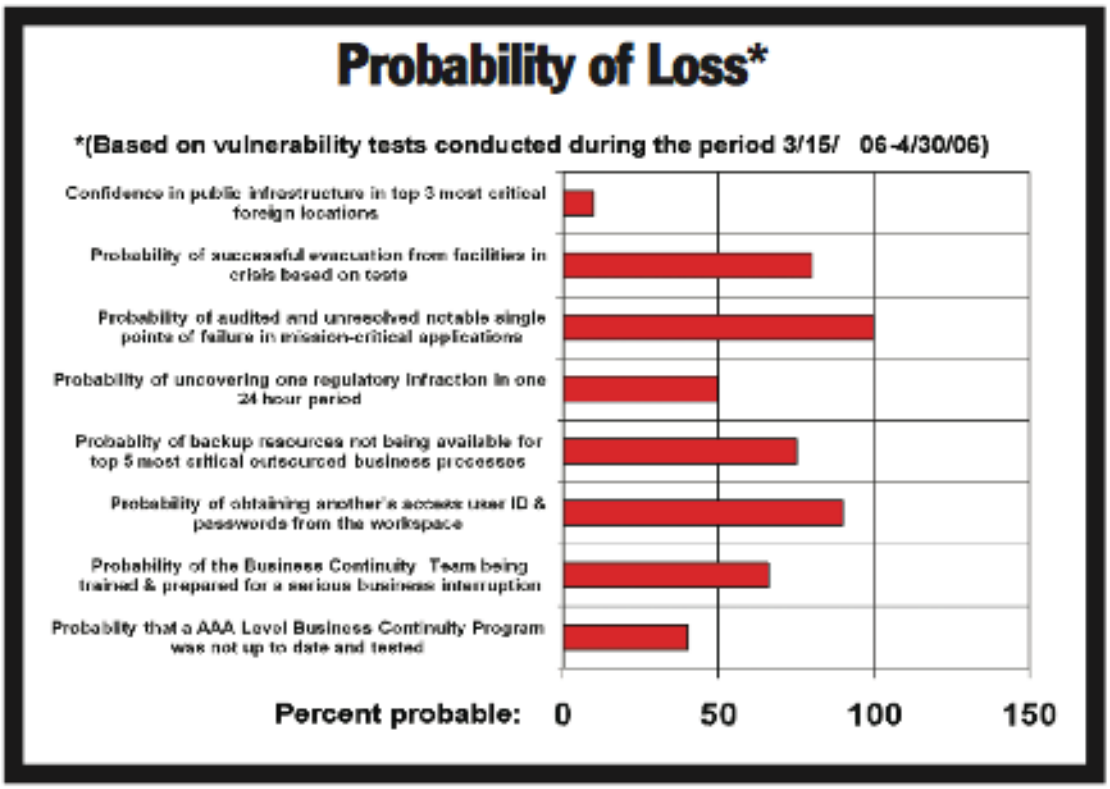
Results Sought: Help management to recognize that the business contains vulnerabilities that may affect customers. Eliminate plausible denial and engage management for follow-up. Obtain support for elimination of vulnerabilities. Increase participation in essential areas of risk ownership and accountability. Ideally, you want to hear: "I support your objectives in assessing these risks. I accept our responsibility to ensure remedial action on each of these corporate risks and will ask our general auditor to track resolution of each of these findings."

Strategy: To obtain this information, conduct multiple tests of policy-based or common sense safeguards in a variety of protection categories over a six-week period. It's important to advertise the tests and methodology in advance and to include objectives in an annual plan. Think of the strategy in four levels or steps:

* Your protection programs and tactics are built around the achievement of clear, measurable results in terms of reduced exposure to risk. Your first step should be to clearly outline those expected results.
* Make sure that assessment programs are an essential component of corporate governance. Present assessment results to senior management and the audit committee.
* Structure your assessments around measurable criteria of effectiveness (success or failure), and measure your risk and protection elements as you have advertised in your annual plan.
* When you know the results of your metrics, thoroughly analyze and report them in a way that is responsive to management's format for action and accountability.

Where Is the Data? The data is in the risk assessments you routinely perform, which examine the adequacy of key protection measures and uncover gaps in the quality of internal controls around critical assets and business processes. If you have appropriately structured your ongoing recorded measures, and have planned your risk assessment processes to

provide comparative metrics, you will have:
* results of tests that yield a percentage of protection system or process failures and successes;
* training records showing preparedness of key players;
* documented frequency and results of prior tests;
* down times of critical systems or business processes; and
*specific benchmarks of protection system performance.



George Campbell *is emeritus faculty of the Security Executive Council and former CSO of Fidelity Investments. His book,* Measures and Metrics in Corporate Security, *may be purchased through the Security Executive Council Web site,* www.securityexecutivecouncil.com. *The information in this article is copyrighted by the Security Executive Council and reprinted with permission. All rights reserved.*

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com