Determine the Exploitability of Selected Security Defects

By George Campbell

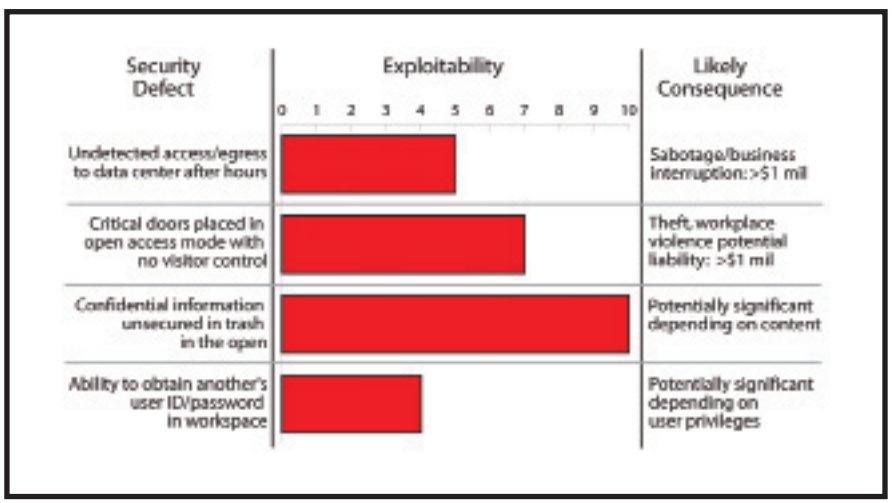
Objective: To estimate the probability of loss in areas of concern, given known vulnerabilities.

Results Sought: Engage management 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."

Risk Management Strategy: In the example on the right, Security has examined the lessons learned from several incidents and reviewed the results of Security Operations' tours and inspections over the past several months. They noted that four security defects were frequently encountered across the range of corporate facilities: undetected access to the 24/7 data center after hours, critical doors placed in open access mode with no visitor control, confidential information found in unsecured trash in the open and the ability to obtain another's user ID and password in the workspace. These defects, if exploited, would have varying degrees of consequence.

To quantify the exploitability of each vulnerability, the security team conducted 10 penetration tests over a two-week period during business and non-business hours, within spaces that management acknowledged to be sensitive. The results were as follows:

1. Five of 10 attempts to gain access and egress to the 24/7 data center after hours went undetected or unchallenged.
2. Seven of 10 tests found critical doors placed in open access mode with no visitor control.
3. All 10 tests found confidential information in unsecured trash in the open within the C-suite.
4. Four of 10 tests discovered examples of the ability to obtain another's user ID and password in the workspace, typically involving a note left in the open on or about a workstation.



Security's plan is to take these four fairly simple and straightforward examples of exploitable security defects first to the "owners" of the various spaces where penetration was achieved. They not only want to make these owners aware of the defects, but they also want to acknowledge where they affirmed the effectiveness of security practices. When pointing out deficiencies, they especially want to avoid accusation or surprise attacks. The goal is to use this data as a strong security awareness tool with the management team.

Where Is the Data? The data for exercises like this is in the risk assessments you should be routinely performing. Establish standards for protection at key locations and within routine business operations. It is essential to examine the adequacy of these protection measures to uncover gaps in the quality of internal controls around critical assets and business processes. This exercise also underscores the value of post-incident, lessons-learned examinations that reveal basic vulnerabilities in security measures. As far as potential consequences are concerned, Security can speculate on impact of the noted defect or they can obtain specific impact data from the business unit.

If you have appropriately structured your ongoing recorded measures and 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 awareness and preparedness of key players;
- documented frequency and results of prior tests;
- downtimes of critical systems or business processes; and
- specific benchmarks of protection system performance. STD

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/?sourceCode=std. The information in this article is copyrighted by the Security Executive Council and reprinted with permission. All rights reserved.