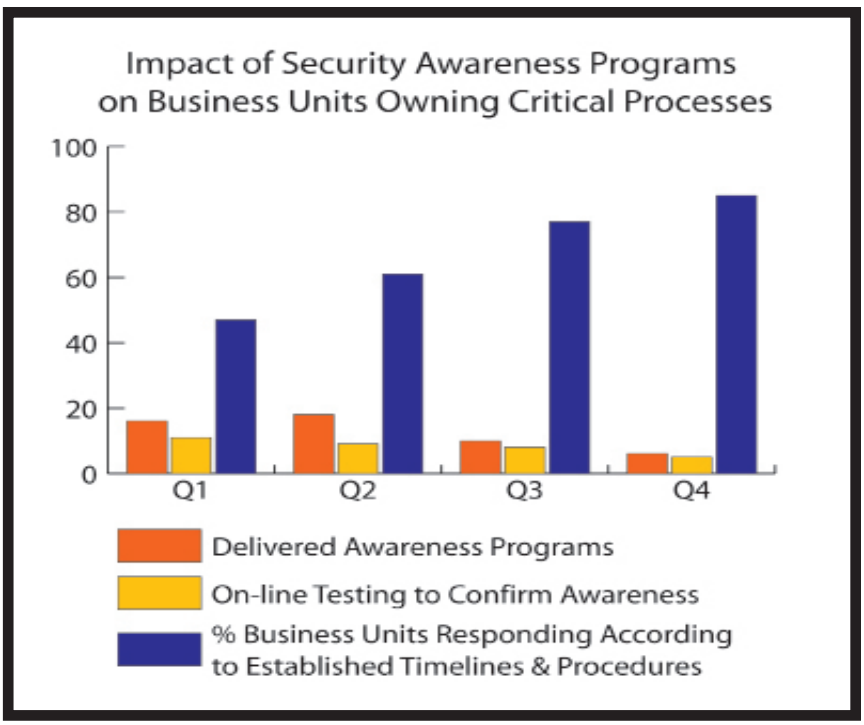
Empower Customers Through Awareness

By George Campbell



Security has a unique perspective on risk that comes from gathering, analyzing and understanding threat and risk data. This insight obligates us to make our customers aware of the risks that could affect them, especially when those customers control the most sensitive and essential business processes in our companies.

Objective: Simple. We have the data and we have the mission. We must tell the story, eliminate plausible denial, enable and empower our customers to own prevention through awareness of "what if."

Strategy: Every enterprise, whether public or private, has a core set of operational processes that are so essential to the company's mission and success that we must implement special protective measures to ensure their continuous availability. A key component of the overall protection strategy is the principle that the owner of each process is accountable for maintaining process integrity, and the employees who operate the process are the first line of defense.

In this example, Corporate Security identified the company's top 50 critical processes and the business units that own them. Security subjects these internal customers to various types of risk assessments at various frequencies to ensure that each process' uninterrupted availability is tested and verified. Security also plays a key support role by providing tailored risk awareness programs.

In the chart above, we see that awareness projects were phased into all of the business units owning critical processes over the course of the past year. To maximize awareness of the most significant risks, Security worked with each customer to tailor the awareness program format and content based on historical incident experience and issues identified in prior risk assessments. Throughout the year, online testing, such as a one-minute quiz on employee response to a specific scenario, was conducted when employees logged into the corporate network. Quarterly spot checks of active preventive measures by security officers on tours affirmed the currency and quality of awareness.

Contingency plans are always arrayed around the most critical business processes and involve both specific steps to be taken to mitigate impact and timelines associated with compensatory measures. The key measure is found in the percentage of critical functions that followed established protocols and procedures when a threat event presented itself. The chart shows a fairly dramatic increase (47 to 85 percent) in the quality of response over the year-long period, which confirms the effectiveness of the awareness programs.

Corporate Security must enable its constituents to be alert to risk and to know what to do when things go bump in the night (or day). We have limited resources and must depend on our customers to be the eyes, ears and, as demonstrated here, the initial responders to threats to critical business operations. We empower them to do the right things when we provide measurably effective awareness of responsibility. ▮

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. The Security Executive Council is a risk mitigation research and services organization for senior security and risk executives from corporations and government agencies responsible for corporate and/or IT security programs. In partnership with its research arm, the Security Leadership Research Institute, the Council is dedicated to developing tools that help lower the cost of security programs, making program development more efficient and establishing security as a recognized value center. For more information about the Council, visit www.securityexecutivecouncil.com/?sourceCode=std.