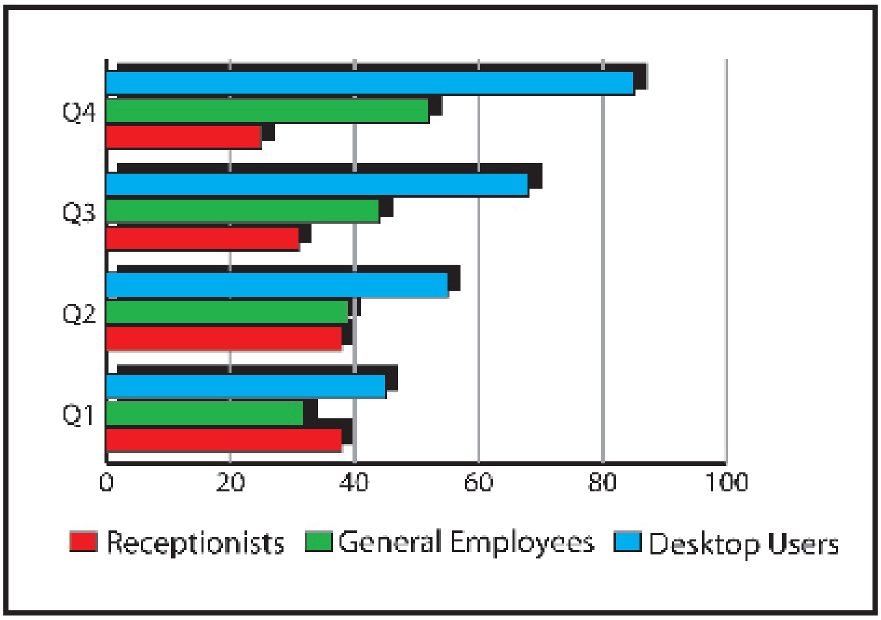
Measuring Security Awareness

By George Campbell



The objective: To measure security awareness by key stakeholders.

Results Sought: Increased ability to anticipate the organization's risk potential.

Risk Management Strategy: Two key measures of the effectiveness of a security program are: (1) how well security communicates the security responsibilities it expects employees to meet; and (2) the affirmation that those expectations are being met.

We all struggle with measuring the likelihood of a security event, but we are paid to anticipate risk. That expectation drives our multiple efforts to identify vulnerability through a variety of means, including risk assessments, countermeasure tests and incident post-mortems. When we use probes like these to better understand what happened and why, we may find that those in the best position to prevent or act responsibly were not aware or were negligent of their role in enterprise protection. We need to test and affirm employee awareness of security responsibilities, and periodic surveys of targeted populations are an effective way to accomplish this.

In the example above, our security organization has focused on a simple testing of awareness of access control responsibilities by targeted receptionists and desktop users and a sample of the general employee population. Receptionists are gatekeepers and should be empowered to maintain access integrity while welcoming visitors. In a more process-oriented way, the myriad of desktop users must follow established authorization procedures to gain access to pre-approved business applications.

The corporate intranet offers a variety of user-friendly means to quiz and reacquaint specific employee categories with security policy while identifying soft spots in awareness. Security officers on tours have frequent contact with receptionists and employees at access points and can pre-advertise an "access awareness day" with a simple quiz and handouts like badge reels or small reminder cards. Similarly, information security teams can engage desktop users at logon or other times to test awareness of security procedures.

Security awareness is a centerpiece of a measurably effective corporate security program. That principle requires us to craft and effectively communicate specific guidance to address potential areas of risk. I use "guidance" because many organizations abhor the term "policy." Use whatever description for your expectations you feel appropriate to your culture, but do not fail to identify critical expectations and advertise them. Logical and physical access control integrity is a fundamental security principle that touches virtually every employee, and it is too easy to allow an unknown tailgater to go unchallenged or to write off a simple computer security procedure because it's inconvenient.

Where is the data? The data you need to understand levels of awareness are in planned or random surveys of targeted employees or other stakeholders (such as vendors in possession of proprietary information or processes), risk assessments and post-incident analysis. Your various business environments may offer a variety of means to gather and reaffirm awareness data on security policy. Be creative; engage employees in the process. If this is done well, it will also help you build good PR for the security organization. **ST&D**

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.