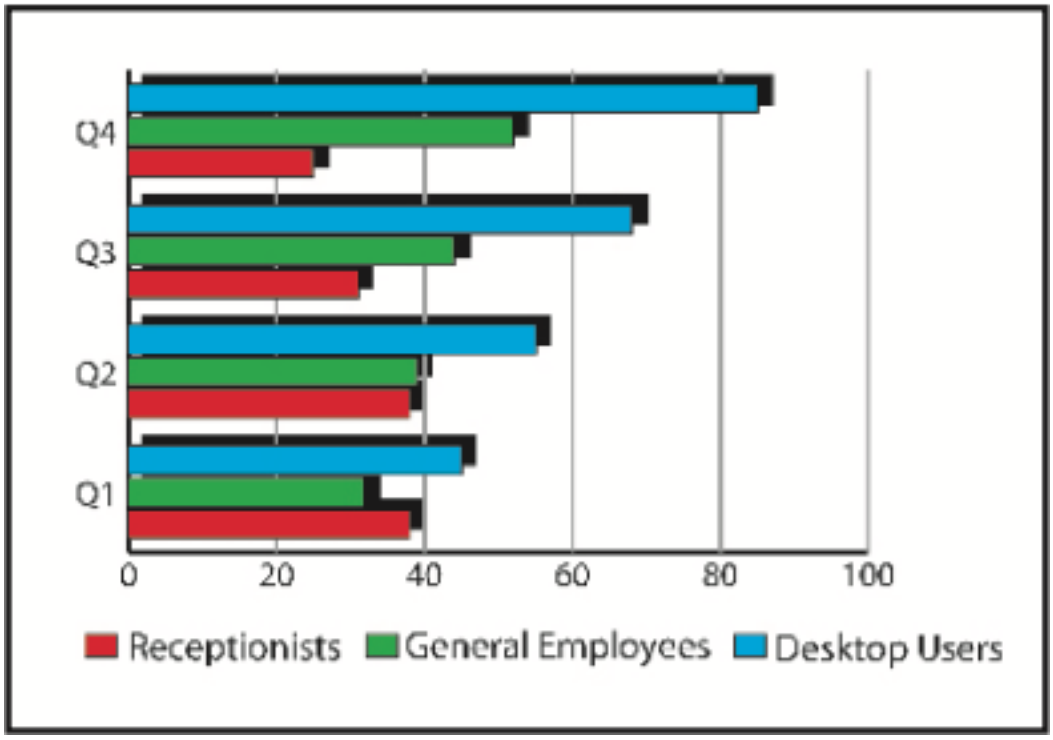
SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Metrics > Employee Awareness Program >

Measuring Awareness of Access Control Responsibilities

By George Campbell, Security Executive Council Emeritus Faculty



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 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 of or were negligent in 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, one 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, 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 aware-

ness. 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 you feel appropriate to your culture, but do not fail to identify critical expectations and advertise them. Access control integrity - logical and physical - 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.

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.

Originally published in Security Technology Executive

Visit the Security Executive Council website for other resources on Security Metrics: Measuring Awareness Programs

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website here: https://www.securityexecutivecouncil.com/

