Warning Signs of Security's Decreasing Influence, Part III

By George Campbell

For the past two months, I have been exploring how to determine the warning signs of security's decreased effectiveness and influence. If you cannot answer "yes" to the following three questions, you may have an influence problem:

1. Does the security program have the influence to help eliminate risky business practices?

2. Do employees and management accept the concept of shared responsibility for asset protection?

3. Does management believe the security program is adding value?

In my previous two columns I have discussed several kinds of warning signs, from budget reductions without consideration of increased risk, to continuing findings of exploitable vulnerabilities, to unresolved security-related audit findings. I will conclude with five more:

1. Security is not consulted before management makes changes to processes, products or relationships with evident security risk impact. Note the word "evident" in this sentence. Ignorance is one thing, but when it is clear that changes involve probability of risk and management still decides not to include us, we are a marginalized player at best.

2. Management fails to approve Security's recommendation for development and communication of a new or revised security policy to mitigate a consistent pattern of risk. What should we conclude when we have a convincing story on what steps should be taken to mitigate risk and they decide to leave things as they are?

3. Increased downtime of critical security safeguards that fail and go unattended. Think about this one! You have a "critical" safeguard (like a duress alarm in the executive suite or consistent unauthorized access to a sensitive area) that is unreliable and nobody is fixing it! Are you watching the dials on your dashboard? Two possibilities: either you are unaware of these vulnerabilities, or you have failed to take appropriate action. In both cases, count on your stock taking take a big hit sooner rather than later.

4. Security fails to effectively analyze its data on security incidents and thereby invites future risk that will seriously deplete leadership's confidence in us. While this closely resembles #3 and others, it really goes to the failure to establish a comprehensive, disciplined and ongoing process of incident and workload analysis. What are the trends and the common denominators? What steps are working and where are the gaps?

5. Decreasing engagement of essential internal partners in matters of clear security concern. This is not an isolated shortcoming — it is a summary result of all the failures mentioned in this series. You have not connected the dots between your security and risk message and the responsibilities of your organization's employees and business leaders. You either have not spoken their language or they have tuned you out.

I have taken a brief look at 15 danger signals that may indicate failing influence on critical issues or will clearly damage the credibility of the security organization and its leadership. Metrics provide an early warning system — they enable positive influence, action, attitude and policy. You have the data, now take an objective look at the competence of your data management capabilities. What metrics really make a difference in your contribution to value and your ability to influence results and standards of protection?

I would like to invite you to visit the Security Executive Council Web site and download a free PDF of my presentation "A Security Metrics Story: Turning Data Into Metrics." This step-by-step guide on how to build your security metrics program will help you demonstrate security's value through clear alignment with business strategy and objectives. Download it here: www.securityexecutivecouncil.com/smstory. ■

George Campbell is emeritus faculty of the Security Executive Council (SEC) and former CSO of Fidelity Investments. His book, "Measures and Metrics in Corporate Security," may be purchased through the SEC Web site. The SEC is a member organization for senior security and risk executives from corporations and government agencies. For more information and inquiries on membership requirements, visit www.securityexecutivecouncil.com/?sourceCode=std. The information in this article is copyrighted by the Security Executive Council and reprinted with permission. All rights reserved.