Q: We are organizing a security awareness program for employees, but we are not sure if such programs are effective. How can the effectiveness of security awareness programs be measured?

A: Security awareness programs help organizations substantially reduce risk. There are three major risk areas that may have vulnerabilities: technology, processes and people. Technology and process vulnerabilities can be detected and controlled, but vulnerabilities created or introduced by people are the most difficult to control. Security awareness training can help. However, people tend to forget, and new threats are always emerging, which makes it is necessary to reinforce security awareness training.

Although it is true that something that is measured can be better managed, measuring the outcomes of awareness training is difficult.

In a recent study, 80 percent of organizations said that security awareness training had reduced their staffs' susceptibility to phishing attacks. That reduction does not happen overnight, but it can happen quickly—with regular training being shown to reduce risk from 60 percent to 10 percent within the first 12 months.[1, 2]

Although it is true that something that is measured can be better managed, measuring the outcomes of awareness training is difficult. There are many metrics available for measurement of security awareness training, but most of them are used for providing assurance on compliance (e.g., percentage of employees attending awareness training, frequency of awareness training, frequency of training content updates). How can the effectiveness of security awareness training be measured?

One of the most important outcomes of security awareness training is to effect behavior change in employees. One of the most common aspects of security awareness training is to teach employees to report any abnormalities observed. To measure the effectiveness of social engineering awareness, employees are sent an email that prompts them to click on a link embedded in the body of email. The expected outcome is that employees report receiving the email to the security team. When most employees report receiving such an email, the organization can be assured that the majority of employees are aware of social engineering tactics.

Another indication of successful awareness training is a sudden increase in employees reporting abnormalities that were previously unnoticed. However, this initial increase fades over time as employees begin to understand the nuances of technology and become better informed.

SUNIL BAKSHI | CISA, CRISC, CISM, CGEIT, CDPSE, AMIIB, MCA

Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.

Developing definitive metrics to measure the effectiveness of security awareness training can be challenging, but organizations can reap the benefits of frequent training both in the short and long term when they are committed to educating employees.

Endnotes

1 Daly, J.; "How Effective Is Security Awareness Training?" Usecure, *https://blog.usecure.io/does-security-awareness-training-work#:~:text=In%20a%20recent%20study%2C%2080,within%20the%20first%2012%20months*

2 Cosgrove, A.; "Why Employee Cyber-Awareness Is Critical Every Day, Not Just During a Crisis," *Infosecurity*, 17 March 2021, *https://www.infosecurity-magazine.com/blogs/employee-cyber-awareness-crisis/*