

Awareness Training Is Necessary to Support Your Information Security Program

Roberta J. Witty, Ray Wagner

An information security awareness training program is a tool that all companies, regardless of size, need to implement. Without one, serious IT risks may be overlooked.

ANALYSIS

Information security awareness training is a much-maligned part of a complete information security program. Taken alone — without technology solutions such as malicious code detection and prevention, vulnerability assessments, firewalls, and identity and access management — a training program will not address all IT risks. Users of IT assets must know their responsibility in protecting these assets, as well as customer information, and the consequences if they fail to comply with information security policies. Therefore, Gartner considers an information security awareness training program to be an essential tool for all companies, regardless of size.

A survey conducted by MIT shows that awareness is considered one of the least-effective approaches to managing IT risk by survey respondents overall, although 70 percent of the respondents reported that their companies have awareness training programs. The survey also shows, however, that businesses with awareness training programs have mitigated statistically significant, higher levels of risk in all four categories (confidentiality, continuity, accuracy and flexibility). This somewhat contradictory position indicates that information security awareness training programs correlate to higher levels of IT risk that are mitigated within the company. These programs should not be dismissed lightly.

In this Spotlight, we present different aspects of an information security awareness training program.

In "Information Security Awareness Training Is Essential to Protect IT Assets," Roberta Witty, Rich Mogull, Ray Wagner, Amrit Williams, Kristen Noakes-Fry and Ant Allan discuss the business drivers and training basics, the roles within a company that require additional, specialized training for information security awareness, how to train your users and how much to spend on your information security awareness training program.

Kristen Noakes-Fry and Roberta Witty, in "Vendors Offer Diverse Methods for Information Security Awareness Training," profile the various technologies that companies can use to train their users, ranging from classroom-based training, to e-learning and customized training programs. Also noted are vendors that provide the ability to track the progress and measure the effectiveness of a training program.

In "Measure the Effectiveness of Your Security Awareness Training Program," Ray Wagner, Rich Mogull, Roberta Witty and Ant Allan outline a number of metrics that can measure how effective the training program within the company. These metrics are categorized as follows: process improvement, attack resistance, efficiency and effectiveness, and internal crunchiness.

Lastly, in "How to Manage an Information Security Awareness Program," Rich Mogull describes the management issues necessary for an effective training program, including creating a security policy and how to enforce it, as well as creating a culture of security within your organization.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509