

BRIAN MCCARTHY

# Security efforts still falling short

SURVEY FINDS COMPANIES PLACE EMPHASIS ON EFFECTIVE SECURITY BUT NONE ON USERS



**F**OR THE PAST four years, the Computing Technology Industry Association has commissioned a major study on information

security threats and responses.

This year's study revealed that human error was responsible for nearly 60 percent of information security breaches experienced by organizations during the previous 12 months. That figure was significantly higher than the prior year, when human error was blamed for 47 percent of security breaches.

Yet despite the prominent role that human behavior plays in information security, just 29 percent of the 574 organizations surveyed said that security training is a requirement for the IT staffs at their companies. Only 36 percent of organizations offer users security awareness training.

For security technology solutions to be truly effective, they must be accompanied by training and mass awareness of information security issues. This education must be pervasive throughout the organization—from the ground floor server room where the critical security patch issued on Friday wasn't installed until the following Monday to the top-floor boardroom where the CEO ignored policy, unzipped a file and unleashed a new virus strain across his company's network.

Ironically, the lack of strategic vision on the importance of security education and training most often occurs at the highest levels of the corporate hierarchy. Executives often have the least training for the security-related issues and problems

that their companies encounter. As a result, they often underestimate the impact that security breaches have on their operations.

Security administrators and director-level managers who have a greater degree of insight into the day-to-day impact of these issues often lack the analytical tools needed to monetize the security issues they face.

Increasing awareness at the executive level is most easily achieved by quantifying problems and creating business cases for solving them. One approach is to demonstrate in real dollars that the financial impact of security breaches can be very significant.

Respondents to the CompTIA survey were asked to monetize the impact of the last security breach, as well as the impact of breaches over the last 12 months. The mean values were more than \$11,000 for the last security breach; and just less than \$35,000 for breaches over the last year. Some reported a financial impact above \$50,000. So while a "garden variety" breach may be little more than an inconvenience, the potential for serious financial harm is always present.

Security awareness training, as distinct from specialized security training and certification for IT and security staff, is obviously an important part of security. But it has not been implemented by a majority of organizations. Just 36 percent of the 574 organizations surveyed indicated that their organization has this kind of training in place. And while 29 percent indicated that their organization will implement it at

some point in the future, 35 percent of organizations said they have no plans to do so.

Yet among those organizations that use security training, 84 percent said that it has resulted in a reduced number of major security breaches since implementation; typically through increasing awareness, giving staff the tools to better identify security risks, and improving security measures in general and response time of staff to problems.

The small amounts of time and money invested in training may suggest to end users that it is not an organizational priority. Greater awareness levels of the real benefits of training and the risks associated with not having it are needed at the highest end of the corporate hierarchy to overcome this.

To be truly effective in preventing and combating information security threats, organizations need to take

**SECURITY SOLUTIONS MUST INCLUDE TRAINING AND AWARENESS OF ISSUES.**

further steps by spreading awareness and knowledge from a select group of IT staff to larger

portions of their employee base. Decision makers must become better informed about the real costs of security breaches and the real return on investment available with both security training and certification.

The best security technology in the world won't work without appropriate human intervention, the skills of implementers and the vision of managers to properly deploy and apply it. *e*

*Brian McCarthy is the chief operating officer for the Computing Technology Industry Association ([www.comptia.org](http://www.comptia.org)).*