

The weakest link in the data security chain?

The person behind the PC.

According to the fourth annual CompTIA (Computing Technology Industry Association) study on information security and the workforce, Human error was responsible for nearly 60 per cent of information security breaches last year. This figure was up from 47 percent in 2004.

Despite the prominent role that human behavior plays in information security breaches, just 29 per cent of the 574 organizations worldwide that participated in the survey said security training is a must for employees. Only 36 per cent of organizations offer security awareness training, the study found.

"The primary cause of security breaches - human error - is not being adequately addressed," Brian McCarthy, chief operating officer of CompTIA, said in a statement. "The person behind the PC continues to be the primary area where weaknesses are exposed."

CompTIA also noted that in the last several years, organizations have equipped themselves with sophisticated security infrastructure that better detect and prevent attacks.

The study found that 96 per cent of respondents use antivirus software while 91 per cent have firewalls and proxy servers, in addition to disaster recovery plans, intrusion detection systems and information security policies.

McCarthy said: "As we get better from a technology standpoint, many organizations seem to believe that technology solutions alone are sufficient to turn back all attacks, and a level of complacency may be setting in."

The CompTIA security study, over the four years it has run, also indicates that virus and worm attacks are a common security concern among respondents. The lack of user awareness, browser-based attacks and remote access, were the next most frequently mentioned security problems.

Source: <http://www.Silicon.com> (Security Strategy article written by [Aaron Tan](#))

Published: Wednesday 12 April 2006