For nearly a decade, CIO Magazine and CSO Magazine have partnered with Pricewaterhouse-Coopers to produce an annual “Global State of Information Security Survey.” The 2012 survey was another massive undertaking with 9,600 respondents from 138 countries sharing their perceptions on key issues in information security.

I would like to share with you what I consider to be key highlights. When asked to describe their company’s “approach to protecting information security,” we got the following results:

> 43 percent (“front-runners”) claimed they have “an effective strategy in place and are proactive in executing the plan”
> 27 percent (“strategists”) said they are “better at getting the strategy right” than they are at “executing the plan”
> 15 percent (“tacticians”) shared they are “just getting things done”
> 14 percent (“firefighters”) lament “they do not have an effective strategy in place and are typically in reactive mode”

Let’s examine some of the key elements that define the front-runners. Front-runners consider identifying client requirements (50 percent) as the number one issue that drives their firm’s information security spending. That’s almost double the percentage in any other group. Front-runners, by wide margins over the other groups, claim protecting customer information (73 percent), financial data (65 percent), and intellectual property and trade secrets (63 percent) are “extremely important.”

Let’s now look at overall responses regardless of groupings. Seventy-two percent say they are confident their organization’s “security activities are effective.” That’s a significant improvement in the ability of firms to get visibility into security issues; in 2007, 40 percent reported that they did not know how many security incidents had occurred in the past 12 months. That dropped to nine percent in the 2012 survey.

Advanced persistent threats remain a “dangerous and increasingly common threat” with significant percentages of respondents agreeing that the issue of advanced persistent threats drives their company’s security spending. Yet only 16 percent of survey participants say that their company has a security policy that addresses advanced persistent threats. In fact, the 2012 survey shows decreases in security incidents for companies that have network access control software, identity management technology, employee security awareness training programs, and centralized security processes. Personnel background checks, monitoring employee use of the Internet, and identity management were listed as the top three security safeguards in place.

“During the past three years there has been a noticeable increase in threats that originate from customers, partners, and suppliers.”

Where are the threats coming from? During the past three years there has been a noticeable increase in threats that originate from customers, partners, and suppliers.

So, are enterprises more or less protected than they were six years ago? The answer is both promising and disconcerting. Here’s the news to be concerned about: if we go back to the 2006 survey, it revealed that 84 percent of respondents were “very” or “somewhat” confident that their company’s information security activities are effective. By 2012, this number dropped ominously to 72 percent. The good news in that data point is there’s plenty of work to be done in protecting our enterprise. If you would like a full copy of the “CIO/CSO/PwC 2012 Global State of Information Security Survey,” email me at gbeach@cio.com.

Gary Beach is the publisher emeritus at CIO Magazine and former publisher for Network World, ComputerWorld, and CIO Magazine. Follow Gary at twitter.com/gbeachcio.