

What's Keeping Infosec Professionals Awake at Night?

An in-depth look at the results of the 2008 annual ISC² Global Information Security Workforce Study reveals the growth both in size and influence of the profession. It also reveals what is worrying security professionals ... and the answer to that is plenty, finds **John Sterlicchi**

Driven by pressure over data loss issues and regulatory compliance, it is a foregone conclusion that IT security will expand significantly over the next few years.

The number of information security professionals worldwide will increase to almost 2.7 million by 2012 from roughly 1.66 million in 2007, according to the study which was undertaken for ISC² by analyst firm Frost & Sullivan.

Together, data loss pressure and compliance have driven accountability for information security to the executive level with 49 per cent of information security professionals reporting to executive management or boards of directors, compared to 21 per cent in a similar study conducted in 2004.

Approximately 40 per cent of the 7 548 respondents to the web-based survey were C-level executives or at the IT manager level. Roughly 30 per cent of respondents were involved in security management in the 2006 study.

They were also more globally representative. Respondents came from the three major regions of the world: Americas (41 per cent), EMEA (25 per cent), and Asia-Pacific (34 per cent). Interestingly respondents from Africa, Latin America, and Oceania (which includes Australia, Fiji, New Zealand, French Polynesia, and Guam) comprised 17 per cent of the total. In all, 100 countries were represented.



Technology solutions are not enough to solve an organization's security problems

Indicating a changing focus in their roles, one third said their primary functional responsibilities are mostly managerial and an additional 48 per cent said their functional responsibilities will be mostly managerial in the next two to three years.

In addition, this year's study showed a marked increase in the number of security professionals, 81 per cent, who consider communication skills to be a critical part of their jobs, while business skills were also seen as very important or important by 69 per cent.

"Frost & Sullivan believes this reflects the realization by executives that technology solutions are not enough to solve an organization's security problems," said the study. "Information security professionals are tasked to perform more education and training functions within organizations."

The security professionals' primary concerns for effectively securing their organizations' infrastructures involve the significance of corporate security policies and why they should be enforced as well as avoiding reputation damage.

Three quarters indicated the impact of service downtime (73 per cent) and damage to the organization's reputation (71 per cent) as top/high priorities while customer issues related to privacy violations (70 per cent) and customer identity theft (67 per cent) are also a top/high priority.

Concern over reputational damage was only just on the radar in the previous study, according to Eddie Zeitler, executive director of (ISC)², but it is a big worry today in light of the growing number of breaches.

"Customers are actually starting to care if organizations they do business with gets their names flashed across the Wall Street Journal," said Robert Ayoub, an analyst and author of the study at Frost & Sullivan.

Three-quarters said viruses and worm attacks are a top/high threat while next in line for concern are hackers and inside employees as potential security threats.

A couple of perhaps less surprising results were highlighted in the report. Banking/insurance/finance sector respondents have a greater concern for all security threats, such as hackers, viruses and other threats compared to other industry segment respondents. Government sector respondents see cyber terrorism (41 per cent) as a top/high concern, much more so than professionals in other sectors.

The study found users following security policy; management support of security policies; training of staff on security policies; qualified security staff and software solutions ranked as the top five factors affecting information security professionals' ability to protect and secure the computing infrastructure from breaches, misuse and abuse.

The study concluded information security is a global, cross-vertical, organization-wide concern that cannot be addressed with technology solutions alone.

Security management will always require the proper balance between people, policies, processes and technology to mitigate the risks associated with today's digitally connected business environment. ■