AMCHAM conference on IT security
new risks and new responsibilities

The American Chamber of Commerce (AMCHAM) last month held a conference on IT Security, with speakers such as David Hagen from CSSF, David Pike from Ernst & Young and Charles Delbrassine from Deloitte & Touche presenting their experiences and research into IT security and risk strategies. The audience of around 70 professionals represented sectors such as law, consultancy, banking, recruitment and technology development.
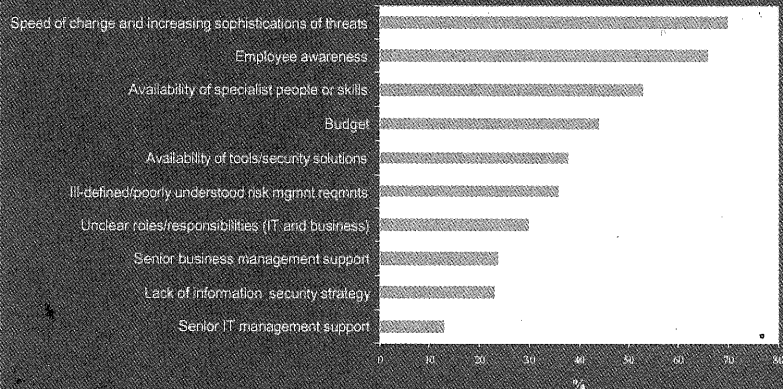
Why secure information?

Keynote speaker David Hagen, head of IT audit at Commission de Surveillance de Secteur Financier (CSSF), discussed today's increased risk, and the fact that companies need to implement security measures in order to avoid trade secrets being revealed as well as to avoid any manipulation of and damage to the information system itself. "Information security is all about determining and controlling its retention or diffusion... stopping it being manipulated and guaranteeing its integrity."

Key barriers to effective IT security

Speed of change and increasing sophistications of threats
Employee awareness
Availability of specialist people or skills
Budget
Availability of tools/security solutions
Ill-defined/poorly understood risk mgmnt reqmnts
Unclear roles/responsibilities (IT and business)
Senior business management support
Lack of information security strategy
Senior IT management support

Source: E&Y Global Information Security Survey 2002

However, Hagen stressed that there is not just a corporate risk but also a danger for individuals, and therefore responsibility for security falls on both sides. For example, 800 portable PCs were lost in France in 2001, largely in taxis and planes, rendering a great deal of corporate information vulnerable. Similarly risky are PDAs with infrared capabilities – it is possible for a hacker to synchronise with the machine from a distance, perhaps if it has been left for just 10 seconds on a table in a restaurant or at the airport. "Social engineering", or manipulating people, in order to obtain information, was yet another method identified to access personal email accounts, credit card details, internal phone lines and passwords.

Consequently Hagen concluded that every employee must adhere to a strict security policy. "Its not enough to install security systems, specialised programmes and other firewalls. It is fundamentally necessary to put in place a security charter which implicates the company's staff and its management." Furthermore, "It is irresponsible to promote an `information` society, a society where e-trade, m-trade and e-business are omnipresent, without teaching the surfers the basics of information protection, whether they be private individuals or professionals."

White Hat Hackers

Charles Delbrassine, senior manager at Deloitte Consulting manages the IT infrastructure department for the company. His White Hat Hacking team identify and expose security weaknesses so that they can fix any breaches before they can be taken advantage of by others (such as Black Hat Hackers). During the conference the team demonstrated hacking into a networked web server and a password-protected document and spoofing emails (giving them the appearance of coming from someone else), with the culmination being the live defacement of a website. In April 2002 alone, 1,126 websites were defaced by hackers.

Return on security investment

David Pike, director of Ernst & Young`s Technology & Security Risk Services, presented the arguments for outsourcing IT security by revealing findings from the company`s 2002 security survey. Highlights included; 40% of organisations surveyed do not investigate information security incidents, only 40% felt "very confident" in their ability to detect attacks and key barriers were employee awareness (60%), specialist skills (50%) and budget (44%). This led to a debate by the speakers on the best ways of demonstrating return on investment and how to marry exposure to risk with cost. As Stephan Schmitz, director of global risk management at PricewaterhouseCoopers pointed out, this demands that IT risk be linked to the overall business risk.

In summary Paul Schonenberg, AMCHAM chairman, referred back to an original argument from Hagen, concluding that a serious threat is posed from individual and internal sources, so companies should first focus on establishing a solid HR foundation, with an adherence to best practices, and an introduction of background security checks.

For further information on AMCHAM events, including a conference on e-learning planned for late September, visit www.amcham.lu