Ειδήσεις για την ΑΣΦΑΛΕΙΑ στις ΤΠΕ απ' όλο τον κόσμο...

Δελτίο 1
28 Δεκέμβρη 2005

"What Tech Skills Are Hot for 2006?"
Computerworld (27/12/05); T. Hoffman

Contrary to the widespread fear that off-shoring initiatives are bleeding the U.S. IT job market dry, 2006 is shaping up to be a banner year for technology hiring. Through 2005, only 5% of U.S. IT workers had lost their jobs to off-shoring, while job postings on Dice.com for developers, project managers, and help desk technicians all rose by 40% or more from January to September of 2005 compared to the same period a year earlier. A recent survey found that the four most sought-after skills in 2006 will be application development, information security, project management, and help desk skills. Most of the jobs going overseas involve basic coding, enabling U.S. companies to catch up with their backlog of projects, which has increased the demand for developers with Java and .NET skills. Employers are also looking for applicants with relationship management skills who have knowledge of a specific industry, enabling them to interact with business managers. Application development has also become more stratified, notes NStar's Eugene Zimon. "I would see the need for application developers as much more specialized in terms of developing integration components, user interfaces, and reusable components," he said. Information security skills are still very much in demand, though the recent proliferation in the number of workers who have obtained clearances has moderated compensation rates. Shortages are beginning to appear in the ranks of workers with government clearances and network security skills, however. Compliance initiatives such as HIPAA and Sarbanes-Oxley have thinned the pool of available project managers with specific skills in those areas. Many companies are also handicapped by their geography, as a constricted labour supply is often a factor unique to a specific location.

"The Thinkers: Data Privacy Drives CMU Expert's Work"
Pittsburgh Post-Gazette (26/12/05); M. Roth

Carnegie Mellon's Data Privacy Lab, headed by L. Sweeney, an associate professor of computer science, has the dual focus of advancing the security of personal data and working with the government to conduct terrorist surveillance without compromising citizens' privacy. Sweeney has demonstrated the ability to identify people with only limited information, prompting her to develop the Identity Angel, software that determines how much of an individual's personal information is available on the Internet, and whether that information could be used to obtain a credit card. Many people include their name, address, and Social Security number on resumes that are posted online, and occasionally add their date of birth, which provides all the information usually required to obtain a credit card. Sweeney insists that surveillance and privacy are not mutually exclusive propositions. One tool developed at the lab changes the image of a person's face on video surveillance so that investigators must make sure that the person is engaging in suspicious activity before they seek an injunction to reveal the person's true face. To generate a new face, the program either fuses together the features of two similar faces, or creates a clown face impervious to detection with facial recognition software. Another tool is designed to track potential bio-terrorism attacks by monitoring the number of people seeking treatment for a specific disease while preserving the patients' ano-

nymity. While the government has yet to fund wide-scale development of Sweeney's research, she is convinced that it is only a matter of time. "It's inevitable for society to adopt anti-terrorism provisions," Sweeney said. "And our type of technology is the only way for society to enjoy the benefit of those increased pursuits while at the same time maintaining the civil liberties that are the cornerstone of the country."

"New Breed of Cyber Attack Takes Aim at Sensitive Data"
USA Today (27/12/05) P. 1B; J. Swartz

Tech-security experts are warning of a new type of cyber-attack that spies on the computers of employees with access to data such as credit-card numbers and bank account numbers. The attacks, perpetrated by Asian and Eastern European organized-crime groups, use malicious email attachments that appear to come from business associates and are difficult to spot. "These new attacks are corporate espionage," says Patrick Hinojosa of Panda Software, which, like Symantec and McAfee, is working on new product features designed to detect such attacks. Corporate spies in Israel this year put malicious code on the PCs of executives at various organizations - such as the high-tech military contractor IMC and the cable-TV company Hot - in order to steal information. Email containing suspicious code was also sent to seven research-and-development employees at a U.S. transportation company in November and December, attacks that were discovered by the email security company MessageLabs. High-tech criminals have made their information-fishing efforts much more targeted now that computer-security software and hardware has become more effective against broader virus attacks.