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

Δελτίο 4
14 Γενάρη 2006

"Recruiter Interview: The Outlook For High-Level Hiring in 2006"
CareerJournal.com, January 3

In an interview about the nationwide executive hiring outlook, a managing director of a Boston-based executive search firm discusses the key trends that will impact the hiring of executives in 2006. In certain key industries, such as digital media, online advertising and Internet security, there are already signs of strong demand over the next 12 months. Moreover, this imbalance in the supply and demand of talent in certain sectors is leading to upward pressure on compensation. The interview also provides insights about the types of management and leadership traits that are most in demand by recruiters as well as tips on how to analyse the hiring situation at any company. In terms of industries showing strong demand for IT professionals, digital media is one of the industries at the forefront. Almost all traditional media companies are looking for talented executives familiar with technological innovation such as streaming audio and pod-casts. In addition, "anything to do with online advertising" and Internet security are drawing the attention of corporate recruiters. In terms of executive positions most in demand, chief executive officers and vice presidents of sales, marketing and business development are at the top of the list. For executives with specific skills, such as familiarity with interactive-marketing tools, there is especially strong demand. In response to the limited supply of talent for these positions, the compensation outlook is becoming rosier as well. At companies of every size, compensation packages continue to become more attractive. As older baby boomers retire and corporations attempt to replenish their ranks, there will likely be increased demand for talented IT workers - but only if inflation remains in check and the economic outlook remains upbeat. Going forward, be aware that there can be a significant difference between what is being told to prospective employees and what the real story is in terms of the company's overall competitive situation. Many companies try to gloss over difficult situations when wooing executive candidates.

"U.S. Call Centers Spawn Subculture in India"
Seattle Times (via Washington Post), January 8

At call centers across India, young workers - many of whom now use American names and celebrate American holidays - are creating a new subculture that in many ways challenges the traditional underpinnings of Indian society. Along the way, these call center agents are absorbing the values and mores of American society and using their new-found wealth in ways unimagined by previous generations. Increasingly, however, there has been a cultural backlash against the country's young BPO workers, as media outlets and outside observers point out that many call centers are nothing more than "swanky sweatshops" where young workers toil day and night in highly regulated work environments and are unable to observe certain religious or family occasions. The emerging call center subculture in India has developed so quickly since many employees not only work together - they also drink together, dance together, date one another and celebrate holidays together. Their jobs require them to learn English better and to keep up with trends in U.S. pop culture. As they become more familiar with American culture and business, they have also developed "boundless expectations" about

their new careers. As more call centers and multinationals enter India, workers have started to perceive themselves as hot commodities worthy of correspondingly high salaries. On the flipside, there is a growing perception that BPO workers are greedy, individualistic, and short-sighted. Citing low pay and dead-end jobs, outside observers are now suggesting that call center jobs have lost much of their initial allure. Popular books and Internet sites, too, are less positive than ever before about India's new call center subculture. Meanwhile, a generational divide has widened, as older Indians complain that their children are too busy, with no time for weddings, holidays or relatives. While young people's social life used to revolve around family, now it is increasingly focused on friends and work.

"Homeland Security Helps Secure Open-Source Code"
CNet (01/10/06); J. Evers

The Dept. of Homeland Security has awarded $1.24 million to Stanford University, Coverity, and Symantec to search for vulnerabilities in open-source software and to improve Coverity's proprietary tool for analyzing source code. Stanford is receiving the lion's share of the money, which the department will pay out over three years. Stanford and Coverity will construct an application that conducts daily inspections of code submitted to popular initiatives, compiling a database open to developers once the system begins operating in March. Developers working in the Linux, Firefox, or Apache spaces, for instance, will be able to repair bugs before they are codified into a public release. "We're going to make automatic checking deeper and more thorough using the latest research and apply this to the open-source infrastructure to make it more robust," said Stanford professor D. Engler. Symantec will contribute security intelligence and conduct tests of Coverity's proprietary analysis tool. The move will help the open-source community catch up with their commercial counterparts, who regularly use tools to analyze source code. Open-source programmers are more likely to manually check each other's work because the analysis tools are prohibitively expensive. Commercial software developers will also benefit from the program, as they will be able to apply Coverity's tool to their own code. Some in the open-source community have criticized the initiative for not going far enough, calling for Coverity to distribute its tool directly to the developers, so that they can check their own code. Among the open-source initiatives that Stanford and Coverity plan to check are Apache, BIND, KDE, Linux, Firefox, OpenBSD, OpenSSL, MySQL, FreeBSD, and Ethereal.

"Microsoft Research India to Work on Cryptography"
Infoworld Netherlands (01/10/06); J. Ribeiro

Microsoft Research plans to take advantage of the superior mathematical skills available in India by establishing a cryptography group at its lab in Bangalore. Cryptography for mobile phones, radio frequency identification units, and other small devices will be the focus of the cryptography group at Microsoft Research India, according to Ramarathnam Venkatesan, senior researcher in cryptography at the lab. "We will be researching methods that don't assume a lot of computation power," says Padmanabhan Anandan, managing director of Microsoft Research in India. More specifically, the lab will develop new cryptographic primitive operations involving encryption, decryption, and authentication algorithms, as well as analyze and attempt to break current algorithms. The cryptography group will have an opportunity to collaborate with experts at the Indian Institutes of Technology and the Indian Institute of Science. The Microsoft Research India group will also work with researchers in Israel and other countries, says Anandan.

"Security Conference Focuses on Collaboration"
Telephony Online (01/10/06); T. McElligott

Keynote speakers from the federal government and the communications, transportation, and utility sectors shared their horror and success stories and wisdom this week at the inaugural Homeland Security for Networked Industries conference in Orlando, where collaboration was a focus of talk. Department of Interior CIO W. Hord Tipton urged more collaboration among the various sectors of private industry and held up his department and its oversight of 70,000 employees and 200,000 volunteers spread throughout several agencies as an example of the challenges that lay ahead. "This is about securing our nation's infrastructure for a better prepared America," said Tipton, who along with others stressed the need for risk assessment, given that not every contingency could be covered. "All assets are not created equal, so you have to be able to pick the ones that matter," said McAfee's Eric Winsborrow, explaining that companies should examine what assets are most vital to them before formulating a policy. AT&T vice president of operations Roberta Bienfait called for a more proactive rather than reactive approach, holding up as an example a potential bird flu outbreak. She said an outbreak "could take 40 percent of our workforce. So we have to know how we would run our network without our employees." Also calling for collaboration between the public and private sector was Donald Purdy, acting director of the Department of Homeland Security National Cyber Security Division. "Information sharing is critical, but it has to move beyond that to real collaboration to mitigate risks within and between these sectors," Purdy said.

"The Legal and Practical Implications of Recent Attacks on 128-bit Cryptographic Hash Functions"
First Monday (01/02/06) Vol. 11, No. 1; P. Gauravaram, et al.

Exploits of 128-bit hash functions MD4, MD5, RIPEMD, and HAVAL-128 presented at Crypto 2004 by X. Wang et al. demonstrate insecurity when the functions are used with processing applications where the property of collision resistance applies, thus disqualifying them as collision resistant hash functions. MD5's vulnerability to these attacks is of particular concern, given its wide usage in applications that include digital signature generation and verification and software integrity assurance of numerous products. This discovery puts the future employment of MD5 in digital signature generation and other applications in doubt, and the National Institute of Standards and Technology (NIST) intends to phase out SHA-1 by the end of the decade, and urges the replacement of SHA-1 and 160-bit hash functions with stronger algorithms available in the NIST-approved Federal Information Processing Standard. Various researchers contend that digital signature technology is critically dependent on the non-repudiation property, and the Xiaoyun exploits allow both the signer and verifier of a digitally signed message that uses MD5 to circumvent this property and thus cheat each other. This debilitates the evidential value of digital signature technology in which all of the mentioned hash functions are used for signature purposes. The attacks on MD5 can also enable a third party to alter the contents of a digital certificate without changing the certification authority's digital signature. Collision attacks on the hash functions apparently do not negatively or significantly impact password verification schemes. In addition to the SHA-1 phaseout and the cessation of 128-bit and 160-bit hash function use, it is recommended that new approaches to hash function design be devised by introducing tough constraints in basic security properties to defeat current and new cryptanalysis methods.

"Computer Security Graphical Passwords"
Technology News Daily (01/10/06)

Rutgers University-Camden computer science professor Jean-Camille Birget and colleagues have developed a new computer security program that makes use of graphical passwords and an icon system. The new program works by having a user select areas of a complex picture (such as a landscape or cityscape), or "click points" that are easier to remember than a password consisting of letters and numbers because of their selection in a relatively random manner. During the researcher's study, users chose 10 icons, which were then scrambled with nearly 200 others. Users gained entry into the system by locating the shapes, such as triangles, that have their icons in the corners, clicking inside the shape, and repeating the process 10 times. The program does not require users to click on their icons, which makes it difficult for someone to steal their password by shoulder surfing. "The main idea behind our model is to allow a user to prove knowledge of a secret, without revealing the secret itself to either the authenticating party or a potential observer," says researcher L. Sobrado.

"FBI Says Attacks Succeeding Despite Security Investments"
SearchSecurity.com (01/11/06); B. Brenner

The FBI has reported that the substantial investment companies have made in cybersecurity has been unable to stem the tide of attacks, and that many security breaches are not reported. The 2005 FBI Computer Crime Survey found that more than 5,000 security incidents occurred in the 2,066 organizations polled, despite the nearly universal existence of security software and hardware. China, the United States, Nigeria, Russia, Germany, and Romania were among the most commonly identified countries of origin for attacks that originated outside of the organization. "I continue to be surprised, not at the variety of incidents, but at the magnitude of flaws in deployed systems and the subsequent attacks and losses, all of which are accepted as business as usual," said Purdue University computer science professor E. Spafford, who was quoted in the report. "So long as we continue to apply patches and spot defences to existing problems, the overall situation will continue to deteriorate. Without a significant increase in focus and funding for both long-term cybersecurity research and more effective law enforcement, we can only expect more incidents and greater losses year after year." The most commonly used security tools were antivirus software and firewalls, while more sophisticated techniques such as biometrics and smart cards were only infrequently deployed. Only 13 percent reported that they did not experience a security incident in the last year, while the typical organization saw several different types of attacks, with almost 20 percent reporting 20 or more incidents. Almost half (44 percent) reported that they had experienced an attack originating from within their organization, highlighting the need for background checks for every employee. Most commonly, organizations added and updated security systems after learning of a breach, though a large number admitted to not reporting the incident.

European Union Is 50 Years Behind the United States for Innovation
Financial Times (01/13/06) P. 2; T. Buck

A recent study has found that the European Union ranks so poorly on measures of innovation such as research and development spending, patents, and science and engineering graduates that it will be at least 50 years before it will catch up to the United States. Sweden, Denmark, Finland, and Germany were the only countries found to be able to rival the United States in its innovation ability. "The innovation gap between the EU25 and Japan is increasing and the one between the EU and U.S. is close to stable," according to the Innovation Scoreboard. Innovation is a critical measure of a nation's technology industry because it determines the ability of a country to convert core research into marketable technology, fueling economic growth and creating new jobs. The report highlighted the diffuse nature of the European Uni-

on, finding that countries such as Finland and Germany led the pack, countries such as the Czech Republic and Greece are gaining ground, while Spain and Poland are declining. Though not in the European Union, Switzerland ranked second in overall innovation, behind Sweden but still ahead of the United States and Japan. Despite their recent economic success, the United Kingdom and Ireland had a worse showing in this scoreboard than in previous studies. Germany has long been credited as an economic leader and boasted a superior innovation score though it was cited as having a lack of science and engineering students and a weak youth education system.