

# The community should unite for security

As criminals get more sophisticated, the only way to guard against the onslaught of phishing, pharming and bot network attacks is to work together, and that's where CIPS comes in

There are a number of key trends right now leading to optimization of technology, such as encryption in Windows Vista. However, optimization of people and process is still needed, as is a common community to receive reliable security recommendations and information.

Organizations are still continually being bombarded by threats such as stealthy viruses, worms, and remotely managed bots parked within thousands of computers systems. Adding to this deluge is adware, spyware, graphical spam (that is harder to detect), denial of service attacks, file-corrupting malware, e-mail, videos and instant messages containing damaging payloads. Financially-focused threats are on the rise and people are the targets.

Good examples are identity theft and the loss of personal or customer data. A glance at headline news about lost hard drives is enough to fire the imagination about the kinds of fraudulent activities being perpetrated by financially-motivated and increasingly organized criminals. There is the notable example of a U.S. Veterans Affairs laptop, stolen with more than 20 million records. Moreover, data protection is essential for compliance and privacy requirements – a major con-

sideration for executives. Educating people and instituting security processes and protocols are key elements for a sound security program. This people-and-process focus extends into wireless, mobile, and VoIP growth, where a more complex security profile is needed to manage and protect data.

Technologically, there is confidence in managing threats. However, the people and process components needs reinforcement by educating users about threats. These include phishing attacks seeking ID and passwords, avoiding e-mails with attachments and restricting Web surfing in which malware automatically downloads into a user's computer. Users also need to be trained on the policies for secure corporate and customer data access, usage and storage. This training should extend to the security around the increased user involvement in social networks such as blogs and wikis.

There is a convergence between social engineering schemes and the data readily available using search engines. Social engineering relies on tricking you to give up confidential information. You may have heard about the false requests for money and support following Hurricane Katrina.

As another example, a criminal can target a particular population base or segment by obtaining e-mail addresses and postal codes using popular search engines. The postal codes can define a particular region where the targeted people are located and then e-mails can be sent, reflecting current localized news such as the wind storms in Vancouver. These e-mails can drive users to password or ID-stealing fake Web sites displaying a popular brand or online service provider who is portrayed as supporting the appeal for funds.

## BEST SOURCE OF SUPPORT

From a corporate prospective, increasing security drives competitive advantage by taking a proactive approach to growing compliance/privacy security requirements. In effect, you are staying ahead of the competition. In addition, an online security presence and branding builds trust with customers and supply chain partners who are increasingly interacting with you through the Web – these enable business growth.

It's clear that security is an important challenge for organizations. The best source for support now is the community and with peers – these can be found in associations and user groups.

This trend is noted in a security podcast appearing in the CIPS/Microsoft IT Managers Connection Blog, quoting a recent IDC survey and demonstrates a dramatic shift from 2005.

For example, CIPS, Canada's association of IT professionals, provides support for the West Coast Security Forum held in the fall, and there are security experts throughout the association's CIPS local sections located in most major cities. CIPS sits on the Advisory Committee for the Security Education Conference (SecTor.ca) to be held in Toronto in November. There are security tracks at the CIPS Informatics conference in May 2007 (See <http://www.cipsinformatics.ca>) and CIPS is hosting security tracks with Microsoft's EnergizeIT Conference in June 2007. Of particular note, CIPS is providing special access to the complimentary MSAT security assessment tool. The MSAT works through a series of questions to look at a business people, processes and technology to create better security behaviour in business, infrastructure, applications, operations and people. The MSAT is a repeatable, scalable and predictable tool focused on core solutions and services that are not vendor specific and that is where you get tremendous value.

**“There is a convergence between social engineering schemes and the data available using search engines”**

STEPHEN IBARAKI, ISP, IS THE CIPS NATIONAL VICE-PRESIDENT AND A CIPS FELLOW. [SIBARAKI@CIPS.CA](mailto:SIBARAKI@CIPS.CA).



STEPHEN IBARAKI