it business.ca

RECENT NEWS

The RCMP needs your help to get its cyber man

Cyber crime is on the increase, and one of the RCMP's senior cyber cops says they need the IT industry's help to fight it

11/22/2007 10:57:00 AM

by Jeff Jedras

Toronto - In a luncheon keynote to IT security professionals yesterday at the SecTor SecTor security education conference, a member of the RCMP's Technological Crime Programmade an appeal for the public, and IT professionals in particular, to work more closely with the force in the fight against cyber crime.

It's a type of crime that is rapidly increasing said Carole Bird, the officer in charge of program management support services for the RCMP's Technological Crime Program, with responsibilty for policy and research analysis, operations coordination and liaison, and integrated cyber analysis.

“We're finding there is no crime that occurs today that does not have a technological component to it,” said Bird.

She has worked in the area of technological crime for two years, and she said people often ask her what the risks are, or the cyber crime statistics. People want to know what the RCMP is seeing. It's hard for the force to say what the risks are though, said Bird, because people in the industry are reluctant to talk to the RCMP.

“If you don't tell us a vulnerability has occurred we don't know it has occurred,” said Bird, adding that lack of information makes it hard for the police to dedicate resources to the right threat areas. “If it doesn't get reported it's very hard for us to track down the person and make sure it doesn't happen again.”

What the RCMP does know, said Bird, is that online transactions are increasing and more people are becoming victims of cyber crime. Computing is becoming more affordable, bringing more people onto the Web as potential victims. The myriad challenges in fighting cyber crime, such as the ability to remain anonymous, global jurisdictional issues, and low penalties make cyber crime an increasingly attractive criminal activity.

“This is what we call a low risk, high yield activity,” said Bird.

It's also becoming easier for criminal elements to get started in cyber crime. Suites of tools can be purchased online to bring a business down, said Bird. People can purchase “hacker toolkits” of Botnets, Trojans and other hacking tools and get started with cyber crime with minimal technical expertise; no longer do they need the technical know-how to develop the tools themselves.

The tools are becoming more sophisticated, she said, but the people that are using them decidedly less so.

“We're moving from people using simple techniques to those that have advanced techniques they can use in a money making format,” said Bird.

On the threat horizon, Bird said she's seeing attacks falling into two categories: malicious software and social engineering. The latter, said Bird, is becoming particularly troublesome, with the amount of personal information people are willingly making publicly available on social networking sites like Facebook and MySpace. Even young police officers, said Bird, are falling into the Facebook trap.

“It's something we in law enforcement need to be cognizant of,” she said.

Bird also recommended IT security professionals dedicate more resources to the insider threat, from internal employees. She also added terrorist, organized crime and foreign intelligence services are increasingly active online.

“Now, of course, we're moving to the realm of cyber war,” said Bird.

And if the fight against cyber crime is to be successful, said Bird, the public and the IT community will need to play a bigger role. The police can't do it by themselves, she said. It needs to be a partnership with the public.

“We need to get the information from you so we can train people in the right areas to mitigate those attacks and held you more quickly get back on your feet,” said Bird. “We know we need to think globally and act locally, but we can't do it without you.”

While the RCMP is doing its best to fight cyber crime, said Bird, even with more help from the public she doesn't think the threat can ever be totally eliminated. Their goal instead is to make the Internet a safer place to be.

“I don't think that's achievable. That's like saying you're going to eliminate shoplifting,” said Bird. “There's always going to be people that use technology for evil and people that use it for good.”

Close Window