

# Hackers terrorize business thieves

Martin Derbyshire, Staff Writer

03/18/06 00:00:00

Cyber crime is a threat to any business, just ask Aurora Cable Internet.

In December, the Internet and cable service provider was hit by a denial of service attack that has cost the company hundreds of thousands of dollars, general manager Linda Morrison said.

Somebody got on to its network and forced the company's servers to send out millions of e-mails, slowing the system to a crawl.

With limited ability to track from where it came or stop it, the company was forced to add more servers just to get things back up to speed.

"We've been attacked here and we're still under attack," Ms Morrison said. "There is nothing more we can do to protect ourselves. All we can do is handle it as it flows."

The perpetrators of this kind of cyber crime may have done it to try and legitimize a spam e-mail by putting the Aurora Cable Internet e-mail tag on it.

Or maybe they just did it on a lark.

The fact its origin is hidden behind different servers across the globe makes it near impossible to tell.

But whether it's a disgruntled employee who rendered the network useless because she's upset with the boss or what cops call a "script kiddie" who uploaded a server scrambling program to impress his teenage buddies, Det.-Const. Phil Shrewsbury of the York Regional Police technological crimes unit said this kind of thing is becoming more commonplace everyday.

"For a business these days, your intellectual assets are likely more at risk than your physical assets," he said. "(We don't have statistics) showing conclusively that there's been any kind of migration from traditional crime to cyber crime, but we're certainly seeing it more frequently than we have in the past."

Businesses offering goods for sale over the Internet can be at risk.

Imagine being hit with a denial of service attack that ensures the servers are so inundated with bogus sales legitimate buyers can't access them.

"It's like thousands of people with no interest in buying anything jamming themselves inside the doors of a store," Det.-Const. Phil Shrewsbury said. "The people who want to buy something can't get in."

Most Canadian businesses seem to be catching on to the fact cybercrime is a reality.

A recent IBM survey showed more than 62 per cent of businesses in the health care, financial, retail and manufacturing industries now believe cyber crime is more costly to them than physical crime.

Like theft in most retail businesses, Det.-Const. Shrewsbury said a good percentage of the cyber crime police see is internal.

Almost 70 per cent of participants in the IBM survey said they perceive threats to corporate security are coming from inside the organization more often than not.

"We're definitely seeing more and more of the disgruntled employee thing," Det.-Const. Shrewsbury said. "Before they might get into an argument and want to punch the boss out, now we're seeing where they've damaged the server rendering it useless, poking around and sharing sensitive information or compromising the integrity of a company's data."

Virus protection, firewalls and intrusion protection software, which help avoid denial of service attacks, are a must in protecting your business from cyber criminals, from outside your four walls or within.

But low-tech solutions can be just as important as the high-tech ones, according to Mike Noble, Internet product manager at Markham's Evron Computer Systems Corp., which helps businesses set up new networks and protect existing ones.

"Most businesses have antivirus software, a lot have firewalls, but it's equally as important to have all the layers of protection in place," he said. "That means paying attention to software and lower tech protection as well, like educating employees about password protection and things like that."

The first step towards protecting your business is awareness, said Amit Sahni, Evron's vice president of technical services.

Denial of service attacks can start with a simple e-mail and no type of firewall or e-mail filtering can help you if employees don't learn to avoid opening e-mails from sources they don't trust, he said.

But it doesn't end there.

"You need security at multiple levels," he said "Cyber crime rarely comes from just one source."

Security -- cyber or otherwise -- just makes good business sense, Det.-Const. Shrewsbury said.

"A business would be remiss in its obligations to itself if it didn't take the necessary steps to protect itself," he said.

Evron helps businesses set up safe and secure computer networks and protect existing ones.

Amit Sahni, Evron's vice president of technical services offers the following tips to help protect your business from cybercrime:

- Set up a firewall, anti-virus and anti-spy software
- Tell employees if they don't know the source of an email, don't open it
- Consider setting up email monitoring and tracking programs
- If you have more than one branch office, consider storing data on servers at a central location where it can be better protected and access controlled
- Teach employees a few low tech security solutions including how to protect passwords, avoid opening pop ups or websites they don't know and logging off the system when they leave for the day

For more information on services available with Evron Computer Systems Corp. check out the company's website at [www.evron.com](http://www.evron.com)

Evron also has a newsletter with tips on how to protect your business, to subscribe email them at [evron@evron.com](mailto:evron@evron.com)