# Spying on cyber crime

***The end of the Cold War combined with the advent of the Internet gave rise to an unprecedented wave of electronic espionage and crime. Michel Juneau-Katsuya witnessed first-hand the rise of cyber crime as a senior manager with the Canadian Security Intelligence Service (CSIS) at the time. In 2000, Mr. Juneau-Katsuya left public service to become founding chief executive of security consulting firm Northgate Group. He recently spoke with Financial Post technology reporter Jameson Berkow about the growing digital threat and how companies should respond. The following is an edited transcription of their conversation.***

Q Was there any one event or experience that made you want to quit CSIS and strike out on your own?

A Back in the mid-1990s, I was the chief of the Asia-Pacific region for CSIS, so all operations from North Korea to Afghanistan were under my authority and I would see all the files passing by. At that period I saw a phenomenal amount of spy activities constantly increasing from 1995 and the early days after the collapse of the Soviet Union. I saw next to nothing was being done to try and warn the public and companies so I decided to get out and try to fill that vacuum. Nobody was talking to the private sector or helping it defend itself.

Q How can you quantify the digital threat Canada's economy is facing?

A Easily. We have confirmed through studies that Canada, among the rest of the G8, is probably the country that is most spied on currently. We lose between $50-billion and $100-billion in Canada every year to economic espionage.

Q Where are the threats coming from?

A Well, the usual villains such as China and Russia, but lots of other countries even in the West have developed offensive capabilities in recent years. But a major threat comes from within — rogue employees. Then there are those with a beef who simply want to make money. Eighty-five to 90% of the spy cases we see are usually connected or done by someone who has already been granted access. Basically, we let the wolf in the barn, only dressed as a pig. Interestingly, cyber espionage is not per se a new form of espionage. It might be a new technique, a new strategy. But using a computer versus using a human being are just two different tools to achieve the same objective.

Q I've seen statistics suggesting as much as 90% of all businesses have their systems breached by hackers on a regular basis. Yet despite the high-profile warning signs in the form of recent attacks against Sony Corp., the Nasdaq exchange and other pillars of capitalism, executives seem to harbour an 'it won't happen to us' attitude. Has that been the case for you?

A Absolutely, and there are a multitude of reasons for this kind of attitude. But first and foremost, the onus is on the government. The government has been taking a 'see-no-evil, speak-no-evil' approach. So if you do not warn your general population and you do not warn your business leaders about the situation that is taking place, they will not necessarily think about the cyber threat or even notice it. Many people still do not realize that since the end of the Cold War, we've moved from a military-confrontation scenario to an economic-confrontation scenario. We don't have separate camps anymore;

we have everybody fending for themselves. So every single country with a cyber-offensive capability is practising some form of offensive economic espionage. They are stealing economic information from Canada in particular because Canada is a knowledge-based economy and intellectual property is the item of choice.

Q So how can Canadian companies stay vigilant in the face of these threats? Is there a specific strategy you recommend your clients should follow?

A From the CEO point of view, you really have to take matters into your own hands. Organized-crime groups are starting to realize that stealing intellectual property and trade secrets is far more efficient and far more lucrative than trying to defraud with credit cards. But as we progress, I have noticed a certain progression, a certain maturity that is gaining more and more in the business world. They are starting to realize that security is a strategic investment and it contributes to the profitability of the company. There is a component now that requires having the security angle built into the DNA of the executive. It really doesn't cost anything at all, just go on the Web and pay attention to what is going on. There are daily occurrences so the best thing to do to start is realize and admit this is happening. Then from the executive point of view, you can just conduct a threat assessment of your company. The challenge there is not to overreact.