Risk of cyber-attacks growing: CSIS memo

Last Updated: Tuesday, May 18, 2010 | 9:17 AM ET **Comments*126*Recommend*73***

By Brooks Decillia, CBC News

Cyber attacks on government, university and industry computers is a growing threat, a CSIS memo says. (CP)

A top secret memo written by Canada's spy agency warns that cyber-attacks on government, university and industry computers have been growing "substantially."

The heavily censored briefing note, obtained by CBC News using Canada's access to information law, outlines the increasing vulnerability of Canada's energy, financial and telecommunications systems face from cyber-attackers.

"Compromises of computer and combinations networks of the Government of Canada, Canadian universities, private companies and individual customer networks have increased substantially," says the June 2009 memo written by the Canadian Security Intelligence Service.

The CSIS memo highlights current concerns about cyber security. A report by North American researchers that made headlines in April revealed how email and Twitter were used to steal sensitive documents from the Dalai Lama's office and national security data from the Indian government.

The report — by the University of Toronto's Citizen Lab, the Ottawa-based think-tank SecDev Group and U.S. researchers from the Shadowserver Foundation — stressed that the federal government needs to take urgent action or risk being targeted by hackers who use social media, such as Twitter, to steal secret government or corporate information.

'Complicated issues'

The CSIS briefing note obtained by the CBC acknowledges that the threat of cyber-attacks is "one of the fastest growing and most complicated issues."

"In addition to being virtually unattributable, these remotely operated attacks offer a productive, secure and low-risk means to conduct espionage," the CSIS briefing says.

Government officials have said they are working to develop a framework to deal with cyber-attacks — the federal government's throne speech in March promised a cyber-security strategy.

However, Canada still has no official plan for responding to a co-ordinated cyber-attack. No one from Public Safety Canada responded to a request from CBC News for a response to this story.

Liberal public safety critic Mark Holland said Canada is vulnerable to a "catastrophic event" involving its power grid or banking system.

"Canada is without a plan and we have a government that has given us little more than words. So, rhetoric is cold comfort for those who are concerned," Holland told CBC News.

Canada dependent

Ron Deibert, director of the Citizen Lab at the University of Toronto's Munk Centre, said Canada needs a "coherent, comprehensive strategy" on cyberspace, given how dependent Canadians are on telecommunications.

"We're a large landmass with a population spread across the country," he said. "We obviously have an interest in making sure that these technologies are open and unfettered" because they benefit our commercial relationships and offer us a way to project our values internationally.

Other countries have made progress.

The U.S. government recently announced a $40-billion US national cyber-security plan to combat cyber-attacks from foreign and domestic hackers. Russia and China have also made the growing threat of cyber-terrorism a top defence-spending priority.

Old computer systems a risk

So-called "ethical hackers" — computer experts who get paid by companies and organizations to identify weaknesses in their computer systems — say Canadian government computers are particularly susceptible to cyber-attacks.

"Some of the systems of government can be up to 20 years old, and they're having a hard time migrating that over to newer technology and until they do that, they are extremely vulnerable," said Terry Cutler, a Montreal-based cyber-security expert and ethical hacker.

However, government — and other targets of cyber-attacks — might never be completely impregnable, said John Aycock, a University of Calgary computer science associate professor.

"There's nothing that we can really do about these attacks, in some sense, because of the way the internet was designed," Aycock said.

"It's not designed to be able to track people back. Having multiple layers of security, educating people about what they should and should not do, all those things are beneficial — but there is no one cure all that's going to do it."

Story comments (*126*)

Sort: Most recent | First to last | Agreed
radar17 **wrote:**Posted 2010/05/18
at 11:10 AM ETDoes anyone at CSIS have a Blockbuster membership?

Pretty sure Hollywood was onto this years ago - maybe the geniuses at CSIS should rent "Live Free or Die Hard" with Bruce Willis or Sandra Bullock's "The Net". There are others too but those 2 are top of mind.

As for the genius poster Kilgore_trout who said, "on the plus side i don't think anyone can die from a cyber attack.." ...well.... next time think a wee bit before you type.

- *2*
- *0*

*2*Agree *0*DisagreePolicy Report abuse
pudgey1 **wrote:**Posted 2010/05/18
at 10:50 AM ETI love this, it is great, anything to bring down the government as it know stands will be fantastic. The 300+ thieves must be turfed and a whole new system needs to be installed.

- *5*
- *11*

*5*Agree *11*DisagreePolicy Report abuse
CasualCritic **wrote:**Posted 2010/05/18
at 10:48 AM ET"The U.S. government recently announced a $40-billion US national cyber-security plan to combat cyber-attacks from foreign and domestic hackers."

I don't want to pick nits but I wish the media would stop using the term hacker in this context.

A hacker is someone who likes to explore and exploit technology, in many cases making it do something positive it was never designed for.

Someone who commits cyber-attacks is simply a cyber-criminal.

- *18*
- *2*

*18*Agree *2*DisagreePolicy Report abuse
buffordyork **wrote:**Posted 2010/05/18
at 10:36 AM ETThe Harper Con government were recently caught spying on Canadian citizens without permission. If the bad boys are attacking the Government systems and the Cons are illegally spying on the public would it not be a wash then. What is the difference

You reep what you sew Harper

- *17*
- *10*

*17*Agree *10*DisagreePolicy Report abuse

bobboberan **wrote:**Posted 2010/05/18
at 10:36 AM ETHow would CSIS know unless they are doing the attacking themselves and getting good at it. Harper needs to sit down and reconstruct the countries privacy and personal security , he has allowed so many laws to disappear there will be small chance of ever seeing those freedoms return. The privacy act has almost completely been dismantled , with discrepancy rules for investigations by his own people and endless line ups of special interest groups , from data research to what you do on the internet to how much a hockey player makes ...the list is endless .

- *1*
- 9

*1*Agree *9*DisagreePolicy Report abuse

- First
- Previous
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- Next
- Last

Comments on this story are pre-moderated. Before they appear, comments are reviewed by moderators to ensure they meet our submission guidelines.

Comments are **open** and welcome until Monday, May 24, 2010 at 11:59 p.m. ET.
We reserve the right to close comments before then.

Post your comment

Note: The CBC does not necessarily endorse any of the views posted. By submitting your comments, you acknowledge that CBC has the right to reproduce, broadcast and publicize those comments or any part thereof in any manner whatsoever. Please note that comments are pre-moderated/reviewed and published according to our submission guidelines.

You must be logged in to leave a comment. Log in | Sign up
Comment:
Post Submission policy