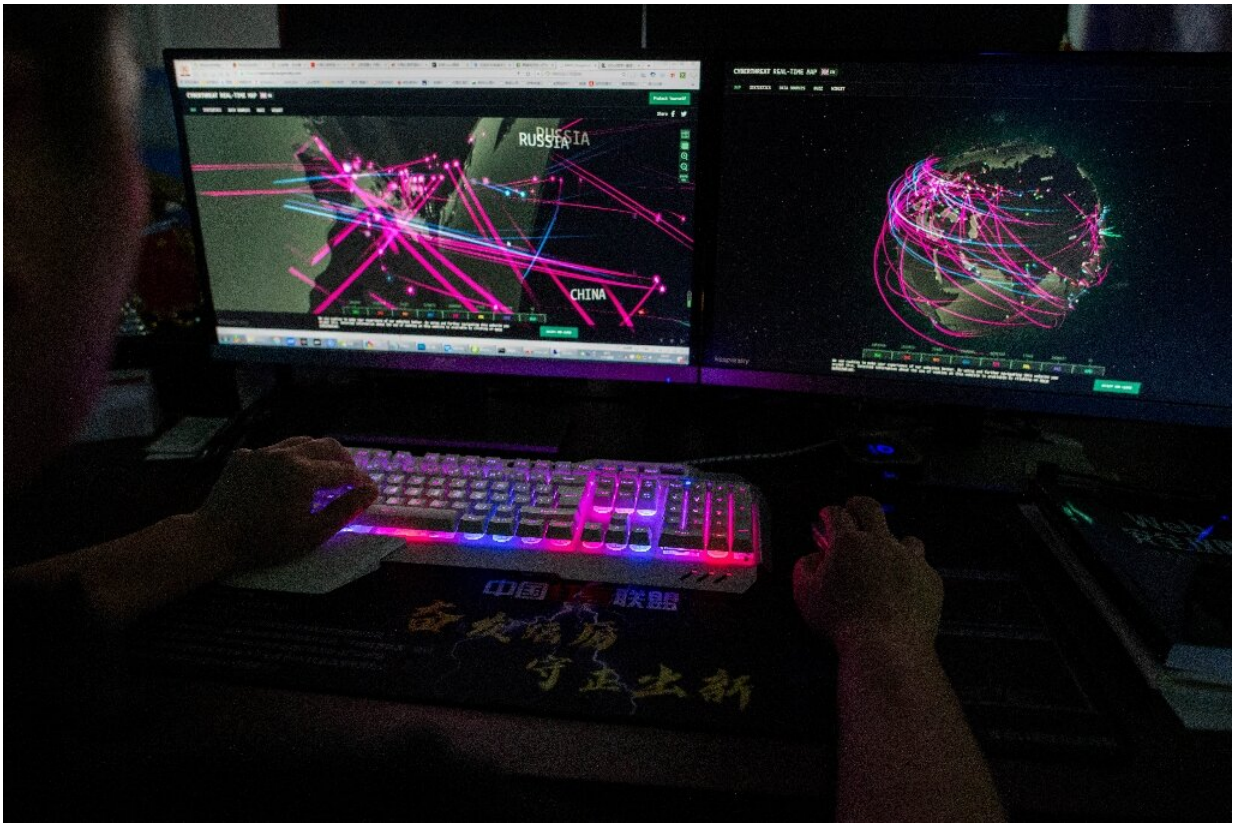
Canadian businesses scrambling to defend against cyberattacks uptick

April 27 2022, by Anne-Sophie Thill



A member of the Red Hacker Alliance in Dongguan, China in August 2020 monitors cyberattacks around the world. Hacks have increased through the pandemic and the war in Ukraine.

Canada's governor general and foreign ministry, hospitals and an airline:

a litany of recent cyberattacks has exposed poor defenses against hackers, despite warnings to be more vigilant since Russia's invasion of Ukraine.

Last week, Canada and four other Western countries, including the United States, warned that Russia was preparing to launch massive cyberattacks against Ukraine's allies in retaliation for support for Kyiv and sanctions imposed on Moscow.

On the rise for years and becoming increasingly sophisticated, "thousands" of cyberattacks, including by Russian hacker groups, target Canada every day, according to Cherie Henderson, a senior official at the Canadian Security Intelligence Service.

Canada was second behind Britain in number of reported victims of phishing, spoofing, extortion and other Internet-enabled frauds, according to an FBI report on Internet crimes in 2020. (The report excludes the United States in the list).

The most recent victim was the Canadian airline Sunwing. A cyberattack hit one of its suppliers, causing a breakdown of the airline's operations that left thousands stranded in vacation hotspots in the United States, Mexico and the Caribbean.

Companies may be "caught offguard and see their business activities considerably curtailed," commented Benoit Dupont, a cybersecurity researcher at the University of Montreal.

Some, especially smaller enterprises, "do not always have adequate resources and investing in cybersecurity is not always a top priority," he told AFP.

Just prior to the start of the war in Ukraine in late February, the

government's Canadian Center for Cyber Security reminded of the need to protect critical infrastructure from Russian-sponsored cyber threats.

Whether it's industrial espionage, vandalism, theft of intellectual property or proprietary information, frozen accounting systems or even entire computer systems, the risks concern companies of all sizes.

Finance, energy, telecom targets

Evan Koronewski, a spokesman for the Communications Security Establishment, said the Canadian electronic eavesdropping agency monitors "cyber threat activity directed at critical infrastructure networks, including those in the financial, energy, and telecommunications sectors."

But, he added, that all sectors "are encouraged to take note and be aware of the possibility of increased cyber threat activity."

Some have taken action, according to Trevor Neiman of the Business Council of Canada, an association representing the nation's biggest employers.

"In the run-up to the to the Russian invasion of Ukraine, Canadian businesses have adopted a heightened state of awareness, and they've taken a number of proactive measures to bolster their cyberdefenses," he said.

Public utility Hydro-Quebec, for example, has stepped up "surveillance specifically for this threat," its spokesman Cendrix Bouchard told AFP.

In Canada, one in four companies reported being hit by cyberattacks in 2021 and more than half paid ransoms to hackers who infected their computer systems with malware, according to a Novipro-Leger survey

last fall.

Ransom amounts have been climbing, and can reach several million dollars.

Ottawa announced last year Can$80 million (US$62.5 million) over four years to bolster the nation's cyberdefenses.

But the Canadian Chamber of Commerce said it was not enough, noting that it is a drop in the bucket compared to amounts spent by Canada's G7 peers.

"The United States, Israel, and the UK are investing billions" to boost their cyberdefenses, it said.

Since the start of the pandemic, which saw more people teleworking, ransomware attacks have increased exponentially around the world.

"Malicious cyber actors, whether state sponsored or otherwise, often seek to take advantage of crises," explained BlackBerry's Marjorie Dickman.

"We saw this during the pandemic when threat actors launched repeated Covid-19-themed attacks and sought to leverage security gaps in the work-from-home setting," she said, adding that hackers now use mentions of the war in Ukraine to lure victims.

"You only have to be successfully attacked one time to really hurt your business," warned Rocco Rossi, head of the Ontario Chamber of Commerce, describing it as "an ongoing battle."

"Even after the war in Ukraine ends," he said, "these cybersecurity issues won't go away."