

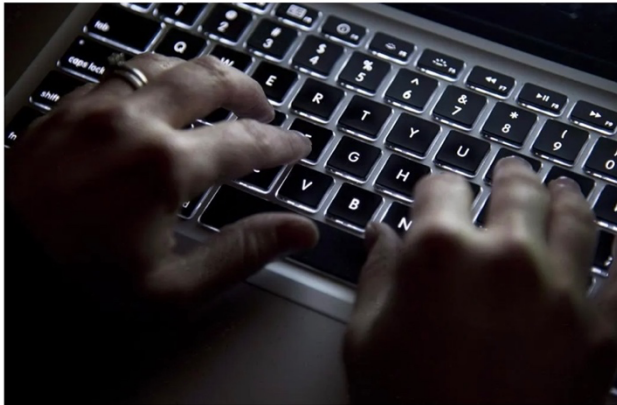
CANADA

## Sask. Good Spirit School Division dealing with cyber attack



By Andrew Benson • Global News

Posted March 6, 2024 4:13 pm • Updated March 7, 2024 6:01 pm • 1 min read



The Good Spirit School Division (GSSD) announced this week that they are currently dealing with a "cyber-incident," THE CANADIAN PRESS/Jonathan Hayward. THE CANADIAN PRESS/Jonathan Hayward

News

## Canada's cybersecurity under siege and even the government is powerless

*The year started with a cyberattack on Global Affairs leading to a data breach, followed by an attack on Canada's financial intelligence unit FINTRAC and the RCMP*

Sam Riches

Published Mar 12, 2024 • Last Updated 1 day ago • 5 minute read



Foreign Affairs Minister Melanie Joly speaks with senior Global Affairs Canada official, Weldon Epp before appearing at committee, Wednesday, March 22, 2023 in Ottawa. In January, Global Affairs Canada was attacked, leading to a data breach that limited remote access to its networks. PHOTO BY THE CANADIAN PRESS/ADRIAN WYLD

CBC • CBC

## Sask. school division asked to monitor 'dark web' for student, staff after security breach

f

X

m

CBC

February 13, 2024 • 5 min read



The South East Cornerstone Public School Division in southeast Saskatchewan said as many as 20,000 people could have had their information stolen during a security breach in February 2023. (David Donnelly/CBC - image credit)

A Saskatchewan school division is being asked to monitor the dark web for current and former staff and students' personal information after a security breach.

The South East Cornerstone Public School Division No. 209 estimated that as many as 20,000 people were affected by a breach to three of its IT systems on Feb. 8, 2023, according to an investigation report from the office of the Saskatchewan information and privacy commissioner. The breach was reported to the office last August, the report says.

It says an unauthorized user was found to have moved data from eight "archive files" to a third-party cloud storage provider, later noting that "unless a separate copy was taken, it is possible that the third party behind this incident lost access to the data as soon as the

Does anyone suspect like me that data breaches and hacking are a runaway epidemic? Of which we are only being allowed to know of a small fraction? Yet as public services and governments become increasingly short-staffed, with the most capable professionals going (where the money is) into private and corporate business, schools and municipalities keep shifting us into online operations; hackers must be delighted, wondering where to start as the hapless victims proliferate. Policing and punishment is negligible. School divisions have got along quite well with standard "the VP calls the sub" to bring in "supply" teachers, but both of the above divisions here have shifted into an automated dispatch system where some "robot" orchestrates clunky phone calls. I know of three longtime substitute teachers who have resigned rather than struggle with this. I cannot even get substitute work with Good Spirit now because their automated system was targeted especially, and the stretched-thin IT staff still cannot get it fully operational two weeks later. Yet the IT types will keep selling similar "cost-effective" ideas to senior administrators who want their operations to look "cutting edge" and "efficient." Meanwhile the "human touch" gets lost further, even in Education. Mme. Joly, so in-over-her-head, will not save us. TJB