Investigation Report IR25-01 - MOVEit File Transfer System Privacy Breach

BACKGROUND AND REPORT SUMMARY

This document accompanies and summarizes Investigation Report IR25-01. For full facts, findings, and recommendations please refer to the complete report.

What happened?
On June 4, 2023, the Nova Scotia Government publicly announced it was subject to a global cyberattack. Threat actors took advantage of a critical vulnerability in a software product called MOVEit. MOVEit is a file transfer system purchased and used by the Nova Scotia Government. It is designed to move large amounts of data over the internet between users, organizations and systems.

A vast scope of personal information, including names, social insurance numbers, addresses, educational backgrounds, personal health information and banking information was stolen by the threat actors that conducted the cyber security attack.

Why did the Office of the Information and Privacy Commissioner for Nova Scotia (OIPC) conduct this investigation?
Following the privacy breach, two Nova Scotia Government departments (the Department of Health and Wellness and the Department of Cyber Security and Digital Solutions) and two health partners (Nova Scotia Health and Izaak Walton Killam Health), collectively referred to as the Nova Scotia Government in this document as well as in *Investigation Report IR25-01*, sent out approximately 168,000 privacy breach notification letters to Nova Scotians. The OIPC then received approximately 110 privacy complaints under the *Privacy Review Officer Act (PRO),* the *Freedom of Information and Protection of Privacy Act (FOIPOP)* and the *Personal Health Information Act* (*PHIA*).

As a result, the OIPC decided to launch an own-motion investigation in order to collectively respond to these privacy complaints. The investigation looked into whether the Nova Scotia Government had reasonable security and information practices in place for its use of the MOVEit file transfer system as required by law. It also assessed the sufficiency of the Nova Scotia Government's response to the cyberattack.

How many people were affected by these privacy breaches?
An estimated 100,000 Nova Scotians were impacted by the cyberattack. Many experienced several breaches because their personal information appeared in multiple files. Approximately 168,000 privacy breach notification letters were sent to Nova Scotians.

The cyberattack impacted an estimated 18.5 million people worldwide.

How much money did responding to the cyberattack cost the Nova Scotia Government?
In total, responding to the cyberattack cost the Nova Scotia Government approximately $3.8 million. An estimated $1 million was spent on third party supports. Approximately $2.85 million was spent on offering credit monitoring services to many of those affected by the privacy breach. Dealing with the aftermath also consumed a tremendous amount of internal resources.

The investigation's findings
As a result of the OIPC's investigation, the Commissioner made 12 findings:

Finding #1: I find that a privacy breach occurred.

Finding #2: I find that the root cause of the breach was that threat actors exploited a critical vulnerability in the MOVEit file transfer system and used it to gain access to the personal information that was stored in the MOVEit repository.

Finding #3: I find that by not conducting a PIA when it began its use of the MOVEit file transfer system or when the Nova Scotia Government's privacy policy was adopted in 2008 and updated in 2018, the Nova Scotia Government failed to have reasonable security and information practices in place and was therefore not in compliance with s. 24(3) of *FOIPOP* or ss. 61, 62 and 65 of *PHIA*.

Finding #4: I find that the MOVEit file transfer system was frequently and inappropriately used as a repository for extraneous records and that this exacerbated the extent of the personal information breached in the cyberattack.

Finding #5: I find that the Nova Scotia Government did not provide sufficient direction to MOVEit users regarding the length of time that files should be kept in the repository of the MOVEit file transfer system and that this exacerbated the extent of the personal information breached in the cyberattack.

Finding #6: I find that the Nova Scotia Government took reasonable steps to contain the privacy breach following its discovery. Specifically, the response was timely and engaged third-party cyber security experts who provided essential instructions.

Finding #7: I find that the harm from this privacy breach is significant and was foreseeable.

Finding #8: I find that the 5-year credit monitoring offered to affected individuals by the Nova Scotia Government is reasonable.

Finding #9: I find that the timing of the indirect and direct privacy breach notification to affected individuals was reasonable.

Finding #10: I find that the notification letters and call centre staff provided insufficient information regarding the breach and the personal information impacted.

Finding #11: I find the contact information used for the notification letters was severely outdated in many cases. This meant that thousands of affected individuals did not receive notification letters and were unable to take measures to protect themselves.

Finding #12: I find that the *Nova Scotia Government's Post-Incident Recommendations* are comprehensive *except* in the following ways:

i. Recommendations are permissive. The Nova Scotia Government should be setting out mandatory requirements.
ii. There is no timeline for completion of the tasks (including deadlines) set out in the *Nova Scotia Government's Post-Incident Recommendations*.
iii. The *Nova Scotia Government's Post-Incident Recommendations* state: "the recommendations will require collaboration across departments, public bodies, and other partners such as NSH and the IWK. It is intended that those involved assess the recommendations and develop plans for implementation." This wording is not strong enough. Whose role is it to assess the recommendations and implement the plans? Who is accountable if the plans are not implemented? Clear, granular roles must be set out in the recommendations, with final accountability lying at the highest level of government – the Ministerial level.

Recommendations made

As a result of the OIPC's investigation, the Commissioner made 8 recommendations:

Recommendation #1: In August 2024, the Nova Scotia Government indicated that a PIA for MOVEit was being completed at that time. If this task is not yet finished, I recommend that the Nova Scotia Government complete a thorough and up-to-date PIA on its use of the MOVEit file transfer system within 60 days of the date of this report.

Recommendation #2: I further recommend that, within 60 days of the date of this report, the Nova Scotia Government make the appropriate portions of the PIA on MOVEit publicly available on its website. Any portions of the PIA that could provide an opportunity for future exploitation by threat actors should not be reported publicly.

Recommendation #3: I recommend that, within 60 days of the date of this report, the Nova Scotia Government create clear retention and disposition schedules for all users of the MOVEit file transfer system that specifies the maximum amount of time that files being transferred can remain in the repository of MOVEit.

Recommendation #4: I further recommend that the Nova Scotia Government commit to ensuring that retention and disposition schedules are adhered to by monitoring use of the MOVEit system on a yearly basis, if not more frequently.

Recommendation #5: I recommend that, within 60 days of the date of this report, the Nova Scotia Government confirm a commitment to consult with the OIPC in advance of issuing privacy breach notification letters for future major privacy breaches in a manner that allows sufficient time for OIPC suggestions to be incorporated into the notification letters.

Recommendation #6: I recommend that the Nova Scotia Government make every reasonable effort to ensure that it has up-to-date contact information for all citizens that it holds personal information about.

Recommendation #7: I recommend that, within 90 days of the date of this report, the Nova Scotia Government complete and post on its website a clear, comprehensive post-incident response plan that:

i. Makes all recommendations set out in the *Nova Scotia Government's Post-Incident Recommendations* mandatory requirements.
ii. Sets out clear timelines and deadlines for completion of all the *Nova Scotia Government's Post-Incident Recommendations* and associated key activities.
iii. Sets out clear accountability at the Ministerial level for implementation of the tasks set out in the post-incident response plan.
iv. Addresses the concerns raised and recommendations made in this report.

Recommendation #8: Further to Recommendation #7, I recommend that, within 1 year of the date of this report, the Nova Scotia Government complete the tasks set out in its published post-incident response plan and post the results to its website for the public to view.

Nova Scotia Government's response to the recommendations

The Nova Scotia Government is considering the recommendations and will have 30 days to formally decide whether it will follow Commissioner Ralph's recommendations.

Key takeaways

It is crucial that the Nova Scotia Government be proactive by continuously reviewing and updating its security systems and practices to stay ahead of ever-evolving threat actors. The increasing number of cyberattacks means that Nova Scotians must demand more of the public institutions that collect personal information about them.