# The Cyber Security Attack on Nova Scotia's MOVEit System

**Public Report**

May 2024

NOVA SCOTIA

# Table of Contents

# Overview

We live in an increasingly digital world. People, businesses, and devices are data factories pumping out incredible amounts of information daily. Technology is expanding at an extraordinary rate. So too are those that wish to exploit that technology. To ensure government was in the best possible position to manage and protect the information it holds, the Department of Cyber Security and Digital Solutions (CSDS) was created in May 2023, embedding digital expertise at the heart of government.

In May 2023, a cyber security attack on Progress Software's MOVEit file transfer system affected multiple organizations worldwide, impacting an estimated 18.5 million people globally, including the Province of Nova Scotia. MOVEit is designed to move large amounts of data over the internet, facilitating the efficient and safe exchange of digital information between users, organizations, and systems. In Nova Scotia, the system is managed by CSDS.

With expertise centralized within CSDS, the department was able to quickly identify and respond to the incident. An estimated 100,000 Nova Scotians were impacted by the attack representing a range of sectors, mirroring the diversity and volume of the files stolen.

Security breaches cost money. They are extremely stressful for those impacted. That is why government is focused on being vigilant regarding cyber security, doing all we can to keep the information Nova Scotians entrust with us as safe as possible.

This report provides an outline of the May 2023 cyber attack, which resulted in a security breach of the MOVEit system and a privacy breach of a number of files contained within that system. This report also outlines the steps taken in the wake of the attack, the type of information taken, and individuals affected. It also addresses what was done to appropriately respond to the attack and the steps that will be taken to minimize the impact of similar events in the future.

# Identifying the Issue

On May 31, 2023, Progress Software posted information on their website about a critical vulnerability in its MOVEit software which could lead to unauthorized access, meaning data could be stolen.

On June 1, 2023, a member of the CSDS team identified the problem with the MOVEit system through proactive monitoring of cyber security industry news. Once discovered, CSDS followed standard cyber security breach protocols and declared a major incident. After assessing the issue, the system was taken offline, and the updates recommended by Progress Software were completed. By the end of day, the incident was downgraded, and the service was restored.

On June 1, 2023, CSDS also received a priority notification from the Canadian Centre for Cyber Security (CCCS) advising the Province may have been using a version of the vulnerable MOVEit software and therefore data could be compromised. As the upgrades (or patching) had already taken place based on the instructions from Progress Software, no further action was taken.

On June 2, 2023, CCCS again contacted the department to recommend further investigation into suspicious IP addresses (the unique address identifier of devices on the Internet). Once again, and in keeping with Province's cyber incident response approach, the system was taken offline immediately. Upon investigation, suspicious IP addresses were indeed found, and a new major incident was declared. At this point, the Province's Chief Information Access and Privacy Officer (IAP) with Service Nova Scotia, was notified. A triage call with IBM's Security Services (who is on retainer with the Province to provide cyber security incident response services) then took place and a forensic analysis of the MOVEit system was requested.

After investigating, IBM's Security Services confirmed CSDS's findings that data had been stolen on May 30 and 31, 2023 before CSDS was made aware of the vulnerability. They also confirmed that no data had been taken since the original patching activities of June 1, 2023, and that the cyber security risk and data theft were restricted to the MOVEit system.

On June 3, 2023, CSDS continued its investigation of the stolen data. Executive leadership meetings were held with Nova Scotia Health (NSH), the IWK Health Centre (IWK), the Chief IAP Officer, and Communications Nova Scotia to raise their awareness of the incident. The department also brought together the appropriate IT teams to examine the impact of the MOVEit breach more closely in collaboration with the Chief IAP Officer.

On June 4, 2023, CSDS brought together privacy leads from the impacted organizations to begin a comprehensive review of the files compromised during the breach. The Chief IAP Officer notified the Office of the Information and Privacy Commissioner for Nova Scotia (OIPC) that a privacy breach had occurred. CSDS confirmed a cyber security incident with the CCCS and contacted Halifax Regional Police. A report was also filed with the Canadian Anti-Fraud Centre.

On June 15 and 16, 2023, similar vulnerabilities were identified by Progress Software. CSDS employees took steps to address the issue by blocking external internet access to the MOVEit server and patching the MOVEit system. It was confirmed no files were taken during the subsequent incidents and that the only stolen files were taken between May 30 and 31, 2023.

# The Response - Acting With Accountability

This illegal attack cost Nova Scotian taxpayers an estimated one million dollars in third party supports and consumed an extraordinary amount of internal resources to deal with the aftermath. Technical, privacy, and program teams from across government were rapidly redeployed, creating capacity for a large-scale breach response to reduce the impact on Nova Scotians.

As soon as the breach was discovered, steps were immediately taken to assess the impact and notify those affected. The CSDS Deputy Minister communicated with every department head in advance of the first news conference on June 4, 2023, and requested departmental leads to support the breach response. Regular communications and meetings began with internal and external program owners and organizations to keep them apprised of the latest developments.

From the early days of the first news conference, the Province vowed to act with transparency and accountability. Regular updates were provided to the public through the media and a second news conference was held on June 6, 2023. News releases were issued province wide on June 4, 6 and 9, 2023. A website was also launched June 4, 2023, to provide Nova Scotians with a single location where they could go to be informed and updated about the latest developments of the breach.

To determine the extent of the breach, and who should be notified, privacy leads from the Departments of Health and Wellness (DHW), Education and Early Childhood Development (EECD), Community Services (DCS), as well as the IWK, and NSH, were brought together with IAP Services. Program and business leads were also brought in to assess the risks involved.

On June 4, privacy leads began a detailed analysis of the files to understand the nature and extent of the data compromised and to ensure compliance with the Freedom of Information and Protection of Privacy Act (FOIPOP) and the Personal Health Information Act (PHIA). This legislation governs the collection, use, disclosure, retention, and protection of personal information and personal health information. The analysis also ensured the Province followed its own privacy breach protocol. The goal was to examine the compromised data as carefully and efficiently as possible to ensure any necessary steps were taken to quickly notify and protect those affected.

The analysis confirmed the stolen files contained sensitive personal information such as social insurance numbers and banking details for some employees. It was also confirmed that some members of the public were affected, and that their personal health information was compromised. Informed by the Nova Scotia Privacy Breach Protocol and best practice outlined in OIPC guidance, the files were categorized as high, medium, or low based on the sensitivity of the information within the files.

Higher priority files contained the most sensitive data, such as social insurance numbers and banking information.

Medium priority files contained less sensitive information but where notification would be recommended.

Low priority files contained information that may already be publicly available and where direct notification may not be necessary.

# Information and Individuals Impacted

Determining how many people were affected by the breach was complicated by the fact that an individual's information may have appeared in multiple files. For example, a certified teacher may have also worked as a public servant or received a parking ticket; therefore, some of their information could be in more than one file. It is estimated that 100,000 people were impacted.

In total, 5,860 files were compromised. Some were compressed files that contained multiple files or documents. Each file was carefully reviewed determining the number of individuals impacted and the level of sensitivity of the exposed data. By June 14, 2023, the initial file review was completed, and the process to notify affected individuals was initiated as soon as possible, with the first notification letters being sent June 16, 2023.

Along with the public notifications through media, staff worked to determine who should receive a direct notification. Again, the goal was to notify individuals as quickly as possible and help them to take the necessary steps to protect themselves. If there was a risk of identity theft or fraud or other harms, individuals were contacted directly and offered complimentary credit monitoring services.

A total of 166,529 letters were sent to individuals whose personal information was breached, while 1,923 letters were sent to those whose personal health information was compromised. Notification was completed by the end of September 2023.

Each person was advised of the date of breach, a description of the information stolen, what steps were taken to contain the breach and their potential personal risk. They were also advised how to protect themselves to further mitigate their risk. Contact information for the Office of the Information and Privacy Commissioner was also included to allow individuals their right to request a review of the Province's response with the oversight body.

For some, credit monitoring services were offered due to the exposure of financial or sensitive personal data, such as social insurance numbers. These services were offered to help safeguard affected individuals' financial and personal information, for a period of five years. The service helps individuals to track their credit reports, receive alerts about changes to their credit profiles, and helps to detect any suspicious activity or identify theft attempts. These services were offered through TransUnion, a credit monitoring agency. 121,126 individuals have been provided with this service. Credit monitoring services were not offered to those under 18, due to a lack of credit history. Credit monitoring services were not available to deceased individuals.

To help those with any additional questions, a toll-free number was created on June 20, 2023 through Service Nova Scotia. The Department of Health and Wellness, NSH, and IWK handled direct inquiries related to personal health information. More complex questions were forwarded and handled by the appropriate privacy leads.

A detailed list of the groups and organizations whose sensitive information was impacted (which has already been publicly disclosed), the type of information stolen, and when notifications were completed can be found at https://novascotia.ca/privacy-breach.

# Moving Forward

The cyber security attack on the MOVEit system was unprecedented and massive in scale. Every possible step is being taken to reduce the impact of future breaches and will focus on priority areas for improvement. Based on learnings from this attack, the government is taking steps to:

- Enhance security within the MOVEit file transfer system.
- Improve breach protocols and incident response to ensure there is enhanced capacity to respond to large scale breaches.
- Improve how data is classified and managed.
- Continuously review, adapt, and evolve our overall Cyber Security Strategy to strengthen abilities to respond to large scale events.
- Introduce recurring mandatory cyber security awareness training for all staff.
- Work closely with national and international jurisdictions to continue to share learnings and build capacity in Nova Scotia.

The Province of Nova Scotia is committed to protecting the security of the information it holds and the personal information of Nova Scotians. Cyber security risks are not going away. We must always be vigilant because criminals are continuously looking for ways to compromise our systems.

CSDS is constantly striving to protect the Province of Nova Scotia from evolving cyber security threats. We have learned from this experience, and we will continue to improve, learn, and adapt. We will continue to review and update our cyber security strategy and operational procedures to address the ever-evolving cyber security threat landscape to ensure our approach remains effective, resilient, and responsive.

# The Cyber Security Attack on Nova Scotia's MOVEit System

## Public Report

ISBN 978-1-77448-657-3

NOVA SCOTIA