Cyberattack on the Newfoundland and Labrador Health Care System

Overview

Prepared by the Department of Health and Community Services and Department of Justice and Public Safety

MARCH 2023

Newfoundland & Labrador

Table of Contents

Overview

On Saturday October 30, 2021, a cyberattack impacted IT systems supporting the delivery of healthcare services in Newfoundland and Labrador. An unauthorized third party accessed parts of the health care technology infrastructure, which resulted in an IT systems outage.

In response to this attack, the Government of Newfoundland and Labrador activated the provincial Emergency Operations Centres (EOC), along with the Newfoundland and Labrador Centre for Health Information (NLCHI), and the four Regional Health Authorities (RHAs) to assess system impacts, coordinate their response, and focus on the continuity of care. Government officials and technical, operational, and communications teams worked together to keep Newfoundlanders and Labradorians informed about impacted systems and alternative plans for the provision of care.

External cybersecurity experts were engaged to assist with efforts to contain, investigate, and safely retore health care systems. As a result of the investigation into the cyberattack, it was determined that the incident was a ransomware attack involving Hive ransomware, and that some personal information and personal health information was taken from certain systems. The appropriate authorities were notified, including the Canadian Centre for Cyber Security (CCCS), the Royal Newfoundland Constabulary (RNC), the Royal Canadian Mounted Police (RCMP), and the Office of the Information and Privacy Commissioner of Newfoundland and Labrador (OIPC).

The province and RHAs provided public updates and notifications as information was confirmed regarding the personal information and personal health information involved. Identity theft and credit monitoring services were also offered and continue to be available for impacted individuals. It was also determined that certain patient health and employee information on an Eastern Health network drive was taken during the cyberattack. Eastern Health has concluded its review and notified the affected individuals as per their public statement. There continues to be no evidence that the information taken during the attack was misused.

Clients who have received health care services at any time continue to be offered access to credit monitoring and identity theft protection services for a period of two years from the date of enrollment, at no cost to them. Patients whose Social Insurance Number and banking/financial information was breached are offered five years of credit monitoring and identity theft protection at no cost to them. Current and former employees, physicians, and locums are also being offered access to credit monitoring services for a period of five years from the date of enrollment.

There is no evidence to indicate that the attack was intended to specifically target NLCHI or the Newfoundland and Labrador provincial health care system. However, the attacker, Hive ransomware group, was known for its aggressive and sophisticated capabilities and its targeting of the health sector. Recently, the U.S. Department of Justice announced the successful disruption of the Hive group network.

The forensic investigation determined that the earliest evidence of attacker activity within the NLCHI-managed environment, which includes the IT domains for NLCHI and the RHAs, occurred on October 15, 2021. At that time, the attacker successfully initiated a VPN connection to the NLCHI-managed environment using the compromised credentials of a legitimate user account. The investigation was unable to determine how these credentials were compromised prior to this activity. The attacker subsequently moved laterally, gained administrative privileges through a privileged user account, and connected to other systems. During the incident, the attacker exfiltrated data from the environment, which resulted in the data breach.

On October 30, 2021, the attacker deployed Hive ransomware and encrypted numerous systems, which resulted in the IT outage and led to the detection of the attack. Since October 30, 2021, there has been no evidence of Hive ransomware group activity in the systems.

Immediate steps that were taken following the attack include:

- Engagement of external cybersecurity experts.
- Deployment of an industry-leading endpoint detection and response (EDR) tool throughout the NLCHI-managed environment for further enhanced monitoring capabilities. The EDR tool was used to verify systems before they were brought back online in the recovery process.
- Implementation of mandatory multifactor authentication (MFA) for authentication to remote connections to NLCHI-managed domains where MFA was not already implemented.
- Holistic password resets on multiple occasions pursuant to external cybersecurity expert recommendations and best practices, including a global credential reset for the NLCHI-managed environment for NLCHI and RHA users.
- Engaging a leading cybersecurity provider for 24/7 monitoring of the NLCHI-managed environment through a comprehensive set of security tools.
- Detailed analysis of operational devices.

Following the attack, systems were brought back online at different times based on priority, as they were confirmed to be safe and secure.

Since the attack, measures have been taken to further enhance the security of information systems and to help prevent an attack like this from happening again, including the steps which are detailed in this document. This work built on the existing cyber risk mitigation work which was already underway.

It is with thanks to the significant efforts of teams from across our health care system that our services were safely restored in a timely manner. We are grateful to our cybersecurity partners and the employees of the RHAs and NLCHI who supported these efforts and continued to provide critical care and services during this challenging time. By working together, we were able to mitigate the risk of further attack and ensure our restoration efforts were carried out in an efficient and safe manner. While these kinds of attacks have become more frequent, we remain committed to continuously reviewing and further strengthening our security measures to help prevent future attacks.

TIMELINE

Initial Systems Access

The earliest evidence of attacker activity within the NLCHI environment occurred on **October 15, 2021**. At that time, the attacker successfully initiated a VPN connection to the NLCHI-managed environment, which includes the IT domains for NLCHI and the four RHAs, using the compromised credentials of a legitimate user account. The investigation was unable to determine how these credentials were compromised prior to this activity. No attacker activity prior to **October 15, 2021** was identified.

On **October 25, 2021**, the attacker moved laterally through the environment, escalated their privileges through an account with administrative privileges and connected to other systems.

Between **October 26 and 29, 2021**, the attacker exfiltrated certain data from the environment, including personal information (PI) and personal health information (PHI).

On **October 30, 2021**, the attacker deployed Hive ransomware and encrypted numerous systems, which resulted in the IT outage that caused widespread system disruption and led to the detection of the attack. Following detection, numerous steps were taken to secure systems

and contain the attack. Some attacker activities and effects took place in the NLCHI-managed environment and others in the environment of a managed service provider (MSP) to NLCHI.

Since **October 30, 2021**, there has been no evidence of any Hive ransomware group activity in the NLCHI-managed environment or the MSP environment.

Privacy Breach

It was confirmed and shared publicly that the following PI and PHI was taken in the attack:

- Social Insurance Numbers of 2,514 patients from Eastern Health, Central Health or Labrador-Grenfell Health.
- Patient registration information for patients whose bloodwork or specimens was analyzed by Eastern Health from 2010 to 2021, such as such as name, address, health care number (MCP), reason for visit, their doctor, phone number, birth date, email address for notifications, in-patient/out-patient status, maiden name, and marital status. This would include private clinics and other Regional Health Authorities, including Western Health.
- Employee information of current and former employees of Eastern Health (approximately 1993-2021), Central Health (approximately 1993-2021) and Labrador Grenfell Health (approximately 2013-2021), including names, addresses, contact information, and Social Insurance Numbers.
- Other employee information of Eastern Health employees, including disciplinary information and other human resources and administrative information.
- Patient information of current and former patients of Eastern Health (approximately 2010- 2021), Central Health (approximately 2006-2021), and Labrador Grenfell Health (approximately 2013-2021), such as name, address, health care number (MCP), reason for visit, their doctor, phone number, birth date, email address for notifications, in-patient/out-patient status, maiden name, and marital status.
- Other medical information of current and former patients of Eastern Health (approximately 1996-2021), such as medical diagnosis, procedure type, health care number (MCP), Social Insurance Numbers and banking/financial information for some patients, and ordering health care provider for some health care services provided in certain Eastern Health departments and

programs (e.g., Laboratory Medicine, Medicine, Surgery, Cancer Care and Cardiology).

Response

Once the attack was detected on **October 30, 2021**, NLCHI took immediate actions to respond, including working closely with its MSP, initiating its internal Emergency Operations Centre, notifying the Office of the Chief Information Officer (OCIO), the Department of Health and Community Services (DHCS) and the four RHAs, and obtaining assistance from external cybersecurity experts.

Efforts were undertaken immediately, and continuously thereafter, to securely contain systems and restore health care operations as soon as safely possible.

On **October 30, 2021**, NLCHI issued a public announcement regarding the IT systems outage, and thereafter coordinated with the province to provide regular public updates.

NLCHI's MSP immediately engaged third party cybersecurity experts to conduct an investigation in the MSP environment and to assist the MSP and NLCHI with system recovery efforts. The MSP also locked relevant accounts on the MSP-managed domain and enabled accounts as needed for the response to the attack.

On **October 31, 2021**, NLCHI notified the CCCS, the RNC, and the RCMP.

Operations committees, including administration, clinical operations and communications, were established to coordinate the system recovery and restoration process. A team was assembled to review impacted applications and work to restore them to service as soon as possible. A separate team was assembled to investigate and eradicate the attacker's presence within the NLCHI-managed environment.

On **November 1, 2021**, NLCHI notified the OIPC, and a public announcement was made regarding the outage.

On **November 2 and 3, 2021**, a third-party cybersecurity expert was engaged. NLCHI also continued its analysis, planning and efforts to restore health system operations and data, and worked to respond to new developments as they emerged. As a result of these efforts, there continued to be intermittent system disruption as certain systems had to be taken offline to securely restore operations.

On **November 3, 2021**, a public announcement of an attack was made. By this time, steps were being taken for the deployment of commercial forensic and investigative endpoint tools, and numerous other containment and mitigation steps were being taken. Extensive work to restore the wide range of systems and services supporting health care, including Meditech and email services, continued at this time and for weeks to follow.

On and after **November 4, 2021**, among other activities, NLCHI continued working with the RHAs to restore Meditech (and in support of RHA staff efforts to enter the backlog of paper records that were accumulating since the start of the outage) and to prioritize the sequencing of restoring and integrating systems.

During the initial response to the attack, numerous containment and mitigation steps were being executed, including taking individual workstations and servers offline as needed, restricting internet access, taking services offline, reviewing privileged accounts, forensic investigation work, systems hardening planning, and other steps for securely restoring systems, including restorations from backups.

On **November 8, 2021**, NLCHI notified the OIPC of the privacy breach and subsequently submitted breach reporting forms. Exfiltrated data was determined to have been taken from the Meditech data repositories and a network drive for Eastern Health.

On **November 9, 2021**, the RHAs were notified of the potential scope of the privacy breach and an initial public announcement was made that a privacy breach had occurred. This was followed up in the latter part of November with public announcements and notifications about resources and information for affected individuals and how they could access free credit monitoring, in addition to direct notifications to certain affected current and former employees and patients.

Continuing to **November 21, 2021**, other containment and mitigation steps taken by NLCHI included global password resets, patching of all gateway components, further enhancing use of a O365 monitoring and reporting tool, completing a vulnerability scan on all RHA and NLCHI internet accessible addresses, conducting a hardware inventory reconciliation, and taking steps towards implementing MFA for all remote access mechanisms that were previously using a single-factor authentication method.

As of **December 5, 2021**, significant progress had been made on system restoration and most of the critical and priority systems had been restored or rebuilt from backups, and all devices (e.g., laptops, desktops, servers) on the NLCHI and RHA networks had been analyzed for evidence of malicious activity.

Systems Restoration

Restoration efforts involved oversight of server restoration, database restoration, security scan, and application restoration and reinstallation with appropriate "User Acceptance Testing" as each application was approved for use. Users of the applications were notified of the application status once all work had been completed.

This process involved multiple cross functional teams, vendor engagement, and business owner engagement to ensure the application and associated data was restored, secured, clinically validated and approval was communicated for clinical use. This process continued until all identified applications were restored to service.

Between **December 8 and 20, 2021,** on-going communications and updates were provided to the OIPC, by the province, NLCHI, and the RHAs. Further public announcements regarding the privacy breach were made on **December 14, 2021**.

In November and into **December 2021**, NLCHI conducted extensive work on the secure restoration of health applications and systems to support the RHAs, based on system prioritization developed by the RHAs and NLCHI, including in respect of a wide range of core hospital operations (including Meditech), email, back-office systems, cancer care, laboratory systems, integration engines, medical imaging, COVID response systems, cardiology, and other areas.

Response - Breakwater

Breakwater is a coordinated and multi-disciplinary effort led by NLCHI and the RHAs to counter the risks of cyber threats and to create resiliency against future attacks. Active priority work in Breakwater continues to this day as part of a roadmap to enhancement of cybersecurity for the provincial health systems, including:

- Continued operationalization of the use of a leading cybersecurity industry endpoint security, monitoring and remediation tool and services.
- Continued scanning of external access points.
- Continued steps toward the implementation of a centralized gateway and firewall to further enhance cybersecurity detection and control capabilities.
- Continued steps toward the implementation of a Provincial Security Information and Event Management (SIEM) system.

- Roll out of a new mandatory cybersecurity training program to NLCHI and RHA staff.
- Ongoing Active Directory review and further enhancement.
- Continued work to enhance IT asset management.
- Implementation of centralized email/URL filtering technology to enhance centralized event protection, detection, and investigation capabilities.
- Data quality and safety through continued review of backfilling of patient data into systems affected by the disruption caused by the attack.
- Enhancement and maintenance of awareness and understanding of cyber-risk across the entire health workforce.
- Enhancement of a culture that enables and encourages vigilance to protect patients and employees from future cyber-attacks.

LOOKING AHEAD

The Government of Newfoundland and Labrador recognizes and is committed to reflecting on the lessons learned and focusing the collective efforts of the Provincial Government, RHAs, and NLCHI, to help prevent potential future attacks like this from happening again. This commitment will continue with the Provincial Health Authority that will be formally established on April 1, 2023, and will consolidate the ongoing security efforts of NLCHI and the RHAs.

A key part of these efforts is Breakwater, introduced above. Breakwater's goal is to protect health data and the information systems that enable the delivery of care. It embodies initiatives to consolidate cybersecurity enhancements that address a wide range of potential security risks. Key components of Breakwater were in progress prior to the cyberattack, after which several aspects were accelerated and enhanced. This approach streamlines ongoing security enhancement efforts and ensures a coordinated approach to security control implementations.

As part of the Provincial Government's continual commitment to enhancing security, we have prioritized potential security risks, with inputs from a wide range of sources including the Department of Public Safety and Emergency Preparedness (Public Safety Canada), third party cybersecurity experts, and internal expertise.

Alongside NLCHI and the RHAs, the Government of Newfoundland and Labrador remains committed to continually investing in enhancing its processes, people, and technology to support secure digital health service delivery in the province.


Newfoundland
&
Labrador