Canadian digital health data breaches: time for reform

Canadian health data experts and class action lawyers say that a data ransom payment, after a massive security breach that potentially involves 15 million patients' electronic records, raises profound questions about the vulnerability of digital health information systems and the need for better prevention guidelines.

The security breach affected Toronto-based LifeLabs, one of world's largest medical testing companies that does over 100 million laboratory tests on Canadians annually. The breach was made public on Dec 17, 2019, when Chris Brown (CEO of LifeLabs) released an open letter to Canadians describing a "recently identified [a] cyber-attack that involved unauthorized access to our computer systems with customer information that could include name, address, email, login, passwords, date of birth, health card number and lab test results". After offering a personal apology, Brown went on to explain that LifeLabs attempted to retrieve the data by making a ransom payment stating, "we did this in collaboration with experts familiar with cyber-attacks and negotiations with cyber criminals".

Responding to questions from *The Lancet Digital Health*, Chris Carson, Senior Vice President, Corporate Affairs, Strategy and Innovation at LifeLabs said, "it was a difficult decision to pay the ransom, but we believed that customers would want us to do everything possible to retrieve their data".

Cyber security experts have advised LifeLabs "that the risk to our customers in connection with this cyber-attack is low and that they have not seen any public disclosure of customer data during their investigations, which include monitoring of the dark web and other online locations", Carson says.

On the same day that LifeLabs disclosed the breach, the offices of the Information and Privacy Commissioners of British Columbia (BC) and Ontario—the governmental bodies that oversee information and privacy laws in Canada's most populous English-speaking provinces—released a statement revealing that LifeLabs had actually reported the breach to the authorities 6 weeks earlier.

"Cyberattacks are growing, criminal phenomena and perpetrators are becoming increasingly sophisticated. Public institutions and healthcare organizations are ultimately responsible for ensuring that any personal information in their custody and control is secure and protected at all times", Brian Beamish, Information and Privacy Commissioner of Ontario, warned in the statement.

In an explanatory document accompanying their statement, Michael McEvoy, Information and Privacy Commissioner for BC, added that "these kind of attacks—and the bad actors who perpetrate them—are becoming increasingly sophisticated. Even if an organization does everything right, there is no guarantee that they will not fall victim to a cyberattack. It's important to be vigilant, and continuously examine cybersecurity systems, including staff training and other technical and administrative measures."

Noting that the "breach of sensitive personal health information can be devastating to those who are affected", McEvoy added that he and Beamish are "committed to thoroughly investigating this breach. We will publicly report our findings and recommendations once our work is complete." Spokespersons for the Ontario and BC privacy commissioners told *The Lancet Digital Health* they cannot say when their report will be released.

Adrian Dix, BC Minister of Health, told reporters that LifeLabs delayed making the breach public because they wanted to first ensure that their systems were secure and not vulnerable to secondary attacks.

At the International Cyber Crime Research Centre in the School of Criminology at Simon Fraser University (Vancouver, BC, Canada) director Richard Frank told *The Lancet Digital Health* that he predicts that parts of LifeLab's database might eventually end up in a market place on the dark web (eg, cryptomarkets), in which payments are made using anonymous and mostly untraceable digital currencies.

Although the data remain on the victim's computer in most ransomware cases, access to it "is revoked through strong encryption", Frank explains. "However, the language used by the Ontario privacy commissioner indicates that in the LifeLabs case, the data were extracted."

Although LifeLabs said it "retrieved the data by making a payment", Frank says, "if the cybercriminals already have a copy, then retrieving it will not suddenly disallow the attackers from further using that data". Frank suggests that LifeLabs likely "fell victim to a ransomware attack, possibly sparked by a phishing email with a malicious link or attachment". At LifeLabs, Carson says that the company "never lost access to its computer systems or customer data" and that LifeLabs "did have backup and recovery procedures in place before this cyber-attack".

Frank argues that the Canadian Government should enact legislation similar to the European Union's 2018 General Data Protection Regulation (GDPR) introduced in 2018.

In August 2018, after the British Airways website was breached and 500 000 customer details were stolen, the UK's Information Commissioner's Office handed down a fine of approximately $321 million, based on a new UK law designed to mirror the European Union's GDPR. "With penalties like that", Frank says, "third-party organizations would have no choice but to take data security

For the **open letter by LifeLabs** see https://www.lifelabs.com/lifelabs-releases-open-letter-to-customers-following-cyber-attack/

For the **ruling from UK High Court on the malware breach** see https://www.bailii.org/ew/cases/EWHC/Comm/2019/3556.html

For more on the **ransomware virus attack on three Ontario hospitals** see https://www.cmaj.ca/content/192/4/E101

seriously, rather than as an operational cost."

The LifeLabs hack is far from the first event of its kind concerning Canadian health data. In September 2019, the computer systems of three Ontario hospitals were crippled by a ransomware virus. Additionally, Frank notes that another attack shut down health care computer systems across northern Ontario earlier in 2019.

Describing the LifeLabs breach as "terrifying", Laura Tribe, executive director of Vancouver-based OpenMedia, a digital privacy advocacy group, complained that LifeLabs waited well over a month before informing the public. Tribe notes than in 2013, the same company admitted that it "lost track of" a computer hard drive with information for more than 16 000 patients.

At Lifelabs, Carson acknowledges that in 2013 "a hard drive containing the results of ECGs, or electrocardiograms for 16 000 patients in BC was stolen. We implemented measures to minimize the risk of such incidents in the future."

OpenMedia is calling for a parliamentary investigation into the LifeLabs breach to examine "ways to increase corporate accountability to stop these breaches once and for all." Canadian class action lawyers are preparing lawsuits. "The scale of the LifeLabs privacy breach is truly massive—it affects over three quarters of all Ontarians and British Columbians", says Cory Wanless, a lawyer with Waddell Phillips, a Toronto-based firm that has launched a proposed class action lawsuit against LifeLabs. "Basically anyone in Ontario or BC who has gone for any form of medical testing over the past several years is affected."

A second class action lawsuit has been proposed for certification in the BC Supreme Court on behalf of Anna Belle Tharani, a BC care aide whose health information was potentially compromised in the data breach. Tharani's lawsuit argues that LifeLabs lacked "adequate security" and "adequate training for employees" ahead of the attack and that customers should have been notified earlier.

A December 13, 2019, ruling from UK High Court of Justice Sir Simon Bryan revealed that an unnamed Canadian insurance company paid a $950 000 ransom to hackers in October 2019. The ruling explains that "a hacker managed to infiltrate and bypass the firewall of that insured customer, who happens to be an insurance company, and installed malware called BitPaymer. The effect of that malware was that all of the insured customer's computer systems were encrypted, the malware having first bypassed the system's firewalls and anti-virus software."

Public disclosure of the hearing "would potentially tip off the persons unknown to enable them to dissipate the Bitcoins", Justice Bryan wrote and "there would be the risk of further cyber or revenge attacks on both the insurer and the insured customer by persons unknown".

Attention is growing to such incidents among health care organisations. On Jan 8, 2020, the Association for Executives in Healthcare Information Security (AEHIS), which is based in Ann Arbor (MI, USA), warned that because "the healthcare system is critical to protecting the safety, health, and well-being of a nation's citizens, it is not beyond the realm of possibility for hospitals and other healthcare facilities to be considered potential targets of state-sponsored cyber-attacks".

"Particular attention should be placed on any public-facing systems and any systems that are used to connect to the internet or open email from third parties", AEHIS noted in a statement.

Health care organisations often do not fully understand on what assets are public facing, the AEHIS statement warns. "If the asset does not require external connectivity, such access should be restricted. For assets deemed critical to being public facing, the organization should ensure that no unnecessary services are permitted or exposed".

As cyber-attacks on health systems continue, patient data can be vulnerable to criminal misuse. Law enforcement agencies and judicial authorities are scrambling to respond. The outcome of the Ontario and BC Commissioners' investigation into the LifeLabs breach, and the proposed class actions lawsuits relating to it, might provide greater clarity on mistakes that were made in failing to protect patients' data and the ability of law enforcement officials to effectively respond.

Paul Webster