Investigation & Research Report: LifeLabs Data Breach

Prepared by: Anastasiya Gruneva

Date: February 7th, 2025

Table of Contents

Executive Summary

LifeLabs, a leading Canadian provider of diagnostic and laboratory testing services, experienced a significant data breach in December 2019, compromising the personal and health information of approximately 15 million Canadians. The breach was attributed to cybercriminals exploiting vulnerabilities in LifeLabs' online appointment booking system, specifically targeting the Telerik UI framework. The attackers deployed ransomware, exfiltrated sensitive data, and demanded a ransom, which LifeLabs ultimately paid to prevent the public release of the stolen information.

The breach was exacerbated by several security weaknesses within LifeLabs, including unpatched vulnerabilities, ineffective patch management, overprivileged accounts, insufficient monitoring, and a lack of network segmentation. These deficiencies allowed attackers to move freely within LifeLabs' systems, escalating privileges and exfiltrating data undetected for an extended period. The breach remained undetected from November 2018 until October 2019, when a third-party security assessment identified the intrusion.

In response to the breach, LifeLabs took immediate steps to mitigate the impact, offering affected individuals identity theft protection and credit monitoring. The company also faced legal repercussions, including a class-action lawsuit that resulted in a settlement of $9.8 million. In addition, the Information and Privacy Commissioners of Ontario and British Columbia issued several orders and recommendations to strengthen LifeLabs' cybersecurity practices.

The LifeLabs breach highlights the critical importance of robust cybersecurity measures in the healthcare sector. Key recommendations for preventing future incidents include the implementation of a Zero Trust security model, data encryption, regular security audits, endpoint detection and response solutions, multi-factor authentication, and comprehensive employee training. By adopting these measures, healthcare organizations can better safeguard sensitive patient data and enhance their cybersecurity resilience.

Victims of Attack

LifeLabs is the leading provider of general health diagnostics and specialized laboratory testing services in Canada. With over 50 years of experience, the company employs 5,700 professionals and offers a comprehensive range of outpatient lab services, including genetic and naturopathic testing. Each year, LifeLabs conducts more than 112 million tests and serves 19+ million patients at its locations. (LifeLabs, n.d.)

On December 17, 2019, LifeLabs publicly disclosed a data breach. The following day, the news was widely reported across all major media outlets. Cybercriminals accessed the personal data of approximately 15 million Canadians, primarily those living in British Columbia and Ontario. The compromised information included names, addresses, email addresses, dates of birth, and national health card numbers from 2016 and earlier. Additionally, customer login credentials, including usernames and passwords, were also reportedly stolen in the breach. (Global News, 2019)

Technologies and Tools Utilized in the Attack

The joint investigation by the Information and Privacy Commissioners of Ontario and British Columbia into the 2019 LifeLabs data breach revealed several key findings regarding the technologies and methods used in the attack:

1. **Unauthorized Access**: The attackers gained unauthorized access to LifeLabs' computer systems.

2. **Ransomware and Data Exfiltration**: After accessing the systems, the attackers exfiltrated personal information and personal health information of approximately 8.6 million customers. They then demanded a ransom from LifeLabs, threatening to publicly release the stolen data and a report detailing their methods if the ransom was not paid. LifeLabs paid the ransom to prevent the data's release.

3. **Security Deficiencies**: The investigation highlighted that LifeLabs lacked adequate information technology security policies and had collected more personal health information than was reasonably necessary. These deficiencies contributed to the breach's severity. (Information and Privacy Commissioners of Ontario and British Columbia, 2020)

To align the LifeLabs data breach with the MITRE ATT&CK and Cyber Kill Chain frameworks, we need to break down the attack into tactics, techniques, and procedures

(TTPs) used by the adversaries. Below is a structured analysis based on the available details.

MITRE ATT&CK Analysis

Initial Access

- T1190 - Exploit Public-Facing Application
  Attackers exploited known vulnerabilities in the Telerik UI for ASP.NET AJAX framework used in the LifeLabs online appointment booking system. The Telerik vulnerabilities (CVE-2017-9248, CVE-2017-11317, and CVE-2017-11357) were made public in 2017. Each of these vulnerabilities received a base score of 9.8 (out of 10.0) on the Common Vulnerability Scoring System (CVSS) within the National Vulnerability Database, which is managed by the U.S. National Institute of Standards and Technology (NIST). A CVSS score of 9.8 signifies a severe vulnerability, characterized by significant impact and relatively simple exploitation.

Execution

- T1203 - Exploitation for Client Execution
  Attackers likely executed payloads by exploiting the Telerik vulnerabilities.
- T1059 - Command and Scripting Interpreter
  Since they gained initial access through a web application, they may have executed malicious scripts or commands.

Persistence

- T1136 - Create Account
  Attackers could have created or hijacked existing accounts to maintain access.
- T1543 - Create or Modify System Process
  They may have established persistence through services or scheduled tasks.

Privilege Escalation

- T1078.002 - Valid Accounts: Domain Accounts
  After gaining access to a compromised web server, the attackers escalated privileges by copying domain administrator access tokens from memory. (Information and Privacy Commissioners of Ontario and British Columbia, 2020)

Defense Evasion

- T1562.001 - Impair Defenses: Disable or Modify Tools
  The LifeLabs SIEM system failed to detect the breach, suggesting that attackers may have disabled security tools or operated under the radar.

Credential Access

- T1558 - Steal or Forge Kerberos Tickets (Pass-the-Ticket)
  If they obtained domain administrator tokens, they may have leveraged Pass-the-Ticket attacks.
- T1555 - Credentials from Password Stores
  They could have extracted credentials from LSASS memory or other sources.

Discovery

- T1018 - Remote System Discovery
  Attackers likely scanned the network to identify high-value targets.
- T1083 - File and Directory Discovery
  They may have searched for sensitive databases and files.

Lateral Movement

- T1021 - Remote Services (SMB, RDP, etc.)
  Attackers moved laterally using administrative privileges, possibly via RDP or SMB.
- T1550 - Use Alternate Authentication Material
  They may have used stolen tokens to access other systems.

Collection

- T1560 - Archive Collected Data
  Attackers likely compressed stolen data before exfiltration.
- T1119 - Automated Collection
  If they scripted data collection, this technique applies.

Exfiltration

- T1041 - Exfiltration Over C2 Channel
  They likely sent sensitive data outside LifeLabs' network through encrypted C2 channels.
- T1020 - Automated Exfiltration
  They may have scripted data extraction.

Impact

- T1490 - Inhibit System Recovery
  Attackers could have wiped logs or disabled security features.
- T1486 - Data Encrypted for Impact (Ransomware)
  Attackers demanded ransom for the stolen data.

Table 1. Cyber Kill Chain Analysis

Kill Chain Phase	Actions Taken
1. Reconnaissance	Attackers possibly scanned public-facing applications for vulnerabilities in Telerik UI.
2. Weaponization	Malicious exploit crafted for CVE-2017-9248, CVE-2017-11317, CVE-2017-11357.
3. Delivery	Attackers launched exploit payload against LifeLabs' web servers.
4. Exploitation	The Telerik UI vulnerability was exploited, granting initial access.
5. Installation	Attackers installed tools for persistence and privilege escalation.
6. Command & Control (C2)	Established remote access for lateral movement.
7. Actions on Objectives	Stole sensitive health data, escalated privileges, and demanded ransom.

Key Failures in LifeLabs' Security:

1. Unpatched Critical Vulnerabilities
   a. Attackers exploited Telerik UI vulnerabilities disclosed in 2017.
   b. LifeLabs failed to apply security updates from Telerik's alerts.
2. Poor Patch Management
   a. No dedicated patch management team.
   b. Security alerts went to a non-security staff member and landed in a junk mail folder.
3. Overprivileged Web Servers

    a. Machine accounts had administrator rights, allowing attackers to escalate privileges.

4. Lack of Privileged Access Monitoring
    a. No logs or SIEM alerts detected the breach.
    b. Privileged accounts were not properly monitored.
5. Flat Network Architecture
    a. No network segmentation, allowing easy lateral movement.
    b. Attackers moved freely across the organization.
6. Ineffective Vulnerability Scanning
    a. Tools failed to detect vulnerabilities in web servers.
    b. Scans started only in 2019, despite known issues from 2017.

The LifeLabs breach was a multi-phase attack enabled by weak security practices, outdated software, and poor vulnerability management. If proper patching, monitoring, and network segmentation were in place, the attack could have been prevented or at least detected earlier.

Timeframe of the Attack

The LifeLabs data breach occurred over an extended period before its discovery. According to a statement of claim filed in a class-action lawsuit, the security breach began in November 2018 or earlier and remained undetected for at least a year until late October 2019. During this time, cyber attackers accessed and exfiltrated customers' personal information. (Babin, 2023)

LifeLabs became aware of the breach on October 28, 2019, following a security assessment by a third party. The company subsequently notified the Office of the Information and Privacy Commissioner of Ontario on November 1, 2019, and the Office of the Information and Privacy Commissioner for British Columbia on November 5, 2019. (Information and Privacy Commissioners of Ontario and British Columbia, 2020)

In summary, the unauthorized access to LifeLabs' network began in November 2018 or earlier and continued undetected until late October 2019, resulting in the exposure of sensitive personal and health information of millions of individuals.

Below is a visual representation of the timeline illustrating key events of the LifeLabs cyber attack.

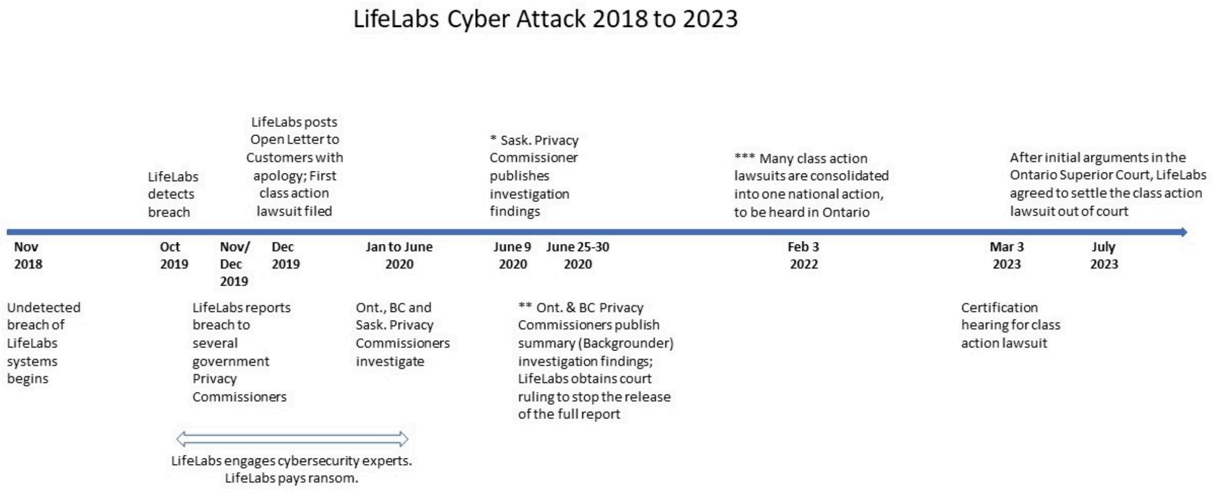
LifeLabs Cyber Attack 2018 to 2023
Nov 2018
Undetected breach of LifeLabs systems begins
Oct 2019
LifeLabs detects breach
Nov/ Dec 2019
LifeLabs reports breach to several government Privacy Commissioners
Dec 2019
LifeLabs posts Open Letter to Customers with apology; First class action lawsuit filed
LifeLabs engages cybersecurity experts. LifeLabs pays ransom.
Jan to June 2020
Ont., BC and Sask. Privacy Commissioners investigate
June 9 2020
* Sask. Privacy Commissioner publishes investigation findings
June 25-30 2020
** Ont. & BC Privacy Commissioners publish summary (Backgrounder) investigation findings; LifeLabs obtains court ruling to stop the release of the full report
Feb 3 2022
*** Many class action lawsuits are consolidated into one national action, to be heard in Ontario
Mar 3 2023
Certification hearing for class action lawsuit
July 2023
After initial arguments in the Ontario Superior Court, LifeLabs agreed to settle the class action lawsuit out of court

Figure 1. Summary Timeline of the LifeLabs Cyber Attack 2018 to 2023. (Babin, 2023)

Systems Targeted by the Attackers

In the LifeLabs data breach, cyber attackers gained unauthorized access to the company's computer systems, compromising sensitive customer information. The affected systems included databases and servers containing personal data such as names, addresses, emails, logins, passwords, dates of birth, health card numbers, and lab test results. (LifeLabs, n.d.)

Motivation of the Attackers

The LifeLabs data breach in 2019 was primarily financially motivated. Attackers infiltrated the company's computer systems, exfiltrated sensitive personal and health information of approximately 15 million Canadians, and subsequently demanded a ransom to prevent the public release of the stolen data. LifeLabs confirmed that they made a payment to retrieve the data, though the exact amount was not disclosed. (Information and Privacy Commissioners of Ontario and British Columbia, 2020)

This type of cyberattack aligns with common ransomware tactics (T1486, MITRE ATT&CK), where attackers encrypt or steal data and demand payment for decryption keys or to refrain from disclosing the information. The primary objective in such cases is financial gain. (Swiss Cyber Institute, 2021)

In summary, the attackers' motivation was financial, aiming to extort money from LifeLabs by leveraging the sensitivity and volume of the compromised data.

Outcome of the Attack

Legal and Financial Consequences of the Breach

In response to the 2019 data breach, LifeLabs took immediate steps to mitigate the impact on affected individuals. The company offered complimentary services, including identity theft protection and credit monitoring, to those whose personal information had been compromised. These measures aimed to assist customers in safeguarding their identities and monitoring for potential misuse of their data. (LifeLabs, 2019)

Subsequently, LifeLabs faced legal challenges due to the breach. A class-action lawsuit was filed, alleging that the company failed to implement adequate cybersecurity measures to protect customer data. The lawsuit sought significant damages, highlighting the severity of the breach and its impact on millions of Canadians.

The LifeLabs data breach class action lawsuit has been settled, with the Ontario Superior Court approving the settlement and appointing KPMG as the administrator. LifeLabs agreed to pay a total of $9.8 million. Given the large number of valid claims received (901,544), each class member received an e-Transfer of $7.86 or a cheque of $5.86 (after deducting a $2.00 cheque processing fee). The distribution process has been completed, and no further claims or payments will be made. (KPMG, n.d.)

Orders and Recommendations Issued to LifeLabs

Following the investigation into the LifeLabs data breach, the Information and Privacy Commissioner of Ontario (IPC) and the Information and Privacy Commissioner of British Columbia (OIPC) issued several legally binding orders and recommendations, which were designed to improve LifeLabs' security practices and ensure compliance with privacy laws.

Order 1:

- LifeLabs was required to subscribe its security team to Telerik's security notification list to ensure awareness of critical security updates.
- The company had to ensure that its security staff actively monitored these alerts and took necessary action.

Order 2:

- LifeLabs was mandated to develop and enforce comprehensive written information security policies that outline IT security safeguards, ensuring compliance with PHIPA and PIPA regulations.

Order 3:

- The company was ordered to stop collecting failed login credentials (usernames and passwords) and to securely dispose of any previously collected records.

Order 4:

- LifeLabs was required to implement a notification process to inform affected individuals about what specific personal health information (PHI) had been compromised without requiring individuals to submit access requests.

Order 5:

- LifeLabs had to clarify and formalize its status under PHIPA in relation to its contractual relationships with Trillium Health Partners and other healthcare providers in Ontario with whom it had similar agreements.

Recommendation 1:

- It was recommended that LifeLabs consult independent third-party cybersecurity experts to determine whether a longer period of credit monitoring would be appropriate for affected individuals, given the sensitivity and long-term risks associated with the breach.

These directives were aimed at rectifying the security failures that led to the breach and strengthening LifeLabs' cybersecurity measures to prevent future incidents.

Ransom Payment and Its Implications

To prevent the public release of the stolen data, LifeLabs decided to pay the ransom demanded by the attackers. This decision was made after consulting with cybersecurity experts and law enforcement agencies, aiming to protect customer information from further exposure. The specific amount paid was not disclosed. (Freedman, 2019)

The payment of the ransom has been a subject of debate. While it may have prevented the immediate release of sensitive data, such actions can inadvertently encourage further attacks by demonstrating that organizations are willing to comply with attackers' demands. This raises concerns about the broader implications for cybersecurity, particularly in the healthcare sector.

The financial burden of the ransom payment was borne by LifeLabs. However, the broader costs associated with the breach, including legal settlements and reputational damage, underscore the importance of robust cybersecurity measures. There is limited evidence to suggest a direct increase in attacks on Canada's healthcare sector as a direct result of this incident. Nonetheless, the breach highlights the critical need for healthcare organizations to be vigilant and proactive in their cybersecurity efforts. (Babin, 2023)

In conclusion, the LifeLabs breach underscores the importance of understanding the evolving threat landscape. Healthcare organizations must implement comprehensive security measures, conduct regular risk assessments, and foster a culture of cybersecurity awareness to protect sensitive patient information and maintain public trust.

Recommendations

The LifeLabs data breach highlighted several critical security failures, including unpatched vulnerabilities, inadequate patch management, overprivileged accounts, insufficient monitoring, flat network architecture, and ineffective vulnerability scanning. To prevent such incidents in the future, organizations should implement the following mitigation techniques and security controls, aligned with industry standards:

1. **Data Encryption:**
   Encrypt sensitive data both at rest and in transit to prevent unauthorized access. Even if attackers gain access to the data, strong encryption ensures that it remains unreadable. (Swiss Cyber Institute, 2021)
2. **Zero Trust Security Model:**
   Implement a Zero Trust Architecture (ZTA), which assumes that every access request—whether internal or external—must be verified before granting permissions. (NIST, 2020)
3. **Regular Security Audits & Penetration Testing:**
   Conduct frequent security assessments to identify vulnerabilities and test defenses against real-world attack scenarios. (Tagade, 2024)
4. **Endpoint Detection and Response (EDR):**
   Deploy advanced threat detection and response solutions to identify suspicious activities and stop cyber threats before they cause damage. (Canadian Centre for Cyber Security, 2022)

5. **Comprehensive Employee Training:**
   Provide ongoing cybersecurity awareness training to employees, focusing on phishing detection, password security, and social engineering threats. (Canadian Centre for Cyber Security, 2024)
6. **Multi-Factor Authentication (MFA):**
   Require MFA for all users, especially for accessing sensitive data, to add an extra layer of security against credential theft. (Cybersecurity & Infrastructure Security Agency (CISA), n.d.)

By implementing these techniques and controls, healthcare organizations can significantly reduce the risk of cyberattacks, protect patient data, and strengthen overall cybersecurity resilience.

References

Babin, R. (2023, December). *LifeLabs: The ethics of responding to a ransomware cyber attack.* Open Access Teaching Case Journal, 1(2). https://doi.org/10.58067/7wmc-gv65

Canadian Centre for Cyber Security. (2022, October). *Choosing the best cyber security solution for your organization - ITSM.10.023*. https://www.cyber.gc.ca/en/guidance/choosing-best-cyber-security-solution-your-organization-itsm10023

Canadian Centre for Cyber Security. (2024, September). *Offer tailored cyber security training to your employees - ITSAP.10.093*. https://www.cyber.gc.ca/en/guidance/offer-tailored-cyber-security-training-your-employees-itsap10093

Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). *Require Multifactor Authentication*. Retrieved February 7, 2025, from https://www.cisa.gov/secure-our-world/require-multifactor-authentication

Freedman, L. (2019, December 19). *LifeLabs Pays Ransom to Retrieve Patient Data*. https://natlawreview.com/article/lifelabs-pays-ransom-to-retrieve-patient-data

Global News. (2019, December 18). *LifeLabs hack: What Canadians need to know about the health data breach*. Global News. https://globalnews.ca/news/6311853/lifelabs-data-hack-what-to-know/

Information and Privacy Commissioners of Ontario and British Columbia. (2020, June 25). *JOINT INVESTIGATION INTO LIFELABS DATA BREACH*. https://www.oipc.bc.ca/documents/investigation-reports/2886

KPMG. (n.d.). *LifeLabs Privacy Breach Class Action*. KPMG. https://lifelabssettlement.kpmg.ca/

LifeLabs. (n.d.). *Company Information*. LifeLabs website. Retrieved February 7, 2025, from https://www.lifelabs.com/about-us/about-lifelabs

LifeLabs. (n.d.). *LifeLabs releases open letter to customers following cyber-attack*. Retrieved February 7, 2025, from https://www.lifelabs.com/lifelabs-releases-open-letter-to-customers-following-cyber-attack/

LifeLabs. (2019, December 17). *An Open Letter to LifeLabs Customers*. https://customernotice.lifelabs.com/

NIST. (2020, August). *NIST Special Publication 800-207. Zero Trust Architecture.* https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420

Office of the Saskatchewan Information and Privacy Commissioner. (2020, June 9). *INVESTIGATION REPORT on LifeLabs LP and Saskatchewan Health Authority*. https://oipc.sk.ca/assets/hipa-investigation-398-2019-399-2019-417-2019-005-2020-019-2020-021-2020.pdf

Swiss Cyber Institute. (2021, May 11). *Lessons Learned: LifeLabs Data Breach Case Study*. https://swisscyberinstitute.com/blog/lessons-learned-3-lifelabs-data-breach/

Tagade, K. (2024, October 8). *Penetration Testing Compliance: Easy-to-Follow Guide*. https://www.getastra.com/blog/security-audit/penetration-testing-compliance/