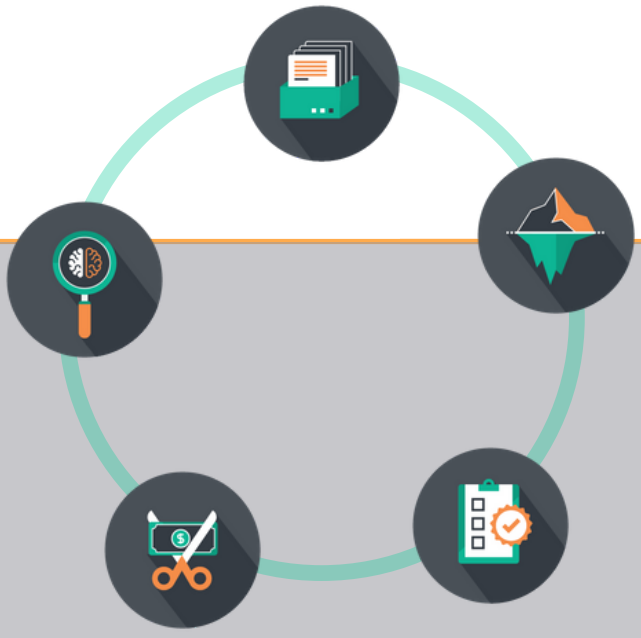
nyxeia
Insight Reimagined™

powered by everteam

THE LESSONS OF LIFELABS and the Evolving State of Data Privacy Protection in Canada



THE EVER-IMPORTANT ROLE OF INFORMATION GOVERNANCE IN CYBERSECURITY

For those following the important topic of data privacy protection in the era of GDPR and CCPA, the news seems to be a never-ending stream of stories related to poor information governance and lax cybersecurity practices.

December of 2019 saw a particularly interesting case come to light, that of Canadian medical laboratory testing services provider LifeLabs.

As one of Canada's leading provider of medical testing services, LifeLabs plays a crucial role in the health and wellbeing of millions of Canadians. Perhaps just as importantly, in dealing with personally identifiable information (as well as medical histories and test results), LifeLabs is a steward to some of the most sensitive patient data imaginable.[2]

LifeLabs was victim to a recent cyberattack that resulted in the compromise of medical information for millions of patients. As part of its response to the breach, LifeLabs paid out an undisclosed sum of money to hackers to retrieve this information. Though this was an unfortunate cyberattack case, there are lessons we can learn . Below are some of the insights we can take away from the LifeLabs data breach.

The importance of a regular sensitive information asset inventories

While details of the LifeLabs case are unclear, it is likely that the organization failed to adequately monitor how sensitive information was being managed within their enterprise. Only through regular audits aimed at uncovering all of the locations where sensitive information may be stored – including enterprise applications, file servers, cloud file shares, groupware platforms, email, instant messaging, and elsewhere – can the organization understand its true position with regard to data privacy protection. Most organizations inadvertently store copies of sensitive information in places that are poorly secured and vulnerable either to hackers or unauthorized internal users. Knowing that all of the systems that host sensitive data are held to the highest security standards is essential to compliant operations in our post-GDPR world. In cases where sensitive data is found in unauthorized locations, it can be removed in a timely way to reduce the likelihood of loss.

The criticality of offsite "hot" data backups to business continuity

LifeLabs paid a ransom not only reduce the likelihood of broad dissemination of sensitive information but because that breach denied them access to data affecting almost 15 million Canadian customers. In other words, the data wasn't just stolen – it was also made inaccessible to LifeLabs. The apparent failure to maintain a so-called "hot" archive of all customer data in a secure off-site location demonstrates the need for diligence with regard to business continuity and disaster recovery planning.

The need for total candor in post-breach communication to customers

In the weeks following the customer data breach, LifeLabs sought to reassure customers by issuing statements indicating that their company's hired "cyber security firms have advised that the risk to…customers in connection with this cyber-attack is low." [1] While this statement may be an understandable attempt to calm the nerves of customers who are worried about identity theft or potential misuse of their sensitive information, it's a potentially irresponsible thing to say. The fact that sensitive data was seized by outside actors means that LifeLabs is no longer in a position to say what will happen next with that data. Saying otherwise sets unrealistic expectations, and compounds the damage to LifeLabs customers and their reputation. Better to avoid making impossible promises, and instead focus on improving tools and processes to avoid future mistakes.

This case -- in which hackers publicly profited from their deeds -- has resulted in substantial damage to LifeLabs individual and corporate customers, as well as to the value of the LifeLabs brand. In the weeks following the breach, customers and their legal representatives embarked on a class action suit aimed at "punishing" the company through a $1.13B fine. [2] Companies wanting to avoid a similar fate must be prepared to invest proactively in tools and training aimed at safeguarding their valuable information assets.

[1] https://customernotice.lifelabs.com
[2] https://www.ctvnews.ca/canada/lifelabs-hack-data-protection-a-big-problem-for-a-lot-of-companies-1.4748607

The Everteam Information Governance Suite provides capabilities that are directly applicable to companies like LifeLabs

The everteam.discover product provides deep insight into unstructured and structured data residing throughout the enterprise to identify information that is potentially hosted inappropriately. With powerful machine learning and natural language processing capabilities, everteam.discover can categorize content in automated, intelligent ways making potential data privacy protection issues in even the largest environments visible and actionable to IT, compliance and records management staff.

The everteam.policy product gives IT, compliance and records management teams the ability to define information retention and destruction policies that are tailored to the needs of their business, their industry, and the regulatory environment in which they operate. By ensuring that data is kept only as long as legal or internal policies dictate, everteam.policy is an important part of minimizing the information "surface area" that is exposed to potential hackers like those that perpetrated the LifeLabs breach. By managing this information where it lives (versus in a centralized records management system), everteam.policy and everteam.discover increase the reach of records managers, compliance teams, and IT in governing their sensitive data.

The everteam.archive product provides a means for organizations to back up structured and unstructured information using an Everteam repository, a third-party repository (like an Enterprise Content Management System), or a file server for secure offline storage. By performing regular archives of sensitive data, the organization can be more confident that even if there is a breach somewhere in the enterprise, the operation will not be subjected to the kind of wholesale data loss seen in the LifeLabs case.

As the cost of such sensitive data breaches becomes more and more evident, Canada is moving quickly to enact protections similar to GDPR and the recently enacted CCPA.

Focused on updating Canada's Digital Charter to meet the emerging needs of data subjects, new regulations are being drafted that will extend Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). These and other measures underway in 2020 should improve the reporting of breaches and establish appropriate penalties and processes aimed ensuring regulatory compliance. [3]

[3] https://portswigger.net/daily-swig/canada-plans-revamp-of-its-data-privacy-law

AN INNOVATOR IN INFORMATION GOVERNANCE

Nyxeia is expert in meeting the information governance and data privacy protection challenges faced by companies like LifeLabs. As an innovator in Information Governance and Enterprise Content Management for nearly 30 years, our teams have worked with some of the world's leading brands to better manage sensitive information for improved competitive position, compliance with GDPR and CCPA, higher levels of customer trust and loyalty.

Nyxeia | 1251 Avenue of the Americas | 3F
New York, NY 10020 | info@nyxeia.com