January 11, 2019

ARTICLE

Unscrambling Digital Laws And Cybersecurity

An Evolving Landscape

The growing importance of data — as well as recent high-profile security breaches — are pushing many nations, including Canada, to review and bolster data protection laws. This is welcome, but even with improved protections, there are no simple answers when it comes to cybersecurity.

As technology evolves, the laws, regulations and standards that shape its use are also changing. There is a broad array of standards that can inform what an organization must do to be compliant. New legislation, regulations, guidance documents and industry-specific recommendations are coming out all the time in Canada. But cross-border data flows and cloud storage mean that foreign laws may also apply.

This evolving regulatory and risk environment can impact different organizations quite differently. The standards that a charity or university will be held to are likely different from those for a bank. This is why it's critical to take a tailored approach to every security scenario.

How Hacks Happen

Data hacks have become one of the biggest risks to an organization hoping to realize the benefits of big data. They can ruin a company's reputation, decimate its stock price and trigger costly legal and regulatory consequences, including class action lawsuits, which are on the rise in Canada.

The good news is that most cyberattacks are relatively unsophisticated. While there have been recent fears about hackers using artificial intelligence to breach cybersecurity defenses, the reality is it doesn't take AI to crack a weak system. A dangerous hack can start with a simple phishing scam, in which an employee is fooled into clicking on a link in an email.

Increasingly, stolen data are being encrypted and held for ransom. If the ransom isn't paid, hackers release the information or destroy it.

Inside the Mind of a Hacker

To fend off attacks, it helps to understand the security weaknesses hackers look for. BLG works closely with technical and forensic experts who have a presence on the dark web, an unregulated part of the internet that isn't visible to search engines. Stolen data often ends up there, for sale to criminals looking to profit from banking information, credit card numbers, and other personal information.

Enormous Consequences

The effects of a data breach can be wide-ranging and long-lasting. Yahoo Inc. experienced a number of massive breaches in 2014, including one by a Russian spy agency. Personal data — names, addresses, telephone numbers and encrypted passwords — for 500 million accounts were stolen.

Altaba, the company then operating Yahoo's email and search-engine service, was fined $35 million U.S. by the U.S. Securities and Exchange Commission. In a settlement reached in a class action lawsuit, Altaba and Verizon, which was in the process of buying Yahoo, agreed to pay $50 million U.S. to up to 200 million users, with affected individuals getting a maximum of $375 U.S. each. This is a reminder that the consequences of a data breach can be enormous.

How to Better Protect Data

A holistic approach to cybersecurity is essential. This means implementing both preventative and remedial tactics:

Before an Incident

- Know what "crown jewels" your organization has and what are its key informational assets
- Adopt best-in-class technology and implement all security updates and patches to render your systems reasonably secure and put your organization in a defensible position
- Understand the potential liabilities and evolving standards of care around big data to mitigate the legal risks of data breaches or misuse of information
- Have cybersecurity and incident response plans in place, as well as the requisite expertise (both internal and external) on a fully constituted response team

After an Incident

- Immediately implement the incident response plan and convene the response team
- Retain an experienced cybersecurity lawyer to serve as "breach coach", manage the response team, and ensure that legal privilege is protected to the maximum extent
- Ensure that evidence of the wrongdoing is preserved in the remediation process
- Be consistent in public communications and reports made to regulators and law enforcement

A breach should be viewed as creating enterprise-wide risk. For that reason, stakeholders from across the organization are often involved in managing it. Their responses need to be coordinated from start to finish. Here's just one example of why:

> If a company's servers are infected with a virus, the IT department may want to take them offline, wipe them and rebuild them. But in doing so, it may inadvertently destroy evidence that is critical in establishing how the breach occurred and who's responsible. That evidence could also prove essential in defending against legal and regulatory proceedings.

A harmonized response can be challenging for most businesses, so it's prudent to rely on knowledgeable experts. BLG has acted as breach coaches in numerous high-profile data breaches in Canada, directing multidisciplinary teams in investigations and remediation to ensure that evidence is properly preserved and handled, and lawyer-client privilege protected.

---

[1] A zettabyte is the equivalent of one trillion gigabytes. So that's 163 trillion gigs of information, the equivalent of everyone on Earth getting 14,927 newspapers a day for a year.

By: Ira Nishisato

Services: Cybersecurity, Privacy & Data Protection