itworldcanada.com

Understanding Current Cybersecurity Challenges in Law: Data Breaches and Increased Data Awareness (Article 5) - IT World Canada

Melissa Lukings and Arash Habibi Lashkari

9-11 minutes

Data breaches are incidents in which information is stolen or taken from a system without the knowledge or authorization of the owner of that system. Data breaches can expose confidential, sensitive, or protected information to an unauthorized person or without the permission of the owner of the information being accessed. In general, data breaches happen due to weaknesses in technology or errors in user behaviour.

In our previous articles in this series, we have discussed: the concept of data sovereignty as a legislative challenge in our global digital world; the role of digital governance and governance strategies in relation to the concept of digital social responsibility; the complexities inherent in assigning jurisdictional authority for the purpose of addressing online content and activities; and the ongoing arguments for and against digital censorship in the Canadian legal landscape. You can view our previous articles here:

- Understanding Current Cybersecurity Challenges in Law: Balancing Responsibilities in Digital Content Censorship (Article 4)
- Understanding Current Cybersecurity Challenges in Law: Determining Online Jurisdictional Authority (Article 3)
- Understanding Current Cybersecurity Challenges in Law: Digital Governance and Social Responsibility Meet User-Generated Content (Article 2)
- Understanding Current Cybersecurity Challenges in Law: Data Sovereignty and Cross-Border Data Transfers (Article 1)

For our fifth, and penultimate, article in our six-part series, “Understanding Current Cybersecurity Challenges in Law”, we will discuss the issues related to data breaches, cybersecurity, and increased data awareness.

What is a data breach?

A data breach is a security violation, in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Other terms are unintentional information disclosure, data leak, information leakage, and data spill. Incidents range from concerted attacks by individuals who hack for personal gain or malice (black hats), organized crime, political activists or national governments, to poorly configured system security or careless disposal of used computer equipment or data storage media. Leaked information can range from matters compromising national security, to information on actions which a government or official considers embarrassing and wants to conceal. A deliberate data breach by a person privy to the information, typically for political purposes, is

more often described as a “leak”.

Data breaches may involve financial information such as credit card and debit card details, bank details, personal health information (PHI), Personally identifiable information (PII), trade secrets of corporations or intellectual property. Data breaches may involve overexposed and vulnerable unstructured data – files, documents, and sensitive information.

Many jurisdictions have passed data breach notification laws, which requires a company that has been subject to a data breach to inform customers and take other steps to remediate possible injuries.

Types of data breaches

- Stolen Information

  Simply having one person leave a computer, phone, or file somewhere that it is unprotected and having it stolen is incredibly common. Errors like this can cost a company hundreds of thousands, if not millions, of dollars.

- Password Guessing

  Many people have been hacked simply because their password was too easy or too guessable. A common method amongst hackers, password guessing is also sometimes known as a brute-force attack. Alternatively, by simply leaving passwords for computers on notes, an individual lowers the security threshold of the protected data.

- Keyloggers

  The function of a keylogger program is to record everything that you type into your device – that is, “the keystrokes” – which can

include data such as credit card numbers, passwords and sensitive information you might enter into a database like names, health data, etc.

- Phishing

  Phishing is a cybercrime in which a target is contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data.

- Malware or Virus
- Malware or viruses can be sent to people with the goal of wiping their computer. This can be harmful to any company, especially those who rely on their data. For example, Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyberattackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files.
- Distributed Denial of Service (DDoS)

  A distributed denial-of-service (or “DDoS”) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Threats, consequences, and costs

Data breaches can be quite costly to organizations with direct costs (remediation, investigation, etc) and indirect costs (reputational damages, providing cyber security to victims of compromised data, etc.). A data breach could ruin your brand –

and your revenue.

Based on a report by IBM and the Ponemon Institute, the average cost of a data breach in 2021 was US$ 4.24 million. This was a 10% increase from the average cost of $3.86 million in 2019.

In the past few years we have seen hundreds of attacks that have breached the privacy of millions of users. From hacks that have affected universities and their students, to breaches that have compromised information at hospitals, the list truly is limitless.

Breach prevention

The annual cost of a Data Breach Report found that the most common initial attack vector was compromised credentials, followed by phishing, cloud misconfigurations, and vulnerabilities in third-party software.

It is very difficult, perhaps impossible, for any company to claim to be completely immune to data breaches. While there is no foolproof method of protecting yourself or your company from data breaches, you can educate yourself and others on the importance of maintaining security by regularly changing passwords and by limiting the amount of sensitive information carried outside of the workplace, as well as the consequences of data breaches.

There are a few protective actions that can be taken to reduce the risk of a data breach for yourself or your business. Ten of these include:

- Protecting the data itself, not just the perimeter
- Paying attention to insider threats
- Encrypting all devices

- Testing your security
- Delete redundant data
- Spending more money and time on cybersecurity
- Establishing strong passwords
- Updating your programs regularly
- Backing-up your data regularly
- Creating a company-wide security mindset

Data awareness

The greater emphasis on data within businesses and in combination with big milestones in the legal world – such as the implementation of the *General Data Protection Regulation* in the European Union – has heightened public attention and awareness of the issues inherent in the evolution of data privacy in the law. From this increase in awareness, we have seen an increase in customer expectations with regard to data privacy and accountability in how businesses manage their data. Data awareness, or “being data aware”, refers to being able to see data opportunities and risks and translate them to actions with respect to securing sensitive data on your devices or within the context of the workplace.

Conclusion

Anyone can be at risk of a data breach — from individuals to high-level enterprises and governments. Further, by not being cautious, any one person may inadvertently put others at risk of such a breach. With impacts ranging from financial costs to reputational damage, data breaches are a large point of concern for both

individuals and companies in our modern world.

Over the past few years, and particularly escalating during the COVID-19 pandemic, we have seen cyber data attacks reach an unprecedented level. This has catalysed a response from governments to ensure reporting of cyber attacks, data breaches, and ransomware attacks, partially to increase the awareness of the need for greater security responsiveness and prevention of data breaches. As we continue to move our work, health, financial, and social information online, it has become increasingly necessary for everyone to understand the implications of having such data protected rather than readily accessible by outside parties.

In our next – and final – article in this series on “Understanding current cybersecurity challenges in law”, we will delve into the exciting and transformative world of artificial intelligence, through the combined lenses of cybersecurity, ethics, human rights, and the law.