Growth in data breaches shows need for government regulations

December 4 2019, by Michael Parent

Credit: Zen Chung from Pexels

Do you remember when 40 million was a large number? Forty million dollars in sales, 40 million customers, 40 million Twitter followers, 40 million protesters —all once conveyed something substantial.

Were it only so for data breaches.

As an academic who has studied data governance for the past 20 years and worked with hundreds of boards of directors and thousands of directors and executives, I am appalled and concerned that the scope and severity of data breaches continue to grow unabated.

Increasing breaches

In 2011, hackers attacked RSA Security, a network security company, stole 40 million security tokens (physical devices used to log in to networks) records. Two years later, another 40 million records containing customer passwords and personal information were stolen from the software company Adobe.

At the time, consumers seemed shocked at the sizes of these breaches and —at least temporarily —lost trust in these organizations. There was a call for more stringent controls and harsher penalties.

Since then, data breaches and theft have increased in both size and frequency. Hackers breached Sony and stole 77 million records in 2011. They did the same to Target Corporation for 110 million records in 2013, eBay for 145 million records in 2014, Equifax for 143 million records in 2017, and Marriott International for 500 million records in 2018; there were many others.

These were all eclipsed by the three billion records compromised in a colossal breach of Yahoo Inc. When the company initially disclosed the breach in 2013, it said it had affected only one billion records. It revealed the true number in 2017.

This is an era of big data breaches. The general availability and collectability of data, and consumers' often passive willingness to share

their personal information has led to an increase in the velocity, visibility and vastness of breaches all increasing at alarming rates.

Government reactions

Congress passed the Sarbanes-Oxley Act in 2002, in reaction to large-scale egregious and fraudulent behaviour by companies like Enron, WorldCom, Tyco, Adelphia and their complicit auditors (notably Arthur Andersen in Enron's case).

Among its many provisions, Sarbanes-Oxley mandates a company's shareholders to elect external auditors that report directly to the organization's board of directors instead of management. The act criminalizes the falsification of financial statements, and it compels the chief executive and financial officers to certify quarterly that the organization's financial statements are compliant.

Sarbanes-Oxley ushered in a new era of corporate governance, with both boards and management coming under increasing scrutiny.

Cybersecurity's tipping point

I believe that cybersecurity has reached its Sarbanes-Oxley moment. Norton, the Internet security company, released a 2019 mid-year report stating that there have been 3,800 publicly reported breaches, exposing 4.1 billion records so far —a 54 percent increase over 2018.

These breaches had no regard for geography or sector, hitting financial services, entertainment, health care and government. They have included individuals' personal information and health care records; alarmingly, these breaches were all perpetrated by criminals who have yet to be identified.

In my opinion, company responses continue to be inadequate, and breaches avoidable. Legislators have begun to fill this oversight void.

The European Union Parliament was one of the first to fill the gap when it enacted its General Data Protection Regulation (GDPR) in 2016, which took effect on May 25, 2018. The GDPR applies to all individuals residing in the EU, and provides for stringent fines (20 million euros or four percent of the organization's worldwide annual turnover of the preceding year, whichever is greater) in the event of privacy breaches. The EU has been aggressive in its enforcement, levying more than 100 fines so far.

The U.S. Securities and Exchange Commission (SEC) unanimously approved issuance of disclosure obligations for cyber incidents in early 2018. In Canada, the federal government has begun modifying its Personal Information Protection and Electronic Documents Act (PIPEDA), to define when a privacy breach should be publicly disclosed and the disclosure requirements.

The most recent initiative is also perhaps the most stringent. The California Consumer Privacy Act (CCPA), which will take effect on Jan. 1, 2020, applies to any organization in California that receives or discloses personal information or derives 50 percent or more of its revenues from selling personal information.

Data ownership

The CCPA will fine organizations and provide payments to those who are affected by data breaches. But the CCPA's most game-changing principle is to assert that consumers own their data, whether willingly disclosed or not, and may opt to not divulge it without discrimination.

In other words, a consumer may choose to prevent Facebook from

collecting information about their online behaviour without being prevented from using Facebook's features. The impact on Facebook and similar companies could be cataclysmic as the majority of their revenue is derived from advertising.

So, what can an organization do? First and foremost, the board of directors or oversight body must have privacy and cybersecurity on its radar and discuss it at every single meeting. Cybersecurity and privacy should be included in the enterprise's risk planning and actively monitored.

Directors should not only be familiar with the regulatory compliance issues, but also of what data the organization possesses, processes and, more importantly, passes on. Protection of the organization's data assets becomes a much more transparent and prioritized process. As a result, a dual benefit is conferred, for protecting client information that is of value to the organization also has the effect of protecting individuals. A virtuous cycle ensues.

A recent breach at Desjardins Group, a Canadian credit union cooperative, provides an exemplary response plan. The breach was small by by global standards: 4.2 million records, but nearly all of the company's individual and business customers.

Guy Cormier, the president and CEO of Desjardins, announced the breach shortly after the bank confirmed it, and provided customers with three remediation measures: identity theft protection for up to five years; individual support from Desjardins to accompany customers through any processes to reestablish their electronic identities, including indemnification for any financial losses; and up to $50,000 per customer to offset any legal or accounting expenses incurred as a result of the breach.

This active engagement of stakeholders, in addition to shareholders and customers, underscores an authentic commitment.

Sarbanes-Oxley has become the standard for sound governance practices. The GDPR, PIPEDA, CCPA and SEC guidelines collectively trumpet a new era in data privacy and protection.

In the absence of taking the initiative, organizations will find themselves under increasingly stringent legislation and concomitant scrutiny. The choice is stark, but simple: start taking data privacy seriously, or have it imposed. Cybersecurity has reached its Sarbanes-Oxley moment.

Provided by The Conversation