DATA SECURITY AND PRIVACY IN CANADA

THE CORPORATE OBLIGATION AND THE IMPERATIVE TO MAINTAIN TRUST

2017

GREG VANIER
DATA SECURITY AND PRIVACY LEAD
EDELMAN CANADA
GREG.VANIER@EDELMAN.COM

THE STATE OF DATA SECURITY AND PRIVACY IN CANADA

No organization is immune to the threat of a data security crisis or privacy breach.

As more of our lives go online and the data we share is used in new and innovative ways, privacy and security have become important reputation and legal issues. For businesses, the growing volume and sensitivity of information being shared, stored and used is driving demand for greater transparency about how such information is being managed and protected. Privacy missteps and data breaches regularly make headlines and are a focal point for lawsuits, social media discussions and legislation worldwide.

As public and private organizations across Canada race to protect their infrastructure against persistent malicious threats, trends fueled by technology, data ubiquity and the increasing value of corporate data, ensuring data security is more difficult than ever.

To better understand how Canadian companies are navigating this evolving corporate threat, Edelman spoke with 101 information, data, security, and technology officers across Canada[1]. We wanted to know how big the problem was and how prepared companies were.

The results were alarming.

Almost one in two security, information and technology officers said their organization had exposed personally identifiable information at least once, and 30 per cent more than once. Of the companies we talked to, only one in three were very confident that their organization understands the potential corporate impact of a cyber-security incident and/or loss of sensitive or private information.

These results are more concerning when viewed through the lens of the Edelman Trust Barometer[2], our keystone annual global study on the state of institutional trust. Our 2016 study of 33,000 respondents across the world, revealed that companies are not perceived to be delivering against protecting consumer data at a level that matches its perceived importance.

As the threat landscape continues to evolve and the public's trust of institutions continues to falter, now more than ever it is critical for organizations to address the growing problem of data security and privacy. Organizations must ensure that the information entrusted to them is secure, that they are transparent about the data they store and process, and that they are prepared to respond to a breach when – not if – it happens.

[1] Edelman's Insights & Analytics team conducted this research with 101 information, data, security, and technology officers across Canada. Respondents were sourced from The Angus Reid Forum panel and the research was facilitated by MARU/Vision Critical Research & Consulting. Field work was conducted in November 2016. The margin of error for the sample is estimated to be +/- 9.65%

[2] The Trust Barometer began as a survey of 1,300 people in five countries in 2001, and has grown into a truly global measurement of trust across the world. Now in its 17th year, the Edelman surveys more than 33,000 respondents across 28 countries

MAINTAINING TRUST

How organizations treat and protect data is now part of a company's brand promise and risk profile. According to a recent study by the Privacy Commissioner of Canada (*2016 Survey of Canadians on Privacy,* December 2016), "Most Canadians (85%) feel a greater reluctance to share their personal information with organizations in light of recent news reporting of sensitive information, such as private photos or banking information, being lost, stolen or made public."

The good news, is that senior leaders are engaged. Of the cyber leaders we surveyed, eight in 10 agree that senior leaders in their organization consider privacy and protection of personal information a corporate priority, and agree that senior leaders in their organization understand the importance of data security and privacy to maintaining trust in an organization's brand.

However, not all information and technology officers believe their organizations demonstrate the appropriate level of concern with managing their exposure to this risk. Almost two thirds of the people we spoke to believed their organization should be significantly more concerned (33%), or were unsure if their organization were concerned enough (31%)

Although the loss of sensitive or personally identifiable information and disruption of business are organizations' most concerning outcomes of a data security breach, organizations underestimate the cost of possible outcomes of data breaches.

- Reputational damage does not fall into the top concerns of a data breach for one in three (33%) organizations in Canada.
- The threat of legal action does not fall into the top concerns of a data breach for almost one in two (47%) organizations in Canada.
- The loss of stakeholder trust does not fall into the top concerns of a data breach for one in two (50%) organizations in Canada.

As security incidents become increasingly common, now more than ever it's critical for companies across all industries to develop a solidified plan to mitigate these issues. Companies have both an ethical and legal responsibility to safeguard stakeholders from this risk, and data security must move from the backroom to the boardroom. There are a few critical actions that senior leaders must take to mitigate the effects of a data security incident:

- The board and c-suite must be confident that the organization fully understands the risks and has developed proper mitigation protocols;
- Leadership must be confident that key tenants of preparedness – from coordination and planning to testing and readiness – are in place and effective; and,
- Leadership must foster a culture of transparency about how and why an organization collects, stores or processes data. Privacy is more than just a policy on a piece of paper.

THE CHANGING LEGAL LANDSCAPE

Even though almost half (46%) of security, information, and technology officers we surveyed said their organization has had at least one security breach that resulted in lost, compromised, or exposed personally identifiable information, levels of reporting under voluntary federal or mandatory provincial programs are low.

Only one in three (35%) said their organization had reported a cyber security event or breach to the Provincial Privacy Commissioner under existing mandatory notification laws. And only one in three (36%) security, information and technology officers said their organization has reported a cyber security event or breach to the Federal Privacy Commissioner under the existing voluntary notification program.

The Digital Privacy Act (Bill S-4) was passed into Law on June 19, 2015. The Act amends and modernizes the *Personal Information Protection and Electronic Documents Act,* which established rules for how private sector companies collect, use or disclose personal information.

The Act will arm the Privacy Commissioner of Canada with increased enforcement power, and outlines mandatory breach notification requirements for the private sector. The obligation to notify (expected to be outlined in 2017), and the threat of punitive fines, will likely result in an increase in the number of breaches that are publicly reported

BEST PRACTICES IN PREPAREDNESS

Even the most sophisticated IT security department cannot prevent a cyber-attack or the loss of sensitive corporate information. Organizations must be prepared to respond, as a well-executed response strategy can not only minimize the operational impacts and harm inflicted, but safeguard the organization from legal liability or reputation damage.

Most of the security, information, and technology officers we spoke to indicated that their organizations have response plans for dealing with a sudden and/or unforeseen cyber security incident, however, one in three say those plans are outdated.

Most companies we spoke to had developed a breach response plan or a crisis communications plan that addresses cyber risk, however, a significant number were not aware if their response plans addressed how their company would maintain or rebuild customer trust following a data security or privacy incident. In addition, a quarter of those companies (23%) have not tested their plans – an essential component of a preparedness program that provides breach response teams with the skills and ways of thinking that transform the crisis from an unnatural crisis environment into more familiar terrain.

Data security and privacy events often require specialized expertise to assist with the response. For example, external legal counsel is integral to protecting the confidentiality of the investigation and the deliberative process of anticipating and addressing litigation risk. From a reputation management perspective, forensic and security experts are essential to avoid the perception of bias in the investigation, and specialized communications counsel can help an organization maintain consumer trust and assist with risk reduction for impacted stakeholders. Despite respondents' high levels of confidence that they are prepared, three in 10 security, information and technology officers indicate their organization hasn't identified the necessary experts to assist with major security incidents.

Based on our experience helping companies manage live data security incidents of all kinds, involving millions of records, and helping several others prepare for a major security incident, Edelman has identified best practices for preparing for and responding to a data security or privacy issue. It boils down to three main principles:

1. Planning
   Having the right response plan with a clear focus on data breach and other security risks is essential to effectively managing a significant incident. The plan should identify the team and clarify roles, outline communications protocols and triggers, include a directory of key external stakeholders, and outline strategies for maintaining trust.

2. Testing and Readiness
   Organizations that have practiced their response in a live event or a mock simulation and subsequently updated their plans tend to perform better. If an organization has not been field tested, yearly simulations should be conducted to test the team's ability to execute, and to ensure the reliability and accuracy of the plan.

3. Communications Integration
   Data security and privacy incidents typically require companies to integrate across departments that may not usually work together, and require specialized third-party expertise. Identifying and contracting legal, forensic and communications experts, and establishing integration points ahead of time is a key factor for success.

Despite the heightened attention of policymakers and regulators, efforts of governments to combat cyber-crime, and high-profile arrests in Canada and across the world, the threat shows no signs of abating. Rather, cybercriminals have become more sophisticated, finding new ways to monetize corporate data and to hold companies ransom. As data security incidents continue to impact companies in Canada and around the world, being prepared to effectively communicate at a moment's notice is more important than ever.

THE EDELMAN CANADA DSP TEAM

Edelman is a leading global communications marketing firm that partners with many of the world's largest and emerging businesses and organizations, helping them evolve, promote and protect their brands and reputations.

Edelman's Data Security & Privacy and Crisis & Risk Team is headquartered in Toronto and spread across Canada - enabling senior leadership on our team to be on-site within hours of learning of a cyber incident. Our dedicated team has years of experience helping companies prepare for and manage the most complex reputation challenges.

With access to a Global network of Edelman Data Security and Privacy experts, we operate on a hub-and-spoke model, scaling activities effectively, efficiently and in the best interests of and outcomes for our clients. Edelman assembles tightly integrated teams that balance our deep experience with data security and privacy and crisis and issues management, enabling us to provide Canadian clients with the very best and most relevant counsel, strategy and executives for any data security or privacy issue.

CANADIAN DATA SECURITY AND PRIVACY GOVERNANCE STUDY

Edelman's Insights & Analytics team surveyed 101 Information, Data, Security and Technology Officers across Canada, including:
49 Officers (e.g. CEO, CFO, CTO, CIO, CMO, CPO, CLO)

- 16 Vice Presidents or equivalents
- 9 Board members
- 27 Directors / Members of Senior Management.

Respondents answering the survey included representatives from a number of different industries, including Professional, scientific and technical services (28), Finance and insurance (12), Manufacturing (9), Management of companies and enterprises (8), Construction(7), Transportation and warehousing (7), Retail trade (6), Information and cultural industries (6), Administrative and support (6), Educational services (5), Health care and social assistance (5), Arts, entertainment and recreation (5), Mining, quarrying, and oil and gas extraction (4), Utilities (4), Accommodation and food services (4), Public administration (4), Real estate and rental and leasing (3), Wholesale trade (2), Waste management and remediation services (2), and agriculture, forestry, fishing and hunting (1).

CONTACT US

GREG VANIER
DATA SECURITY AND PRIVACY LEAD
EDELMAN CANADA
GREG.VANIER@EDELMAN.COM