PUBLICATION

Cybersecurity and COVID-19: Is your Data Secure?

Austin S. Paladeau
Saptarshi (Rishi) Chakraborty

March 12, 2020

The outbreak of 2019 novel coronavirus disease (COVID-19) has rapidly spread to many countries throughout the world, including Canada. This has resulted in major disruption to business across the country. Many companies have activated their crisis management/business continuity plans, including full or partial shut-down of operations. And with increasing number of employees working from home, major news outlets such as the BBC and the US Department of Homeland Security are now reporting a significant uptick in email scams linked to COVID-19. Security experts note that this is the worst they have seen in years. We remind businesses that their IT systems may be particularly vulnerable to a cyber-attack.

What to do if your data security may have been compromised:

Step 1

Contain the Breach

Key Items to Consider

- Assemble your breach management team immediately and appoint an appropriate individual to lead the initial investigation
- Consider who needs to be made aware of the incident internally, and potentially externally
- Do not destroy valuable evidence that may help in determining the cause of the breach

Personnel Involved

Senior management, board members, operations and IT (internal/external)

Step 2

Evaluate the risks

Key Items to Consider

- Determine what type of data was compromised
- Assess the cause and extent of the breach and identify which individuals were affected
- Consider the extent of the harm that is foreseeable from the breach

Personnel Involved

Senior management, board members, operations, IT (internal/external), legal, communications and insurance provider

---

Step 3

Notification of the Breach

This is a requirement mandated under privacy laws in Alberta (and similar federal laws if it applies to the business)

Key Items to Consider

- Conduct a through legal/business assessment if the breach needs to be notified to the privacy commissioner(s), individuals and other stakeholders

Personnel Involved and Commentary

Personnel Involved: senior management, board members, operations, IT, legal and communications

Threshold for notification: Real risk of significant harm (may include bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property)

Timing: Without unreasonable delay. Breaches are typically reported within a week from the date of the breach. However, in light of profound effect of Covid-19 on businesses, we anticipate Alberta's Privacy Commissioner may grant businesses some additional time and latitude to report breaches.

Content of the Report: In writing and as mandated by law

Penalties: There are prescribed penalties under privacy laws for failure to notify the privacy commissioner, individuals and other stakeholders.

In addition, businesses may be exposed to private civil suits for damages, class action law suits and reputation hardships that may result due to non-compliance.

Step 4

Prevent the Breach

Key Items to Consider

- Look at the root cause of the breach and ensure that steps are taken to prevent it from occurring again.
- Consider the following: a audit of both physical and technical security; review of internal policies and procedures and any changes required; and a review of employee training practices and service delivery partners (i.e. dealers, retailers, outsourced work, etc.)

Personnel Involved

Senior management, board members, operations, IT (internal/external), legal and insurance providers

---

In addition, note that sector-specific laws and regulations exist that impose additional obligations for businesses that typically carry higher information security risks, such as those in financial services (IIROC dealers and MFDA members), health care, and telecommunications. Publicly traded companies must disclose material business risks, which can include cybersecurity issues and data breach or other cyber incident details.

Please note that this article does not constitute legal advice. It's intended to identify basic issues, and is not meant to be interpreted with specific application to a specific factual scenario. Should your organization have questions, or should you require more information, please contact Rishi Chakraborty.