KPMG

Audit Point of View

Preparing for new data breach reporting laws

Data breach disclosure legislation is changing. Are you prepared?

As data breaches continue to impact Canadian organizations—increasingly resulting in reputational and financial damage—the federal government plans to strengthen laws to enhance transparency around data privacy and security. It's expected that at some point in 2017 new mandatory data breach reporting legislation will require Canadian organizations to record all data breaches and publicly disclose them to any affected individuals at real risk of significant harm, as well as to the Office of the Privacy Commissioner.

Historically, Canada has lagged behind other countries in mandatory data breach reporting. While specifics vary (required notification times can range), other countries such as the U.S. have already instituted rules requiring organizations to inform individuals whose details have been compromised, as well as regulators. With Canada now on-board, the cost of breaches is expected to rise as organizations take on increased responsibilities surrounding identifying and locating the victims and determining how to best notify them (online, text messages, mail, phone, etc.).

What does the impending new legislation mean?

For one thing, notification will be at the top of audit committee (AC) and board agendas. They will need to take a close look at what is really required. Only breaches that the organization concludes have a real risk of significant harm will need to be disclosed. To avoid unnecessarily disclosing a breach, ACs should proactively:

- Establish a definition of what a "real risk of significant harm" means or the factors that should be considered when making this determination
- Contact a third party or lawyer experienced in disclosure and breach matters to verify that the definition criteria used to qualify breaches is aligned with industry good practices and relevant data breach related litigation cases
- Identify which person or team internally should determine if a breach meets a real risk of significant harm
- Update incident response processes as appropriate to ensure:
    - All incidents are raised to the appropriate person or team to make the qualification on if it meets a significant risk of harm
    - Communication experts assist in drafting pre-defined notification messaging to victims
    - There is capacity to manage client inquiries after breach notification is sent

Questions ACs should ask around data breach response preparation

There are a number of questions ACs can ask either internally or by working with a service provider to assess what steps they need to take to prepare for the legislation in a timely and effective manner:

Do we have an incident response process?

Do we test the process regularly?

Based on that process, have we defined what "real risk of material harm" means?

© 2017 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.
The KPMG name and logo are registered trademarks or trademarks of KPMG International.

How is the notification threshold triggered (for example, by having policy-based qualifiers, or a process where senior executives decide)?

Have we determined what information is important enough—in terms of regulatory and commercial protection requirements—to require notification?

What security controls are in place across the organization and can they provide a cyber-defensible position to limit impact in the event of a breach?

Have we ensured that any gaps identified as a result of a breach will get fixed?

It is important to address the breach legislation now

ACs' oversight role includes ensuring the organization takes appropriate steps to be prepared in the event of a cyber-attack. Going forward, establishing and demonstrating a strong cyber-defensible position will be key to reducing reputational and legal risks associated with the new mandatory data breach reporting legislation. The exact timing of the legislation is unclear, but it is expected to be imminent. Organizations need to be proactive now – to understand the legislation and clarify how they plan to respond when and hopefully before it arrives, as the fundamental changes they will be required to make may be time-consuming.

Contact us

Yassir Bellout
Partner, Advisory Services,
Cyber Security
T: 514-840-2546
E: ybellout@kpmg.ca

© 2017 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.
The KPMG name and logo are registered trademarks or trademarks of KPMG International.