NOV. 1, 2018 – D-DAY FOR COMPLETING PRIVACY BREACH PREPAREDNESS

By George S Takach

If you or your organization has been procrastinating on implementing best practices data breach policies and procedures, you have an action forcing deadline coming up – November 1, 2018. That`s the date the new federal rules on data breach reporting come into effect in Canada. It`s an important milestone, and you need to be ready.

A brief recap of the legislative history is in order. PIPEDA, the federal data privacy/protection law, has been in effect since 2004. It contains a fairly comprehensive regime of what organizations need to do if they wish to collect, store, use and share personal information of customers, employees and others. In June, 2015 the *Digital Privacy Act* added several provisions to PIPEDA, including requiring organizations who have experienced certain types of data breaches to notify the Office of the Privacy Commissioner (OPC), and the individuals affected by the breach. The enactment of these breach notification provisions, however, were postponed, to allow Canadian organizations to get ready for them.

In September, 2017, the draft regulations for the data breach notification regime were published. And then recently, in March, 2018, the Order-In-Council was published that provides that on November 1, 2018, the data breach notification sections of the DPA will come into force. Presumably prior to Nov. 1, 2018, the final version of the Regulations will be enacted as well.

Assessing the Data Breach

What the new law means, is that from and after November 1, 2018, if you experience a breach of security safeguards involving personal information, and if this breach creates a real risk of significant harm to an individual, then a strict procedure will have to be followed by your organization. First, you and your technical/forensics team will have to determine if the security breach creates a real risk of significant harm in respect of any personal information you hold. Therefore, you will have to undertake a risk assessment – what exactly happened; what data sets were penetrated; what can be done with this data; do you know anything about the data perpetrators and their behavior on prior hacks; etc.

This activity sounds simple, but it can be quite challenging. The initial job is simply to find out what went on. In the data breach litigation defence work that we have been involved with to-date, it turns out this initial step can be difficult. The forensic data scientists have to be called in. And if the hackers have done a good job of covering their tracks, it can be fiendishly difficult just figuring out what went down, by whom, and when.

Once you get your arms around the issue of “what happened”, you have to wrestle with what can often be a tougher query: what was the harm done by the breach, and what potential harm remains ? This is of critical importance, because under the new law, only breaches that pose a real risk of significant harm have to be notified by the company collecting the data. Moreover, the government in the Regulations, has decided not to give statutory guidance on this all important question of what constitutes “significant harm”.

We do have some guidance from the OPC, however. The following questions may be asked: how sensitive is the private information ? So, for example, is the information in question medical information, or financial payment information, or certain government information, such

as a social insurance number ? And what is the likelihood that the information that was hacked will be abused ?

Who to Notify – What to Say ?

If you conclude there is a significant harm from the data breach, then you will have to notify both the OPC, and the affected individuals. With respect to the former, here is what you`ll have to cover in your notice: what caused the security breach, and the circumstances surrounding the breach; the timeline for the breach; the particular types of personal information that were accessed as part of the breach; some figures surrounding the number of individuals impacted by the breach, and the degree of a real risk of significant harm to them; the measures you are taking to limit the risk of harm, or to at least mitigate the harm to the impacted individuals; and how you propose to notify the individuals impacted. You also need to provide the name of your primary contact person who will likely end up liaising with the federal Privacy Commissioner's office.

As for notifying the individuals whose personal information has been compromised, here is what you have to mention in that notice: describe the circumstances of the security breach; when (the specific day) or the period of time the breach occurred; describe the personal information that has been compromised; the measures you are taking to reduce the risk of harm, or to mitigate the damages, to the impacted individual data subjects; the measures those individuals could take to reduce the likelihood of harm befalling them; communication co-ordinates (email address; 1-800 number, etc.) by which impacted individuals can call you for additional guidance and information about the breach event; and the ability of the individual to bring a complaint about your organization to the OPC under PIPEDA. In effect, the overall nature and quality of this notice to impacted individuals is to allow them to comprehend the importance of the security breach and to help them diminish the likelihood of harm befalling them.

Keeping Records

The new rules on data breach notification require you to keep records of each data breach, including those that do not trigger the notifications discussed above. This record-keeping obligation is not a trivial responsibility. The information that you keep must allow the OPC to be able to confirm that you have done everything you were supposed to do under the breach notification rules – that is, the OPC has to be able to get comfortable, from the paper and electronic trail that you keep, that you notified to the OPC and relevant individuals as required. While seemingly a simple task, it is actually quite challenging in the real world. And finally, you have to keep these records for 24 months from the date you discovered the data breach.

As you navigate through the new record keeping requirements, you should remain mindful of privilege issues related to the data breach. It is important, therefore, how you structure the relationship with your outside legal counsel, as well as how the non-legal managers in your organization conduct their communications with your in-house legal colleagues. Just because you have a new statutory record keeping obligation doesn't mean you should be waiving privilege where it is appropriate to maintain it.

An Up-To-Date Data Breach Policy

Once you have reviewed the issues discussed above, and determined what needs to be done in your organization under the new data breach notification rules, it is important that you update your written data breach policy accordingly. And, if you don`t yet have a formal, written data

breach policy, now is a great time to prepare one; and I suggest you not put off this initiative any longer, given that the firm date for compliance – Nov. 1, 2018 – is fast approaching.

There are a number of important items that should be covered by the data breach policy. It should be clear, for example, who is on the data breach response team. And as for external legal counsel, your relevant insurance policy may well provide that you can only use a law firm pre-approved by the insurance company – so this is the sort of planning matter you want pre-approved and ready to go, because when the data breach occurs, time will certainly be of the essence. And in this light, don't forget to test your data breach plan – if you haven't tested it in six months, assume you don't really have a plan!

Cyber Risk Insurance Review

While you are considering what updates and fine tunings you need to make to your data breach policy, you should also review your organization`s insurance coverage from the perspective of the specific threats posed to you by data breaches and industry standard data security. This is generally called assessing "cyber risk". And if your organization does not have a cyber risk insurance policy, now is certainly the time to consider what your options are in this regard. The insurance market has made great strides in the past half dozen years in coming to market with various offerings in this space. While you should be careful not to be over insured, it certainly is a bad idea to be under insured.

It is important, in this regard, to understand thoroughly your "first party liability" – that is, what costs, expenses and damages could come to roost on your shoulders. But you also need to comprehend the "third party" liabilities issues as well – what damages would impact your customers, or partners in your supply chain, if you were compromised.

Essentially, if you acquired a cyber risk policy several years ago, now is an optimal time for reviewing that coverage with your insurance broker. Just in the last couple of years some new products have come to market, and at different price points than previously was the case. Particularly if you are in the midst of updating your data breach policy, you will be in a good position to understand your up-to-date risk profile, and to articulate what changes make sense to your cyber risk insurance coverage.