Responsibility For Security Breaches: Towards a Workable Standard[1]

Mark S. Hayes
Blake, Cassels & Graydon LLP, Toronto

1. Abstract

The primary function of personal information privacy legislation is the setting of standards of behaviour for organizations that use personal information. One of the core standards that most modern privacy statutes set is the level of security that must be applied to the storage of personal information in the care of the organization. Most Canadian privacy statutes have set that security standard in general terms by requiring that "reasonable" security be used. However, a number of privacy decisions, in particular those of the Privacy Commissioner of Canada, have adopted a standard that in practical terms appears to be one of strict liability. Using such a *post hoc* standard to assess the culpability of organizations is inappropriate and could lead to incorrect decisions being made by organizations about the appropriate level of security to apply to personal information.

2. Introduction

Privacy has been described as "the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others."[2] In fact, most of the regulatory thrust of private sector personal information privacy legislation in Canada has concentrated on regulating organizations that collect, use or disclose personal information, on the theory that restricting the personal information use of those organizations will provide greater control to individuals.

In general, Canadian private sector personal information privacy statutes impose several categories of restrictions on organizations, all of which are subject to some levels of qualifications and exceptions:

- a prohibition on the collection, use and disclosure of personal information without consent;

---

1 This article was prepared for presentation at the7th Annual Privacy and Security Workshop & 15th CACR Information Security Workshop in Toronto on November 3, 2006 and is intended to be a general review of law and should not be considered to be legal advice or to create a solicitor-client relationship between the author and/or Blake, Cassels & Graydon LLP and any reader. If you wish further information about any of the topics discussed in this article, please consult a lawyer. Any opinions expressed in this article are solely those of the author and do not necessarily represent the position of Blake, Cassels & Graydon LLP or any of its clients.

2 Westin, *Privacy and Freedom* (1970), at p. 7, cited in *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, at para. 67.

- a prohibition on any collection, use and disclosure of personal information that is not reasonable;

- an obligation to provide an individual with access to their personal information in the possession or control of the organization; and

- a variety of "administrative" requirements, including obligations to have policies, responsible privacy officials and to keep personal information secure.

The security obligation contained in all of these private sector personal information privacy statutes is critical to the efficacy of the other obligations. It matters little if an organization abides by all of the other privacy obligations but then makes an individual's personal information susceptible to unauthorized access by other individuals or organizations who often are not as constrained to obey the law. In this way, the security obligation in privacy laws can be seen as fundamental to the entire concept of providing individuals with choice about how their personal information is to be collected, used and disclosed.

While each of the Canadian private sector personal information privacy statutes provides some standard that must be met by organizations, these standards are by necessity rather general and vague. In most cases, organizations are required to use "appropriate" or "reasonable" security measures to ensure that personal information is protected against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. In all cases, it appears that the standards to be applied are intended to be objective; in other words, an organization is not to be judged by whether its security measures are ultimately effective in each case, but by whether those measures could reasonably have been expected to be effective in view of the information and means available to the organization at the time that the measures were implemented.

The application of such security standards by privacy commissioners and the courts has an important impact on the effectiveness of privacy regulation in Canada. The way in which the flexible security requirements of Canadian private sector privacy laws are interpreted sends important signals to market participants about what type of security measures an organization should invest in if it wants to be compliant with privacy laws. This requires a delicate balancing act. On the one hand, if security standards are set too low, organizations may not have enough incentive to invest in measures that are necessary, although one could argue that the embarrassment and adverse publicity associated with privacy breaches would likely outweigh the costs associated with an adverse finding by a privacy commissioner. On the other hand, if standards are set so high as to be unreasonable, then organizations may well decide not to investigate or invest in reasonable security measures on the theory that "nothing is good enough".

This paper examines how the issue of reasonable security measures has been approached in the decisions that have thus far been published on this topic, and whether it appears that the proper balance has been struck.

3. PIPEDA

The federal government introduced the *Personal Information Protection And Electronic Documents Act* ("PIPEDA") in 2000, and it first came into force on January 1, 2001. It was fully expected that all of the provinces would introduce their own private sector privacy legislation soon after PIPEDA was announced. However, in order to ensure that there would be uniform privacy rules across Canada in the event that such laws were not in fact passed by all provinces, and to act as something of an incentive to the provinces, PIPEDA provides that, after a three year moratorium (which ended on January 1, 2004), PIPEDA would apply to all provinces in which "substantially similar" legislation was not passed.[3] Somewhat surprisingly, only two provinces (British Columbia and Alberta)[4] responded to the federal government's invitation and introduced such legislation by the beginning of 2004.[5] PIPEDA is therefore applicable to private sector personal information use in all provinces except Quebec, British Columbia and Alberta.

The security requirements in PIPEDA are quite general in scope. Organizations must employ security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. The nature of the reasonable safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection.[6] The methods of protection required to be employed should include physical measures (locked filing cabinets and restricted access to offices), organizational measures (security clearances and limiting access on a "need-to-know" basis) and technological measures (passwords and encryption).[7]

The fact that Principle 4.7 provides for a range of methods and that they must be "appropriate" suggests that the organization's compliance must be assessed on the basis of an objective assessment of the reasonableness of the methods used, rather than whether a breach in fact occurred. Such a test has not been consistently applied by the Privacy Commissioner of Canada to date, however. While there have been a number of cases where the Commissioner applied a negligence test in finding that the organization failed to proper secure personal information,[8] in other cases the organization was found to have

---

3 PIPEDA, s. 30(1).

4 Quebec had already had private sector personal information privacy legislation in place since 1994.

5 The cases under the B.C. and Alberta statutes are discussed in Section 4 below.

6 PIPEDA, Principle 4.7.

7 PIPEDA, Principle 4.7.3.

8 For example, PIPEDA Case Summary #335, Customer receives banking information of other clients, http://www.privcom.gc.ca/cf-dc/2006/335_20060627_e.asp; PIPEDA Case Summary

breached its security obligations even though there was no identifiable failure to provide adequate security:

- In Case Summary #52,[9] several participants in online contests run by an organization received telephone calls from a person or persons falsely claiming to represent the company. After an internal investigation, the organization could not determine how unauthorized persons had obtained personal information collected from contest entrants, but believed the computer database in which the information was stored might have been compromised. An inspection by an outside firm could not confirm how or even whether the database had been compromised. The Commissioner found a violation of Principle 4.7 based solely on the fact that there had been a security breach.

- In Case Summary #277,[10] an organization admitted that its sub-contractor had, on the organization's behalf, erroneously sent an e-mail message to 618 contest entrants that allowed all of their e-mail addresses to be viewed by the individuals who received the message. While the Commissioner was satisfied that the organization had a privacy policy in place, that there had never been a previous incident and that the sub-contractor had appropriate safeguards in place, the organization was still found to have violated Principle 4.7 because "it would appear that either the employee did not correctly use the software or it did not function properly".

- In Case Summary #289,[11] a complaint was made to the Commissioner after a laptop containing customer banking information was stolen from one of the bank's financial advisor's car. The complainant customer was concerned that his personal information had been compromised. Although the laptop was equipped with various security features, including password protection, and the bank's laptop security policy was PIPEDA-compliant, the Commissioner found that the bank was in breach of PIPEDA because the financial advisor had failed to keep personal information in her possession secure.

All of these cases seem to apply a strict liability standard to personal information security, a result that likely was not intended by the drafters of PIPEDA.

#344, Couple's safety deposit box opened in error, http://www.privcom.gc.ca/cf-dc/2006/344_20060717_e.asp

[9] PIPED Act Case Summary #52, Company accused of failing to safeguard information of online contest entrants, http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020613_e.asp

[10] PIPEDA Case Summary #277, Mass mailout results in disclosure of contest entrants e-mail addresses, http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040902_02_e.asp

[11] http://www.privcom.gc.ca/cf-dc/2005/289_050203_e.asp

However, it is clear that the Commissioner is not employing a strict liability standard in all cases. For example, in certain circumstances an organization will not be to blame for security breaches where the individual has not taken reasonable steps to protect their own personal information. In Case Summary #315,[12] an individual complained that she believed that her Internet account had been compromised. The ISP responded to her enquiries by suggesting that she change her passwords and her challenge question, but she did not do so. The Commissioner noted:

> while organizations are responsible for protecting the personal information in their possession, there is some onus on the individual to protect his or her own personal information. The company cautions users to choose a challenge question no one else can guess. Indeed, in one of its e-mails to the complainant, it reminded her to ensure that her challenge question could only be answered by her. Asking what her mother's maiden name is was not information that likely only she knew.
>
> It was therefore difficult for the Assistant Commissioner to hold the company accountable, when the complainant had not taken the company's advice to fully protect her own personal information. The Assistant Commissioner deemed the company's measures reasonable and found that the company was not in contravention of Principle 4.7.[13]

At best, the decisions by the federal Privacy Commissioner are inconsistent and do not provide a coherent basis to judge the security measures taken by organizations. The approach in many of the reported case summaries appears to have been to make a finding of unreasonableness solely based on the fact that personal information was (or may have been) improperly disclosed.

4. Alberta and B.C. PIPA

As noted above, B.C. and Alberta were the only two provinces to respond to PIPEDA by enacting new private sector personal information privacy legislation. That legislation, in both provinces entitled the *Personal Information Protection Act*, came into effect on January 1, 2004.[14] B.C. and Alberta reportedly worked together very closely in developing their respective PIPAs, and the statutes are similar in style and content, although, as is inevitable, there were a number of differences in the statutes when they were introduced before their respective legislatures.

---

[12] PIPEDA Case Summary #315, Web-centred company's safeguards and handling of access request and privacy complaint questioned, http://www.privcom.gc.ca/cf-dc/2005/315_20050809_03_e.asp

[13] See also PIPED Act Case Summary #137, Telecommunications company accused of not protecting account against unauthorized access, http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030306_6_e.asp

[14] *Personal Information Protection Act*, S.B.C. 2003, c. 63 ("B.C. PIPA"); *Personal Information Protection Act*, S.A. 2003, c. P-6.5 ("Alberta PIPA").

PIPA requires an organization to protect personal information by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.[15] The reasonableness standard indicates that an organization should be judged based on the measures it takes to prevent data security breaches, not whether those measures are ultimately successful.

Some early decisions seemed to indicate that decisions under PIPA might follow the same pattern as was exhibited by the federal Privacy Commissioner under PIPEDA. Retailers were involved in a series of investigation reports[16] by the Alberta Commissioner in respect of personal information discovered in the possession of criminals by the Edmonton Police during a fraud investigation. In each of *Linens 'N Things*,[17] *Nor-Don Collection Network Inc.*[18] and *Digital Communications Group Inc.*,[19] the Commissioner appeared to apply a number of different standards in determining whether the organizations in question had in fact taken proper precautions to protect the personal information that had been acquired by unauthorized third parties.

In *Linens 'N Things*, the complainant's credit card had been used by a third party after being obtained in an unknown manner from a Linens 'N Things return receipt. While the Commissioner was not able to determine exactly how the information had been obtained by the criminals (the two theories that were discussed was that the information had been stolen or that it had been inadvertently discarded into the trash), he found that Linens N' Things "did not properly secure their records as they moved through their life cycle" and offices and blue bins were not properly locked. As a result, even though there was no direct evidence as to how the information was disclosed, the Commissioner concluded "that the organization failed to properly dispose of sensitive customer information by permitting them to be placed in a garbage bin without being securely shredded".

In *Nor-Don*, the police recovered some of Nor-Don's records which listed debtors' names and the amount of their respective debts. There appear to be no evidence that this information had in fact been used for criminal purposes. Nor-Don had in the timeframe in question been conducting a drawn-out move of its business premises, and the evidence before the Commissioner was that security over the vacated premises, which continued to house some of Nor-Don's records, was not very good. Even though the disclosure of the records found by the police could not be tied directly to any of the security failures listed

---

15 Alberta PIPA, s. 34; B.C. PIPA, s. 34.

16 An Investigation Report is not a full decision by the Commissioner, which is only issued after an inquiry pursuant to s. 50 of Alberta PIPA. Both the Alberta and B.C. Commissioners commonly issue Investigation Reports to provide details of issues that have come before them but have not resulted in an inquiry.

17 Alberta Investigation #P2005-IR-001, http://www.oipc.ab.ca/ims/client/upload/P2005_IR_001.pdf

18 Alberta Investigation #P2005-IR-002, http://www.oipc.ab.ca/ims/client/upload/P2005_IR_002.pdf

19 Alberta Investigation #P2005-IR-003, http://www.oipc.ab.ca/ims/client/upload/P2005_IR_003.pdf

by the Commissioner, he concluded that Nor-Don "contravened section 34 of PIPA by failing to make reasonable arrangements to protect personal information in its custody."

In *Digital Communications*, the police recovered a number of cell phone contracts, some of which related to individual subscribers and contained personal information. It appeared that there had been a number of previous incidents in which cell phone contracts from the same company had been found by the police in the hands of unauthorized persons. While Digital Communications disputed the number of times that this had occurred, it admitted that some of its security practices prior to the summer of 2004 were not sufficient and it had undertaken, after consulting with the police, to implement a number of specific improvements. It was not clear from the report by the Alberta Commissioner whether all of these security improvements had been implemented by October 2004, the date of the cell phone contracts that were located by the police. The Commissioner's conclusion was as follows:

> Despite the new measures implemented in 2004 customer information that had been in the custody of [Digital Communications] was found in the hands of criminal suspects. This investigation, along with information provided by [the police] and [Digital Communications], suggests that the records recovered by [the police] were either improperly disposed of or (as is suggested by the condition of the records) taken by an employee.

It may be that this conclusion was justified by the circumstantial evidence relating to the previous breaches and evidence that Digital Communications had not made a sincere effort to improve its security, but this is unclear as the Commissioner did not identify any specific security measure that Digital Communications failed to take and that could have caused the security breach. The danger for tribunals assessing the adequacy of security measures, however, is the temptation to "work back" from the fact that a breach occurred to find fault based on whatever happened to lead to the unauthorized disclosure.[20]

A more sophisticated approach to data security breaches was taken by the B.C. Privacy Commissioner in Investigation Report F06-01[21] made under the B.C. public sector privacy legislation.[22] The facts in this case were straightforward. An individual had purchased a number of computer tapes at a B.C. government auction. Upon reviewing them, the purchaser discovered that they "containing extensive and sensitive personal

---

[20] In April, 2006, the Alberta Commissioner issued Investigation Report P2006-IR-003, http://www.oipc.ab.ca/ims/client/upload/Investigation%20Report%20P2006_IR_003.pdf, which dealt with a similar issue. In that case, Monarch Beauty Supply clearly failed to properly dispose of documents containing personal information when they were placed into an unsecured dumpster and the reasonableness issue did not arise in any substantial way.

[21] Investigation Report F06-01, Sale Of Provincial Government Computer Tapes Containing Personal Information, March 31, 2006, http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF06-01.pdf

[22] *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 ("B.C. FIPPA").

information of thousands of British Columbians". Rather than returning the tapes, he provided them to a Vancouver newspaper, which reported on the privacy breach.

The B.C. Commissioner approached the problem in several steps. First, he examined what "reasonableness" means in the context of the legislation:

> [49] By imposing a reasonableness standard in s. 30 [of B.C. FIPPA], the Legislature intended the adequacy of personal information security to be measured on an objective basis, not according to subjective preferences or opinions. Reasonableness is not measured by doing one's personal best. The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, "reasonable" does not mean perfect. Depending on the situation, however, what is "reasonable" may signify a very high level of rigour.
>
> [50] The reasonableness standard in s. 30 is also not technically or operationally prescriptive. It does not specify particular technologies or procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect personal information vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.

While noting that the sensitivity of the personal information in question will be a factor, the Commissioner put this factor into context by noting that "[i]nformation security measures are properly established through a methodical assessment of risk that assesses both the foreseeability of a privacy breach (intentional or accidental) occurring in the context of current threats to or weaknesses in existing information-security measures and the severity and extent of the foreseeable harm that could result from a privacy breach."[23] Because a breach involving sensitive information will almost always involve a significant risk of harm to the individual, such information requires more stringent security measures.

The Commissioner then noted other factors that would influence the decision as to the appropriate level of security to be applied to protect personal information, including the application of generally-accepted and proven security practices, the medium and format of the record (which will influence both the type of security measures that are available and the security threats that are foreseeable) and the cost of security measures when compared to the marginal improvement in security that might be realized by resorting to them.[24]

---

[23] *Ibid*, at para. 54.

[24] The cost factor was somewhat attenuated in this case because it was a public sector obligation. The impact of cost consideration is discussed further below in respect of subsequent Alberta cases.

The Commissioner also discussed whether public sector entities should be responsible if the security breach was caused by a third party's criminal acts. In an earlier case,[25] the Ontario Information and Privacy Commissioner had suggested that "criminal activity is not contemplated in the concept of 'reasonable measures.'" The B.C. Commissioner found that the possibility of criminal activity must always be taken into account in the formulation of reasonable security measures, although it was always possible that a determined criminal could circumvent otherwise reasonable security measures.[26]

Against this backdrop, the Commissioner then turned to the issue of whether there had been a breach of B.C. FIPPA. This required a two-stage analysis: had there been unauthorized access to personal information, and, if so, had there nevertheless been reasonable security measures in place? The Commissioner had no trouble deciding that, in the circumstances, both conditions had been satisfied,[27] although there seemed to be a lack of clarity about which facts were relevant to which of these issues. The Commissioner found that there were three factors in particular that pointed to the unreasonableness of the steps taken to protect the information in question:

- the personal information in question was very sensitive and extensive;
- there were relatively simple steps that could have been taken to ensure the safe and proper disposal of the personal information; and
- the predictability of risk of disorder at the time of the office move that proceeded the auction sale of the tapes.

The more nuanced approach of the B.C. Privacy Commissioner appears to have influenced the Alberta Commissioner in subsequent decisions. For example, in two decisions rendered in September 2006,[28] the Commissioner revisited the question of reasonable security arrangements and provided a more detailed and sophisticated analysis.

---

25 Privacy Complaint No. PC-020036-1 (July 18, 2003), [2003] O.I.P.C. No. 176, para. 38, http://www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&P_ID=14575&U_ID=0

26 *Supra*, note 21, at paras. 62-63.

27 *Ibid*, at paras. 69-72.

28 Report on an Investigation into Reasonable Safeguards and Retention of Personal Information in Custody of a Union, September 14, 2006, Alberta Regional Council of Carpenters, Investigation P2006-IR-004, ("*Carpenters*") http://www.oipc.ab.ca/ims/client/upload/Investigation%20Report%20P2006_IR_004.pdf and Report of an Investigation into the Security of Personal Information, September 26, 2006, MD Management Ltd., Investigation Report P2006-IR-005 ("*MD Management*"), http://www.oipc.ab.ca/ims/client/upload/ACFAB50.pdf

Carpenters initially involved a complaint by a union member that the union was storing personal information of its members in a database stored on a server operated by the union's international parent body located in Las Vegas, Nevada. The international aspect of the case became less important, however, when during the course of the investigation it was revealed that a trusted Canadian employee of the union had improperly accessed the personal information of union members by installing and configuring a file sharing program which circumvented the security of the systems and permitted a software download.

The Alberta Commissioner adopted the approach taken by the B.C. Commissioner in Investigation Report F06-01 and stated that "it is incorrect to assume that an employee's unauthorized use and disclosure of personal information is conclusive evidence of unreasonable security practices."[29] The Commissioner found that in view of the long service of the employee in question and his trusted position, the union could not have foreseen the privacy breach that occurred. After reviewing the security measures that were in place both locally and in Las Vegas, the Commissioner determined that, even though there had in fact been a security breach, the measures taken by the union were reasonable and complied with Alberta PIPA.

The analysis in *MD Management* was much more detailed and the implications of this report by the Alberta Commissioner more far-reaching. The facts are fairly straight-forward, and all too commonly encountered. MD Management offers financial products and services to Canadian doctors and their families. A senior employee of MD Management copied a spreadsheet file onto his company laptop in order to review the client list of the financial consultants reporting to him. The laptop was carried in a soft briefcase-style bag. While en route from one MD Management office to another, the employee made a stop at a store. While he was away from the vehicle, someone unzipped the back passenger-side window of the soft top and stole the bag containing the laptop. The information on the laptop included personal information of approximately 8,000 individuals, including the following data: name, age, month and year of birth (no day of birth), medical specialty, home address and phone and fax numbers, business address, phone and fax numbers, home and/or business email address, total financial assets with MD Management (in some cases) and a unique identifier number (in some cases). The laptop did not contain Social Insurance Numbers (SIN), day of birth, investment account numbers, credit card numbers or banking information. While there were security measures on the laptop, including access passwords, the data was not encrypted.

In determining the reasonableness of measures taken by MD Management, the Alberta Commissioner adopted most of the criteria used by the B.C. Commissioner in Investigation Report F06-01, including the foreseeability of the security risk, the likelihood of damage to the individuals in question, the seriousness of the potential harm, the cost of preventative measures and the relevant standards of practice.

---

[29] *Carpenters*, *supra*, note 28, at para. 28.

The Commissioner first noted that MD Management had a policy in place that forbid employees from leaving laptops unattended in vehicles. After finding that the risk of laptop theft was a foreseeable risk and it was obvious that such policies had not in the past prevented employees from leaving unattended laptops available for thieves, the Commissioner found that such a policy, while somewhat useful, was not in itself an effective security measure against laptop theft and had to be combined with other measures that did not rely on implementation by employees.

MD Management also had employee-independent security measures in place, including the operating system's log-on password. However, relying on statements made on the Microsoft web site,[30] the Commissioner found such passwords to be inadequate and a very weak form of protection. The Commissioner then noted that Microsoft recommends the encryption of data on laptops[31] and, after noting that encryption is included as one of the methods of securing data in PIPEDA,[32] the Commissioner stated that "encryption is included as a safeguard in federal law suggests that it was considered by the legislators as an established measure of protection." This last conclusion is somewhat suspect, since Principle 4.7.3 is a recommendation only (as a result of the use of the word "should") and clearly is not doing anything more than providing a menu of the various types of security measures that could be used in individual circumstances. In the result, while strongly recommending that personal information on laptops be encrypted, the Commissioner stopped short of stating that such encryption is required, and he concluded that "organizations may consider any number or combination of the security measures discussed other than encryption."[33]

In a recent decision,[34] the B.C. Commissioner used the criteria from Investigation Report F06-01 to find that the security measures used by a film production company were reasonable in the circumstances and satisfied B.C. PIPA.

---

30 www.microsoft.com/uk/businesscentral/newsletters/bulletins/laptop-security-advice-prevention-against-hacking.mspx

31 "Encryption is vital. Although it is a bit fiddly to set up at first, it means that if your laptop is nicked, there are virtually no consequences apart from an insurance claim."

32 Principle 4.7.3 of PIPEDA states as follows: "The methods of protection should include (a) physical measures, for example, locked filing cabinets and restricted access to offices; (b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and (c) technological measures, for example, the use of passwords and encryption." [emphasis added by Commissioner]

33 *MD Management*, *supra*, note 28, at para. 63.

34 Order P06-04, Twentieth Century Fox Film Corporation, October 26, 2006, http://www.oipc.bc.ca/PIPAOrders/2006/OrderP06-04.pdf

5. Conclusion

While some of the case summaries published by the federal Privacy Commissioner appear to have employed an inappropriate standard of liability, it appears that more detailed decisions by the B.C. and Alberta Commissioners have created an analytic framework that is likely to be adopted in future cases. The standard that is applied is a flexible one that examines a number of factors relating to the personal information in question, the harm that could result from unauthorized access to the information and the costs and availability of preventative measures. While such an analysis does not provide an exact blueprint for organizations to examine in order to determine their compliance with statutory standards, it will be a relief to organizations and their advisors to at least have a checklist of factors that should be considered in assessing security measures.

Going forward, it will be important for organizations and privacy regulators to work together to further refine the standards to be applied when there are security breaches. In particular, clarification will be required concerning such issues as: the role of third party security providers and the extent to which their efforts can be relied upon by organizations; the evaluation of security measures taken in other jurisdiction in which personal information is processed or stored; the assessment of physical security measures to protect information; and the role of notification in providing security protection for personal information after a breach.