Privacy Law Bulletin

Aird & Berlis LLP
Barristers and Solicitors

# Data Breaches – From Accidents to State Sponsored Attacks: Vulnerabilities and Strategic Plans

By Paige Backman*

## Context

Data breaches continue to grow and evolve. They have become a hot topic for the private sector, governments and international agencies. The ever-growing pervasiveness of new technologies, combined with the collection of real time highly sensitive data and the capacity to aggregate and synthesize such data, has created extremely valuable assets to target. Whether breaches occur as a result of an inadvertent act or because of a sophisticated and targeted network attack by foreign governments or their representatives, corporations suffer hundreds of millions to billions of dollars in damages, and millions of individuals have found themselves victims as a result.

A significant subset of data breaches involve privacy breaches. Different views of what a privacy breach is have been proposed through laws and scholars. For purposes of this article, we will assume that a privacy breach occurs when personal information is accessed, collected, used or disclosed in contravention of applicable privacy legislation, privacy policy or contract. "Personal information," which is defined differently in different statutes, is the cornerstone to most privacy laws. Personal information usually refers to information that is about an identifiable individual. Examples of personal information include information pertaining to an individual's home address, nationality or ethnic origin, colour, religion, age or marital status; education, health, employment or criminal history; personal identification numbers, such as those listed on a driver's licence or a bank account number; as well as sexual preference or political affiliation. Increasingly, we are also seeing highly sensitive biometric identifiers such as fingerprints, retinal scans and body imaging being used as identifiers in day-to-day activities.

A data breach or privacy breach may arise intentionally or inadvertently, but the effect may be equally devastating on its victims. Intentional breaches can consist of theft[1] or an abuse or manipulation of the technologies that are so often used to catalogue and protect information.[2] Hacking, which consists of breaching computer systems and electronic safeguards, is a serious problem, particularly due to the heavy reliance organizations place on computerized databases. Such intentional breaches are often vicious in nature and consist of a deliberate desire to access, collect, use or disclose an individual's personal information with a view of causing a disturbance or perpetrating a crime.

While deliberate, bad faith activities, such as hacking and theft, are serious crimes that cause risks to corporations and individuals whose information has been exposed, and are often profiled in media reports, human error or ignorance is often the cause of data breaches. Data breaches based on human error or ignorance typically arise in cases of careless practices, mistaken disclosures, or operational, technical or communication breakdowns.[3] The damages caused by inadvertent data breaches, though done without malice, can be just as serious as those breaches that occur intentionally.

1 In January 2007, a laptop computer containing the personal health information of approximately 3,000 patients at the Hospital for Sick Children was stolen from the car of a physician who had taken the laptop home to do data analysis. See discussion in Curtis Rush's "Sick Kids' laptop theft angers watchdog" (7 March 2007), online: *The Star* <http://www.thestar.com>.

2 In September 2008, an Agriculture and Agri-Food Canada (AAFC) IT system administrator discovered that two servers had been hacked and that approximately 60,000 personal data records of agricultural producers were exposed. See "Findings under the *Privacy Act*: Amateur hacks into Agriculture and Agri-Food Canada computers" (18 June 2010), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca>.

3 See "Johns Hopkins University e-mail attachment error exposed personal info" (22 October 2010), online: PHIprivacy.net <http://www.phiprivacy.net>. In this case, approximately 85 staff members at Johns Hopkins University received an email from the Applied Physics Laboratory's benefits office that contained an incorrect attachment, identifying names, Social Security numbers and birthdates on 692 dependents of the Lab's staff members.

Data breaches can expose businesses to staggering damages, such as those outlined below, and individuals to risks such as financial loss, loss of employment or business opportunity, physical risks to safety and identity theft. Financial loss and identity theft have been recognized as two of the most serious and fastest growing crimes in North America.

Whether an organization suffers an intentional or unintentional breach, and regardless of whether the disclosed personal information is used for the perpetuation of fraud or not, the organization is equally responsible for the data breach and for having contravened privacy and other applicable legislation. It is therefore important for organizations to be aware of their responsibilities regarding the handling of personal information and their obligations under applicable laws. One of the key elements of an organization's responsibilities includes implementing practices designed to prevent breaches from occurring and enabling the organization to respond in a quick, efficient and effective manner should a breach occur.

## Privacy Breaches – A Costly Affair

If *bona fides* aren't reason enough to implement best practices for the prevention of privacy breaches, then the economics certainly are. Data breaches can impact a business's bottom line in an exceptional and virus-like manner.

Businesses have to account for hard costs such as legislative fines and penalties, third-party compensation, customer compensation, loss of profits, shareholder litigation and legal defence costs. Businesses also have to account for soft costs such as loss of goodwill, bad publicity, affected turnover and customer loyalty. While the calculation of such costs is not evident – with soft costs being so difficult to quantify and economic losses being incurred over a period of years – the effect can be staggering.

Below are several examples of some high profile and costly data breaches: *JP Morgan Chase ("JPM")* – 2014. Hackers were able to identify and exploit a weakness in the bank's systems, compromising the accounts of 76 million households and 7 million small businesses. Specifically, it is alleged that the hackers found a JPM server that its security team had neglected to update with a simple and industry standard two-step authentication process. As a result, the hackers were able to use stolen employee credentials to enter JPM's network without having to enter a second one-time password normally required.[4] Despite initial concerns, JPM stated that there was no evidence that passwords and social security numbers had been compromised.[5] Nevertheless, after the breach, the bank promised to enhance its security measures at an increased cost of $250 million per year.[6]

*Target Corp ("Target")* – 2013. The credit card numbers of more than 40 million people and personal information of 70 million people were compromised as a result of malware installed on 40,000 credit card terminals at Target stores. The malware first attacked employees of a Target contractor through a phishing attack, eventually ending up on Target's credit card terminals and stealing information from the magnetic strips found on debit and credit cards as they were swiped.[7] In August 2014, Target estimated its net breach expenses at $146 million, including a year of free credit screening services for customers[8] and estimated probable losses for breach-related claims by payment card networks.[9] However, according to industry analysts, the breach could eventually cost Target more than $1 billion due to the roughly $1.4 billion to $2.2 billion in fraudulent charges on customer cards covered by banks, for which Target will likely bear some responsibility.[10] The cost estimates do not include the significant drop in sales and profits that followed the breach.[11]

*Sony Pictures Entertainment ("Sony Pictures")* – 2014. Hackers, suspected to be of North Korean origin, installed malware on Sony Pictures' network[12] and released personal information about employees and others (including Social Security numbers), emails between Sony Pictures executives, and multiple films that were previously unreleased. The specific malware used by the hackers acts as a backdoor, allowing access into the network, and provides the user the ability to take over the network and access any data saved within.[13] The attack has been suggested to originate at the behest of Kim Jong-un, who was reportedly upset about the release of a comedic movie called The Interview in which journalists work with the CIA to assassinate him. Sony's preliminary fiscal third-quarter financial results, released on February 4, 2015, stated that the hack has thus far cost $15 million due to investigation and remediation efforts.[14] However, experts in cybersecurity have estimated the cost of the attack could reach into the hundreds of millions.[15] Additionally, former employees of Sony Pictures have filed four lawsuits against it alleging negligence in securing its network and, in particular, sensitive employee information.[16]

4 Matthew Goldstein, Nicole Perlroth & Michael Corkery, "Neglected Server Provided Entry for JPMorgan Hackers" (22 December 2014), online: New York Times <http://dealbook.nytimes.com/>.

5 Robert Cordray, "Top 5 high-profile cyber security breaches that have affected millions" (18 December 2014), online: Itbusiness <http://www.itbusiness.ca>.

6 Alessandria Masi, "Accounts Compromised, Says New Report On Bank Hack" (2 October 2014), online: International Business Times <http://www.ibtimes.com>.

7 Robert Cordray, "Top 5 high-profile cyber security breaches that have affected millions" (18 December 2014), online: Itbusiness <http://www.itbusiness.ca>.

8 Rachel Adams, "Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop" (5 Aug 2014), online: New York Times <http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html?_r=0>.

9 Target Corp Quarterly Report (20 August 2014), online: Target Corp <http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&id=1959682>.

10 Tom Webb, "Analyst sees Target data breach costs topping $1 billion" (1 January 2014), online: Pioneer Press <http://www.twincities.com>; Robert Cordray, "Top 5 high-profile cyber security breaches that have affected millions" (18 December 2014), online: Itbusiness <http://www.itbusiness.ca>.

11 Tom Webb, "Analyst sees Target data breach costs topping $1 billion" (1 January 2014), online: Pioneer Press <http://www.twincities.com>.

12 Elyse Betters, "Sony Pictures hack: Here's everything we know about the massive attack so far" (5 February 2015), online: Pocket-lint <http://www.pocket-lint.com>.

13 Edgar Alvarez, "Sony Pictures hack: the whole story" (10 December 2014), online: Engadget <http://www.engadget.com/>.

14 Cecilia Kang, "Sony Pictures hack cost the movie studio at least $15 million" (4 February 2015), online: *Washington Post* <http://www.washingtonpost.com/>

15 Ibid.

16 Ralph Ellis, "Lawsuits say Sony Pictures should have expected security breach" (20 December 2014), online: CNN <http://www.cnn.com/>.

*Home Depot – 2014*. The credit and debit card numbers of more than 56 million people were stolen due to a data breach caused by infected point-of-sale systems in stores throughout the U.S. and Canada. As with Target, the hackers attacked employees of a third party associated with Home Depot to gain access to the network and then deploy malware.[17] The breach is said by security experts to be the largest theft ever of credit card information from a single company.[18] Thus far, Home Depot has stated that the breach has cost $62 million, including expenses for credit monitoring for customers, increased call center staffing, and legal services.[19] One estimate has the costs eventually reaching as high as $500 million.[20]

*Sony Online Entertainment Services – 2011*. Sony Pictures' recent hacking scandal is not the first time Sony has suffered a privacy breach. In April 2011, hackers attacked the PlayStation Network, Sony Online Entertainment and Qriocity – respectively, Sony's gaming console network, online multiplayer game network and video streaming service. One security expert testified to the U.S. Congress that Sony was using outdated software on its networks and did not have a firewall installed prior to the attack.[21] As a result of the breach, personal data found in 102 million user accounts was compromised, including login credentials, names, addresses, phone numbers and email addresses.[22] Additionally, approximately 24,000 users in Europe had their credit card data stolen.[23] In May 2011, Sony estimated its costs associated with the breach to be $171 million, excluding legal settlements.[24] In 2014, Sony settled a class action lawsuit arising from the breach for approximately $15 million, along with $2.75 million in legal fees.[25] One analyst estimated the total cost of the breach, including lost sales, at $1.25 billion.[26] As of the date of this article, Sony was still battling through the courts in an effort to get its insurers to cover some of the damages suffered.

*Heartland Payment Systems ("Heartland") – 2009*. Said to be the largest data breach in history to date, Heartland's security compromise allowed hackers to break into the payment processor's networks and steal over 130 million credit and debit card numbers. It is alleged that the hackers first attacked Heartland's corporate network, which used old coding that was vulnerable to a fairly simple attack known as SQL Injection. Using their access to the corporate network to enter the separate payment processing network, the hackers installed malware to steal credit and debit card numbers.[27] In May 2010, Heartland's breach expenses were estimated at $140 million, including settlement payments of nearly $60 million with Visa and $3.5 million with American Express, as well as $26 million in legal fees.[28] Heartland has since come to an arrangement with MasterCard whereby Heartland agreed to pay MasterCard issuers $41.4 million to settle claims over the data breach.[29] Heartland is still dealing with the aftermath of this breach, the total costs of which are still uncertain.

*Bank of New York Mellon ("BNY Mellon") – 2008*. The personal information of more than 12.5 million people was compromised as a result of BNY Mellon's loss of six to 10 unencrypted tapes containing Social Security numbers, names, addresses and birth dates.[30] A year later, BNY Mellon reached a settlement agreement with the Connecticut Department of Consumer Protection and the Connecticut Department of Banking, agreeing to provide an additional year of creditor monitoring to the individuals who were notified and to reimburse any individuals who had funds stolen from their accounts as a direct result of the breach. In addition, BNY Mellon agreed to pay $150,000 to the State of Connecticut General fund.[31]

*TJX Companies ("TJX") – 2007*. TJX suffered a considerable breach resulting in the theft of 94 million customers' credit and debit card numbers.[32] Hackers first decoded the data streaming through the air at a single TJX store in Minnesota by breaching the store's weak and outdated wireless network. This helped the hackers steal usernames from TJX employees and use them to collect transaction data.[33] The company lost $17 million and 3 cents per share by the end of its first quarter alone.[34] Although original estimates placed the damages at $4.5 billion,[35] the actual costs of the breach suffered are approximately $1.6 billion.[36] The company is said to have spent more than $20 million investigating the incident, notifying customers and hiring lawyers to deal with the dozens of associated lawsuits.[37] To date, TJX has entered into a number of settlement agreements, notably

17 "The Home Depot Reports Findings in Payment Data Breach Investigation" (6 November 2014), online: Home Depot <https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf>.

18 Robert Cordray, "Top 5 high-profile cyber security breaches that have affected millions" (18 December 2014), online: Itbusiness <http://www.itbusiness.ca>.

19 Ed Roberts, "Home Depot Data Breach Costs Rise To $500 Mil." (23 September 2014) online: Ct Financial News <http://ctfinancialnews.com>.

20 Ibid.

21 Matthew Lynley, "Security expert: Sony used outdated software before Playstation Network breach" (5 May 2011), online: <http://venturebeat.com/>.

22 Robert Cordray, "Top 5 high-profile cyber security breaches that have affected millions" (18 December 2014), online: Itbusiness <http://www.itbusiness.ca>.

23 Ibid.

24 Statement from Sony (23 May 2011), online: Sony <http://www.sony.net/SonyInfo/IR/financial/fr/20110523script.pdf>.

25 Mike Futter, "[Update] Court Approves Sony Settlement In 2011 PSN Data Breach Case" (24 July 2014), online: Gameinformer <http://www.gameinformer.com>.

26 Juro Osawa, "As Sony Counts Hacking Costs, Analysts See Billion-Dollar Repair Bill" (9 May 2011), online: *Wall Street Journal* <http://www.wsj.com/>.

27 Julia S. Cheney, "Heartland Payment Systems: Lessons Learned from a Data Breach" (January 2010), online: Federal Reserve Bank of Philadelphia <http://www.phil.frb.org/>.

28 Jaikumar Vijayan, "Heartland breach expenses pegged at $140M –so far" (10 May 2010), online: Computerworld <http://www.computerworld.com>.

29 "Heartland settles with MasterCard over data breach" (20 May 2010), online: InfoSecurity <http://www.infosecurity-us.com>.

30 Jonathan Stempel, "Bank of NY Mellon data breach now affects 12.5 mln" (28 August 2008), online: Reuters <http://www.reuters.com>.

31 Connecticut Department of Banking, "News Release: Department of Consumer Protection and Department of Banking Announce Settlement with Bank of New York Mellon for 2008 Data Breach" (3 February 2008), online: State of Connecticut <http://www.ct.gov>.

32 Robert Cordray, "Top 5 high-profile cyber security breaches that have affected millions" (18 December 2014), online: Itbusiness <http://www.itbusiness.ca>.

33 Joseph Pereira, "How Credit-Card Data Went Out Wireless Door" (4 May 2007), online: Wall Street Journal <http://www.wsj.com/>.

34 Sharon Guadin, "T.J. Maxx Breach Costs Hit $17 Million" (17 May 2007), online: InformationWeek <http://www.informationweek.com>.

35 Ibid.

36 Joseph Gacinga, "Will Target's Information Security Breach Play Out Like That of The TJX Companies?" (26 December 2013), online: The Motley Fool <http://www.fool.com/investing/general/2013/12/26/will-targets-information-security-breach-play-ou-2.aspx>.

37 Ki Mae Heussner, "10 of the Top Data Breaches of the Decade" (14 June 2010), online: ABC News <http://abcnews.go.com>.

with MasterCard International Inc. ($24 million),[38] Visa ($40.9 million),[39] several banks, namely AmeriFirst Bank, HarborOne Credit Union, SELCO Community Credit Union, and Trustco Bank ($525,000),[40] 41 different U.S. States for legislative breaches ($9.75 million total),[41] and the individual victims of the breaches themselves (where TJX offered vouchers, cheques, reimbursement, insurance and legal fees, depending on the individual circumstances).[42] While these settlement amounts are impressive and provide a hint as to the ultimate cost suffered by TJX, they do not reflect the internal costs incurred by TJX in rectifying the breach, which are likely substantial.

## Data Breaches and Law Firms

If you think law firms are exempt, think again. The British Security Service (MI-5) and the Federal Bureau of Investigation (FBI) have each assessed law firms as a significant target for malicious hacking and data breaches. Governments, financial sectors and other core industries see law firms as significant targets and points of vulnerability because law firms maintain sensitive and confidential information pertaining to company secrets, business strategies, inventions, trade secrets, military weapons systems and contract negotiations[43]. MI-5 and the FBI have each alerted law firms to data breaches and have ongoing discussions with the law firms in their jurisdictions about security risks and cyberattacks. Mary Galligan, then head of the FBI's cyber division in New York City has said, "As financial institutions in New York City and the world become stronger, a hacker can hit a law firm and it's a much, much easier quarry."

The financial services industry has long been held as a key target for cyberattacks. The Financial Services - Information Sharing and Analysis Centre out of the United States, the top level group in the financial services sector and a leader in the war against cyberattacks, confirmed it is now collaborating with a few representative law firms. Eric Guerrino, the executive vice president of operations at the FS-ISAC, has been quoted as saying it is important for the financial services industry to work with law firms "because many of these law firms are custodians of sensitive confidential information pertaining to financial firms' intellectual property, mergers and acquisition deals within the sector and personally identifiable information for member's clients and customers".[44] FS-ISAC is expanding its talks to include representatives of the International Legal Technology Association, an association of approximately 2,000 law firms. An example of a state sponsored cyberattack against law firms on Canadian soil is set out below.

*Bay Street law firms and Canadian government – 2010*. Seven of Canada's leading law firms and the federal Finance Department and Treasury Board were hacked by foreign hackers in connection with a bid for Potash Corp. The hackers appear to have been hunting exclusively for information on a bid to buy Potash Corp., with some theorizing that the hackers were backed by the Chinese government, which was reportedly against the takeover bid.[45] China's state-owned chemicals and fertilizer group, Sinochem Group, is thought to have considered its own bid for Potash Corp. out of fear that the other bidder would control the global supply for potash if successful.[46] The hackers used a technique known as "spear-phishing" wherein victims are tricked into opening attached documents that contain a malware program.[47] Opening the attachment activates the malware which is usually programmed to steal data from the machine or take control of it.[48] The hackers sent employees at each target organization a series of emails purporting to be from senior federal officials or firms involved in the Potash Corp. deal, tricking the victims to open malware attachments in later emails.[49] Additionally, the hackers posed as federal government officials and sent emails to departmental technical staffers, conning them into providing key passwords unlocking access to government networks. This technique is known as "social engineering."[50]

The above cases are some of the higher profile and economically significant instances of data breaches. However, these cases also demonstrate the different types of hard and soft costs all organizations risk suffering in the wake of privacy breaches. What these numbers do not generally do is measure the internal costs of rectifying such breaches, nor the loss of goodwill that has undoubtedly been suffered by these organizations.

Globally, the average organizational cost of a data breach is $3.5 million, while the average cost per compromised record is $145. It is relevant to note, however, that the average cost per record compromised due to a malicious or criminal attack, which is the most common cause of a breach, is $159. On the other hand, the average cost per record compromised due to a system glitch or human error is $126 and $117, respectively. These statistics come from a 2014 report, sponsored by PGP Corporation, that analyzes the cost of data breaches in 10 countries, including the United States, United Kingdom, Germany,

38 "TJX, MasterCard settle" (3 April 2008), *The Globe and Mail*, online: Thomson Reuters, 2008 WLNR 6236375.

39 Linda McGlasson, "TJX, Visa Agree to $40.9 Million Payout for Data Breach" (4 December 2007), online: Bank Information Security <http://www.bankinfosecurity.com>.

40 Jaikumar Vijayan, "TJX agrees to settle another breach lawsuit for $525,000" (3 September 2009), online: Computerworld <http://www.computerworld.com>.

41 Mitch Lipka, "T.J. Maxx owner pays $9.75 million, settles with 41 states over massive data breaches" (23 July 2009) online: WalletPop <http://www.walletpop.com>.

42 Wendy Gross, "TJX Enters into Proposed Settlement Agreement of Customer Class Actions" (8 August 2008), online: McCarthy Tetrault <http://www.mccarthy.ca>.

43 Matthew Goldstein, "Wall St. and Law Firms Plan Cooperative Body to Bolster Online Security" (23 February 2015) online: *The New York Times*

44 Allison Grande, "Law Firms, Banks Join Forces to Tackle Cyberthreats", (24 February 2015), online, Law360.

45 Greg Weston, "Foreign hackers targeted Canadian firms" (29 November 2011), online: CBC <http://www.cbc.ca/>.

46 Jeff Gray, "Hackers linked to China sought Potash deal details: consultant" (30 November 2011), online: *The Globe and Mail* <http://www.theglobeandmail.com/>.

47 Greg Weston, "Foreign hackers targeted Canadian firms" (29 November 2011), online: CBC <http://www.cbc.ca/>.

48 Nestor Arellano, "How to not get phished like the Canadian government" (18 February 2011), online: Itbusiness <http://www.itbusiness.ca/>.

49 Greg Weston, "Foreign hackers targeted Canadian firms" (29 November 2011), online: CBC <http://www.cbc.ca/>.

50 Greg Weston, "Foreign hackers attack Canadian government" (16 February 2011), online: CBC <http://www.cbc.ca/>.

France, and Australia (all converted into U.S. dollars).[51] Of these 10 countries, the average organizational cost of a data breach was greatest in the United States, where the average data breach costs $5.85 million. Germany came in second at $4.74 million. France and the United Kingdom were third and fourth, with average costs at $4.19 million and $3.68 million, respectively. Brazil and India came in last with $1.61 million and $1.37 million, respectively.[52]

## Best Practices to Limit Data Breaches

The best defence is a good offence. To limit data breaches, organizations need to be proactive and aggressive, and build their data and privacy practices on four pillars. First, management needs to understand their organization's obligations under law and applicable standards. While this exercise may begin with an understanding of statutory and regulatory obligations, it does not end there. Organizations then need to take a look at their own policies, contracts with third parties and any industry standards to which the organizations are bound or to which they have voluntarily agreed to adhere.

Second, management needs to have a good understanding of their organization's information handling practices. This includes understanding the nature and source of information on intake, understanding how the organization uses, stores, transfers and discloses personal and non-personal but sensitive information, and, of course, how the organization renders anonymous, deletes or destroys information for which it no longer has any reasonable use.[53] Wireless and technology based security protections are key to develop and implement, particularly in today's digital age. Thefts or hacking may be impossible to prevent, given the technological advancements that are made every day. Nevertheless, the use of strong encryption programs, password protection and digital locks will prevent unauthorized access to data that is stored on such electronic systems. Encryption has become the standard for storing personal information and health information on portable devices[54] and practicing privacy breach prevention can be as simple as deleting a data cache or wiping a hard drive.[55]

Third, management needs to ensure their organization has a data security policy as well as a privacy policy (for internal and external distribution) that reflects the organization's personal information handling practices and, of course, compliance with laws and applicable standards.[56]

Fourth, once the policies are developed, management needs to implement the provisions of such policies. A key element of such implementation involves management ensuring its employees, officers, directors, consultants and third parties with whom such organizations do business understand and comply with the organization's policies. If employees, officers and directors are not properly educated, both with regard to obligations at law and the organization's particular policies, data breaches are virtually impossible to prevent. Once an organization ensures that its own personnel understands their obligations, the organization needs to ensure that each third party to whom such organization has disclosed, transferred or otherwise granted access to information is also aware of and complies with the organization's data policies.

Compliance obligations with third parties should be set out in written contractual terms to establish agreed upon standards and avoid misunderstanding. Contractual terms should address security obligations, restrictions on use and disclosure of the information, breach notification obligations as well as obligations to assist in investigating allegations of breaches and/or responding to inquiries and claims from individuals and government officials. To ensure such third party compliance with its obligations, the contract should include an audit in favour of the organization relating to the third party's practices.

## Destruction and Disposal of Personal Information

Once an organization has done its job and rationalized the information that it collects, uses and/or discloses, the organization will still need to ensure the information it does collect, use and/or store is returned, destroyed or deleted in an appropriate manner. Adequate destruction and disposal policies are a key element in the breach prevention equation.

Disposal and destruction policies and processes need to account for both physical destruction and technological elements to a file. Paper and hard copy records that contain personal or sensitive information should be shredded (ideally cross shredded), and their destruction should be systematically monitored and certified, even if it occurs off-site.[57] As for electronic files, unnecessary or unused sensitive data should be wiped, rendered unreadable and/or destroyed. This is particularly true if the organization intends to dispose of or donate its old computers, such that the computers

51 Ponemon Institute, LLC, "2014 Cost of Data Breach Study: Global Analysis" (May 2014), online: IBM <http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/>.

52 Ibid.

53 The corollary of this review has been that management then needs to rationalize such practices to ensure the least amount of personal information is collected, used and disclosed and, otherwise ensure compliance with laws.

54 Encryption, for example, has become the standard in Canada for storing personal or health information on portable devices. See, e.g., "Level of security on stolen laptops simply not acceptable, says Commissioner" (24 June 2009), online: Office of the Information and Privacy Commissioner of Alberta <http://www.oipc.ab.ca/Content_Files/Files/News/NR_AHS_Laptops_Jun_09.pdf> and "Hundreds of Ont. patient health files stolen: Privacy commissioner calls for more data security education" (4 August 2010), online: CBC News <http://www.cbc.ca>.

55 See, e.g., "How safe is your scan? Copy machines spill identity secrets" (19 October 2010), online: CBC News <http://www.cbc.ca>, where it is revealed that personal information that has been scanned into certain digital photocopier hard drives can be easily tapped, unless the units are wiped clean.

56 As laws relating to privacy are in relative infancy, and because technologies used to collect, store, transfer, process and steal personal information are always evolving, there may be circumstances when an organization may not know how to develop adequate privacy policies to ensure appropriate protection relating to the personal information in its care and for which it is responsible. In those circumstances, organizations should approach their legal departments and privacy or data commissioners.

57 When a traveller complained to the Office of the Privacy Commissioner of Canada after discovering a passenger manifest in a recycling bin at Toronto's train station, the Office of the Privacy Commissioner launched an investigation that showed that the information printed on the document could have allowed unauthorized access to personal information. The train company, VIA Rail, made immediate changes to its procedures for handling passenger manifests and directed all employees, as a result, to shred such documents before recycling them. See "Findings under the *Privacy Act*: VIA updates procedures after passenger finds manifest in recycling bin" (18 June 2010), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca>.

could find their way into the hands of a third party.[58]

## Responding to Data Breaches

Despite implementation of best practices and preventative measures, data breaches do still occur. Often, weaknesses in data protection do not come to the attention of an organization until after a breach has occurred. While such a breach may be the result of faulty business practices or operational break-downs, the organization should take key steps to immediately rectify any damage caused. The first 72 hours of the breach are crucial to its containment and to the containment of the potential harm or damages that may be suffered by third parties. If the organization does not act immediately and aggressively seek to contain and rectify the situation, the potential damages to individuals impacted by such breach becomes difficult to manage and the organization's ability to limit its liability as a result is severely compromised. As well, from a pure business perspective, getting out in front of a data breach with effected parties allows the organization to ensure it can control the message and limit the damage to its reputation.

The first elements of a data breach response are containment and assessment. Containment and assessment of the breach are essential to the mitigation of the organization's potential liability and damages, as well as to the suppression of adverse consequences felt by those individuals targeted by the breach. Containment need not be complicated, but should be immediate. Without immediate containment, the organization is permitting the breach to continue to occur and can widen the liability exposure of the organization. The organization needs to shut down the unauthorized practice, seek to recover the compromised records, if possible, and make changes to the system that was breached, such as a change to access codes or a system shutdown, so that a subsequent or ongoing breach is inhibited.[59]

The organization should coordinate an investigation to determine the scope of the breach and how the breach occurred. To do so, the organization should designate a responsible individual, if not a team of individuals, to administer the investigation. This investigation should commence concurrently with the shutdown process. If the breach is found to have resulted from a criminal activity, the organization should notify the police, as they too can play a crucial role in breach containment and the restoration of compromised data. Neglecting to notify police of a breach caused by criminal or potentially criminal activity can compromise the ability of an organization to investigate and mitigate the breach.[60]

Alongside the investigation, the organization needs to consider and scope the potential damage that may be caused by the breach. This assessment requires a review of which data elements have been compromised, the sensitivity of those elements, and the context in which that information might be manipulated or abused. Understanding the risks associated with the breach is a key element in focusing the breach response and in managing the risks to the individuals and the liability of the business.

## Breach Notification

After assessing the personal information involved, the cause and extent of the data breach, the individuals affected by the breach and any foreseeable harm from the breach, the organization should consider notifying any affected individuals, government regulators and the police. Many jurisdictions have mandatory breach notification requirements and an organization should be familiar with such requirements, as well as any obligations imposed on that organization by industry standards and/or contracts. While breach notification legislation is currently in its infancy in Canada,[61] many states within the United States have established breach notification legislative provisions, many of which carry significant costs for failure to notify and for multiple violations.[62]

Organizations are not often willing to notify individuals affected by a privacy breach. Notification can lead to heightened consumer response, media involvement and loss of goodwill. Organizations will usually want to avoid any negative publicity or public backlash unless they are compelled at law to do so. A choice not to notify is typically premised on the belief that consumers and/or media would not otherwise find out about the breach. In this age of instant communication, premising a business strategy on a belief that word of the breach will not get out is flawed and can be quite costly. Depending on the jurisdiction where the breach occurred and the jurisdiction where damages are suffered, organizations responsible for data breaches can risk facing serious lawsuits and substantial monetary penalties.

While breach notification will likely affect heightened inquiries and complaints from individuals and publicity, breach notification, if handled correctly, can be beneficial to an organization. Breach notification can be an important tool

58 See discussion on disposal of personal information and best practices at "Audit Report of the Privacy Commissioner of Canada: Personal Information Disposal Practices in Selected Federal Institutions, Section 37 of the *Privacy Act*, Final Report 2010" (2010), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca>.

59 "Key Steps for Organizations in Responding to Privacy Breaches" (28 August 2007), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca>.

60 See, e.g., PIPEDA Case Summary #2008-395: Commissioner initiates safeguards complaint against CIBC (25 September 2008), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca>. In this case, the Office of the Privacy Commissioner of Canada (OPC) had criticized one of Canada's largest banks, the Canadian Imperial Bank of Commerce (CIBC), for its mishandling of a privacy breach situation. The bank had shipped a disk drive with unencrypted personal information of more than 400,000 clients from Montreal, Quebec to Markham, Ontario. When the package had arrived in Ontario, the disk drive was missing. The OPC noted that the CIBC should not have waited 24 days before notifying the Montreal police of the breach.

61 The Leader of the Government in the Senate, the Honourable Claude Carignan, recently introduced new legislation in the Senate that would legislate a data breach notification requirement for private-sphere organizations. See Bill S-4, *An Act to amend the Personal Information Protection and Electronic Documents Act*, 2nd Sess, 40th Parl, 2013, cl 10 (first reading 8 April 2014).

62 See, e.g., section 445.72 of Michigan's *Identity Theft Protection Act*, 2004, Act 452 (available online: Michigan Legislature <http://www.legislature.mi.gov>), which provides that the aggregate liability of a person for civil fines for breach notification failures arising from the same security breach can cost up to $750,000.00.

in mitigating an organization's damages and can allow the organization, and not the press or privacy commissioners or regulators, to control the message being sent to the public.

Some argue that an organization which notifies individuals impacted by a data breach will limit its potential damages as a result of the breach. That belief is based on the premise that notification empowers those affected individuals to take action in mitigating any harm that otherwise would have been suffered by them. In turn, this mitigation of damages mitigates the organization's liability.

## Content of Breach Notification

The content and type of breach notification is not always legislated and may vary, depending on the type of breach and the individuals affected. Notifications may be direct or indirect. Direct communication is more personal, it addresses the specific personal information at issue for that individual, and as a result can be more effective. Unfortunately, direct communication is not always practical. Content of the notification will vary, as appropriate, and may include information about the incident, details on what the organization has done and will do to control or reduce the harm, information on how individuals can protect themselves and contact information should the individuals have any questions or concerns about the breach.[63] Notification content should also be considerate of whether or not a police investigation of the breach is ongoing, as disclosure of some information may not be sensible in certain circumstances.

## Canadian Privacy Laws and Breach Notification

To date, outside of Alberta and certain provincial health information legislation, Canada has not had clear breach notification requirements for businesses facing a breach of their privacy safeguards in respect of the personal information it holds. Though the Privacy Commissioners across the country had provided examples of "best practices" in such situations, the majority of businesses are not required by law to disclose a privacy breach.

Organizations in Alberta, to the extent subject to *Personal Information Protection Act (Alberta)*, must provide notice to Alberta's privacy commissioner, without unreasonable delay, of an incident involving the loss of, unauthorized access to, or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.[64] In addition, Alberta's privacy commissioner may require organizations to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure.[65]

Amendments have also been proposed to the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), as set forth in Bill S-4. Should Bill S-4 become law, PIPEDA would impose a breach notification level at which an organization must report to the Privacy Commissioner of Canada and notify individuals whose personal information has been compromised by the breach. As a result of section 10.1 of the proposed Bill S-4, an organization would have to inform the Privacy Commissioner of Canada and an individual of a breach of the privacy safeguards implemented by it if it is reasonable "to believe that the breach creates a real risk of significant harm to an individual." The provision sets forth a broad spectrum for the kind of harm that qualifies as "significant harm," including but not limited to humiliation, financial loss and identity theft. It also sets out factors to consider in evaluating the harmful nature of the breach to the individual, such as the sensitivity of the personal information involved in the breach and the probability that will be misused.

Under section 10.2 of the proposed Bill S-4, an organization that notifies an individual of a breach under section 10.1 must also notify any other organization or government institution it believes may be able to reduce the risk of or mitigate the harm from the breach.

## Post-Breach Management

Once an organization finishes managing the immediate consequences of the breach, it should take the information learned from the breach investigation and re-evaluate its policies and safeguards. It is not sufficient for an organization to mitigate breach consequences. Organizations must implement preventative practices, such as those noted above, to prevent future occurrences of privacy breaches.[66] In developing or updating its practices, an organization may wish to consider conducting a security audit of both physical and technical information handling practices; a review of policies and procedures; a review of employee training practices; and a review of partners, including consultants and other service providers.[67]

The resources expended by organizations in implementing best practices for the prevention of data breaches pales in comparison to the above statistics. One rising consideration in risk management is the purchase of data breach liability insurance. Policies may cover damages that arise out of unauthorized access to, collection of, and use or disclosure of information that results in harm to employees or third parties; defence expenses as a result of regulatory or criminal investigations; crisis management and notification expenses; and/or

63 "Key Steps for Organizations in Responding to Privacy Breaches" (28 August 2007), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca>.

64 Section 34.1 of the *Personal Information Protection Act*, S.A. 2003, c. P-6.5

65 Ibid, Section 37.1

66 A positive example of how to manage the after-effects of a privacy breach can be seen in the Canada Border Services Agency's handling of a recent privacy breach. The Agency had released a document to the public that had accidentally included a page containing personal information belonging to other individuals. Upon discovery of the breach, the Canada Border Services Agency pledged to review its procedures and to implement a manual quality assurance process of all information that it releases, such that similar data breaches do not occur in the future. See "Findings under the *Privacy Act*: Software glitch at border services agency triggers data breach" (18 June 2010), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca>.

67 "Key Steps for Organizations in Responding to Privacy Breaches" (28 August 2007), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca>.

network security liability.[68] While insurance policies may be costly, organizations may wish to pursue them as a protective measure against the otherwise exorbitant costs entailed in managing and mitigating a data breach.

While data security and privacy protection may not always be seen as a main priority, it is indisputable that the effects of a privacy breach can be devastating, both to the affected individuals as well as to the organizations involved. Data breaches not only undermine the affected individuals' confidence in the organization responsible for the breach, but also risk adversely influencing consumers' confidence in commercial markets generally. Data breaches risk discouraging consumerism and making individuals increasingly wary of where and how they transact. Organizations and business models are increasingly dependent on amassing significant amounts of personal information, globally, through electronic databases.

The global scope and reach of privacy and data breaches have considerable long-term effects on consumers' confidence in electronic commerce and business models and, consequently, on the global economy in general.

*Paige Backman is a partner in Aird & Berlis LLP's Corporate Group and Chair of the Privacy Industry Team. Acknowledgement and great appreciation is extended to Daanish Samadmoten, an articling student at Aird & Berlis LLP for his assistance with research for this paper and to Karen Levin, previously an associate at Aird & Berlis LLP, for her assistance with a prior version of this paper.*

68 Murn Meyrick, "Privacy Liability and Insurance", available online: Nymity <http://www.nymity.com/~/media/Whitepapers/ESRI%20Chapter%20on%20Privacy%20Insurance.ashx>.

For more information on privacy-related issues, please contact any member of the Aird & Berlis LLP Privacy Team, as listed below:

**Lawyers:**


| | | |
|---|---|---|
| Paige Backman | 416.865.7700 | pbackman@airdberlis.com |
| Meghan A. Cowan | 416.865.4722 | mcowan@airdberlis.com |
| Donald B. Johnston | 416.865.3072 | djohnston@airdberlis.com |
| Corrine Kennedy | 416.865.7709 | ckennedy@airdberlis.com |
| Aaron Baer | 416.865.4636 | abaer@airdberlis.com |


AIRD & BERLIS LLP
Barristers and Solicitors

Brookfield Place
181 Bay Street, Suite 1800
Toronto, Ontario, Canada
M5J 2T9
**T** 416.863.1500 **F** 416.863.1515
www.airdberlis.com