DW
Deeth Williams Wall

Helping Your Ideas Take Flight.

Data Breaches: What's an In-House Lawyer to do?

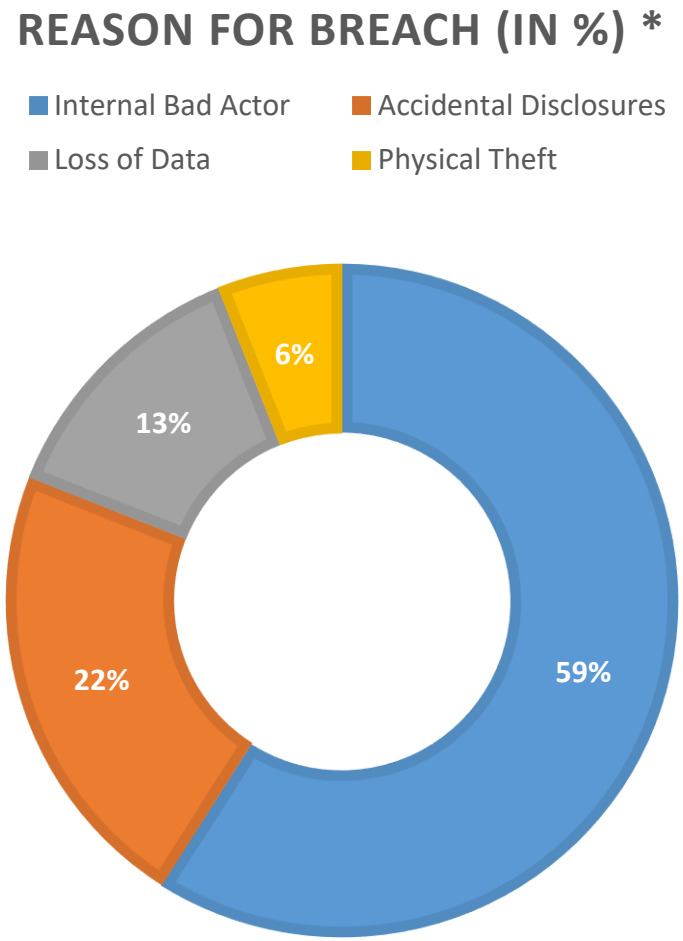
Amy-Lynne Williams, Richard Austin, Jennifer Davidson

September 19, 2019

Agenda

1. Introducing the Matter: How Data Breaches Impact Today's Organizations
2. Framing the Discussion: In-House Counsel's Role in Data Breaches
3. Essential Preparation for In-House Counsel
4. Learning Through Application: Data Breach Scenarios
5. Conclusion: Take-Home Message for In-House Counsel

Data Breach Statistics



- **Average total cost** of a data breach is USD 3.92 million
- Canada has the highest direct cost at **$81 per compromised record**
- Most expensive industry is **healthcare** at USD 6.45 million
- Average size of a data breach is **25,575 records** **

* https://www.ctvnews.ca/politics/19-million-canadians-have-had-their-data-breached-in- eight-months-1.4572535

** https://cutt.ly/nwPToMc

Statutory Obligations

Relevant Canadian Legislation

1. Personal Information Protection Act (PIPA)
   - PIPA AB
   - PIPA BC

2. Act Respecting Protection of Personal Information in Private Sector (ARPPI)
   - Quebec

3. Personal Health Information Protection Act (*PHIPA*)
   - Notification obligations for health information custodians
   - Notification obligations for agents

4. Office of the Superintendent of Financial Institutions (OSFI)
   - Data breach obligations for federally regulated financial institutions (FRFIs).

International Legislation that may apply

- California Consumer Privacy Act (CCPA)
- General Data Protection Regulation (GDPR)
- Data breach obligations for the United States of America

The Personal Information Protection and Electronic Documents Act (PIPEDA)

Applies to every organization in regards to personal information that:

- the organization collects, uses or discloses in the course of commercial activities
- s 4(1) PIPEDA

Does not apply to:

- any government institution to which the Privacy Act applies
- any individual in respect of personal information that the individual collects, uses, or discloses for personal or domestic purposes and not for any other purposes
- s 4(2) PIPEDA

PIPEDA: Notification Provisions

It is mandatory to notify if the parameters are met:

- The Privacy Commissioner of Canada
- Individuals
- Other organizations and Government Institutions

s 10.1(2): Notice should be given "as soon as feasible" after determining that a breach has taken place

PIPEDA: Record Keeping Provisions

- The organization must maintain a record of every breach for 2 years
- Records must include sufficient information for the Commissioner to verify that the organization is complying with its obligations under *PIPEDA*
- Minimum requirements:
  - the date or estimated date of the breach;
  - a general description of the circumstances of the breach;
  - the nature of the information involved in the breach; and
  - whether or not the breach was reported to the Commissioner or individuals affected by the breach

PIPEDA: Penalties for Contravening Obligations

The organization can be guilty of:

- an offence punishable on **summary conviction** and liable of a fine not exceeding $10,000; or

- an **indictable offence** and liable of a fine not exceeding $100,000

In-House Counsel’s Role in Data Breaches

Obligations of In-House Counsel

"[In-house counsel] are regarded by the law as in every respect in the same position as those who practice on their own account. The only difference is that they act for one client only, and not for several clients … They are subject to the same duties to their clients and to the court. They must respect the same confidences. They and their clients have the same privileges."

Crompton v Commissioners of Customs and Excise, [1972] 2 All ER 354 (QB), cited in *R v Campbell*, [1999] 1 SCR 565.

Rules of Professional Conduct

1. Competency

- Rule 3.1-2
  - … The quality of service required of a lawyer is service that is competent, timely, conscientious, diligent, efficient and civil.”
- Rule 3.1-1
  - “competent lawyer” means a lawyer who has and applies relevant knowledge, skills and attributes in a manner appropriate to each matter undertaken …
  - Commentary [15.1]: **“**The Law Society Act provides that a lawyer fails to meet standards of professional competence if there are deficiencies in… (c) the records, systems, or procedures of the lawyer's professional business…”

Rules of Professional Conduct

2. When the Client is an Organization

- Rule 3.2-3
  - "Notwithstanding that the instructions may be received from an officer, employee, agent, or representative, when a lawyer is employed or retained by an organization, including a corporation, in exercising his or her duties and in providing professional services, the lawyer shall act for the organization."

  - Commentary [1]: "… While the organization or corporation will act and give instructions through its officers, directors, employees, members, agents or representatives, the lawyer should ensure that it is the interests of the organization that are to be served and protected. …"

Rules of Professional Conduct

3. Duty of Honesty

- Rule 3.2-2
  - “When advising clients, a lawyer shall be honest and candid.”

- Rule 3.2-7
  - “A lawyer shall not

    (a) knowingly assist or encourage any dishonesty, fraud, crime, or illegal conduct… .”

Rules of Professional Conduct

- Rule 3.2-8
  - A lawyer who is employed or retained by an organization to act in a matter in which the lawyer knows that the organization has acted, is acting or intends to act dishonestly, fraudulently, criminally or illegally, shall do the following, in addition to their obligations under rule 3.2-7: …

    (c) if the organization, despite the lawyer's advice, continues with or intends to pursue the wrongful conduct, withdraw from acting in the matter in accordance with rules in Section 3.7.

  - Commentary [5]: "… In some but not all cases, withdrawal means resigning from their position or relationship with the organization and not simply withdrawing from acting in the particular matter."

  - Duty to report misconduct?
    - To the Law Society: Rule 7.1-3
    - To police and others: Rule 3.3-3. Commentary [5.1]

Rules of Professional Conduct

4. Employees, Unrepresented Persons and Contractors

- Rule 1.1-1
  - Definition of “client” includes a person “having consulted the lawyer, reasonably concludes that the lawyer has agreed to render legal services on their behalf”

- Rule 7.2-9
  - When a lawyer deals on a client's behalf with an unrepresented person, the lawyer shall: …

    (b) take care to see that the unrepresented person is not proceeding under the impression that their interests will be protected by the lawyer; and

    (c) take care to see that the unrepresented person understands that the lawyer is acting exclusively in the interests of the client and accordingly their comments may be partisan.

Rules of Professional Conduct

- Rule 7.2-8

  "A lawyer retained to act on a matter involving a corporation or organization that is represented by a legal practitioner shall not, without the legal practitioner's consent or unless otherwise authorized or required by law communicate, facilitate communication or deal with a person

  (a) who is a director, or officer, or another person who is authorized to act on behalf of the corporation or organization;

  (b) who is likely involved in decision-making for the corporation or organization or who provides advice in relation to the particular matter;

  (c) whose act or omission may be binding on or imputed to the corporation or organization for the purposes of its liability … "

- Commentary to Rule 7.2-8

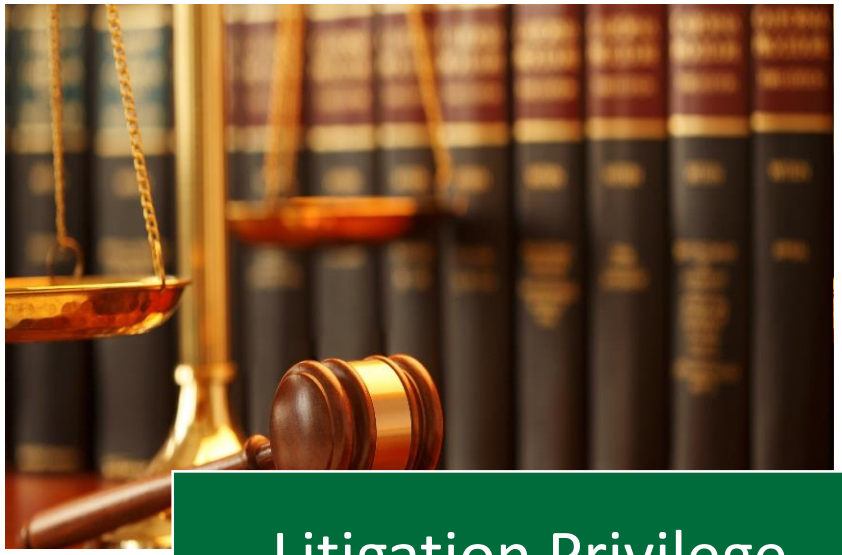
Privilege

- Sensitive documents could be the subject of legal disclosure obligations

- An organization must show that the circumstances surrounding the information makes it applicable to a privilege claim

Types of Privilege

Solicitor-Client Privilege



Litigation Privilege

Solicitor-Client Privilege / Legal Advice Privilege

- Based on the rationale that the relationship and communications between the solicitor and client are essential to the **effective operations of the legal system**

- Solicitor-client privilege **lasts forever** and can only be waived by the client

"If an in-house lawyer is conveying advice that would be characterized as privileged, the fact that he or she is 'in-house' does not remove the privilege, or change its nature."

Pritchard v Ontario (Human Rights Commission), [2004] 1 SCR 809 per Major J at paras 20 -21.

Litigation Privilege

- Protects communications between lawyer and client, communications between lawyer (or unrepresented litigant) and third parties as well as materials of a non-communicative nature
- Arises only in the context of litigation: purpose is to create a “zone of privacy” in relation to pending or apprehended litigation
- Comes to an end upon termination of the litigation (broadly defined)

Litigation Privilege

- To be qualified under litigation privilege, the communication's **"dominant purpose"** must have been its intended use in the litigation

- *Kennedy v McKenzie*, [2005] OJ No 2060 (SC) requirements:
  - In answer to inquiries made by an agent of the party's solicitor
  - At the request or suggestion of the party's solicitor
  - For the purpose of being laid before counsel to obtain legal advice
  - To enable counsel to prosecute an action or prepare or defend a brief

Role of Lawyer & Loss of Privilege

- Privilege can be lost when morphing from an advisory to an investigative role

- Courts scrutinize claims for solicitor-client privilege and litigation privilege during the fact finding phase of an investigation:
  - *Gainers Inc v Canadian Pacific Ltd.,* (1993) 8 Alta LR (3d) 399 (Alta QB)
  - *Slansky v Canada (Attorney General),* 2013 FCA 199, leave to appeal refused 2014 CanLII 5977 (SCC)
  - *Howard v London (City),* 2015 ONSC 156
  - *Kaplan v. Casino Rama Services,* 2018 ONSC 3545
  - *Re Experian Data Breach Litigation*, US District Court, Central District of California, Case Number 8:15-cv-01592 (class action settlement)

Prepare a strategy for maintaining litigation privilege

COUNSEL'S ROLE IN INVESTIGATIONS	REPORTS
Clarify the counsel is playing	Preferable for consultant/investigator to be retained by external counsel
If external counsel retained, provide written instructions	Retainer is to provide advice with respect to the data breach and any related litigation
Advise witnesses investigation is being conducted by counsel, as counsel and information kept confidential	Document that the consultant's report is to assist counsel and not for general business purposes
Keep legal advice in a separate file, mark it clearly and store it securely and separately	Instructions and communications with external counsel
Limit distribution of communications and instruct others to do the same	Report based on analysis of information preserved for disclosure
Re-assess role of in-house periodically, including as litigation becomes more likely	Report is delivered to external counsel, with disclosure limited to purpose consistent with litigation privilege

Essential Preparation for In-House Counsel

Essential Preparation for In-House Counsel:

1. • Assess current environment for compliance and agreements
2. • Prepare a playbook
3. • Configure and train a response team
4. • Educate employees and board
5. • Cyber-Insurance

Essential Preparation for In-House Counsel:

6. • Communications templates
7. • Reporting form
8. • Record retention strategy
9. • Tri-party agreements
10. • Mandatory immediate data breach reporting in agreements

Breach Scenarios

Scenario #1

A ransomware infection has hit servers hosting critical web applications. Attackers are demanding $300,000 USD for the decryption key. Searches through intelligence sources reveal no information about the attacker group. Little is known about them, but they have given your company 48 hours to pay the ransom or the files will be released. Work has been done to confirm the cause, mitigate the problem and verify that the servers can be restored within 24 hours.

Whether to Report the Attack

Ask:

- Was the information compromised by the breach?
- If unclear, did the breach result in a “real risk of significant harm” (RROSH)?

If no real risk of significant harm, no need to report it. However, must still keep a record.

** For reporting obligations, refer to PIPEDA and PIPA AB. Note that the organization may also need to report the breach to **OSFI.**

Whether to Notify the Police

Ask:

- Would notifying mitigate the risk of harm?
- Does the data breach have a criminal element?

Consider: loss of privilege, confidentiality, control issues

Should You Pay the Ransom

- Royal Canadian Mounted Police and Canadian Underwriter recommend that you not pay the ransom
- Head of the Canadian Centre for Cyber Security at the Communications Security Establishment said:
  - “The key action with paying a ransom is, you have **to measure that against**, 'How do I get my business back up and running.' And that's an individual decision for an organization to work out internally and with its insurance company”…
- Important to consider the role of when determining whether to pay the ransom.

Scenario #2: *Breach in the Supply Chain*

You work for a commercial shipping company (ABC Inc.). A third party supplier (XYZ Inc.) manages the organization's Customer Relationship Management (CRM) application. XYZ's systems were infected with a virus that may have allowed the release of ABC's customer information. ABC believes that this may have been the work of a bad actor at XYZ.

Dealing with the Supplier

- **"63%** of all data breaches are linked in some way to third parties such as contractors, suppliers, or vendors that have access to a business' system"*
- *PIPEDA*'s notification provisions apply even when an organization has given its data to a third party
- Walk in with a collaborative approach
- Supplier contracts

* Soha Systems Survey on Third Party Risk Management.
online: https://revisionlegal.com/data-breach/third-party-data-breaches/

Conclusion: Checklist for In-House Counsel

- ❑ Understand your obligations as in-house counsel
- ❑ Assess current environment
- ❑ Get cyber insurance
- ❑ Prepare the Playbook
- ❑ Develop a privilege strategy
- ❑ Find experienced legal counsel
- ❑ Set up a response team
- ❑ Run practice drills
- ❑ Educate yourself and others
- ❑ Update plan regularly
- ❑ Establish record keeping practices

Questions?

Amy-Lynne Williams
Partner
(416) 941-9047
awilliams@dww.com

Richard Austin
Partner
(416) 941-8210
raustin@dww.com

Jennifer Davidson
Associate
(416) 941-9607
jdavidson@dww.com