**Framework for Ethical Decision Making in Information Technology**

**A case study of Security Breach**

**(COMP 249-001 - Info Security, Privacy and Ethic)**

**By:**

Muhammad Taukirul Islam

Oluwabunmi Olanrewaju

Abimbola Adelegan

Jaden Gerolami

Contents

[Consider the scenario 3](#_Toc536388153)

[Deontological views of Ethics 4](#_Toc536388154)

[Step 1: Reporting the Breach 4](#_Toc536388155)

[Step 2: Containing the Breach 4](#_Toc536388156)

[Step 3: Evaluating the Risks Associated with the Breach 4](#_Toc536388157)

[Step 4: Notification 5](#_Toc536388158)

[Step 5: Record Keeping Requirements 6](#_Toc536388159)

[Teleological views of Ethics 7](#_Toc536388160)

[Brown University methodology 8](#_Toc536388161)

[Recognizing an Ethical Issue 8](#_Toc536388162)

[Consider the Parties Involved 8](#_Toc536388163)

[Gather all the Relevant Information 9](#_Toc536388164)

[Formulate Actions and Consider Alternatives by asking the following questions: 9](#_Toc536388165)

[Act 10](#_Toc536388166)

[Reflect on the Outcome 10](#_Toc536388167)

[Intended Consequences: 10](#_Toc536388168)

[Unintended Consequences: 10](#_Toc536388169)

[CIPS code of ethics 11](#_Toc536388170)

[The Four CIPS Imperatives 11](#_Toc536388171)

[Imperative #1: Protect the Public Interest and Privacy of Information 11](#_Toc536388172)

[Imperative #2: Avoid Conflicts of Interest 11](#_Toc536388173)

[Imperative #3: Take Professional Responsibility 11](#_Toc536388174)

[Imperative #4: Contribute to the IT Profession 11](#_Toc536388175)

[The CIPS Process of Ethical Decision-Making 11](#_Toc536388176)

[Case reflection 12](#_Toc536388177)

[Group Decision 13](#_Toc536388178)

[**References** 13](#_Toc536388179)

# Consider the scenario

Data-Time Inc. is a company which manages databases for a large city in Colorado. Included in these databases is information collected from the city’s homeless shelters and free clinics. Specifically, the databases contain personal information of the users of these services over the past 10 years; this includes people’s Social Security numbers and health records.

This data is highly secure and only accessible to the employees of Data-Time Inc. Employees are given a laptop when they are hired which allows them to access the database remotely. Unfortunately, one of these laptops is stolen and the security of the database is compromised.

A majority of the people whose information was compromised are homeless; therefore there is no easy way to contact them in order to alert them of the security breach. How should Data-Time Inc. manage this breach in security?

# Deontological views of Ethics

Deontological ethics also known as “duty-based” ethics, it states right action consists in following our duty, irrespective of the consequences. It is based on following a set of rules in order to carry out one duty.

The set of rules to be followed in this scenario will be Canada’s *Personal Information Protection and Electronic Documents Act* (“[PIPEDA](http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf)”) as it provides [regulations](http://gazette.gc.ca/rp-pr/p2/2018/2018-04-18/html/sor-dors64-eng.html) relating to mandatory reporting of privacy breaches in Canada.

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information. From the scenario, there was a privacy breach as security of the database was compromised through the stolen laptop. The following steps should be taken to handle the breach:

## Step 1: Reporting the Breach

* The employee with the stolen laptop should immediately inform his or her immediate supervisor and the information security unit / Privacy Officer of the company.

Once the breach has been confirmed, the privacy Officer will implement the remaining four steps of the breach incident protocol.

## Step 2: Containing the Breach

The Privacy Officer should take the following steps to limit the scope and effect of the breach:

* Work with units to immediately contain the breach by, for example, recovering the records or shutting down the system that was breached
* Notify the police if the breach involves, or may involve, any criminal activity.

## Step 3: Evaluating the Risks Associated with the Breach

The following factors will be among those considered in assessing the risks:

* **Personal Information Involved:**
  + What data elements have been breached? The more sensitive the data, the higher the risk. From the case study, Health information, social insurance numbers and financial information that could be used for identity theft are examples of sensitive personal information.
  + What possible use is there for the personal information? Can the information be used for fraudulent or otherwise harmful purposes?
* **Cause and Extent of the Breach:**
  + The cause of the breach (Stolen Laptop).
  + Is there a risk of ongoing or further exposure of the information?
  + What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?
  + Is the information encrypted or otherwise not readily accessible?
  + What steps have already been taken to minimize the harm?
* **Individuals Affected by the Breach:**
  + How many individuals are affected by the breach?
  + Who was affected by the breach homeless individuals and those that patronise the free clinics?
* **Foreseeable Harm from the Breach to the individuals**

Harm that may occur includes Security risk (e.g., physical safety), Identity theft or fraud, Loss of business or employment opportunities, negative effects on the credit record, Hurt, humiliation, damage to reputation or relationships or loss of property etc.

* **What harm could result to the Organisation:** Loss of trust in the organisation and litigation.

## Step 4: Notification

An organization must notify individuals of any breach of the security of safeguards involving their personal information if it is reasonable to believe that the breach creates a “real risk of significant harm.” Concurrently, the organization must also report to the Privacy Commissioner of Canada.

* **Notifying** **Affected Individuals**

1.      Notification to individuals can occur in person when they visit city’s homeless shelters and free clinics

2.      Telephone, mail, email.

3.      Indirect notification - website information or posted notices.

Contents of the notification should include:

* Description of the circumstances of the breach;
* The day or the period during which the breach occurred, or the approximate period;
* A description of the personal information subject to the breach
* A description of the steps taken by the organization to reduce or mitigate the risk of harm from the breach;
* A description of steps individuals can take to reduce the risk of harm that could result from the breach; and
* Contact information that the individual can use to obtain further information about the breach
* **Report to Commissioner**

The report to the Privacy Commissioner must be sent by any secure means of communications and contain the following:

* Description of the circumstances of the breach and the cause, if known;
* The day or the period during which the breach occurred, or the approximate period;
* A description of the personal information subject to the breach, if known;
* The number of individuals or approximate number of individuals affected;
* A description of the steps taken by the organization to reduce or mitigate the risk of harm to affected individuals;
* A description of the steps that the organization has taken or intends to take to notify affected individuals in accordance with PIPEDA; and
* The name and contact information of a person who can answer the Commissioner’s questions on behalf of the organization.

PIPEDA also require organizations to notify additional government institutions if the organization believes that the organization may be able to reduce or mitigate the risk of harm to the affected individuals by issuing the notification.

**Timing of Notifications**

Notification to impacted individuals and the Privacy Commissioner should occur as soon as feasible after the organization determines a breach has occurred.

## Step 5: Record Keeping Requirements

Most notably, PIPEDA will now require organizations to keep and maintain a record of every breach of security safeguards for twenty-four (24) months. What constitutes a record is subject to interpretation, however, the record must contain any information that enables the Privacy Commissioner to verify compliance with PIPEDA. On request, an organization must be prepared to provide the Privacy Commissioner with access to, or a copy of, a record.

# Teleological views of Ethics

Teleological ethics, (teleological from Greek *telos*, “end”; *logos*, “science”), theory of morality that derives duty or moral obligation from what is good or desirable as an end to be achieved.

* First, inform your supervisor or boss when you have noticed the stolen laptop. If possible, change password.

# Brown University methodology

According to Brown University, there are three frameworks for ethical decision making. They are;

**Consequentialist Framework**

This framework focuses on the future effects of the possible course of action, considering people who will be directly or indirectly affected.

**Duty Framework**

Focuses on the duties and obligations that we have in a given situation and consider what are the ethical obligations we have and what things we should never do.

**Virtue Framework**

This framework identifies the character traits (either positive or negative) that might motivate us in a given situation. We are concerned with what kind of person we should be and what our actions indicate about our character. We define ethical behavior as whatever a virtuous person would do in the situation, and we seek to develop similar virtues.

The management of Data-Time Inc. needs to apply the following processes on making ethical decisions for the case at hand:

## Recognizing an Ethical Issue

* How can we limit the impact of privacy breach?
* What impact will this theft have on affected individuals?
* How does this affect company reputation and brand?
* Is there a way to have prevented this exposure from occurring?
* Is there a way to forestall recurrence?

## Consider the Parties Involved

* Decision makers at Data-Time Inc.
* Data-Time IT department
* Privacy commissioner office
* E-Health Canada
* Police
* Management and employees of homeless shelters and free clinics.
* Homeless people involved (we assume Data-Time has back-up information on a server)
* Next of kin of homeless people
* Other individuals who are not homeless (these can be contacted directly)

## Gather all the Relevant Information

* Get contact details of those reachable
* Data-Time has information on affected citizens on other connected computers and server
* Can the stolen laptop be remotely programmed to self-destruct any stored information?
* Make a list of people involved

## Formulate Actions and Consider Alternatives by asking the following questions:

*Which action will produce the most good and do the least harm? (****The Utilitarian Approach****)*

* Put up signs at shelters and clinics about the possible breach
* Get the information out on local and social media

*Which action respects the rights of all who have a stake in the decision? (****The Rights Approach****)*

* Inform the Privacy Commissioners office and law enforcement
* Contact those who could be reached

*Which action treats people equally or proportionally? (****The Justice Approach****)*

* Public announcement
* Contact affected individuals and inform the next-of-kins of those we don’t have contact information on

*Which action serves the community as a whole, not just some members?* ***(The Common Good Approach)***

No single action serves the entire stakeholders. A collection of actions is involved, such as;

* Investigate the theft and build stronger data handling protocol
* Make sure computers containing such sensitive information are better-protected and secured onsite.

*Which action leads me to act as the sort of person I should be? (The Virtue Approach)*

* Report to appropriate authorities and don’t attempt a cover-up

**Make a Decision and Consider It**

After examining all of the potential actions, which best addresses the situation? How do I feel about my choice?

* The **Common group approach** may be the best in this situation, so that we can reduce the risk of future recurrence by domiciling such sensitive information to a secure onsite server.
* Cooperate with law enforcement agents to make sure the employee whose laptop was reported stolen had no malicious intent

## Act

Many ethical situations are uncomfortable because we can never have all of the information.  Even so, we must often act.

* Report to Police and Privacy Commission
* Revise remote access rights of employees
* Notify the public of the incident
* Adhere to recommendations of privacy office

## Reflect on the Outcome

What were the results of my decision?  What were the intended and unintended consequences? Would I change anything now that I have seen the consequences?

### Intended Consequences:

* People who potentially got their private information exposed are aware of the issue.
* Words will get out that the firm was involved in data security breach

### Unintended Consequences:

* Reputation damage
* Possible negative backlash from the public
* Cost of conducting damage control

# CIPS code of ethics

## The Four CIPS Imperatives

Distinguishing marks of a profession are its acceptance by the public, and the profession's acceptance of its responsibility to the public. The following statements are a set of high ideals to which all CIPS members aspire. CIPS members have an obligation to:

### Imperative #1: Protect the Public Interest and Privacy of Information

* Carry out work or study with primary regard for public interest (including health, security, safety, privacy, protection of the environment and social responsibility) and in accordance with regulatory requirements and legislation.
* Report to the relevant authority the breach in security such as Privacy Officer of the company and police

### Imperative #2: Avoid Conflicts of Interest

Act so the welfare of others takes precedence over personal interests and provide full disclosure to impairment of personal judgment.

### Imperative #3: Take Professional Responsibility

Serve their employer/clients competently, carry out their work with due diligence, maintain and advance their knowledge and exercise uncompromised professional judgment.

### Imperative #4: Contribute to the IT Profession

Respect the rights and professional aspirations of colleagues and uphold the integrity, dignity and image of the profession.

## The CIPS Process of Ethical Decision-Making

Members should take the following steps when making ethical decisions and resolving ethical dilemmas:

* Identify the key ethical issues in the situation: **Security Breach**
* Identify what ethical imperatives are relevant to the situation: **Imperative 1**
* Determine what standards of conduct are of major importance to the situation and begin to implement some possible actions by:
  + generating alternatives and examining the risks and benefits of each
  + securing additional information
  + consulting with colleagues, the CIPS Registrar, or with other appropriate sources
  + examining the probable outcomes of various courses of action
* Take a moment to reflect. (Include in the decision-making process the feelings and intuitions evoked by the ethical challenges. You might decide that you would feel uncomfortable with certain alternatives even if the action can be justified)
* Determine action plan
* Take action (follow a concrete action plan, evaluate the plan, and be prepared to correct any negative consequences that might occur from the action taken).  Such requests may be general in nature or may refer to a particular hypothetical or real situation or be submitted (in confidence) in writing to the Registrar’s Office of CIPS.

In addition, any CIPS member may request interpretation, clarification or amplification of any part of the Code of Ethics.

## Case reflection

The CIPS Methodology would result in additional steps that was not considered previously. The additional steps would include

* Identify the key ethical issues in the situation
* consulting with colleagues, the CIPS Registrar, or with other appropriate sources
* examining the probable outcomes of various courses of action
* Formulation of more concrete written action plan

So the following steps can be useful for Data-Time Inc to secure their data and privacy according to CIPS code of ethics

* **Conduct a Risk Assessment**

The risk assessment forces providers to review security policies, identify threats and uncover vulnerabilities within the system. Data-Time Inc. should conduct a routine maintenance and risk assessment including security patches, operating system upgrades etc.

* **Provide Continued Education to Employees**

Educate and re-educate employees on data security can significantly reduced data breaches, so Data-Time inc should arrange proper training for employees.

* **Monitor Devices and Records**

Remind employees to be watchful of electronic devices left unattended. More often than not data breaches occur due to theft of these items from a home, office or vehicle. While it is IT’s job to safeguard patient information, employees should be reminded to do their part in keeping data safe as well. Make sure to always lock your device whether it’s a laptop, desktop, or phone and password protect it.

* **Encrypt Data & Hardware**

Encryption technology is key in avoiding data breaches. so Data-Time Inc should encrypt their data on regular basis which can prevent data breaches.

* **Developing a secure way of accessing data remotely**

Data-Time Inc can develop a system so employees will be able to access data remotely from server instead of taking device outside the office which will be convenient for both employees as well as company.

Following these additional steps would result a more comprehensive solution to decide. By identifying the key ethical issues of the situation and consulting with colleagues, the CIPS Registrar, or with other appropriate sources would help to get additional insight into the matter. Examining the probable outcomes of action and preparing concrete written action plan would help Data-Time Inc to follow proper ethical procedure.

# Group Decision

What course of action would your group recommend in this case?

* The **Common group approach** may be the best in this situation, so that we can reduce the risk of future recurrence by domiciling such sensitive information to a secure onsite server.
* Cooperate with law enforcement agents to make sure the employee whose laptop was reported stolen had no malicious intent
* Remotely wipe the OS or contents of the stolen laptop so that whoever has access to the physical laptop cannot access the database
* Seek advice from CIPS or privacy office on how to go about resolving the breach

**References**

1. “Brown University.” *Decameron Web | Society*, Brown University, [www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions](http://www.brown.edu/academics/science-and-technology-studies/framework-making-ethical-decisions).
2. <https://www.cyberadviserblog.com/2018/09/mandatory-data-breach-notification-in-canada-understanding-your-new-obligations/>
3. <https://www.mun.ca/iap/privacy/Managing_a_Privacy_Breach0526.pdf>
4. <http://www.cips.ca/sites/default/files/CIPS%20Code%20of%20Ethics%20and%20Standards%20of%20Conduct%20-%20June%202018.pdf>
5. <https://www.britannica.com/topic/teleological-ethics>