by John Wunderlich

## Collect Only Necessary Information to Reduce the Risk

The life cycle of payroll/HR data from a privacy perspective begins with information coming into the organization. Privacy legislation is concerned with the collection, use and disclosure of personal information. Collecting unnecessary personal information increases privacy risk and should be avoided. By limiting collection to the minimum necessary information, you minimize the risk associated with that information through its life cycle in your organization.

Collection encompasses any means by which personally identifiable information comes into your organization's custody and control. When you ask an employee to complete new hire forms, you are collecting information. When you do a search on a social network about an employee (which is not a recommended practice outside of an investigation already under way for justified purposes, by the way), you are collecting personal information. When you record that an employee took a sick day in his or her file, you are collecting information.

Once you've collected the information, you are responsible for it. Having custody and control of personal information increases your risk exposure. Risks from a privacy breach include loss of reputation, loss of customers and remediation costs; a recent court decision in Ontario may also add civil damages to the list.

To manage the risk, you must decide what to do with each piece of information:

- **Eliminate** the risk by not collecting that information.
  - Not an option for information required for statutory remittances.
  - Not an option for the information required for initiating, maintaining or terminating the employment relationship.
- **Remediate** the risk by collecting the information but implementing controls to reduce the possibility of a privacy breach during use. Examples include:
  - Move the payroll printer to a secure area.
  - Distribute pay statements in sealed envelopes instead of stacks of printouts.
  - Train your payroll staff in privacy.
  - Outsource payroll to reduce exposure from internal staff.
  - Bring your payroll in house if you want more direct control.
- **Accept** the risk, collect the information and make no changes. If you have an experienced payroll department, this might be okay. Nonetheless, you should consider getting a third party validation (Privacy Impact Assessment) of your payroll department's privacy capabilities. At the very least, this validation enables you to provide assurances to your stakeholders.

By far the best risk strategy you can adopt is to minimize the amount of information that you collect about your employees. Sensitive information you don't have is not at risk. For the remainder of the information, there are risk management formulations to determine the level of risk.

At its most basic, the amount of risk equals the likelihood of a breach occurring in a given time period multiplied by the impact of that breach occurring.

> *Example:* Assume that the impact of losing an employee's pay statement is $100 in rework and lost time. Further, assume that an organization loses one pay statement for every 1,000. If that organization runs a monthly payroll for 250 people, then we can expect to lose three pay statements in an average year. This means that the annual loss expectancy is $300. This is very likely a risk that an organization could accept.

Unfortunately, in the real world, it is hard to assign impact so precisely. One way to formalize your risk perception risk is to categorize your information as low, medium or high risk based on a system that makes sense to you.

As an example, in the following table, I've identified five pieces of information and have assigned arbitrary numbers for low (1), medium (5) and high (9) risk in categories I invented for this exercise. "Changeability" indicates how often/easily the information can be changed. "Identifiability" indicates the utility of the information for identity theft or data linkage. "Sensitivity" indicates what people reveal through surveys and the like. These categories make sense to me as the key elements to evaluate in determining the impact of a privacy breach. While your categories and evaluations may differ, the methodology shown in this table will enable you to prioritize the impact and make risk management decisions.

| Data | Changeability | Identifiability | Sensitivity | Impact Level |
|---|---|---|---|---|
| Date of Birth | 9 | 9 | 5 | 405 |
| SIN | 9 | 5 | 9 | 405 |
| Address | 5 | 9 | 5 | 225 |
| Bank Account | 5 | 1 | 9 | 45 |
| Hours Worked | 1 | 1 | 1 | 1 |

High impact numbers indicate pieces of information that should only be collected if required and must be protected at the highest level reasonably possible.

By doing this exercise with the payroll data you collect, you will have the basis for determining if you are applying the right types of controls to the information you collect. It might even persuade you that you could reduce the amount of personal information that you collect.

In future columns this year, we will look at the next stages in the life cycle of payroll/HR data from a privacy perspective: sharing the information within and outside of the organization (use), storing the information while at the organization (retention), and destroying the information once no longer needed (disposal).

Send you questions and feedback to **john@wunderlich.ca**. Include "**CPA Life Cycle**" in the subject line. ■

*John Wunderlich is an information privacy and security consultant, based in Toronto. For more information, check out his intermittently updated website at* **compliance.wunderlich.ca.**

**Notice:** This column reflects solely the opinions of the author. Individuals are encouraged to seek qualified legal advice on points of law or matters of interpretation.