by John Wunderlich

Are You Ready to Meet Your Regulator? Assessing Your Privacy Management Plan

Your IT department has just notified you that an external party has had access to your payroll/HR database for the last 10 days. Although the individual was not able to change any data, he or she has been able to read everything. In other words, you have a security incident that includes a probable privacy breach. Does your organization have an incident management plan? Does it include provisions for privacy breaches? Does it also include how to deal with the regulator?

Organizations must realize that privacy breaches are not a question of "if," but rather, "how frequently?" and "how serious?" Most Privacy Commissioner websites have good information on how to respond to these situations. With appropriate planning, you will ensure that the first significant breach is handled properly. In many cases this includes notifying the people whose information has been breached. If this is the first such incident, you should be ready to deal with serious internal resistance to notification. No one likes to publicly admit to an error.

You should also be prepared for the fact that the parties affected by the breach may file a complaint with the Privacy Commissioner or another appropriate regulator. Are you also prepared to face the commissioner or other regulator? This is an important but often-overlooked part of the plan.

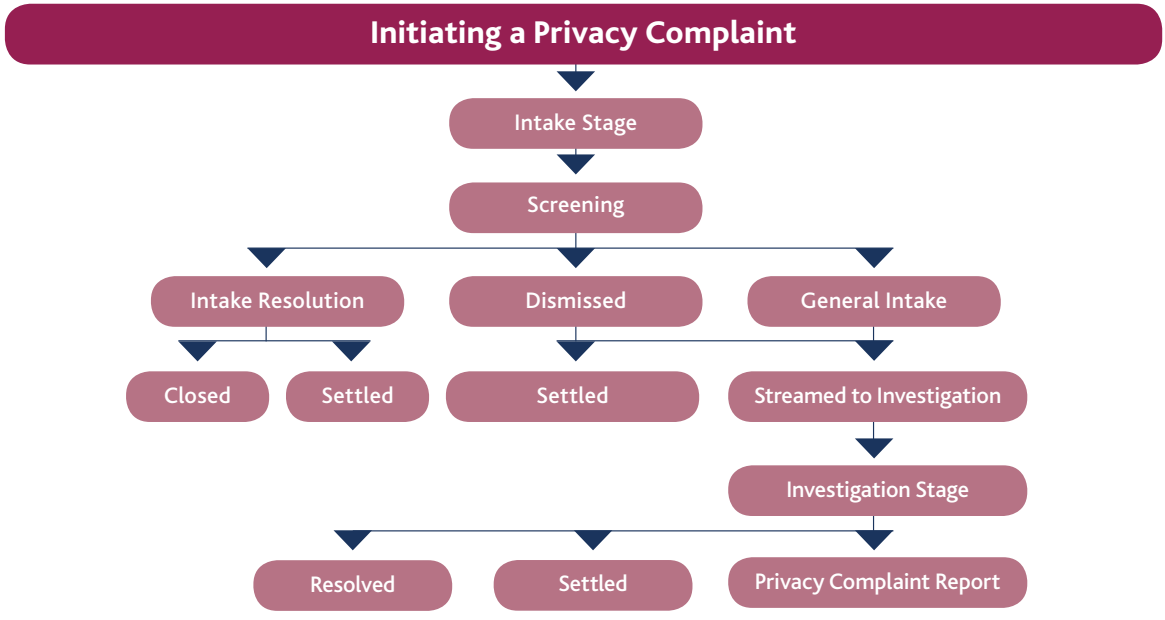
What is a privacy complaint?

A privacy complaint occurs when someone contacts a Privacy Commissioner or another appropriate regulator because that individual believes his or her privacy rights have been violated. What happens then? What can an organization do to prepare?

It is best to start with the following four points:

- Assume that there will be complaints.
- Regulators must listen to all complaints.
- You must be prepared to respond to all complaints.
- The time to prepare is before you get the first complaint.

Although your organization may be in the right and the complainant unfounded, this will only be revealed through the investigative process. In other words, you may not dismiss any complaints without demonstrating the merit of your organization's position. To do so, your organization must submit to a screening by the regulator at minimum. This flowchart outlines the Information and Privacy Commissioner of Ontario's complaint process as an example.



(Modified from the original flowchart, which can be found at ***http://www.ipc.on.ca/english/Resources/IPC-Corporate/IPC-Corporate-Summary/?id=567)***

Let's walk through this step by step. A complaint is formally initiated when it is sent to the Registrar at the Commissioner's Office. In the intake stage, an analyst attempts to resolve the complaint informally, dismiss the complaint, or prepare the complaint file for investigation. In the screening stage, based on the analyst's work, the Registrar determines whether to stream it to resolution, dismissal or investigation.

More often than not, the Commissioner's Office is able to close, settle or dismiss a complaint without a formal investigation. A complaint is closed when the Registrar or the intake analyst is satisfied with the outcome. It is settled when the issues have been resolved to both parties' satisfaction. It is dismissed when it is determined that the complaint is not within the Office's jurisdiction or when, in the Registrar's view, it does not merit further action.

If a more formal investigation is required, it proceeds to the investigation stage. An investigator reviews the circumstances of the privacy complaint and attempts to settle some or all of the issues. Again, at this stage the complaint may be resolved or settled. If this is the case, the file is closed through a letter to the parties involved, and no report is prepared. However, if it is not resolved or settled, a public report is issued. The report may include a summary of the complaint, a discussion of the investigation, conclusions, findings and recommendations. Depending on which particular acts or regulations are involved, the report may take the form of an Order. Commissioners' Orders have the force of administrative law and must be complied with.

The point of this quick tour through the complaint process is to illustrate that it is not a painful exercise. In most cases, the Commissioner's Office will work with both parties to close or settle the complaint without a formal report. You will be given multiple opportunities to avoid a public report or Order. That is not to say that egregious violations won't lead to Orders. However, even in such serious situations, the risks can be mitigated by cooperation. ■

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