by John Wunderlich

What's the Harm?

Determining whether to notify employees and customers of an incident that breached their privacy is becoming simpler.

There are two opposing views on privacy breach notification:

- Every affected individuals and relevant regulatory bodies should be notified every time personally identifiable information is unaccounted for.
- Data breach notification requirements should be eliminated, and only those who can prove that real financial harm occurred and it was due to the breach should be compensated.

While these statements represent the extreme sides of breach notification—most organizations fall somewhere in the middle—both positions have a certain logic.

The former statement, privacy advocacy, is based on the idea that privacy is a right, so data processors are obliged to divulge any breaches to affected individuals. The latter statement supposes that privacy breaches are harmless in and of themselves, so individuals must demonstrate monetary harm to receive monetary compensation; to act otherwise would be an unreasonable restriction on the conduct of business.

The question for a payroll practitioner becomes: "What is the reasonable middle ground between these two extremes that is consistent with Canadian regulation, HR/payroll best practices and the expectations of management and staff?" Let us look to a competent authority for guidance.

A 2010 amendment to Alberta's *Personal Information Protection Act* (PIPA) added a new requirement for organizations to notify the Information and Privacy Commissioner of incidents "involving the loss of or unauthorized access to or disclosure of personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual." It also gave the Commissioner the power to require organizations to notify individuals to whom there is a real risk of significant harm as a result of such an incident.

Since the amendment has come into force, there has been a small stream of breach notification decisions[1] that provide guidance on what qualifies as a disclosure with a real risk of significant harm to an individual. In May 2010, the decision concerned payroll specifically.[2]

PAYROLL BREACH

In the case, the organization, which used an external payroll provider, noticed an unauthorized special pay period had been added to its system, as well as three new employees, and an unsuccessful attempt was made to move money into the accounts of these new employees. The external payroll provider con-

[1] http://www.oipc.ab.ca/pages/OIP/BreachNotificationDecisions.aspx

[2] P2011-ND-008: http://www.oipc.ab.ca/Downloads/documentloader.ashx?id=2812

firmed that the organization's system had been accessed using authentication information from the organization's accounting administrator and that the payroll data entered included financial and demographic information. Neither the organization nor its payroll provider "could provide an audit trail of exactly what information was viewed or perhaps copied during the time period of the unauthorized access to the payroll system."

Did the systems' safeguards work? On one hand, the accounting person who reviewed the accounts, or the administrative safeguard, noticed the discrepancy. Similarly, the technical measures in place by the payroll provider prevented an unauthorized transfer of funds. Therefore, with respect to the financial security of the system, there was no harm.

However, because the system was unable to identify what personally identifiable information may have been viewed or copied, there was a fundamental failure of privacy controls.

The Commissioner stated, "I have decided that there is a real risk of significant harm to individuals as a result of this incident. I have based my decision on the fact that the type of information involved could be used to commit identity theft which is a significant harm. There is no audit trail to confirm what information was accessed and given the sensitivity of the information, there remains the possibility information in the payroll system was viewed or copied."

It may be of some importance to readers to know that the report named the organization whose payroll was breached but not the payroll provider. This illustrates where the accountability always lies: with the organization. Although most providers provide high-quality privacy and security controls, it is important to remember that the organization is ultimately responsible.

WHAT CAN AN ORGANIZATION TAKE AWAY?

The lesson to be learned is that the simple viewing of payroll data is a potentially serious privacy violation. In other words, assertions that data was not altered or copied are insufficient to provide privacy assurances. This must be made clear to all payroll practitioners and all technical people who support payroll systems.

To help ensure privacy is maintained, access to payroll systems—the data they contain—*must* be limited to the minimum number of people required to perform the payroll function. ■

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.