By John Wunderlich

Management Considerations: Finance, Payroll and Risk

Accounting and payroll personnel are probably among the most trusted in an organization. Executives depend on them for analyses and advice that can easily determine the fate of the organization. In most organizations, payroll accounts for the most significant amount of its expenses, and is part of the finance or accounting function, reporting to the Chief Financial Officer (CFO). It seems to me that the relationship between finance and payroll should be characterized by two main questions:

1. Is the payroll function running efficiently, delivering value for money?
2. Is the payroll function managing risk appropriately, including privacy risk?

The first question is best dealt with by accountants and business analysts in consultation with payroll staff. But the second question—managing risk in payroll, as it relates to risk management and fraud, particularly—relates directly to this column.

Financial analysts, auditors and accountants need to have full access to all the information they deem necessary if there is a suspected case of fraud—including the personally identifiable information of any employees who are reasonably suspected of being involved in, or whose information may be used in, the perpetuation of the fraud. It is also the case that when auditors come calling, they have a reasonable basis for requesting access to at least some types of personally identifiable information. Similarly, if finance is doing a risk assessment to determine the likelihood of a civil suit, and you don't have the results of a privacy impact assessment[1] (PIA) or some other form of evidence, you will probably have to share your processes and perhaps your data with the person(s) doing the risk assessment.

Notwithstanding reasonable claims of access by finance, the payroll department is still accountable for ensuring that employee data remains appropriately protected even after it has been shared. There are a number of tools available to help payroll professionals maintain their commitments to employees. These include disclosing the minimum necessary data set, applying administrative controls, and privacy training and role based controls for finance personnel. Needless to say, these tools can be useful for similar purposes with other stakeholders who have similar requirements for access to personal information.

For access to personally identifiable information there are really only two acceptable justifications; consent or legislative authority.

If the requestor has legislative authority, it may come from a statutory authority, such as the Canadian Revenue Agency (CRA) with respect to investigations related to taxes, or from a judicial order like a warrant. You have a due diligence requirement to validate the authority, and to keep some form of evidence that you have done so. You may also need to notify the person or persons whose data has been requested that you have disclosed their information pursuant to a legal request. The privacy protective default position is to notify the individual unless the authority that has requested the information also has the authority to request that you not notify the individual and that they exercise the authority.

With respect to employee personal information, it is the case that consent is generally not required for information or purposes that are reasonably necessary for the purposes of creating, maintaining or terminating the employment relationship. In that case, where an audit for the purposes of insuring the financial integrity of the payroll system is being conducted, or some similar employment-related purpose, it is reasonable to disclose the information to the auditors.

If the requestor does not have legislative authority or is not fulfilling an employment-related purpose, then you must have employee consent for the release of information. In that case, you need to ask whether the requestor, in the fulfillment of their duties, also meets one of the purposes for which consent was granted.

Once you have determined that you have to, or may, disclose employee information, consider the following:

- **Apply administrative controls.** These include contractual clauses (or letters of intent or memoranda of understanding or statements of work) requiring recipients to acknowledge their receipt of personally identifiable information and their commitment to hold it confidential and to use it only for specified purposes. Further, they should be bound to apply the same conditions to any entity with whom they share the information. The clauses should include a mandatory notification clause in the event of a breach and a requirement to return or destroy the data when the business use is complete.
- **Ensure that the recipient is qualified to handle personally identifiable information.** This could include asking questions about their privacy training and whether they apply role-based access, encryption or other controls to limit access to your data. The weaker their privacy program and controls are, the stronger your requested administrative controls should be. You can ask for the ability to audit their controls from time to time if the recipient is getting a data feed (like a benefits provider) instead of a one time request (CRA).

At the end of the day, remember that you have made a commitment either explicitly or implicitly to your employees to protect their personal information, and they have had no choice but to trust you. Make sure you enforce your accountability with anyone who requests access to your employees' data. ■

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.

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

[1] A privacy impact assessment or PIA is a tool for assessing privacy risks and for making recommendations to reduce privacy risk. An appropriately scoped and executed PIA will significantly reduce both the likelihood and potential impact of a civil suit, as well as other privacy risks.