CANADIAN
PAYROLL REPORTER
NOVEMBER EDITION
PUBLISHED BY CANADIAN HR REPORTER
www.payroll-reporter.com

Is the cloud the right choice for payroll?

Cloud providers insist safety is priority, but companies must ask questions: Lawyer

| BY ZACHARY PEDERSEN |

LINDA WOOLLEY REMEMBERS when payroll administration was a lot more hands-on.

"I've seen it go from punch card to mini computers to PCs to servers and PCs, client servers, web servers, Internet," says the president of Nortek Solutions, a payroll and human resources software provider based in Uxbridge, Ont.

When new technology was introduced, she was always hesitant to embrace the change — something she sees in potential clients when she brings up payroll's newest technology.

"I had that same fear when we gave up the punch cards because I couldn't feel our programs anymore. I couldn't see them, touch them," she says. "There was just a period of time where you had to go through this build up of confidence and we're at that stage right now where most people now know the word 'cloud.'"

Software deployed solely over the Internet and licensed to customers through a subscription is known as cloud computing. Local software isn't necessary because the application is web-based. This means information can be accessed from any location and maintenance or upgrades are conducted by the provider.

ADP Canada's latest product, Workforce Now, is cloud-based and offers ease-of-use to clients, says Chaayanath Mysore, Toronto-based vice-president and chief information officer of ADP Canada.

"We manage (the system), we push changes out and clients have access to these changes," he says, adding upgrades happen almost instantly. "The client (doesn't have) to do anything other than come in the next day and just log in to this cloud and they see the changes that are available."

ADP has been offering similar services since 2001 in the software as a service (SaaS) model, he says.

SaaS offerings are end-user applications hosted by third party vendors that can be accessed remotely. Cloud computing is when a third party provides and supports computing infrastructures and services that companies pay for according to usage.

Offering a cloud-based product gives clients the ability to combine applications, Mysore says.

"They're not looking for one vendor for payroll, another vendor for HR and another vendor for time because the moment you do that you're really incurring an additional cost having to integrate the solutions," he says.

Cloud services keeps costs down because the subscription model creates predictable cost modelling as expenses are calculated per employee, says Woolley, whose latest payroll application, Curos, is cloud-based.

"You don't have to worry about your growth. You pay a little bit more money for more resources, but these cloud vendors have the ability to ramp up quickly," she says. "In fact, (with) in-house (products), what you have to do is anticipate your needs over the next three to five years and you have to buy up front enough to give you that life cycle, but with the cloud you pay for what you use. It's cheaper."

Cloud-based services drive costs down further by eliminating the need for in-house servers, Woolley says. Not only do companies not need to invest in the server itself, but the corresponding infrastructure isn't needed, either.

"There are no computers, there's no power consumption, there's no server rooms, there's no heavy air conditioning, there's more freed up floor space," she says, adding this is more environmentally friendly. "One could say, 'Well, you're just moving the servers from in-house to the hosting provider.' That's true, but these companies… it's their business to get the most efficiency possible out of their servers. You can be sure their utilization of their hardware is much more effective than any one in-house."

Privacy in the cloud

Security is more effective than in-house systems, too, says Mysore, acknowledging it's a difficult concept for people to believe.

"Clients should actually feel more comfortable that their data is more secure at an ADP site than their own site," he says. "I'm not suggesting that it's more secure at ADP, I'm just saying that there is a cost involved in making sure that your data is secure and I can tell you comfortably that security is the number one thing at ADP for its clients."

But security should be top of mind when exploring third-party cloud systems, says Timothy Banks, a partner with Fraser Milner Casgrain LLP in Toronto.

"Payroll information is some of the most sensitive financial personal information that an employer will have," he says, listing social insurance numbers, banking information and wage and benefits information as the most notable pieces of sensitive information. "All of that can be used in order to do identity left on the employee, which will be a nightmare for the employee, but also for the employer."

Companies also need to be concerned with corporate espionage, says Banks. Many inferences can be drawn from payroll information.

"If you want to know what's going on in a particular facility, understanding the number of employees there and what they're earning, their composition may be of interest in determining what's going on in the facility," he says.

An even worse scenario would be if unauthorized access leads to someone setting up a fake employee to divert funds from the organization.

"That may go undetected in an organization with a very large payroll… that could be significant amounts of money," he says.

Information being sent to a third-party system needs to be encrypted, Bank says, adding it is safer to house that information on the cloud provider's server in an encrypted state, as well.

Companies will more than likely want to house their information in a multi-tenancy system, he says.

A multi–tenancy system, like Workforce Now and Curos, is when a software application serves multiple customers, also known as tenants, on one system.

"There has to be logical partitions to prevent me from seeing the data that's supposed to be just for you and you seeing the data just for me," he says.

A reputable cloud service provider will offer multi-tenancy services, says Woolley.

"In 2009, we said this is where we are going to head and it's going to be multi-tenanted," she says. "So no client would ever fear the risk of access by another client."

Another consideration employers will want to concern themselves with is the total number of parties involved with providing the cloud product, according to Bank.

"There may be a number of vendors in providing the whole infrastructure, platform, software and also back-up services," he says. "Each of those providers may be touching your data at some point and the weakest link in that will pose a significant security concern for you. Do they meet the outsourcing organization's security requirements?"

Companies should ask cloud service providers how often penetration tests are conducted on the system, Banks suggests, noting it's important to know a plan is in place if something does go wrong.

"What kind of security checks do they do on their employees? What kind of security training do their employees have both at the outsourcing organization's level and then right through the chain of all the service providers?"

This is a founding principle of ADP, says Chaayanath.

"You have to design your applications expecting things to go wrong," he says. "Every switch is constantly monitored so that when it goes down, we've got monitors that will trap it… and corrective actions are immediately taken."

There are non-security issues companies should be considering as well, says Banks.

"What happens if the cloud service provider becomes insolvent?" he says.

In the HR field, there are lengthy document retention requirements under tax and employment standards legislation and companies will have to be able to produce those payroll records if audited or in legal proceedings, he says.

While no company likes to think something like that could happen to it, it's a best practice to know where and how those documents can be accessed.

"What happens if you want to change vendors? How will you get your data out?" he says. "Provision needs to be made for that.

There's one piece of advice Banks says will serve as a good guide for any company considering a move to the cloud.

"(They should) think about what they're going to have to say to their employees as an employee relations problem if and when the employee data is improperly accessed. That is an employee relations nightmare," he says. "If you keep that in mind… it will focus your mind on the fact that you need to really consider the security practices of the cloud vendor."