THE SECURITY RESPONSIBILITIES OF THE CIO IN A CLOUD ERA

Edmonton Series

SPONSORED BY

BLACKIRON
ROGERS Business Solutions

PRESENTED BY

CanadianCIO

OVERVIEW

CanadianCIO gathered with IT leaders from 20 different organizations, largely from the public sector, to explore "the best ways to safeguard corporate data by choosing the most appropriate products and services, establishing the ideal vendor relationship and coaching your IT team for success."

The facilitated discussion focused on how to maximize the benefits of cloud investments and preparing Canadian organizations for a more flexible, dynamic, on-demand future. The event was moderated by Shane Schick, Editor of CanadianCIO magazine.

ADOPTION TRENDS AND ASPIRATIONS

While none of the CIOs would describe themselves as highly experienced users of cloud infrastructure solutions, they were proactively trying to arm themselves with information that would help steer decision-making around this emerging model. Several were in the midst of making board of director recommendations or conducting privacy impact assessments, indicating they are close to making a move.

Up to date technology: From an application perspective, several CIO guests suggested that having access to the most current releases of key software programs would prevent users waiting on refreshes for undue periods of time. Similarly, managing infrastructure through the cloud would provide them, in theory, the latest data centre technologies.

A solution for big data: One CIO noted that regardless of industry sector, most organizations are beginning to realize they are going to be managing an increased amount of unstructured information, the volume and velocity of which may change without warning. Cloud solutions may be a way of staying ahead of potential problems.

Redundancy/disaster recovery: While they still have some reservations around whether certain cloud services are ready for prime time, there was a recognition that in some scenarios, working with a good provider could ensure that critical information is not merely stored on premise where it could be damaged by natural disasters or tampering from employees.

KEY SECURITY CONCERNS

Lack of clear business requirements: CIOs understand that business needs change rapidly and that it's up to them to help facilitate business processes more effectively, but they said they are sometimes under pressure from users in their organizations to turn to a potentially insecure cloud solution without a measurable use case. They don't want to be on the hook for moving to

the cloud prematurely and experiencing negative repercussion if data is compromised. “Our role is to ask, ‘What is your ultimate goal?” one CIO said. “I can help you achieve it, but with more security, and if you don’t want more security, someone is going to have to sign for the risk.”

Continuity of service: Despite vendor assurances that the cloud provides impeccable uptime, CIOs expressed doubts about whether the delivery of key IT resources might be subject to interruption, having witnessed what’s happened in the consumer space with similar services. “How do we back up? If that service that’s somewhere, who knows where, in the cloud, goes down, what happens to that information?” one asked. “It’s the same as losing money. If you put $10 million in the bank and the bank foreclosures, where’s your money?”

Perception vs. reality: Many of the guests around our table came from the provincial or municipal public sector, where a big component of what they do surrounds interacting directly with citizens. Even if they know their cloud provider keeps data safe, fostering the same trust among the public may be difficult. “Citizens may perceive that putting data in the cloud may make them vulnerable to attack,” one CIO said, and educating or convincing them is much different than working through the same process with management or internal employees.

‘Tier 3’ vendor syndrome: While most people we gathered together had deep experience in traditional outsourcing with large firms, the cloud market includes a number of players that may require more vendor management oversight than CIOs want to offer. “It’s the one-offs, the click-the-button ones where you assume there’s a contractual agreement in place but there’s no substance behind it,” one guest said. Those without a substantial track record or reputation may be more difficult to assess from a security perspective, others added.

Job security: CIOs at our table were concerned not only by employees who rush to embrace the cloud but senior leadership teams who don’t understand the real risks and may misinterpret how it might change their role. “It’s a huge amount of work talking to them about it,” said one CIO, who estimated his board of directors had an average age range of 50-60. “They didn’t understand what we do before the cloud. Now that it’s coming that becomes even harder.”

CANDID COMMENTS FROM OUR CIO PARTICIPANTS:

“I didn’t realize the degree of resistance we would run into from a security aspect.”
“For me, the issue with cloud computing is not when the process hits procurement, law or IT. It’s when the business units do something on their own and move into the cloud and then we find out about it afterwards. I have a lot of work keeping up with that.”

“When we move to the cloud, we give up our custodianship of that information to the service provider. What kind of contracts do we have to be liable for them for that? We need to explore that.”

"We could lose data, we could experience performance problems . . . There's potential for a lot of error, especially in shared cloud environments."

"Where we're running into interesting conversations is with our vendor community, where standard agreements have included hosting, those vendors are now moving out of the hosting and moving their services to the cloud. They're changing the nature of the contracts."

"Forget about the legal and procurement rules surrounding all of that, it's getting in front of the client and making sure they're making educated decisions with their purchases and understanding the implications of that, which we don't truly understand ourselves."

"It's not about stopping the business, but moving side-by-side with them. That's what the cloud is about: "I can get a solution just like that, I can get it immediately." So we need to work with them as opposed to against them."

CONCLUSIONS

CIOs were very concerned that they would not become the ones in their organizations to say "no" to cloud computing. If anything, it's more a question about how they can say "yes" in the right way. A big part of this is not just mitigating risk but figuring out what staffing will look like in the future. Many acknowledged that job cuts could come as a result ("It's the elephant in the room," one admitted) while others saw staff reductions come primarily through attrition. In either case, what will be the key focus areas for those who continue to be employed within IT departments, and how can CIOs begin preparing them for those new areas of focus today? This is a place where smart cloud providers will offer some thought leadership based on experiences they've had with successful early adopters.

Every new technology concept or model needs time to mature, but CIOs in Alberta are particularly anxious to see a critical mass of adoption and to be influenced by large organizations within their peer group. Several guests mentioned they would be looking for clearer direction from organizations such as Service Alberta to help define the path many of them would follow to take advantage of the cloud while avoiding the worst of the risks. While that happens, cloud providers will need to spend considerable energy to source client testimonials and case studies from their first customers to convince others in the same sector to get on board.

Finally, CIOs want to move at their own pace, not at one dictated by vendors, analysts or the media. In many cases, those gathered around our table have only recently migrated major parts of their business from paper-oriented processes to digital ones. The cloud represents an even more potentially overwhelming transition, so they will need providers who take the time to deeply understand not only their risk appetite, but their change appetite. There is no doubt, however, that the cloud has made CIOs hungry to provide greater value in nearly everything they do.