THE SECURITY RESPONSIBILITIES OF THE CIO IN A CLOUD ERA

Ottawa Series

GUESTS

AJ Byers,
President of
BLACKIRON Data

Richard McConnell,
Director of IT, Gowlings
Henderson Lafleur LLP

SPONSORED BY

BLACKIRON
ROGERS Business Solutions

PRESENTED BY

CanadianCIO

OVERVIEW

CanadianCIO gathered with IT leaders from 11 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. Moderated by Shane Schick, Editor of CanadianCIO magazine, the participating executives on the panel included:

AJ BYERS, President of BLACKIRON Data
Richard McConnell, Director of IT, Gowlings Henderson Lafleur LLP

ADOPTION TRENDS AND ASPIRATIONS

Our CIO guests were largely in the early stages of cloud adoption and in the "research" phase of the buying cycle. In most cases, they had some experience with software-as-a-service, most often for productivity applications such as word processing and e-mail. IT infrastructure-as-a-service offerings were of high interest for a variety of factors, primarily for three reasons:

Simplification of infrastructure management: While CIOs seek more dynamic allocation of IT resources, they do not want to be in the business of having to fine-tune workloads on a regular basis.

Improved use of IT department resources: One CIO described it as "reducing the amount of talent needed on the bench for keeping IT up and running," while others suggested a move to the cloud was not necessarily about layoffs so much as redeploying to more higher-level activities around applications.

Cost savings: CIOs understand that some of the early promises around the financial aspects of cloud computing may have been overblown but they continue to see the possibility of savings through a more on-demand approach to acquiring and delivering compute resources, particularly at peak periods.

KEY SECURITY CONCERNS

The BYOD Influence: Cloud services offer a tremendous opportunity to get around barriers that corporate IT will demand of users around authentication, backup and regulatory compliance. This is what drives some users, even at the executive level, to begin using cloud-based applications. CIOs said they are spending too much time policing this activity and trying to get one step ahead of it and not as much time as they would like to explore the opportunities around moving IT infrastructure into the cloud. “We have to be looking at putting out services that are as good or better than what they can get on the market for free, and make sure we’re very clear through policies.”

Data Control: CIOs are worried about cloud agreements that may not properly stipulate how data will be collected, stored and shared across data centres and potentially across geographies. As one CIO pointed out, there are also concerns about what cloud providers do with customer data for their own purposes, such as aggregating it or mining it for intelligence which they can then sell as an offering to third parties. “We’re now on a level where we have to worry about, who owns the data? When do I get my data back?” said one CIO. “My data physically is sitting where? At one point do I get a comfort level that it’s okay?”

Reduced layers of protection: There are many areas of enterprise IT today that have been managed with two-factor encryption or better, and some CIOs had the perception that cloud providers can host information without necessarily offering more protection than a user name and password. One gave e-mail archiving as an example. “The tradeoff you’re looking at is mostly around things like encryption and auditing. There might be specific things you were doing before which will now be closed to you when you move to the cloud,” said one CIO. “I don’t think I would be happy with that tradeoff.”

Vendor vulnerability: Given the highly competitive nature of the cloud services market, CIOs are attempting to align themselves with partners that will not only provide them what they need, but will have the wherewithal to survive. One CIO pointed out that his firm is contractually obligated to keep all customer records for at least three years “Will that (cloud) provider be around for three years?” he said. “I need to know I can get that data if they get bought, merge or go out of business.”

CANDID COMMENTS FROM OUR CIO PARTICIPANTS:

“There’s a downward pressure on revenue. We are under constant pressure to reduce our costs in every way possible . . . for us, cloud services and everything related to that, they’re being used to drive costs out of the business. We’re kicking every tire and looking under every rock to figure out how can we do it better, how can we do it cheaper, and how can we do it faster?”

“There are so many problems with all the various definitions of the cloud. (Among senior

management), there are perceptions that have been created, and those perceptions have not necessarily been realized when you try to implement this."

"We have 300-plus data centres that we've been trying to consolidate. I don't think we can do it without a cloud-based service."

"One of the things we're most interested in is, what kind of executive level metrics you would use to monitor the effectiveness of IT security in the cloud? We're particularly interested in things like, how do you maintain that kind of security when you're changing delivery agents?"

"In terms of security, there's no fixed perimeter, so it's very nebulous to understand the cloud. Cloud is just a fancy word for outsourcing."

"We have three applications in the cloud, and are in negotiations to take on a fourth. We want to be completely in the cloud within the next two years. I find that if you're in the cloud, your back end infrastructure costs are less than half of what it is today. It hits your bottom line, and it hits it within 12 months. And I think any business that's not in the cloud, you're probably going to be out of business."

CONCLUSIONS

In some respects, Canadian CIOs are better-positioned to deploy IT infrastructure than they think. They have deep experience in working with major vendor partners, they know their compute workload intimately and they have clear business drivers around cost, flexibility and utilization that should prove convincing to their senior leadership.

Some challenges in Canadian adoption may stem from the branding around "cloud." As vendors try convey the sense of new benefits and efficiencies to be gained from hosted, on-demand service provision, they may have inadvertently sent a message that the cloud entails complication. More of the marketing and branding around cloud should focus less on things like uptime, resource allocation and scale but instead emphasize the ease of setting up contracts, establishing solid service-level agreements and, most importantly, mapping out parameters around data usage and transport. These things would go a long way towards answering security questions around cloud computing before they have been asked.

Finally, the cloud has occasionally been used by business leaders to suggest it will reduce the need or importance of the CIO role and that of the IT department. Cloud vendors need to help CIOs not only improve business outcomes through more effective deployment and management of IT infrastructure but about how CIOs can redefine their value to everyone from the board of directors to everyday employees. CIOs aren't just worried about whether their data, servers and applications are secure – they're thinking about job security, too.