

The Risk of Hosting in Canada



An ebook by

 **TriNimbus**
Cloud Management Solutions

Index

	Introduction.....	1
	Financial Risks.....	3
	Legal Risks.....	5
	Security Risks.....	8
	Technical Risks.....	10
	Conclusion.....	12
	Contact.....	12



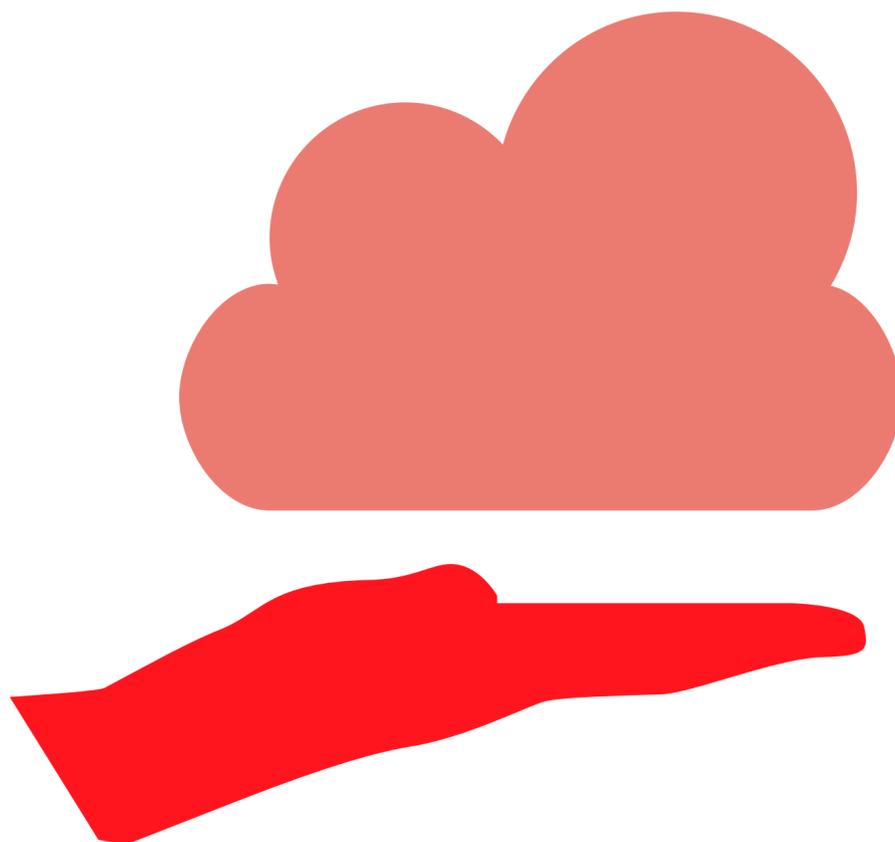
Introduction

Hosting your applications or IT environment on the cloud is a bold decision, and like most bold decisions, it tends to involve complex and far reaching factors. While cloud hosting gives you the power to securely access your data anywhere in the world, it also makes the data more susceptible to virtual and physical probes in the form of cyber attacks, hacking and government policies. Canada seems to be the natural place to host your business online, if you are a Canadian enterprise. Also, it makes sense to keep your servers on Canadian soil if you are a Canadian business owner. Although this seems obvious there are risks associated with these assumptions and many factors need to be considered before migrating to the cloud.

It's important to define what we mean by the cloud, as we are only referring to the public cloud and not to a private cloud hosted in an organization's on-premise infrastructure.

In this ebook we review the different risks when considering hosting in Canada including financial, legal, security and technical. Including discussions on the dreaded concern of the US PATRIOT Act, which gives the US Government power to seize data from foreign servers under the suspicion of terrorist activities. As well as other factors like cost, innovation, issues in bandwidth, latency and government policies are also prominent.

Faced with these risks and opportunities, the best thing for organizations to do to reap the vast benefits of hosting their business on the cloud is make logical decisions, based on facts, and understand the risks associated with their decisions. Moving your business to a cloud based service provider should provide flexibility, capacity for growth, cost savings and a more secure environment. This is the promise of the cloud. However all of these are truly not yet available from a Canadian host provider and hosting in Canada will mean sacrificing on one or more of them, specifically flexibility, capacity and cost savings.





Financial Risks

Higher Costs

A major risk of hosting in Canada is higher and increasing infrastructure costs. In most cases opting for a Canadian provider means that you need to provision your resources and get tied into long term contracts. This almost equates to buying equipment as a capital investment for a 3 year term. Unfortunately there is no real utility computing at scale in Canada, where you can turn on 1,000 servers, run them for a few hours, then turn them off, and only pay for those 2 hours of usage. There are providers who offer Cloud-like utility in Canada, but it's limited and the business models are not yet built to offer these services especially when you include operating systems and database software licenses as part of the equation.

When we compare this situation with the cloud leaders AWS' offering, it becomes obvious. Their capacity for scale and true utility-like computing

is unmatched with Gartners Magic Quadrant for Cloud Infrastructure as a Service report released in August 2013 stating that AWS offers five times the utilized compute capacity of the other 14 cloud providers in the Gartner Magic Quadrant including Microsoft, Google and IBM. To add, AWS has decreased their costs on various services 12 times since they began operating in 2007.

Obviously cost is only one of the major factors that determine your decision on where to host. Selecting Canada is certainly more costly. Based on our research by as much as 50% depending on the workloads and applications you intend to run.

Cost Comparison Between Canadian Host Provider and Amazon Web Services

Case	Environment	Average Canadian Hosting Quote	Cost of AWS Estimated	Savings
SaaS Produc	9 Servers with 2TB Storage (Linux)	\$2,000/month	\$1,000/month	50%
Business Applications for Mid-Size Organization	9 Servers with 3TB Storage (Windows)	\$7,000/month (OS & SQL licenses not included)	\$5,000/month (OS & SQL licenses included)	33% (if already own licenses)

Growth

In Canada, technology is growing at a much faster rate than infrastructure. What this means for the organizations is that the local service providers will find it difficult to keep up with the cutting edge technological needs of business owners. A good example is the fast growing Big Data opportunity. Its still a costly exercise for organizations to take advantage of Big Data with a Canadian provider, making this technology unaffordable in Canada for most mid-size companies. Where on AWS you can spin up a Big Data Hadoop environment and run it for a few hours and turn it off when you're done for only a few hundred dollars. The equivalent in Canada would cost you many thousands not just in dollars but in time for setup and resources. This is a classic case where the local service providers will only offer the most popular services, and the customer will have limited choice and ability to take advantage of the latest technologies and advances.



Legal Risks

Hosting in Canada Because of Prism & the Patriot Act

There are two main driving forces why Canadian companies host their data in Canada. Firstly, they must comply with government or industry regulations. Secondly, they do not want the potential of their data exposed to foreign governments, particularly the United States.

Regulations

Regulations rule the day, where the legal and business risk of non-compliance are enormous and force organizations data to remain at rest in Canada. In understanding compliance we must must consider what is regulated data, where majority of the data being stored is unregulated and can run anywhere. Meaning you could use Canada for only regulated data, and the Cloud for everything else. Further reading into the compliance documentation you may find that it does

not distinguish between active and passive data, nor backup or disaster recovery environments. It simply states your data must reside in Canada. As an example organizations could have their data backed up in Canada but running in a Cloud environment elsewhere. Or have their main environments in Canada, but Disaster recovery on the Cloud. Many large regulated Canadian organizations are using the cloud for their non-regulated data and workloads like public websites and Big Data. The regulations and compliance for all industries is different however it's worth taking a closer look to truly understand its limitations.

Patriot Act

Organizations feel that having their data hosted in the US is a big risk. The major dread is what is known as the US Patriot Act of 2001. After the huge impact the terrorist attacks of 9/11 had on its citizens, the US government signed the Patriot Act to strengthen its security controls. The prime repercussion of the Act is the ability of the US Government to request information from any US based host provider without a warrant, based on the suspicion of a national threat or terrorist activities. More importantly, the section 215 of the Patriot Act, titled 'Access to records and other items under the Foreign Intelligence Surveillance Act', coupled with the recently exposed National Security Agency (NSA) program, PRISM, where the program facilitates extensive, in-depth surveillance on live communications and stored information. The US law allows for the targeting of any customers of participating firms who live outside the US, or those Americans whose communications include people outside the US. Simply what this means is if the US Government is suspicious they can access your data if it resides in the US.

What does this mean in terms of Canadian organization risk? If you're doing something bad, than we're all glad that you're under suspicion and hopefully get caught. Every organization in Canada by law must publicly provide a privacy statement. In that statement you need to disclose where your data resides and you can be as vague or as detailed as you like. Example, "we host our environment and data in Canada and as well as many international jurisdictions". Or "we host our customers private data in Canada, USA and Ireland...". Further you can state that legal authorities may access this information and your organization will comply by law. This disclosure reduces business risk dramatically where now customer, vendor or 3rd party cannot sue the organization if their data is accessed by a foreign government authority as you disclosed its residence. The risk is really how business leaders and particularly their customers feel about their data being accessible by the US Government, or any foreign government, and this may have a negative effect on their business.

In this day and age of cyber terrorism it's a fact of life. We believe that it matters less and less where the data is at rest as Government organizations, including the US and Canada have agreements to share data on suspicious activity to protect it's citizens. This means that Canadian citizens and companies are as exposed in Canada as they are in the US. In fact, recent legal studies based on the usage of the Patriot Act in the Canadian provinces of Nova Scotia and British Columbia shows just how easy it is for this information leakage to happen. A testament to this fact is the Canadian cryptologic agency, Communication Security Establishment (CSE) commented that US Government's PRISM "would undermine CSE's ability to carry out its mandate." Privacy Commissioner Jennifer Stoddart's lament regarding Canadian standards regarding online privacy says it all - "We have fallen far too behind."

We also believe that transmitted data, even encrypted, across the internet, is exposed to the prying eyes of Security Agencies. If you truly feel this risk, and want to protect yourself, it's not a decision of where to host, it means you need to put your servers in a dark room, disconnected from the internet, and operate your business there, which is not a reality for 99.9% of business in Canada today.

Ultimately the decision to host in Canada comes down to regulatory requirements and how your customers feel about their private data being elsewhere. If those are material risks, then you must consider Canada. If they are insignificant the logical conclusion is to host where you receive the most cost and performance efficient environment for your needs

Governmental Policies

We all face the shear rate with which technology is changing and the challenge to keep up with it in terms of legal frameworks and investigative practices. With this increasing pace it is absolutely essential to build laws with foresight and flexibility which can stand the test of changing scenarios by protecting users more effectively for longer terms.

We live in a world where data is global and we need global laws to secure and protect it. Unfortunately, in Canada and elsewhere, that is likely a long way off. Governments seems to be playing catch-up rather than being proactive and we don't see this trend changing any time soon.



Security Risks

Changing Cyber Law and Insurance

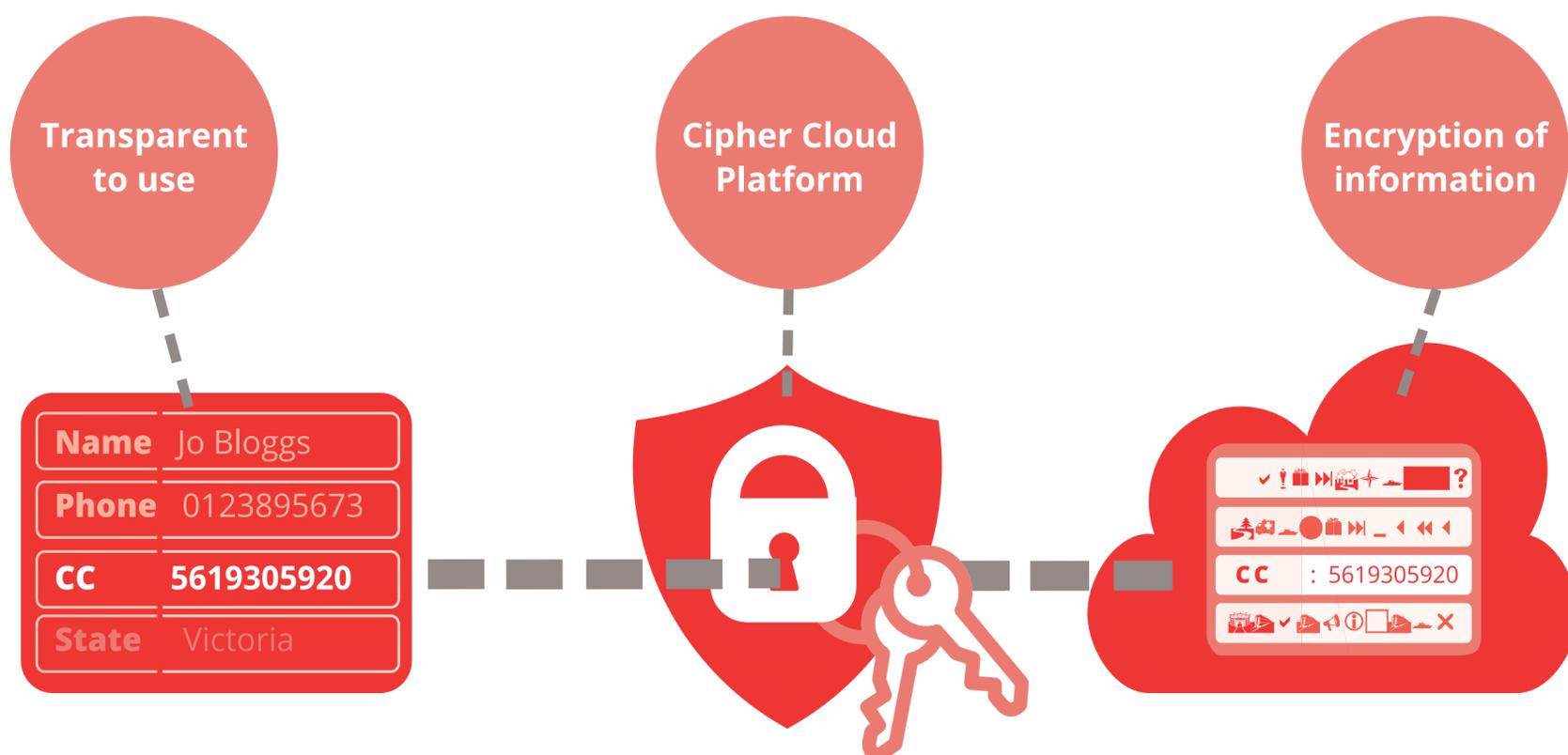
We argue that hosting data in the cloud offers greater security than your on-premise centre. Simply the large providers, because of their economies of scale, hire armies of the best security professionals, equipment and 24/7 monitoring, something most IT departments cannot afford. This is slowly dawning on businesses as they start to accept the cloud.

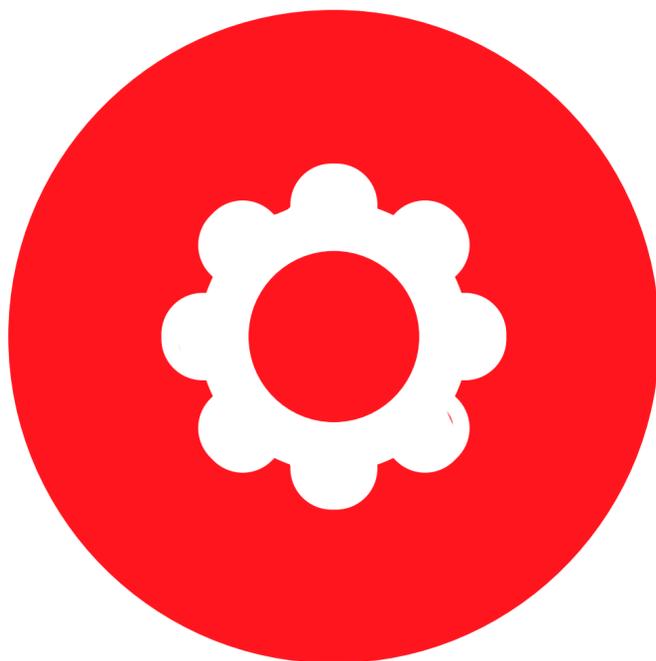
However the concern for hacking is a warranted and a very real risk, no matter where your data resides. Companies can only rely on the law after the fact to protect them and must rely on stringent security policies and procedures. Many host providers in Canada provide these procedures however it's once you get hacked that the real risk sets in. Sadly, as opposed to the US, the Canadian cyber law is not yet stringent enough. Soon Canadian laws will be passed that require hacked organizations to notify their violated account holders. This is a very expensive exercise.

As this law already exists in the US, Insurance companies have established policies to protect organizations from this risk. The concept of insurance companies offering policies to protect companies from cyber infiltration is still relatively new in Canada, however more and more Canadian insurers are offering cyber protection policies. We encourage businesses to understand those if they are hosting risk prone data, no matter where it is.

Higher Risk of Being Hacked

The actual risk of getting your server hacked is higher in Canada than it is in most parts of the world. A recent WebSense survey shows that Canada was ranked second in the world, ahead of major offenders like Egypt and Russia, for hosting malware and phishing. In addition, last year, the Canadian Public Safety Minister Vic Toews expressed concern regarding this fact. In 2012, the Canadian press reported a worrying statement from the Public Safety Department which says, "Plainly said, we may be moving from being mostly 'targets' of organized cyber-crime hosted in outside jurisdictions, to 'hosts' of online cybercrime operations and activities."





Technical Risks

Innovation

Most innovations in Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) are being produced outside of Canada. The host providers in Canada are mostly recipients of this technology. We look to organizations like Amazon Web Services, Microsoft Azure and Google for leadership in this space. AWS in particular prides themselves and track their innovation with a list of over 250 innovations in 2013. Host organizations in Canada simply don't have the scale or capital to keep up. The risk of hosting in Canada means limited ability to take advantage of the latest technologies, which in terms means lack of competitive advantage. We believe this negative cycle will only worsen as the cloud densifies and the pace of technological innovation increases.

Another good example are Google's business apps and Microsoft Office 365 online applications. Using these services your data is hosted outside

of Canada. Simply put, organizations who want to take advantage of these innovative services need to make the decision on how they are going to deal with the data residency issue. If you are using Microsoft's Office products you are likely running on-premise, you have very limited choice other than to stay on the existing version. The path to upgrade involves the cloud outside of Canada, and surely many organizations are struggling to figure out a way to deal with this challenge.

Bandwidth in Canada is Slow

One of the primary keys to having a smoothly running cloud based operation is bandwidth. A server with slow bandwidth is the last thing a business wants. When the online traffic to your server is high, it means that your online interests are popular. But having a server running on a slow bandwidth kills all the effort behind setting up a quality online product. This means that your server will not be able to handle the incoming online traffic above a certain threshold. Despite putting out a popular online presence, you will miss out on reaping the benefits.

Canada does not even rank in the top ten of the fastest connected countries. The reasons for this are actually understandable. Canada's sheer size, with vast mountain ranges and some of the most beautiful secluded views in the world are an immense natural treasure. But when it comes to connecting the country with optical fibre, the same terrain and size makes it a daunting task.

The discussion here points to your where your customers are located. Even if the majority are Canadian it means you will likely get improved network performance by hosting your environment in a US datacenter.



Conclusion

There are many risks you need to analyze before making the decision of where to host. The purpose of this document was to enlighten you with some information that can help you make a more informed decision.

One can argue there is no true cloud offering in Canada yet and this hampers organizations who are trumped by compliance and have no choice but to host in Canada.

Higher costs remain the biggest risk, including the opportunity cost of not being able to take advantage of innovation. In order to remain competitive, if your organization is not hampered by risks associated with compliance, or dealing with personal information is not an issue, you should be considering the cloud.

You should also be questioning your compliance agency and their

documentation to review what is possible. Regulation is necessary for our markets to exist, however outdated regulation is a curse on markets, and it should be constantly addressed to balance its legal purpose, especially when it relates to the fast paced and innovative world of technology and data.



Get in touch with Trinimbus to take advantage of the Cloud

At TriNimbus we specialize in Amazon Web Services (AWS) and provide expertise and experienced resources for Canadian companies wanting to migrate to the cloud, improve their cloud architecture or need 24/7 help supporting and maintaining their environments. We have an immensely talented pool of experts who can guide you through every step of building a high performing, cost efficient, safe and secure cloud environment