CIO JOURNEY

Great-West Life

Accelerating the Financial Services Sector to the Cloud

Company:	Great-West Life	**Revenue:**	$30 billion
Sector:	Financial Services	**Employees:**	24,000
Driver:	Philip Armstrong	**Countries:**	4
Role:	CIO		

Company IT Footprint: GWL is the oldest insurance brand in Canada, and it has major subsidiaries in the United States, Ireland, the UK, and Germany. Of its 24,000 global employees, 3,200 are in information technology.

"And technology transformation does not happen in a vacuum. There are cultural and economic changes to consider."

Philip Armstrong, Chief Information Officer, Great-West Life

Excerpt from: Stiennon, Richard "CIO Journeys" *Secure Cloud Transformation: The CIO's Journey*. IT-Harvest Press, 2019, pp. 222-232.

Great-West Life Journey Overview

Business Objectives

- Consolidate and transform legacy systems
- Reskill IT to be cloud-first
- Move to a hybrid cloud model
- Modernize through digital transformation

The Solution

- Modernize brand
- Integrate service channels — voice, text, web, smart device
- Move to the cloud:
  - Adopt SaaS apps for discrete functions
  - Identify strategic priorities
  - Plan for elasticity
- Develop multi-cloud, DevOps, monitoring skill sets
- Centralize cloud oversight
- Secure everything:
  - Integrate partners, third-party contractors
  - Create defensive redundancy

Impact

- Data center/cloud integration, consolidation
- Cultural shift to cloud, elasticity, monitoring
- Cloud migration prioritization strategy in place
- Improved security, malware detection
- Cost savings from replacing remote-office security appliance stacks

Great-West Life (GWL) is a holding company of multiple insurance and financial management firms. In all of its programs, it administers 1.2 trillion dollars in assets. Philip Armstrong is the Chief Information Officer at GWL. In this next journey, he describes GWL's journey to the cloud.

In the words of Philip Armstrong:

Since joining GWL in 2016, my challenge has been to reinvigorate our brands in the face of changing technology and communications channels to our customers. Every day, we must help our clients use their benefits or their pension programs to realize their financial dreams.

As an established company, we have everything from 1970s-era mainframes, which can't be beat for cost-effectiveness, to artificial intelligence (AI). So I have to ask: "How do we take that spread of technology and perform open heart surgery to improve it?" And technology transformation does not happen in a vacuum. There are cultural and economic changes to consider.

I have been in technology since I left school. I have worked in 40 countries and have lived through every hype cycle. But despite the hype, cloud is impacting the way we all do business. If you are like me, you are moving parts of your business to the cloud.

At GWL, we are pursuing a hybrid model. We have five data centers and will continue to use them. We will use appropriate cloud providers. In some cases, where cloud does not make sense, workloads are moving back from the cloud. I think of the cloud as a fantastic tool for augmentation.

Modernizing through digital transformation

We are on a journey to refresh our brand. We are looking at robotics, process automation, and AI. We want to provide all of our services in the language our customers choose. We are transforming how people think about our business and how to plan for problems we don't even know about yet.

In Canada, 50% of our workforce is made up of millennials. Without a doubt, they have a different risk tolerance. Consumers are becoming increasingly tech-savvy. Our entire business is changing, from our base infrastructure to our products and service channels—voice, text, websites, or other means (Alexa, Google Home). New ways to connect with our customers are popping up all over the place.

“When the cloud first became popular, some of our business units were excited for all the wrong reasons.”

Customers do not care if they came in over one channel last week and another this week. They expect us to know about those transactions. People now expect a certain level of technology from their providers. At GWL, we have to meet those expectations.

We work with thousands of financial planners and independent agents. We have to support them with technology that is easy to use and does not interfere with their current business processes.

SaaS adoption and beyond

Like most companies, we have gone through stages of transformation. We rapidly transitioned to Salesforce for customer engagement, Concur for expense reporting, and SuccessFactors for human resources. These are discrete functions that are easy to move to the cloud without disrupting our core business.

But there are architectural patterns you need to know about. When the cloud first became popular, some of our business units were excited for all the wrong reasons.

From the adoption of these discrete applications, we matured over the last two years. We started in the United States by moving workloads to Amazon East and West and Amazon was slow to open data centers in Canada. Our organization did a significant foray into AWS, and we had big decisions to make about whether to invest in data centers and recovery centers or whether our users and needs were the best fit for the cloud. We have been on that journey for about two years.

Why has it taken so long? We wanted to do it right. We went through each of our applications. We hired specialized talent from Silicon Valley. We re-engineered to take advantage of cloud benefits like monitoring and elasticity. And we spent a lot of time getting ready.

We are looking at IaaS for end-of-the-month processing peaks, when we need extreme amounts of compute power. We have found that it is not true that cloud is always cheaper. One lesson learned was that moving to the cloud means you are transporting a lot more data. It’s cheap to bring it in, very expensive to pull it out. It can cost you a fortune in data transfer expense.

Our largest IT suppliers—Cisco, IBM, and Oracle—have been gradually pushing their preferred environment, the cloud. That has a financial impact. It shifts your IT budget from predictable, contracted costs to a subscription model where expenses are variable. That shifts your budgets around. The accounting department complains about how lumpy your spending is. It impacts financial planning. One way we addressed that is by investing in Apptio. It measures usage, so I can cost out the technology in my data center and keep a close eye on who is spending what on cloud resources. And yes, it is cloud-based.

Another advantage is that large cloud providers have invested in security. More often than not, breaches are an internal mistake rather than some flaw in the way cloud infrastructure is architected.

Building the workforce

The shift to the cloud is a big cultural and training disruption, and you have to go through massive education for internal users. It's important to look at different departments and how people collaborate.

When it comes to moving a large organization, cloud transformation is 70% cultural and 30% technical.

Getting experienced cloud resources is difficult. Most companies are transitioning, are in the cloud, or have a hybrid. When you start to move to the cloud, you need developers that can develop applications in the cloud and you are paying a premium for toolkits, which are changing rapidly. If you are looking for someone with three to four years of in-depth cloud experience, then it is an arms race. You train them, and then they leave for a higher salary.

The other problem is the number of clouds. Spin up a public cloud instance; it drops down to AWS, then to my own data center. Between the clouds, you are actually going into the internet. You have to find people with multi-cloud experience to architect all of that.

You need financial people who can monitor usage, and DevOps people who can extend their knowledge into cloud. You also need cybersecurity people who need a whole host of skill sets. All of these skill sets are very expensive.

We have had a very deliberate strategy of partnering with large tech companies and leverage good professional services arrangements with them.

Should internal applications move to the cloud?

There are two schools of thought on moving workloads to the cloud. The companies that are starting their cloud journey look at obvious workloads. They have progressed to: "I am going to understand the benefits and cherry pick my internal apps to move to the cloud." Do they need elasticity to support a variable workload? Do they need the availability and easy access? Can they take advantage of the built-in security?

The other school of thought is that legacy applications are going to take a lot of money to move. Is there a hybrid approach that does not require complete rewrites? Keep in mind that if you do the hybrid approach, you will have some users going to the cloud and others who will be routed to your existing data centers. It is still early days in big organizations. Many are not ready to drop the VPN and authentication tokens. It's getting there, though.

Now we are starting to hear about large companies partnering to drop stacks into your data center. Cisco and Microsoft have partnered to drop an Azure stack in the data center, if I want it in-house, for whatever reason. That allows me to virtually "run it in the cloud."

I get exasperated when I hear CIOs say they are moving everything to the cloud. I have five mainframes. We view these as so cost effective, I doubt they will ever move to the cloud.

Securing it all

I am a believer in defense in depth, so I will have overlapping security capabilities. We have different types of detonation chambers in the cloud. We are using Zscaler for web traffic and Proofpoint for email. That will filter less sophisticated threats, the

“I am a believer in defense in depth, so I will have overlapping security capabilities.”

everyday burden of a constant flood of attacks. Therefore, volumes of incidents are reduced drastically.

We have very sophisticated appliances for application firewall defenses. As you drill your way into our data center, we use firewalls from multiple vendors. We are shifting to Microsoft Windows 10 and use Active Directory and Intune for mobile device management. We also have a privileged user management system for server access and track alerts in an SIEM (security information and event management). We have a large cybersecurity team, and we are under pressure to deliver on the promise of all this technology by ensuring that security is done right.

Partners and financial advisors can be a problem. Some work directly for us, so we can control their desktops and monitor their activity. Then we have people who have a commercial agreement with us, but own their own infrastructure and hardware. What we try to do with them is give them tools that they can access securely via Zscaler Internet Access. You have to look at how they are accessing your applications, data stores, and tools before deciding how to protect those elements.

Complete independents can also sell our products. You have to ensure they come through routes you can secure. What we have found is you cannot stop everything, so you need these multiple levels of defense. You cannot monitor and measure everything, so you have to apply the more sophisticated technology, like AI, so your team can be freed up to focus on the important things.

The bad guys are starting to use AI to package their malware. They want to be able to bypass the sandbox technology everyone is deploying to catch their malware.

Zscaler saw the writing on the wall. The difference with Zscaler is they can inspect traffic inline. Detonation chambers have been around a long time, but they run in a virtual environment, and the sophisticated stuff detects the virtual environment and goes to sleep. Zscaler has built its own environment without the standard virtual machines, so the malware detonates and is detected.

One of the great things about working with cloud vendors is if I get infected by something, and I show the vendors what I have seen, they will learn from it. Then they implement protection in real time into the cloud.

An example of our security working is that we had no issues with WannaCry. We saw some attacks in North America and a couple in Europe. We had already patched for it.

What we are seeing is that we are in pretty good shape to screen out the run-of-the-mill stuff. It's the very sophisticated stuff that we have to worry about. It gets past your first line of defense, lands in an inbox, and somebody clicks on a link. Either Zscaler gets the link and blocks it, or our endpoint solution sees the unusual behavior and the device is quarantined until it can be cleaned up.

For a lot of companies, the cloud has complicated things. How do you extend your security fabric to multiple clouds? It's simple: just get a cloud cybersecurity service.

Before our transformation journey, we had a traditional 1970s hub-and-spoke design. Cisco helped us build a leaf-and-spine design—a fully meshed network between access switches and the backbone, many to many—using Cisco Unified Access Data Plane (UADP) switching ASICs. We spent all of 2017 building that. The design they helped us with is complete, and it is already implemented.

But we also recouped costs from all those remote offices that no longer needed the full stack of security appliances. It allowed us to invest in our future model.

Moving forward

It was rather hard to sell the transformation internally. I have been here two years. We were quite a traditional shop and we were happy building a moat around the data center and securing it. But when it comes to talking about different services, we could not build that ourselves, so we saw we needed to use public clouds. As we did research, people's attitudes came around. The biggest hurdle to overcome was around security.

I spent three days in Redmond at Microsoft doing a deep dive on the Azure architecture. When I came back, my boss asked what I thought of the security of Azure. I told him, “They are more secure than we are.”

We had some savvy board members that encouraged me, and our first forays have been quite positive. We are proceeding with caution. We have an internal checklist for any app we plan to move to the cloud. If we believe there is a good business case, we will do it.

Large financial services are slow and steady. They are risk averse and heavily regulated. They are in the trust business. That comes with the responsibility to think very carefully about the fit of the cloud.

Lessons learned

The very first thing you have to do is take a temperature check of your internal culture. It is normal to be excited about moving things out to the cloud. Vendors will go directly to your internal people, bypassing any oversight you may have. If everyone says, “Yes move everything to the cloud,” I would be equally worried. Ask yourself what is the primary driver. Is it security? Agility? Flexibility?

The ice that is under the water—that hidden infrastructure—is quite expensive. It is hard to find people with that knowledge of the architectural patterns.

What not to do

- Try to prevent your internal business users from going directly to cloud suppliers themselves. They can punch a hole in your cyber fabric. They can enter into contracts that leave a nasty cost surprise. They can leave critical digital assets lying around. You have to be the cloud broker.
- Avoid moving things to the cloud simply because you don’t like working with your internal IT people.
- If you move to the cloud and realize it was a mistake, acknowledge that and move it back.

Ready to transform your company?

Create business value with Zscaler today.

CONTACT US

REQUEST DEMO

https://www.zscaler.com/company/contact

https://www.zscaler.com/custom-product-demo

About Zscaler Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.