Ready, Secure, Cloud:

A discussion about cloud security governance in an insecure world

Long View

WWW.LONGVIEWSYSTEMS.COM • INFO@LVS1.COM • 1.866.515.6900

Table of Contents

INTRODUCTION

With many organizations looking to become more agile, more cost-effective and more focused on business innovation, we are seeing "cloud-first" become a common technology strategy.

This means that large-scale cloud migrations are part of the fabric of many customer engagements here at Long View. Our goal is to help our clients realize the benefits of their cloud choices while ensuring that solid security practices are woven in, from the first strategy discussion through to deployment. Public cloud, hybrid, multi-cloud, private, governance, modernization and optimization: Customers want deep expertise to ensure that their infrastructure is secure, managed and agile, and their business protected.

We all see the news: 2019 was on track to be the the worst year on record for data breaches, with a 54% increase in the first 6 months.[1] Yet recent research states that only 49% of organizations are encrypting sensitive data in the cloud and only 17% of companies are increasing their information security budgets. So, while more enterprises are spending money on off-premises cloud, to the tune of a 79% increase year over year, there is a disconnect in the security requirements from a focus and budget perspective.[2]

We produced this eBook to share a wealth of knowledge about cloud migration and security. In particular, we review how our customer, EQ Bank, a new player in the consumer banking industry, ensured that they were laser-focused on protecting their customers' data as the first Canadian bank to shift their core banking systems to Microsoft Azure.

Long View recently celebrated our 20th year in business, and I couldn't be prouder of the growth and success that our company has achieved. Partners, employees and customers have all been instrumental in our journey since Long View started in 1999. We look forward to another 20+ years ahead of providing the best service and results that our partners and customers have come to experience with Long View.

Dave Frederickson
EVP Sales
Long View

"Cyber threats continue to grow but the response is not keeping pace. Security budget increases are averaging near the inflation rate but still only account for 10% of overall IT spend. And it's not just about the money - many organizations continue to operate with "informal" security programs and roadmaps that have not been tested or updated to reflect the many changes (i.e., moves to the cloud) that are underway."

Garry Hawkings, Chief Information Security Officer, Long View

CHAPTER 1:

How Secure Are You?

Only 50% of companies have defined roles & accountability for safeguarding sensitive information stored in the cloud.

- Are you the other 50%?

48% of all corporate data is stored in the cloud, yet only 49% of companies are encrypting sensitive data in the cloud.[3]

- Are you the other 51%?

Only 32% deploy a 'security-first' approach to storing data in the cloud.[4]

- Are you the other 68%?

Based on these statistics and what the public data breaches tell us, we have to assume that many companies believe that once they push that magic cloud button, their security requirements are taken care of. It just isn't the case, and companies, independent of their cloud provider, need to be accountable for the security of their data, especially customer data. A recent study revealed that 46% of them stated that storing customer data in the cloud increased their compliance and security risks by 56%.[5]

There are very broad transformations that IT teams are undertaking within their environments that are moving faster than we have ever seen from a legacy approach to modern IT. With the compliance, regulatory requirements and overall risk, where does security fit in the midst of all of this?

More people are spending more money on off-premises cloud. It is the highest category of spend, to the tune of 79% increase YoY. The median budget increase for security is only 20%.[6]

Capital One breach that impacted 106M people

July 2019 - Capital One had been breached, spilling hundreds of thousands of social security numbers and account details into public view.

The New York Attorney General is investigating whether Capital One is negligent, but the broader story is familiar: A big company let a lot of sensitive data go missing, and customers bore most of the risk.

Only 10% of IT Professionals stated that security was built into DevOps implementations with security elements.

IT Transformations

Monolithic Applications →	Microservices
Self-contained Apps →	Applications that are meshed together and require cooperation
APIs →	Function-as-a-Service
IT as a Practice →	Dev Ops and DevSecOps
Data Centres →	Cloud
Networks →	5G
Enterprise Apps →	IOT, OT, Consumer, AI

(source 451 Research[7])

"Ninety per cent of the data that we have today was created in the last two years. That's the explosion of compute and data."

Satya Nadella, CEO Microsoft

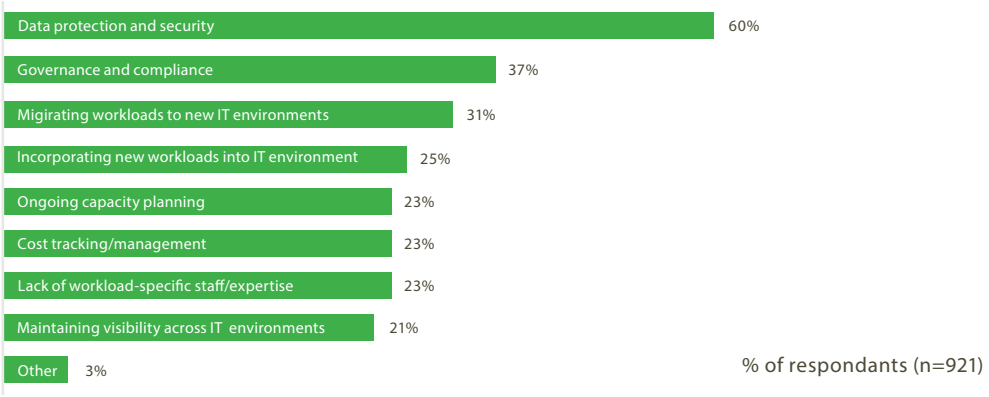
CHAPTER 2:

Cloud Security Trends – The misalignment between serious need and execution

Misconfigurations of cloud migrations or internal systems have opened the doors for attackers who are taking aim at companies' lack of security. We have to remember, there is big money in the hacking game, and only prestige for some. This is costing companies in excess of $3M USD in direct costs alone, and for the more public companies, the legalities are endless, as customers' personal information is being compromised.[8] Even those organizations that are under regulatory bodies are not safe if all eyes are not on their security requirements.

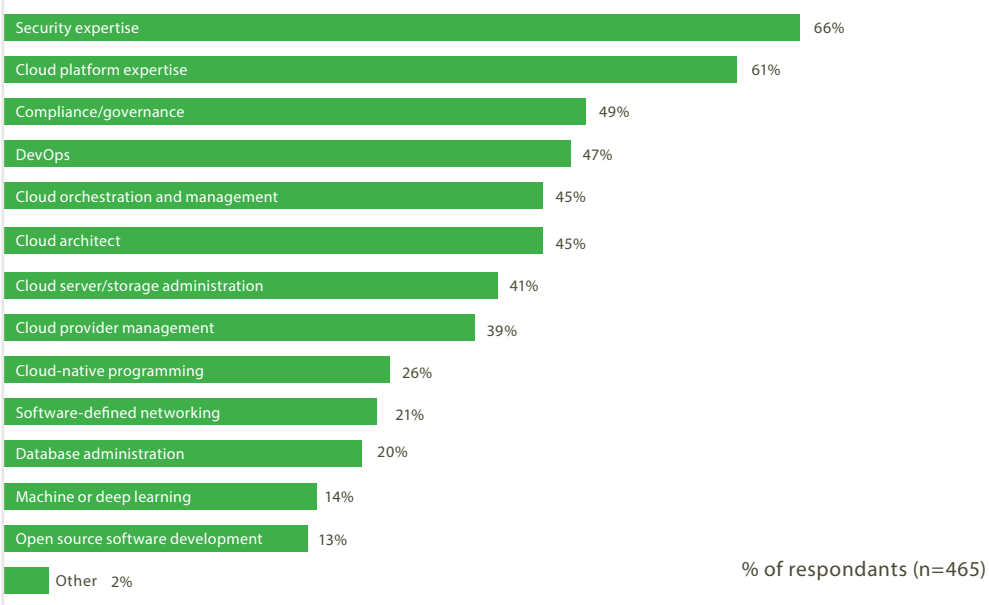
At the recent 2019 SecTor Conference held in Toronto, Canada, several of the sessions discussed the misalignment between serious need and execution when it came to security in the cloud.

Data Protection & Security is the greatest issue enterprises are facing with regard to workloads



Source: 451 Research, Voice of the Enterprise: Digital Pulse, Wororkloads & Key Projects 2019

Companies rated security expertise as their top requirement for IT leaders, yet the same survey showed that having the right security expertise was their biggest gap. Thirty-six per cent felt that they had a gap in security expertise within their teams.[9]



Source: 451 Research, Voice of the Enterprise: Cloud, Hosting & Managed Services, Organizational Dynamics 2019

Don't waste someone else's crisis waiting for your own to take place

Now is the right time to learn and discuss not if a security breach is going to happen to your company, but when that security issue or crisis will arise.

Cloud Adoption Trends:

With all this fear, uncertainty and lack of preparedness from even the largest organizations, why are companies shifting to the cloud? Here are some of the top business benefits that organizations reap with Digital Transformation:

- Customer experience, with greatly improved satisfaction and reduced churn rates
- Faster time-to-market for new products
- Improved employee productivity due to data-driven business intelligence and analytics
- Reduced operating expenses, by 36% on average
- Fewer security or data breach situations when leveraging the expertise of partners and experts
- New digital business revenue streams that were not possible with legacy systems
- Automation, optimization and innovation, all downstream benefits

Organizations are not getting what they need to react when or if a security breach happens. Only 52% are inviting their CISO to the table when making public cloud spending decisions.

- Who are the 48% that are not?
- Are you one?[10]

An alarming factor is that cyber attacks and security breaches seem to exploit a different vulnerability of the cloud network. The target organizations belong to different industries and are of different sizes, from small to large.

This also defeats the argument that as large organizations spend more on cyber security, they are bound to be immune from cyber threats.

Don't plan for IF a cyber security breach is going to happen, plan for WHEN

CHAPTER 3:

A Case Study – EQ Bank Securely Moves to the Cloud

Work Completion: July 2019 – Ongoing

EQ Bank is the first Canadian bank to migrate its core banking system to Azure Cloud as it challenges the Canadian banking industry with unique consumer options and prepares for Open Banking

- EQ Bank is the 9th-largest independent bank in Canada
- $31b in assets – more than doubled in five years
- Digital Banking leader – disrupting traditional models
- Time from strategy to launch – 18 months
- Time as a Long View Client – 4 years

The era of digital banking has arrived, and consumers are looking for more innovative and competitive banking that meets their needs, and with preferential rates. That is exactly what EQ Bank is planning as it challenges the Canadian banking industry, which has seen a legacy approach for the past 200+ years. EQ Bank, the digital deposit arm of Equitable Bank, launched in 2016 and has exceeded growth expectations beyond even their own lofty goals and dreams. Consumers are benefitting from improved rates, service levels and innovative banking products.

Long View has worked with EQ Bank for over four years and was side-by-side during the first and fastest cut-over of a core banking system to the cloud ever completed in Canadian banking history: only 18 months from strategy to launch.

Fair, Open Banking is the Future

Open Banking is a new concept in the 200-year-old banking industry. It improves competition in a healthy way and gives consumers options over what has existed for 100s of years. EQ Bank's vision: To ensure that the average Canadian consumer is the beneficiary of a digital bank that meets their needs. The whole concept of having chequing and savings accounts only makes sense to a bank. It is all to maximize a bank's profits, not to benefit the needs of the consumer. EQ Bank continues to win over Canadians by challenging how people have been told to bank by their current institutions. EQ offers completely digital, branchless services, with a high-interest savings account that includes the added features
of a chequing account, that just make sense.

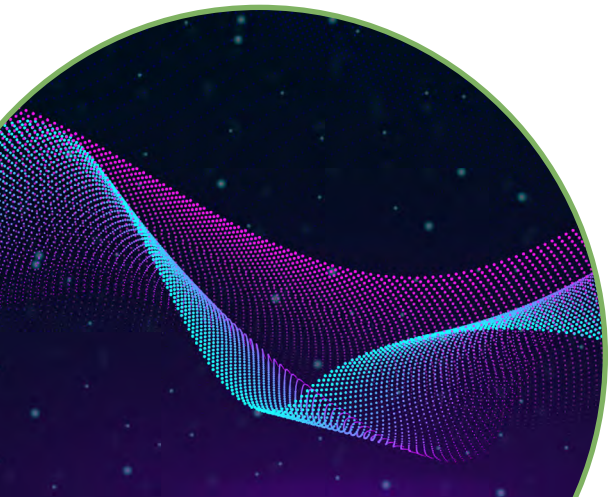
How the business of technology can enable business growth

EQ Bank selected Microsoft Azure as the cloud platform for its banking services, which will reduce overhead costs. In turn, they will pass these savings on to their customers. The migration of their core banking system creates a flexible platform that allows EQ Bank to create and offer more products to their customers quickly and at scale.

Why Microsoft Azure? Temenos, EQ's core banking provider, had a strong relationship with Microsoft already, and EQ Bank had the confidence in their cloud platform. Microsoft Azure also provides confidence by providing many advantages over other cloud providers. For example, Azure has been designed based on a SDL (Security Development Lifecycle), which is an industry-leading assurance process. Azure comprises security at its core, and private data and services remain secured and protected within the Azure cloud. In addition, Azure provides similar if not better capabilities than AWS and GCP for PaaS services. Azure PaaS services provide application developers with the environment, tools and building blocks to quickly build and deploy new services to the cloud. Azure also provides a rich DevOps experience, which allows teams to take advantage of important things like monitoring, managing and continuous improvement for applications and infrastructure.

Becoming an innovator and change-maker was the opportunity that interested Dan Dickinson, CIO and Senior Vice President, when he joined Equitable Bank five years ago. "Our mission is always to deliver better, safer, easier and more intuitive ways to bank in Canada. We are retiring the old banking methods and the technologies that go along with them to move faster with innovative banking products to serve our current and future customers who are looking for something better."

EQ Bank's approach to security is not just building higher or more walls



Parameters are different today now that security breaches reaching all-time highs. IT Departments and business leaders have to assume attackers are in your walls or trying to get in. It is just the nature of security today.

"Microsoft has more security people working for them than we have employees. Microsoft is just good at what they do, and we relied on both their and Long View System's expertise to reach our project and business outcomes," stated Dan Dickinson, CIO and Senior Vice President of EQ Bank.

"The bank is still responsible for securing and protecting the customer data wherever it sits. When EQ Bank made the Azure decision, it was based on where can I put data, where the best and most protection exists, and there are smart people who know how to ensure our customers' data is well managed, well maintained, well governed, well secured. Azure, for us, was the way to do that."

Go where the expertise is

When a strategic business and IT project as critical as EQ Bank's shift to the cloud in 18 months is at play, there is a need to surround yourself with the best in the industry. Whiteboarding sessions, challenging business assumptions about security, and assessing both current and future technology requirements need a team of collaborative people. This includes experts from outside the EQ Bank team.

"We had been working with Long View for years as they manage our Network Operations Centre. Long View is a specialist in setting up the environment so that EQ Bank could go live when we made the move to the cloud," Dickinson shared. "There is a difference between partners and vendors. With Long View as a partner, we would get a bunch of smart people in the room and solve problems. When I needed someone, I just had to pick up the phone so we could figure out the right thing to do at that time. Long View has earned that partner status with EQ Bank, as they have a level of expertise that other players we have worked with in the past don't have. They know their stuff and are always offering up recommendations for how we can do things better, with our best interests in mind. We have a trust relationship, with business values and a corporate culture that align."

Long View is a leading Microsoft Partner across North America. Microsoft honoured them with another "Country Partner of the Year Award" in 2019, which makes them the only Partner to have ever won this coveted award twice, let alone two years in a row.

"We love where Microsoft is headed—all cloud, all mobile and globally secure with scale. We've built our key managed services offerings on the foundation of Microsoft technologies and roadmaps because security is paramount in today's world."

Brent Allison - CEO, Long View

CHAPTER 4:

There is no silver bullet to cloud; there are best practices

Cloud Governance Best Practices

When it comes to moving to the cloud for your own organization, you want the best experts in business today. Thought leadership from an architecture point of view means having a direct correlation between business outcomes and value. Whether you are migrating to the cloud for the first time or future optimization, there are steps that need to be taken. You don't want to be on the wrong side of the statistics around cloud and security governance.

Data Centre Strategy: Content Summary

These are the steps we suggest as you begin to document your journey:

1. Assessment: Start with an assessment of your current environment, and define what your future business and IT goals are.

    - Why do you want to go to the cloud?
    - What is your compelling business reason?
    - How will you transform your organization as a result? List all of the reasons:
        i. Financial – cost savings or revenue generation
        ii. Agility - faster time-to-market with products or services
        iii. Productivity – ensuring employees are more effective and working more strategically
        iv. Strategic – support M&A activity, improve customer satisfaction
        v. Operational - streamline and optimize
        vi. Other
    - How will you measure success?

2. Data Centre Strategy: What is your objective, whether it is a multi-, poly- or hybrid-cloud scenario? We are seeing many large enterprises looking at a multi-cloud situation with at least two cloud platforms, and with Microsoft Azure being one of the two selected.

    - Public, Private, Hybrid Cloud, Multi-Cloud?
    - IaaS, SaaS, PaaS?

3. Adoption and Migration to the Cloud: Build on the original assessment of your applications, dependencies and upgrade requirements for migration to the cloud. Remediation is a key step that many miss because they just assume that everything can lift and shift to the cloud.

    - Application placement criteria

4. Cloud Migration Methodology: What are we going to do across each of the applications?

   The 6 Rs of Application Migration Methodology:

   1. Re-host – lift and shift to the Cloud
   2. Re-platform – upgrade underlying OS
   3. Re-factor – change the application architecture as part of migration
   4. Replace – replace workloads with new technology
   5. Retain – unsuitable for cloud, set aside
   6. Retire – decommission the workload, no longer required

7. Guiding Principles: We dig deep into your specific security, governance and optimization from a management perspective. Once the shift is completed, management and monitoring are still required, and Long View will create a modernized environment. We offer a complexity assessment along with vendor-based tools that have been developed over years of experience.

   - Application Complexity Values Assessment
   - Migration Complexity Values Assessment
   - Microsoft Application Assessment Tools

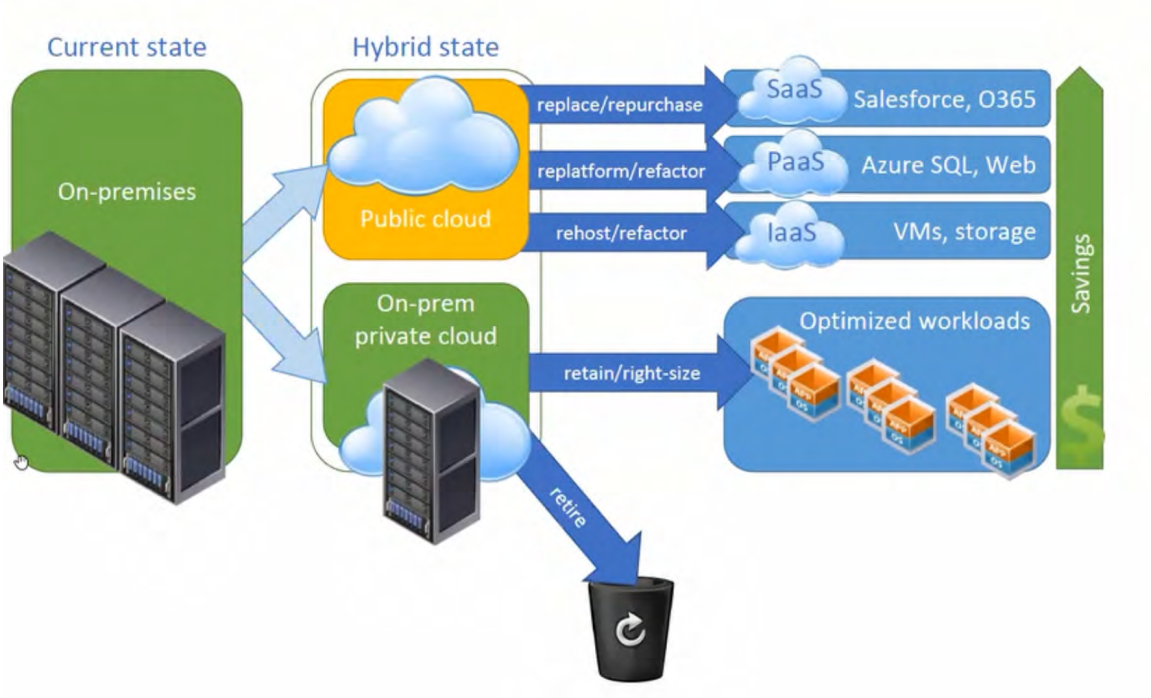
8. High-Level Architecture for Public Cloud or Hybrid Model: Each client, workload and application has its own need, legacy and future requirements. Long View collaborates with the business and IT owners to ensure that all is considered for the end result to drive the business value milestones.

9. Bridge between Security and Engineering: Developing a Security Hardening Requirements (SHR) document is critical to accelerating and safeguarding your data during your migration planning. This is customized for each unique customer and industry where regulatory compliances must be followed. There could be several SHRs for each customer.

   - Data Loss perspective
   - Identity
   - Availability
   - Resilience
   - Due Diligence to protect your assets

Customers that are looking at cloud look to Long View to help them make the right decisions. Customers rely on Long View to be that expert-level decision maker that is aligned with their business goals.

Data Centre Strategy: Application placement criteria



Long View asked Dan Dickinson for one final piece of advice for his CIO/CISO counterparts as it relates to security and governance for cloud migration.

"There is no silver bullet to cloud. It doesn't instantly solve your problems. While it gives you more flexibility and adaptability, it still needs to be managed just as tightly, and maybe even stronger. It should force you to shift how you think with regard to controls and governance, and with a zero-trust model, as there are players in the middle who you don't control except by contract. Never let business pressures dictate the speed at which you implement, if sacrificing security protocols is required."

Getting Started

Schedule a virtual 30-minute whiteboard session to begin to understand your cloud migration and security requirements based on industry best practices and Long View's expertise. Our team will better understand your business needs to help you navigate your cloud migration and security governance plan.

[1] https://www.sddatacenter.com/news/data-breaches-increased-54-in-2019-so-far

[2] https://safenet.gemalto.com/resources/2019-thales-global-cloud-security-study-ponemon-institute-report/

[3] https://safenet.gemalto.com/resources/2019-thales-global-cloud-security-study-ponemon-institute-report/

[4] https://www.helpnetsecurity.com/2019/11/13/cloud-migration-projects/

[5] https://safenet.gemalto.com/resources/2019-thales-global-cloud-security-study-ponemon-institute-report/

[6] https://sector.ca/sessions/cloud-adoption-trends-and-recommendations-for-security-teams/

[7] https://sector.ca/sessions/cloud-adoption-trends-and-recommendations-for-security-teams/

[8] https://www.ibm.com/security/data-breach?cm_mmc=Search_Bing-_-Security_Optimize+the+Security+Program-_-WW_NA-_-%2Bcost%20of%20a%20%2Bsecurity%20%2Bbreach_p&cm_mmca1=000000NJ&cm_mmca2=10000253&cm_mmca7=5206&cm_mmca8=kwd-81020405744748:loc-32&cm_mmca9=CMTKoejGrOYCFbeTxQIdvbwJ6g&cm_mmca10=&cm_mmca11=p&msclkid=c1d34e2a2832177c6eed13da7cce9d71&utm_source=bing&utm_medium=cpc&utm_campaign=Search%7CGeneric%20-%20Services%20-%20Cost%20of%20Data%20Breach%20Study%20LP%7C000000NJ%7CWW%7CNA%7CEN%7CBMM%7C10000253%7CNULL&utm_term=%2Bcost%20of%20a%20%2Bsecurity%20%2Bbreach&utm_content=Cost%20of%20Data%20Breach_UN%20(BMM)&gclid=CMTKoejGrOYCFbeTxQIdvbwJ6g&gclsrc=ds

[9] https://sector.ca/sessions/cloud-adoption-trends-and-recommendations-for-security-teams/

[10] https://sector.ca/sessions/cloud-adoption-trends-and-recommendations-for-security-teams/