THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

CLOUD

Cloud finance: A review and synthesis of cloud computing and cloud security in financial services

MICHAEL B. IMERMAN | RYAN PATEL
YOON-DO KIM

CLOUD

#55 MAY 2022

a wipro company

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

CLOUD

CRYPTO

CYBER

DEAR READER,

Welcome to edition 55 of the Capco Institute Journal of Financial Transformation. Our central theme is cloud computing, which has transformed from an efficiency initiative for our clients, to an indispensable growth driver for financial services.

The pandemic has changed consumer expectations, with consumers now demanding 24/7 access to their financial resources from anywhere, as well as hyper-personalized products that reflect their lifestyle choices.

In this edition of the Journal, we explore the power of cloud and its potential applications through the lens of a joint Capco and Wipro global study, and take a deeper look at the financial services data collected in Wipro FullStride Cloud Services' 2021 Global Survey. The survey was focused on perceptions of cloud and its importance to business strategy from over 1,300 C-level executives and key decision-makers across 11 industries.

The study indicates that cloud is becoming ever more intelligent, hyperconnected, and pervasive, and enables companies to offer their end users the personalized, user-centric experience that they have come to expect. It's clear that only the financial services firms that can successfully leverage cloud, will thrive.

In addition, this edition of the Journal examines important topics around digital assets and decentralized finance, including central bank digital currencies, and bitcoin's impact on the environment, and cybersecurity and resilience.

As ever, you can expect the highest calibre of research and practical guidance from our distinguished contributors, and I trust that this will prove useful in informing your own thinking and decision-making.

Thank you to all our contributors and thank you for reading. I look forward to sharing future editions of the Journal with you.

Lance Levy, **Capco CEO**

CLOUD FINANCE: A REVIEW AND SYNTHESIS OF CLOUD COMPUTING AND CLOUD SECURITY IN FINANCIAL SERVICES

MICHAEL B. IMERMAN | Associate Professor of Finance, Peter F. Drucker and Masatoshi Ito Graduate School of Management, Claremont Graduate University; Visiting Scholar, Federal Reserve Bank of San Francisco

RYAN PATEL | Senior Fellow, Peter F. Drucker and Masatoshi Ito Graduate School of Management, Claremont Graduate University

YOON-DO KIM | Quantitative Analyst, Federal Reserve Bank of Minneapolis; Ph.D. Student in Financial Engineering, Claremont Graduate University

ABSTRACT

Cloud computing is hardly a new concept, although its embracement by the financial services industry has mostly occurred in the past few years. Unlike traditional computing infrastructure used by financial services firms, such as data centers and mainframes, cloud computing relies on the internet to access storage hardware as well as software applications from anywhere at any time. This is proving to be of tremendous value for many firms especially as remote work becomes more common and on-the-fly data access is expected by stakeholders. However, it is not without its risks and challenges. In this article, we review the current state of cloud computing as it applies to financial service firms and outline both the benefits and challenges, including cybersecurity issues for data and applications based in the cloud. Further complicating matters for incumbents in the financial services industry is the fact that fintech challengers are "cloud native", in that they are built upon a cloud-based computing infrastructure and are, therefore, able to more easily adapt to changes with the technology.

1. INTRODUCTION

Cloud computing, defined as the use of computing services that are accessed over the internet rather than via onsite hardware and software, went from being an emerging technology used by only the earliest adopters just over a decade ago to now being ubiquitous in almost every organization from higher education to healthcare as well as financial services. In this review article, we discuss the evolution of cloud computing paradigms with particular emphasis on their application to financial services and fintech.

We start with a very brief literature review. A quick Google Scholar search of the terms "cloud computing" and "financial services" returns over 17,000 hits just since 2018! That being said, rigorous studies that analyze the implementation of cloud platforms and implications for business strategies are few and far between. As previously noted, with cloud computing becoming ubiquitous in financial operations – from the legacy firms (or incumbents) to the fintech startups – more analysis, especially from a risk management perspective, is warranted.

As a review article, we then proceed to cover the state of cloud computing. Topics such as public, private, and hybrid cloud models are discussed in enough detail to familiarize the reader but without getting overly technical. We then proceed to discuss the importance of cloud computing technology to financial services and fintech. The following section goes on to address cybersecurity issues and their importance to cloud computing in financial services. Finally, we conclude with some remarks for investors, regulators, startups, and incumbents about how they may want to approach cloud computing in financial services and fintech going forward.

2. LITERATURE REVIEW

While there has been quite a bit of scholarly attention on cloud computing, until recently few studies have focused on its applications in financial services. Most of the previous research on the application of cloud computing note its benefits to financial services firms. One of the earlier papers that discusses how cloud computing can optimize financial services is Ghule et. al (2014), who specifically look at banking activities. One of the primary benefits that is highlighted is automation in many of the bank's processes. Going further, the authors list cost savings, business continuity, business agility, and environmental friendliness as other benefits of cloud computing applications. These benefits, other than environmental friendliness, are reiterated by Yan (2017).

However, it has been noted that the applications of cloud computing in financial services are not without challenges. Yan (2017) notes that information security issues can be one of the biggest risks, which are associated with data breaches and cloud destruction. Furthermore, utilizing cloud computing in banking can lead to more general business continuity issues. This is because cloud computing providers might lack capacities that the banks require, thereby forcing the bank to go to yet another external vendor that may not be compatible with the bank's existing systems. At the furthest extreme, if the cloud services provider declares bankruptcy and liquidates, this could have massive implications for the bank's business operations. Lastly, this article points out that the lack of technical standards on its regulatory rules and policies on the application of cloud computing represent both a risk and challenge. A more recent paper by Sampson and Chowdhury (2021) highlights data breaches as the biggest concern for financial institutions such as banks. For instance, in a high-profile well-publicized case, Capital One was victim of a data breach in summer 2019. This breach included data from over 100 million of its customers, including personal information such as names, addresses, phone numbers, birth dates, social security numbers, and bank account numbers.

In order to address these challenges, a few articles have suggested the need for standardization and regulation of cybersecurity in cloud computing, although further studies are certainly needed. A very well-done paper by Scott et. al. (2019) points to the existing regulatory frameworks for cloud computing applications in financial services – one designed by Federal Financial Institutions Examination Council (FFIEC) for the use in the U.S., and the other by European Banking Authority (EBA) in Europe. These frameworks require financial services firms and their regulators to perform a preliminary risk assessment on the cloud computing service providers as well as monitor and audit them. We agree with the authors' assessment that this is an area that is going to require more resources from regulatory agencies for ongoing monitoring and risk control when it comes to financial institutions' use of cloud computing.

The recent study by Tissir et. al. (2021) proposed that cybersecurity for cloud computing be standardized according to the frameworks offered by International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST). They note that the purpose of such standardization would be to achieve improved levels of security with stronger controls in place in a cost-effective and reliable cloud environment.

3. CLOUD COMPUTING: A REVIEW

Cloud computing is a technology that is being used for development and deployment of a variety of fintech solutions. The technology has evolved so dramatically over the past decade that anything written about cloud computing in 2012 would be out of date in describing applications today in 2022. In this section, we examine the current state of cloud computing and discuss its importance to applications in fintech and, more broadly, financial services. First, we will provide a definition of what cloud computing is and then we will make a distinction between private and public cloud.

3.1 Definition of cloud computing

Cloud computing generally refers to the model where computing services are accessed over the internet rather than from in-house, onsite hardware and software. The hardware to which we refer may include storage or processing. These used to be synonymous with cloud computing in years past, but now much of the value added comes from software, which could include database management systems (DBMS), business intelligence and analytics platforms, customer relationship management (CRM), enterprise resource planning (ERP), ML algorithms and AI tools (e.g., TensorFlow and sentiment analysis, respectively), and cybersecurity solutions.

The economic model and accounting processes for cloud computing are dramatically different from traditional IT management in financial services. With cloud computing, access to the hardware and/or software is based on a pay-as-you-go or pay-as-you-use model. Traditionally, when it comes to systems, financial institutions have relied on massive

physical servers based out of their own data centers as well as legacy mainframe-based systems that are built on top of half-century-old technology. These require substantial upfront investments, which, from an accounting perspective, would be depreciated over time.

Cloud technology plays a vital role in the fintech space by providing a more flexible and agile business model that is more readily able to adapt to changing market demands. Sometimes, when dealing with cloud computing technology, you will hear about IaaS (infrastructure-as-a-service) and SaaS (software-as-a-service), respectively, as cloud computing providers market their hardware and software solutions. Increasingly, most cloud computing platforms incorporate both the hardware and/or software components, depending on the client's needs; consequently, a model that falls in between IaaS and SaaS is platform-as-a-service (PaaS).

Many fintech companies are "cloud native", meaning that they are built "in the cloud" and have been cloud-based from their inception. This is particularly important, as the inherent flexibility that cloud models provide is conducive to the agile framework that allows startups and challengers (in any industry but especially in the finance industry) to fail fast, pivot, and move in a new direction much faster than the incumbents. However, it does necessitate the reliance on public cloud providers, which can have a complicated cost structure and introduce potential risks. Consequently, before going further we will define what is considered "public cloud" versus "private cloud".

3.2 Different types of clouds

3.2.1 PUBLIC CLOUD

Public cloud refers to situations where the cloud computing technology is maintained by a third party. The public cloud market is dominated by the big three providers: Amazon (with Amazon Web Services or AWS), Google (with Google Cloud Platform or GCP), and Microsoft (with Azure). Another player in this space is IBM, a case we will come back to later in the section. In 2020, 6 percent of companies who had embraced cloud computing used a single public cloud [Flextra (2020)]. Reliance on the public cloud is a bit like using a utility. In that respect, from an accounting perspective, it is a part of your IT overhead but with a variable cost component, since you pay for what you use. Consider a fictitious company's hypothetical electricity bill. Management may know and expect that there will be a $1000 distribution fee per month regardless of usage. However, as they use more kilowatt hours (kWh) per month, the monthly charge will increase proportionately. If the utility charges 20 cents per kWh, then there could be an extra $600 for 3,000 kWh or $30,000 for 150,000 kWh, or anywhere in between. Using a public cloud provider is similar in that respect. You may pay a nominal periodic subscription fee, but the costs will increase proportionately with usage. The more apps that are used or the more storage that is required the higher the cost.

The firm can control costs – to some extent – by scaling up or down their cloud service needs. Hence, the economics and accounting associated with traditional financial services IT costs changes dramatically when moving from in-house computing to cloud computing. Rather than a large initial upfront cost that is then depreciated over time, there is this pay-as-you-go or pay-as-you-use model, which not only introduces flexibility in terms of how and what the software and/or infrastructure is used, but also introduces flexibility in terms of investment. This can be crucial for a startup with limited funds. But it can also lend a paradigm shift to the incumbents and their cost structures, if they make the leap.

3.2.2 PRIVATE CLOUD

Private cloud can be classified into several different categories, including virtual private cloud and on-premises private cloud. Virtual private cloud refers to situations where the cloud computing technology is maintained by a third party, but only for a single entity or a single organization. It provides higher security by constructing a firewall and only grants access to in-network users through virtual private network (VPN). The downside of a virtual private cloud is that the cost of services is significantly higher than that of public cloud.

On-premises private cloud requires an organization to completely build their own cloud infrastructure. It is an in-house private cloud that offers greater flexibility as well as higher security. However, there are many downsides to this type of private cloud. Firstly, it requires the users to be physically in the network, which limits accessibility. This was particularly a problem during the pandemic when remote work (work-from-home) became a mainstay in many industries. Secondly, it requires cloud professionals and consistent maintenance for higher security. Lastly, on-premises private cloud requires an enormous amount of equipment, which includes data centers. The data centers that make up on-premises private clouds are much bigger than they were 20 years ago, which makes sense given that we are in the age of "big data". When there were just a handful of servers in the data center, each one would

have a name and would be referred to as a "pet". The IT folks knew their pets well. In today's data centers, which make up the so-called private cloud, they are no longer pets, but rather "cattle"; nameless, rather assigned a number, each server is a replaceable member of the herd.[1]

3.2.3 MULTI-CLOUD AND HYBRID CLOUD

To wrap up our discussion on the types of clouds, we address one issue that perhaps requires more attention from practitioners who are dealing with cloud computing in a financial services firm: relying entirely on one public cloud provider can be risky. This is a concept that financial services firms, especially investment companies, know very well and it has to do with diversification. Committing to one cloud provider opens the company up to both cyber risk and financial risk. Suppose that the cloud provider is the victim of a data breach or hack. Relying entirely on that one provider could result in being fully compromised. From a financial standpoint, if that one cloud provider fails for whatever reason (think Lehman Brothers in 2008), you are back to square one shopping for a new cloud service provider but with one less competitor (ergo giving them more pricing power).

To address the issue of risk, most companies these days – 93 percent in fact – are using a multi-cloud strategy [Flexera (2020)]. This could be splitting business across the big three, mentioned above, using other specialty cloud services, or a "hybrid cloud" model, which is becoming increasingly popular.[2] Hybrid cloud refers to a combination of using a public cloud provider and still using some private cloud, which offers protection for classified data from public cloud security breaches. Apart from the de-risking and diversification elements, there is the fact that some cloud service providers may be better for certain tasks than others and that is part of the decision that has to be made in constructing the multi-cloud strategy.

3.3 Cloud architecture and deployment models

In terms of cloud architecture, there are two trends that we feel are relevant to the reader. The first is serverless computing, or function-as-a-service (FaaS), and the other is the movement from virtual machine (VM)-based cloud platforms to distributed cloud computing architechture. Serverless computing does not require any infrastructure management, is highly scalable, and makes the most efficient use of resources. With serverless computing, the servers are still running the code, but the developer has no direct interaction with it, which allows their teams to focus on innovation and creating more value for the organization.[3] In addition to the big three, to which we have repeatedly referred – AWS, GCP, and Microsoft Azure – two other companies to consider in this FaaS space are IBM and Oracle.

When discussing modern cloud architecture and deployment, in any industry, a company that often comes up is Kubernetes. Kubernetes uses "containers", which effectively breaks up and distributes software across multiple systems simultaneously (i.e., in parallel). This is different to the previous deployment model, which used a single virtual machine (VM) to run all software on the cloud. Containers are modularized units on which apps can be developed and deployed. This allows for more efficient utilization of resources, which is particularly important when the app or cloud-based program uses a massive amount of data (think Netflix, which uses its own container deployment solution called "Titus").[4]

The idea of containers is not new and easily goes back decades to the advent of UNIX, Linux, and Solaris when server-based computing rose to prominence for larger organizations. The modern commercialization of containers can be attributed to Docker, which was released in 2013. This made for a new deployment model that could be used by organizations large and small, including startups whose entire value proposition is predicated on cloud-based app development. And, in fact, this brings us full circle to why cloud computing is so important to the growth and success of fintech.

3.4 Why is cloud computing so important for fintech?

Finally, we come back to the question: why is cloud computing so important for fintech? Well, we have already mentioned that fintech companies are "cloud native" and that the incumbents are scrambling to "migrate to the cloud" to remain competitive, but that does not really answer the question.

In order to answer the question (in part) we need to define APIs or "application programming interfaces". APIs have become the lifeblood of fintech apps. APIs allow data from multiple sources to come together on one platform, seamlessly, and

[1] This is, in fact, the analogy that practitioners in the area of cloud computing use [Menchaca (2018)].
[2] In fact, Flexera (2020) indicates that of the 93 percent of companies that are using a multi-cloud strategy, 87 percent are using a hybrid cloud strategy.
[3] Microsoft, "Serverless computing: an introduction to serverless technologies," https://bit.ly/3pYIqjS.
[4] https://bit.ly/3i6QBVW.

analyzed as if the data resided in the app itself. Plaid, the banking infrastructure company, was valued at U.S.$5 billion (USD) in the M&A transaction with Visa in February 2020.[5] Perhaps it is a bit of an overstatement to say that all of that value comes from its clever use of APIs in connecting banks and other financial service providers to various different technologies and software, but that is a large part of it.

In the fintech industry, as with many other industries that rely on digital solutions, data is a valuable commodity, and one way in which this commodity can be monetized is through APIs that provide access to data from different sources. Another important reason is that much of the growth of fintech has been due to the increasing reliance on mobile technology. Apps that run on mobile devices, such as tablets and smartphones, could not be developed or deployed without going through the cloud. To be a bit more technical, the containers that were previously discussed are conducive to microservices, which have become a standard component in developing apps such as the ones that fintech companies create and market.

4. CYBERSECURITY ISSUES

One area where we have seen, and will continue to see, attention being paid to in financial services is cybersecurity (as well as business strategies that prioritize good data management and cybersecurity). As with any kind of innovation, investors associate enhanced cybersecurity with a premium. On the flip side, firms that have lapses in cybersecurity will be penalized by the market. This is similar to the trend with corporate social responsibility (CSR).[6] It took time for companies to realize that this is something that customers demand and investors want.

We have seen increasing innovation and investment in cybersecurity in recent years, and perhaps nowhere is this topic more relevant than in discussing cloud computing and its application to financial services. As the financial services industry becomes increasingly more digitized, it is almost a veritable certainty that the industry will encounter more cyberattacks. Financial institutions, technology providers, and fintech companies alike need to provide a message to their stakeholders, be proactive, and, importantly, have solid recovery plans in place. They have to carefully consider (and reconsider) those recovery plans, with those strategies continually being updated as situations change.

When it comes to cybersecurity, firms need buy-in from senior management. This is another area where fintech firms may also have an advantage given their digital upbringing. Incumbents in financial services may find cultural frictions between the cybersecurity teams and the C-suite. This is where it becomes critical that the cybersecurity experts at banks and other financial institutions really understand their audience. They must spend time breaking down complex issues into simple, digestible terms. Additionally, cybersecurity teams should identify allies among their leadership teams and their boards to help encourage and drive a better environment where there is not fear, but rather a mutual understanding. This high-level strategy needs to come out of a real conversation between the technical experts and leadership.

As the internet of things (IoT) becomes increasingly intertwined with fintech services, and fintech providers and digitally enabled financial services incumbents collect exponentially more data from users, it is natural to worry about what is being done to protect that data. This worry has an added layer when that data resides with a third party, as is the case with cloud computing. It is also important to realize that consumers often have the right to "opt out" of sharing data. The question is, then, are consumers aware of what data is being collected and how that data is being used? This comes back to the idea of education with respect to cybersecurity and fintech. As the financial services industry invests more in cybersecurity solutions, they also need to realize that empowering customers will help lead to data trust, brand loyalty, and better customer experience.

It is important that the regulation of cybersecurity among financial incumbents, bigtech, and fintech firms ensures the private data is being protected. Service Organization Control 2 (SOC-2), a procedure developed by the American Institute of Certified Public Accountants (AICPA), examines the standardized technical audits for security, availability, processing integrity, confidentiality, and privacy.[7] It is specifically designed for SaaS providers to minimize the risk and exposure to confidential data. The certification of SOC-2 might demonstrate that the certified firm has high security against the cybersecurity risk, but it does not necessarily mean that the firm is risk-free. We can think of situations where a person has a driver's license but is still a bad driver.

[5] This deal was blocked in January 2021 by the U.S. Department of Justice. See "Visa and Plaid abandon merger after antitrust division's suit to block," https://bit.ly/3q1sbRY.

[6] Though not directly related to the topic of the present paper, the idea of market participants rewarding CSR compliant firms and penalizing firms with businesses that are at odds with CSR principles is a very active area of research. See, for example, Mackey et al. (2022).

[7] https://bit.ly/3laPpey.

For financial services firms and fintech firms alike to become more resilient in terms of their cybersecurity and establish a level of digital trust with their customers, it is essential to have validation processes at the federal level. Indeed, in the U.K., the Bank of England proposed something similar in 2019 [Jones (2019)].

One area that industry participants and regulators should be keenly aware of is the development and deployment of artificial intelligence (AI) from cloud-based platforms. As AI becomes increasingly more prevalent in financial services, and those algorithms are running off a cloud-based platform, validation and governance of these models, their data, and the underlying infrastructure will become paramount. Many of the AI algorithms being used by financial institutions and fintech companies are black-boxes to the employees of these firms let alone their customers.

What insights are the algorithms providing the companies about the users? This is an important question that needs to be addressed as well. Perhaps this is an area where fintech and technology companies can learn from the financial services incumbents. Banks and securities firms are required by their respective regulators to have rigorous model documentation and validation processes in place. Such documentation must highlight the assumptions, weaknesses, and limitations of the models that are used by the firm. Inputs must be "stressed" (i.e., taken to the most extreme values) to see if the models function properly. Any changes to the model over time must be catalogued and documented. With fintech companies largely flying under the regulatory radar (for now), many of them are not required to engage in these processes.[8] However, it is not a bad idea to begin a practice of validation, documentation, and governance with respect to machine learning (ML) models and AI algorithms at fintech companies. When things go wrong in the firm – whether it is a data breach, cyberattack, or algorithm misbehaving – investors and regulators demand transparency and accountability.

As financial apps are increasingly being run off mobile devices, and residing on the cloud, biometric protections should also be an area in which financial services firms and fintech companies need to continue to improve. It is bad enough for customers to try to remember 14 different passwords across all of their accounts and financial services providers, but when these passwords are stolen, it is very easy for criminals to access their sensitive data. Whereas passwords can be hacked through brute force or stolen, biometrics leverage unique features that are physically unremovable from the customer and can be used across platforms, accounts, and service providers. When combined with multi-factor authorization or other biometric authentications, these protections can be very powerful. When facial recognition or someone's fingerprint is used to access data, an account, or any sensitive service, a simple text to the user's mobile phone or private email asking them to verify access can provide not only additional piece of mind but also added security.

> *"Cloud technology plays a vital role in the fintech space by providing a more flexible and agile business model that is more readily able to adapt to changing market demands."*

5. CONCLUSION

5.1 For investors

Cloud computing still represents a major opportunity for investors despite the technology becoming increasingly mainstream. There are several approaches that investors could take to gain exposure to cloud computing technology. These are covered in greater detail in Imerman and Fabozzi (2020), who discuss investing in fintech innovations using their conceptual framework of a fintech ecosystem. One strategy is to find pure plays in the cloud computing space. This could be the aforementioned bigtech companies that control a large portion of the public cloud market and hybrid cloud strategies or going for niche cloud software companies that are developing more tailored, specific solutions for financial

[8] One exception might be robo-advisors and their automated investment tools, which are considered registered investment advisors (RIAs) by the Securities and Exchange Commission (SEC) and, therefore, "must describe the criteria and methodology used, including the tool's limitations and key assumptions," https://bit.ly/34FNEZf.

applications. To drill down even more into a particular sector of financial services – what Imerman and Fabozzi (2020) refer to as fintech verticals – investors can look for startup companies that are developing cloud-based solutions for digital banking, insurance, or wealth management. For investors looking to make a broad play on the overall cloud computing technology and its long-term growth, they can seek out an ETF that tracks indexes on cloud computing companies.

5.2 For regulators

This is actually a very exciting time for regulators to be exploring applications of new technologies to financial services. Cloud computing aside, for the moment, the next 10 years are going to see major advances in applications of quantum computing, blockchain and distributed ledger technology, IoT, as well as augmented reality and virtual reality being applied to financial services. Returning to the topic of cloud computing, many of the aforementioned emerging technologies rely on, or are fully integrated with, cloud computing platforms. And, as we noted earlier, of all the emerging technologies making their way into financial services, cloud computing is one of the more mature in terms of adoption and utilization. For both of these reasons, financial regulators need to remain vigilant in their ongoing monitoring of how cloud computing is being used by financial services firms, from banks to insurance companies to broker-dealers. Understanding how data is managed, handled, and stored is important for ensuring the integrity of the models that are using the data as well as to protect said data from cyberattacks and breaches. For this reason, cybersecurity in the cloud is likely to continue to be an important issue going forward. Furthermore, as AI models run off the cloud, having a framework for validating not only the models but the processes and the data (inputs and outputs) will be increasingly important for regulators to monitor in their supervisory efforts.

5.3 For startups

Any entrepreneur looking to provide innovations in the fintech space ought to be familiar with the paradigms of cloud computing. That is because fintech startups – unlike the incumbents in the financial services industry – are cloud native. This has many benefits over the incumbents, who quite frankly can learn from their startup competition. One benefit is the agility and flexibility that cloud-based solutions provide the company. The cost-benefit of pay-as-you-use storage is also beneficial to a startup that needs to be careful with every invested dollar of capital. Decisions must be made about whether a private, public, or hybrid cloud should be used; however, again, the ability to pivot from one strategy to another is much easier in a cloud environment than it would be with a data center filled with servers or a basement of mainframe computers. Then deciding what software and/or models are going to be run on in-house hardware versus off the cloud becomes both a strategic and an economic decision. We are likely to see the trend of increasing amounts of software and models run off the cloud. But with that point we should remind startups to consider the risks – operational, cybersecurity, systemic, etc. – associated with being fully dependent on the cloud.

5.4 For incumbent financial institutions

The time is now to migrate from mainframe and server-based system to cloud-based storage and software. In this market environment, where innovation moves at the speed of now, it is imperative to embrace a more agile mentality when it comes to IT systems so as to not lose more ground to startups, which are cloud native and have agility in their proverbial business DNA. That being said, such migrations are not without their risks. Cybersecurity issues, which have been highlighted in this article, must be addressed with contingency plans in place in the event of a breach. Furthermore, relying on one vendor for cloud services is risky from the standpoint that if something happens to that provider it could dramatically affect the institution's operations potentially for a long period of time. There is also the issue of systemic risk, which was not a main focus of this article but is certainly an area that warrants much more examination from academic researchers and regulators alike. Given that the public cloud is essentially an oligopoly – made up of Amazon's AWS, Google's GCP, and Microsoft's Azure (with IBM as a close fourth though their recent strategy seems more focused on a hybrid cloud) – should something happen to one of these companies or their respective products, it could represent a massive shock to the global financial system to the extent that the world's largest banks and clearinghouses are relying on those specific cloud products.

REFERENCES

Flextra, 2020, "2020 state of the cloud report," https://bit.ly/3MGSMxz

Ghule, S., R. Chikhale, and K. Parmar, 2014, "Cloud computing in banking services," International Journal of Scientific and Research Publications 4:6, 1-8

Imerman, M. B., and F. J. Fabozzi, 2020, "Cashing in on innovation: a taxonomy of fintech," Journal of Asset Management 21, 167–177

Jones, H., 2019, "Bank of England calls for 'super shield' against cyber attacks," Reuters, May 14, https://reut.rs/3J5v6k6

Mackey, T. B., A. Mackey, L. J. Christensen, and J. J. Lepore, 2022, "Inducing corporate social responsibility: should investors reward the responsible or punish the irresponsible?" Journal of Business Ethics 175:1, 59-73

Menchaca, J., 2018, "DevOps concepts: pets vs cattle," May 6, https://bit.ly/36fzUVI

Sampson, D., and M. M. Chowdhury, 2021, "The growing security concerns of cloud computing," in 2021 IEEE International Conference on Electro Information Technology (EIT), pp. 050-055

Scott, H. S., J. Gulliver, and H. Nadler, 2019, "Cloud computing in the financial sector: a global perspective," Program on International Financial Systems 2019, https://bit.ly/37sxnYO

Tissir, N., S. El Kafhali, and N. Aboutabit, 2021, "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal," Journal of Reliable Intelligent Environments 7:2, 69-84

Yan, G., 2017, "Application of cloud computing in banking: advantages and challenges," Advances in Economics, Business and Management Research (AEBMR) 23, 29-32

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy specializing in driving digital transformation in the financial services industry. With a growing client portfolio comprising of over 100 global organizations, Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to deliver end-to-end data-driven solutions and fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its Innovation Labs and award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Twitter, Facebook, YouTube, LinkedIn Instagram, and Xing.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
a wipro company