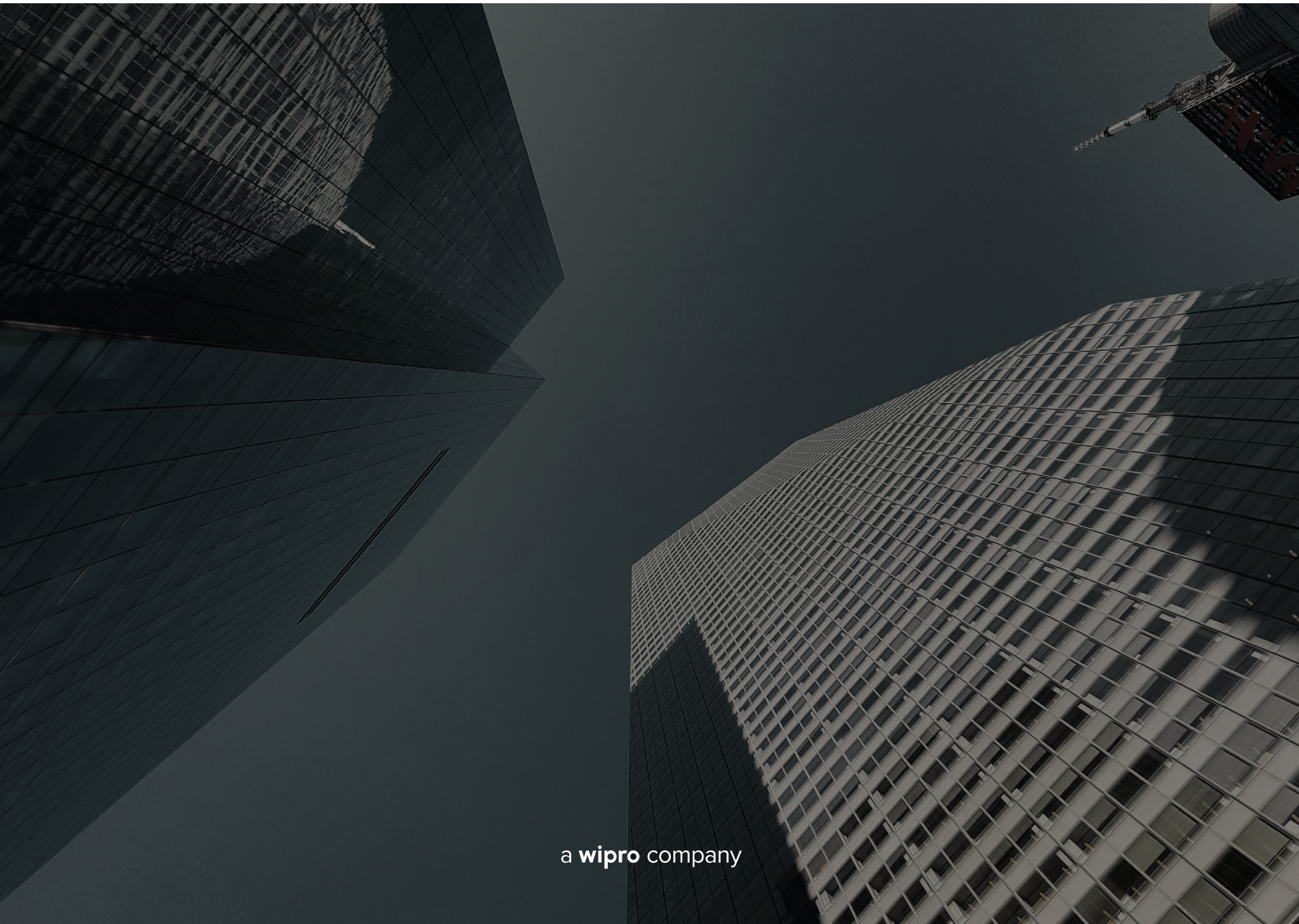
CAPCO

WHEN GOVERNMENTS MOVE FASTER THAN BANKS

LESSONS FROM THE PUBLIC SECTOR'S APPROACH TO CLOUD



a **wipro** company

To unlock the true value of the cloud, banks should learn from the public sector's experiences of cloud adoption, address security concerns as one body and truly use cloud computing for business growth.

Accelerated by the Covid pandemic, the UK Government is investing in cloud technologies at pace.[1] Given strict security requirements and the challenges in attracting tech talent to the public sector, how has the government pursued growth in this area – and what lessons can be learned by the financial services sector? Below we consider four key aspects: cloud cyber-security strategy, technical risk, maximising the value of the cloud and shifts in ways of working.

DEFEND AS ONE

For banks, security is top of the agenda when adopting cloud technologies and fear of cyberattacks has been a factor in slowing the pace of adoption. This hesitance is unsurprising when financial service firms suffered on average 703 weekly attacks per organisation last year.[2] With an arguably even tighter focus on security in order to maintain public safety, the UK Government has tackled this issue using a two-pillar strategy: build organisational cyber resilience (organisation level) and 'defend as one' (central government level).

Founded in 2013, NHS Digital is tasked with transforming healthcare by streamlining and automating data collection within the cloud. The NHS holds data on approximately 53 million individuals and robust security arrangements are therefore vital.[3] Under pillar one of the government's two-pillar strategy and to build their organisational cyber resilience, it developed a four-step process (their Good Practice Guidelines) through which risks can be assessed and controls implemented to maintain security.

Building on this, the 'defend as one' strategy brings together all government organisations as one central body to tackle cyber resilience through shared capabilities and services. This strategy provides timely access to security data and enables collaboration across all government bodies to address cyber security risks, spot patterns of attacks and provide access to expertise. The Government also uses the Cyber Assessment Framework to ensure consistent assessment of risk across government bodies. This centralised strategy has empowered each government body to take ownership of their cloud security and grow their cloud usage more confidently with 47% going as far as using AI to add value to their business.[4]

This approach has worked well in the public sector, but how might the financial services industry respond?

There are some financial services initiatives, but they are not yet as fully inclusive as the UK Government's. The Cyber Security Information Sharing Partnership (CiSP) is a joint industry and government initiative set up to allow UK organisations to share cyber threat information in a secure and confidential environment. Whilst not global or FS specific, this is a free service open to all that can provide a sponsor. There are also several FS specific risk frameworks (e.g. CRI profile, National Cyber Security Centre cloud security guidance), but each use different terminology and structure.

The US-based Financial Services Information Sharing and Analysis Center (FS-ISAC) offers an financial services focussed platform, Intelligence Exchange, for financial service firms to share cyber intelligence alongside training in responding to cyber-attacks. However, platform membership is offered on a tiered basis and is based on institution size, meaning those in the lower tiers don't have equal access to all services and are less incentivised to share. This initiative is only effective should everyone contribute and get equal value from participating.

So what should banks do in order to ensure security of their data? Should they adopt a two-pillared approach? Should the regulators create a mandatory platform for information sharing? There is also the added complexity of ensuring regulatory compliance across borders to consider; how does this affect the process?

Although the existing platforms and frameworks begin to address the issue, ideally the UK financial service sector needs to be part of a global unified approach like 'defend as one' so that it can effectively defend itself from the ever-increasing volume of cyber-attacks and have confidence to move more services to the cloud.

AVOID LOCK-IN

The UK Government also provides guidelines on choosing a hosting strategy that minimises technical risk and on how to manage vendor lock-in. In this vein, HMRC took the strategic decision to move away from big contracts that could lead to lock-in and stick to short contracts that can be replaced when a better technology or commercial offer is available.[5] Signing contracts with both Microsoft and Amazon, they have chosen a multi-cloud approach also reducing potential cloud concentration risk.

Government guidelines suggest those with multi-cloud strategies should plan how to host applications on different platforms and test this regularly to manage technical lock-in.[6] Consistent with the Government's guidelines, Network Rail determined that "technology should not exist in isolation" and invested in solutions that were able to integrate with existing technologies (Azure and a private cloud).[7] This has allowed them to grow by ensuring they have minimised technical lock-in and maximised the potential for future growth.

Complete avoidance of vendor lock in is difficult, but there are steps banks could take to mimic this model by ensuring contracts are of a suitable length or rolling so that they can change their technology strategy in an agile way. Taking advantage of the portability of a cloud native design, where suitable, would allow for workloads to be managed appropriately, keeping this in mind from day one.

USING THE POWER OF THE CLOUD TO ACHIEVE INSIGHTS INTO BUSINESS DATA

UK government bodies are progressing from using the cloud simply as a data centre extension to using it to add real, focussed business value. Clinical data is often unstructured, in multiple formats and inconsistently documented. Through the cloud, the NHS was able to use a natural language processing tool to improve structure in this data, providing insights used to inform diagnostics, in health surveillance and in medical research.[8] It has been estimated that as much as 80% of data in banking is unstructured highlighting the wealth of potential value waiting to be unlocked.[9] Migration to the cloud has enabled the DVSA to create a risk rating algorithm, moving from subjective to objective assessments of MOT testing sites. Aside from the benefit of increasing fraud detection rate, they are now recognised as a technology leader.[10]

The Government has traditionally struggled to recruit in technology, with the private sector offering a more competitive deal, but with tangible shifts towards digitisation, they have attracted talent further fuelling their tech development. Banks will soon begin to struggle to recruit in this area, if they are not already, with more agile fintechs and firms outside of financial services poaching talent such as at Facebook or Apple.

The financial services industry is also starting to use the cloud in more advanced ways. For example, HSBC have been combining access to real time data with AI, moving away from manually forecasting when their ATMs will run out of cash with their new iCash tool.[11] This is done simply by maintaining a dashboard of live data – something that was not possible prior to the cloud. They are not only reducing costs but also reducing risk as they have been able to move away from pre-scheduled cash deliveries that are susceptible to theft. This example is just one of many that could be applied should banks move away from simply using the cloud as an extension to data centre capacity and begin to unlock the potential from its unstructured data, to gain business insight.

WELCOME NEW WAYS OF WORKING

The Office for National Statistics (ONS) migrated to the cloud to improve operational efficiencies. Aside from security concerns, they faced challenges introducing new ways of working despite their ultimate benefits.[12] They believe that engaging more staff from day one could have alleviated some of these challenges but found open communication resolved them. They had multiple channels of communication, agile coaching and a technology week where they discussed all cloud matters both technical and non-technical.

Resistance to change is a challenge faced across industries, but implementing lessons learned from the ONS could ease the transition. Banks should consider this during transformation projects and ensure that staff are provided not only with adequate communication and training but with new career paths that reflect that change in ways of working.

CONCLUSION – SO WHAT NEXT?

The public sector has clearly invested significant amounts of time and money into a cloud-first strategy with some organisations being faster adopters than others. It still has a long way to go before it can be declared a leader in cloud computing, with 67% of organisations saying they allocate only a couple of days a month towards unlocking value from data, and security remaining unsurprisingly a top concern amongst government bodies.

However, they have a clear set of guidelines covering all aspects of cloud adoption and a unified approach with the mantra of being “a defensive force greater than the sum of our parts”.[13] To unlock the true value of the cloud, banks should learn from the public sector’s experiences of cloud adoption, address security concerns as one body and truly use cloud computing for business growth.

REFERENCES

1. Top 10 UK Government Cloud Spending (The stack). https://thestack.technology/top-10-uk-government-cloud-spending/ [Online]
2. Check Point Research. [Online] https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/
3. NHS Digital. [Online] https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/our-strategy
4. UKCloud. [Online] https://ukcloud.com/hub/state-of-digital-and-data/
5. Public Technology. [Online] https://www.publictechnology.net/articles/features/qa-hmrc-tech-chief-how-department-%E2%80%98leading-way-government-cloud-adoption%E2%80%99
6. Gov.uk. [Online] https://www.gov.uk/guidance/managing-technical-lock-in-in-the-cloud
7. Gov.uk. [Online] https://www.gov.uk/government/case-studies/how-network-rail-implemented-its-hybrid-cloud-strategy
8. NHSX Artificial Intelligence: How to get it right. [Online] https://www.nhsx.nhs.uk/media/documents/NHSX_AI_report.pdf
9. FinTech Futures. [Online] https://www.fintechfutures.com/2020/10/unlocking-the-benefits-of-unstructured-data-in-banking/
10. AWS: DVSA Case study. [Online] https://aws.amazon.com/solutions/case-studies/dvsa/
11. HSBC News & Media. [Online] https://www.hsbc.com/news-and-media/hsbc-news/icash-managing-our-atms-with-ai
12. Gov.uk. [Online] https://www.gov.uk/government/case-studies/how-ons-changed-workplace-culture-to-get-the-best-out-of-cloud
13. Government Cyber Security Strategy. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf [Online]

AUTHOR

Jessica Bevan, Senior Consultant, jessica.bevan@capco.com

CONTACTS

Peter Kennedy, Partner, peter.kennedy@capco.com
Lawrence Aggleton, Managing Principal, lawrence.aggleton@capco.com

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