

GET YOUR HEAD IN THE CLOUDS

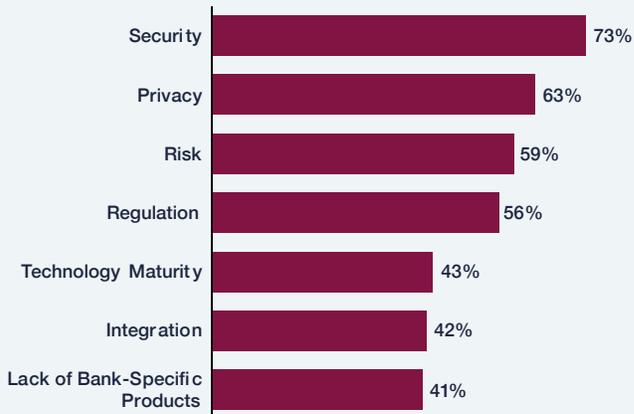
In order for banks to fully realize the benefits of the cloud, back-office payments need to be added to the list of banking functions managed in the public cloud. Benefits of the cloud are well known, and there are already a plethora of front-office and non-core banking functions in the cloud. But as margins shrink and the pressure to innovate increases, the full benefits of the public cloud including lower cost to begin project, improved operating efficiency, scalability, and automated maintenance must be embraced to strengthen high-performing teams that covet agile, fast-fail, and high ROI projects.

You’ve heard the reasons people are skittish to move to the public cloud, and many of them involve the fear of the unknown. The main three risks cited by banks are security, privacy, and (what we’re calling) the risk of risk itself. We wanted to tackle these in two major categories:

1. **Data Protection** and
2. **Regulatory Risk.**

Cloud-Wary

U.S. banks that are avoiding cloud technology say security concerns are the chief reason.



Source: Forrester
<https://wc9234aww.americanbanker.com/news/is-it-almost-time-to-put-core-processing-in-the-cloud>

In the traditional model of data protection, safety means keeping data infrastructure as close to home as possible so everything is done in-house (see what we did there?). This requires significant capital expenditures to maintain the security infrastructure and software security development. But, is this the best way to handle data? In many cases, it’s not. Verizon’s latest **Data Breach Investigations Report** shows that “sloppiness” causes many data breaches. Moving non-core functions into the public cloud will reduce that sloppiness around security and data protection.

“The Verizon DBIR beats the same security drum each year: Many of these attacks could have been prevented with basic security

hygiene. System administrators need to update server software, including operating systems, web applications, and plugins.” - InfoWorld

In a public cloud model, the provider maintains the physical security, hardware & OS-level security therefore eliminating many of the “hygiene” risks mentioned in the Verizon report. Plus security capital costs become Operational Expenditures correlated directly to revenue. Finally, the best-practice security models including cryptographic keys managed by Hardware Security Modules, and dual-factor authentication become the norm for handling your company’s data.

In a public cloud model, the provider maintains the physical security, hardware & OS-level security, therefore, eliminating many of the “hygiene” risks mentioned in the Verizon report. Plus security capital costs become Operational Expenditures correlated directly to revenue. Finally, the best-practice security models including cryptographic keys managed by Hardware Security Modules, and dual-factor authentication become the norm for handling your company’s data.

The second major concern holding banks back from moving payments to the cloud is Regulatory Risk. There are worries that compliance standards aren’t upheld in the public cloud, but major cloud providers like **Amazon Web Services (AWS)** now offer compliance certifications that ease regulatory and reporting requirements for their clients. The AWS platform also has built-in, audit-friendly service features for PCI, ISO, SOC, and other compliance standards. Using the AWS platform, banks maintain control of their data.

“AWS gives customers ownership and control over their customer content by design through simple, but powerful tools that allow customers to determine where their customer content will be stored, secure their customer content in transit or at rest, and manage access to AWS services and resources.” - Amazon Web Services

In order to compete with neo-banks and respond to threats by disruptors, banks are inevitably going to have to move more and more non-core functions like payments into the public cloud. The cloud allows banks to reallocate spend toward innovation, forge partnerships with cloud-based providers, avoid fighting for resources with internal stakeholders, and position themselves to innovate and compete in ever-changing regulatory landscape. But the public cloud, with its improved security, operating efficiency, data analytics, and collaboration, is the next logical evolution and competitive requirement.

Modo is the better, faster way to connect payments systems. By bringing payments to the public cloud, our payments utility requires low investment, delivers faster time-to-market, is highly adaptive and massively scalable while delivering the economic and operational benefits of public-cloud computing. The Modo utility creates true interoperability by using a state machine that can connect any payment systems together without requiring changes to the existing systems. This means you can launch innovations with minimal technical debt to continue bringing new ideas to market. Our utility is PCI compliant, allows you to maintain control of your funds as we do not hold, touch, or move money, and uses AWS to assure data security.

And don’t just take our word for it. Modo has brought one of the largest US-based banks to the public cloud allowing them to launch innovative applications leveraging their legacy infrastructure, and positioning them for even greater success in the future. Let’s chat about bringing you into the Cloud.

We’re a team of **#paymentsgeeks** that are dedicated to doing the most good for the most people by reducing friction in payments. We would love to enable interoperability and reduce payments friction for you. **Reach out to us.**