RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 039 – 19 April 2022

Securing Financial Institutions: Emergence of Open Banking

By Adam Palmer & Wias Issa

SYNOPSIS

As the global financial industry continues to innovate, concepts such as open banking have emerged, creating opportunities to improve consumer banking experiences and accelerate growth. While innovative, they have introduced new data security risks, which require equally innovative security strategies to mitigate them.

COMMENTARY

THE CONTINUED spread of cyber crime attacks on banks in Singapore, and on banks in the Ukraine just before its invasion, highlight the national security risks facing the financial services sector as critical infrastructure. Simultaneously, the global pandemic has accelerated the need for financial institutions (FSIs) to undergo digital transformation accelerating new initiatives like "Open Banking" and cloud adoption.

These innovative approaches, however, also give rise to new data security issues. Best practices for addressing these new data security concerns were highlighted in the recent regulations published in Singapore related to application security.

The Emergence of Open Banking

The global regulatory cyber security landscape for FSIs continues to evolve. The enactment of the European General Data Protection Regulation (GDPR) and its broadened security requirements inspired a global surge of new data privacy laws, including the Singapore Personal Data Protection Act (PDPA), and the California Consumer Privacy Act (CCPA) in the United States. These regulations now apply broad privacy and security requirements to many organisations processing personal data. Z

Data security, and especially security in emerging technologies, is a common focus of these new regulations. In the financial services sector, there is increasing attention to security in areas such as cloud infrastructure and "Open Banking," which provides third-party service providers easier access to financial data (see Figure 1 below).

Figure 1: Open Banking Overview

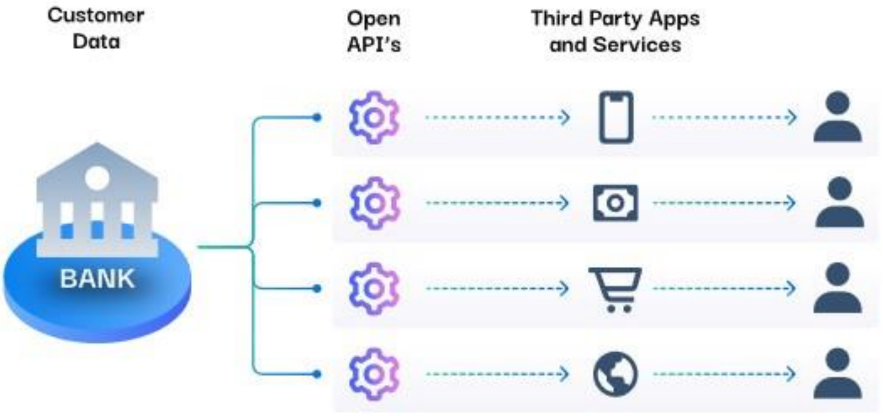

Figure 1 – Source: Ubiq Security

In June 2021, the Monetary Authority of Singapore (MAS) released an Advisory on "Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption" and in January 2022, the US-based National Institute of Standards and Technology published a draft guidance on Cybersecurity Considerations for Open Banking Technology and Emerging Standards.

FSIs are undergoing a digital evolution in open banking and cloud adoption. Offering new business opportunities and value for customers with improved service options, especially where physical access to banks is limited. However, the emergence of these new platforms also requires a renewed focus on integrated security standards and processes within the IT architecture.

The Expanding Data Security Challenge

To support open banking, FSIs need to expose application programming interfaces (APIs) and allow approved third-party providers to access sensitive consumer financial data.

Open banking is often closely tied with a growing transition to cloud-based infrastructure (where customer data is stored and/or processed by external, third-party cloud providers), which provides flexibility, scalability, and cost savings. However, when adopting these new platforms, FSIs need to ensure that the security framework for these new approaches is also in line with regulatory requirements, internal policies, and protects customer privacy.

The emergence of open banking and the transition to cloud-based infrastructure creates a complex web of new relationships for FSIs. For open banking, FSIs need to open access to sensitive data to third-party service providers, but also ensure they are protecting that data and maintaining regulatory compliance.

Cloud computing creates additional security complexity as FSIs are dependent on infrastructure that they do not own and do not fully control.

Creating a Security Architecture

Third-party applications with legitimate access to FSIs through APIs are among the greatest risks to data security. If a third-party application or API is compromised, sensitive customer and financial data may be exposed to an unauthorised user. Security reviews for third-party vendors and service providers are essential to minimising an organisation's supply chain risk.

However, this approach is generally unscalable and ineffective, as it can be arduous, expensive, and at times superficial, leaving FSIs unable to fully eliminate all data security risks. FSIs should instead work to minimise the risk and impact of a supply chain breach by implementing granular access management policies and encryption for sensitive customer data.

Data encryption is often a good solution for minimising data security risk and most organisations rely on cloud-native, storage data encryption controls. However, these controls are mostly ineffective against modern threats, as they implicitly trust authorised user accounts, which are often compromised by attackers.

The previously noted MAS Security Advisory on a shared security responsibility in the cloud (see Figure 2 below) suggests that FSIs should be mindful of their own responsibility for, and control over, data security.

More specifically, Section 22 of the Advisory supports a new application-level encryption strategy and *"Bring-Your-Own-Key" (BYOK) and "Bring-Your-Own-Encryption" (BYOE)*. BYOK allows financial services organisations control and management of cryptographic keys that are uploaded to the cloud to perform data encryption. In BYOE, data is encrypted before it enters the cloud, and the keys are not transferred to the cloud.

Figure 2: Shared Security Model

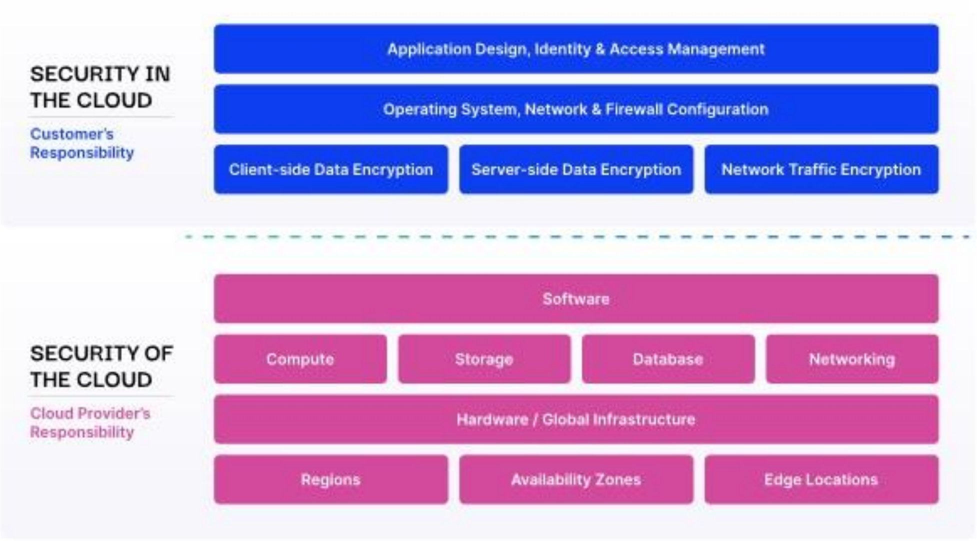
SECURITY IN THE CLOUD
Customer's Responsibility
Application Design, Identity & Access Management
Operating System, Network & Firewall Configuration
Client-side Data Encryption
Server-side Data Encryption
Network Traffic Encryption
SECURITY OF THE CLOUD
Cloud Provider's Responsibility
Software
Compute
Storage
Database
Networking
Hardware / Global Infrastructure
Regions
Availability Zones
Edge Locations

Figure 2 – Source: Ubiq Security, adapted from AWS' Shared Security Model

What FSIs Can Do To Protect Themselves

There are at least six steps that organisations can consider in developing a secure approach to cloud and open banking:

- Adopt mature policies, standards, and procedures to provide the necessary requirements and guidance for new platforms;
- Create an inventory of applications and assign a criticality rating to each application based on risk exposure;
- Define minimal, security requirements based on risk level that must be adhered to when developing and deploying new applications and systems;
- Expand the capabilities of IT and security teams to build and support application security capabilities;
- Focus on integrating security into all application and cloud architecture development processes; and
- Implement granular, role and attribute-based access control and application-level encryption into applications.

A Security-by-Design Strategy

The evolution to open banking and cloud computing provides FSIs with a great opportunity for innovation. However, there is a need to also design security that meets evolving business and regulatory requirements. Recent supply chain cyber attacks have generated a renewed focus on how cyber threat actors can also leverage relationships with trusted service providers to attack companies.

As FSIs re-architect their infrastructure with emerging technologies, "security-by-design" is essential for enterprise-wide data security and regulatory compliance.

Organisations should ensure that they can protect data in these new environments, which requires a review of the overall architecture to fill the gaps sometimes left by traditional security strategies.

FSIs should use security strategies, as described above, to create a robust set of "security-by-design" principles: Implement security throughout the lifecycle of all systems and applications; build an enterprise-wide security architecture; and integrate security reviews into all critical processes.

Adam Palmer is an Adjunct Senior Fellow at the Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. He also the Chief Information Security Officer (CISO) at First Hawaiian Bank in the US.

Wias Issa is a cybersecurity expert with concentration in threat response countermeasures and cryptography. He has held several executive level positions at Symantec and Mandiant in Singapore, Japan, and the US. He is CEO of Ubiq Security in the US.