Fortifying fintech

A board-level blueprint for prioritised cyberdefence

Part I – Identifying cybersecurity priorities for non-technical fintech leaders

Abstract

As the region sets out on an ambitious growth path for fintech, cybercrime remains a board-level priority across the financial sector. Trust in fintech is heavily reliant on solution providers' ability to ward off cyberattacks and capably protect end users' data. Recent fintech breaches such as the Lykke cyberattack in June 2024 and the Revolut hack in July 2023 have rattled stakeholders' confidence.

This article, the first in PwC's four-part thought-leadership series, provides actionable insights to fintech leaders on the core technology domains to prioritise in their cybersecurity purview. A baseline fintech architecture is established and validated against the practical case of a digital wallet executing a payment process. An objective analysis of the baseline architecture is then performed to distil three focal areas crucial to fintech cybersecurity. The author argues that these focal areas warrant ongoing board oversight in order to ensure sustained cyber assurance, mitigate risks, and to elevate public trust in fintech.

Introduction

Fintech in the MENA region is poised for robust growth, built on the foundation of visionary national transformation agendas, a strong regulatory environment, and a young and ambitious population. The MENA fintech market size is estimated at US$1.51 billion in 2024, and is expected to reach $2.40 billion by 2029, with a healthy annual growth of 9.71%.

With strong government ambition setting the region's fintech vision, the growth roadmap stems from initiatives strategically dispersed at various financial hubs. These range from Abu Dhabi Global Market (ADGM) and Bahrain Fintech Bay to Fintech Saudi and the Dubai International Financial Centre (DIFC) FinTech Hive.

National fintech strategies have also been established by Bahrain, Saudi Arabia, Qatar, and the UAE. Further fintech impetus is provided by government-sponsored accelerators and incubators such as regulatory "sandboxes".

[1] https://www.lykke.com/incident-updates/faq
[2] https://www.bloomberg.com/news/articles/2023-07-09/thieves-stole-20-million-via-revolut-us-payment-flaw-ft-says
[3] https://www.mordorintelligence.com/industry-reports/mena-fintech-market

Elevating trust in fintech: The pivotal role of cybersecurity

End users play a major role in the MENA fintech growth story. A predominantly young user base with a tech-first mindset to their finances is enabling fintechs to scale growth, riding on already well-established infrastructure for internet and mobile connectivity.

However, fintech's MENA growth path is not unhindered. Most of the MENA population, as much as 83%, still follows traditional, time-tested approaches to money management, with roots intact in legacy banking systems.

Elevating fintech trust requires a paradigm shift in users' mindsets that encourages a pivot from traditional banking towards fresher fintech alternatives. Trust in fintech sits upon several pillars: Brand equity, regulatory compliance, transparent billing plans, alliances with established financial bodies, financial stability, and data privacy. The most pressing issue has consistently been **cybersecurity**.

Cybercrime undermines trust in fintech, as illustrated by recurrent instances of cyber fraud in the sector. PwC's report delves into recent fintech cyber incidents that rocked market confidence in the sector.

Cybercrime's omnipresent, always-on character warrants board-level oversight in the context of business survival, as opposed to a regulatory afterthought. Fintechs' tech-first approach to managing money means that a robust cybersecurity strategy anchored in clear governance and accountability is a board-level imperative.

Establishing a board-level blueprint for prioritised cyberdefence

Boards, venture capitalists (VCs), and executive leaders have traditionally struggled to quantify the business implications of cybersecurity. CISOs rely on metrics such as Return on Security Investment (RoSI) and compliance with regulatory frameworks from bodies including the Saudi Data and AI Authority (SDAIA), Saudi Central Bank (SAMA), and Central Bank of the UAE to convey cybersecurity performance in business language.
Fintech boards can do more to deepen their oversight. Whilst deep technical reviews would be a disproportionate response, boards should instead opt for a prioritised approach – one that reviews the cyber postures of their most crucial technical elements.

[4]https://www.imf.org/en/Publications/fandd/issues/2023/09/unleashing-mideast-fintech-amjad-ahmad#:~:text=Still%2C%20only%2017%20percent%20of,percent%20in%20the%20United%20States.

Conceptualising a baseline fintech architecture

While no two fintech solutions are alike, and each solution provider operates out of a unique architecture comprising user interfaces, business logic, and capabilities, a baseline architecture outlining the core elements is necessary for understanding fintech functionality.

Most fintech solutions may be broken into three broad layers:

01

The **user layer** comprises the end user accessing the fintech solution through a mobile application or a browser.

02

The **core layer**, comprising the fintech solution including its business logic, database, cloud infrastructure, and middleware.

03

The **external layer** comprises third parties such as banks and regulators with which the fintech solution interfaces.

The baseline fintech architecture and associated flows of user data are illustrated in Figure 1.1.

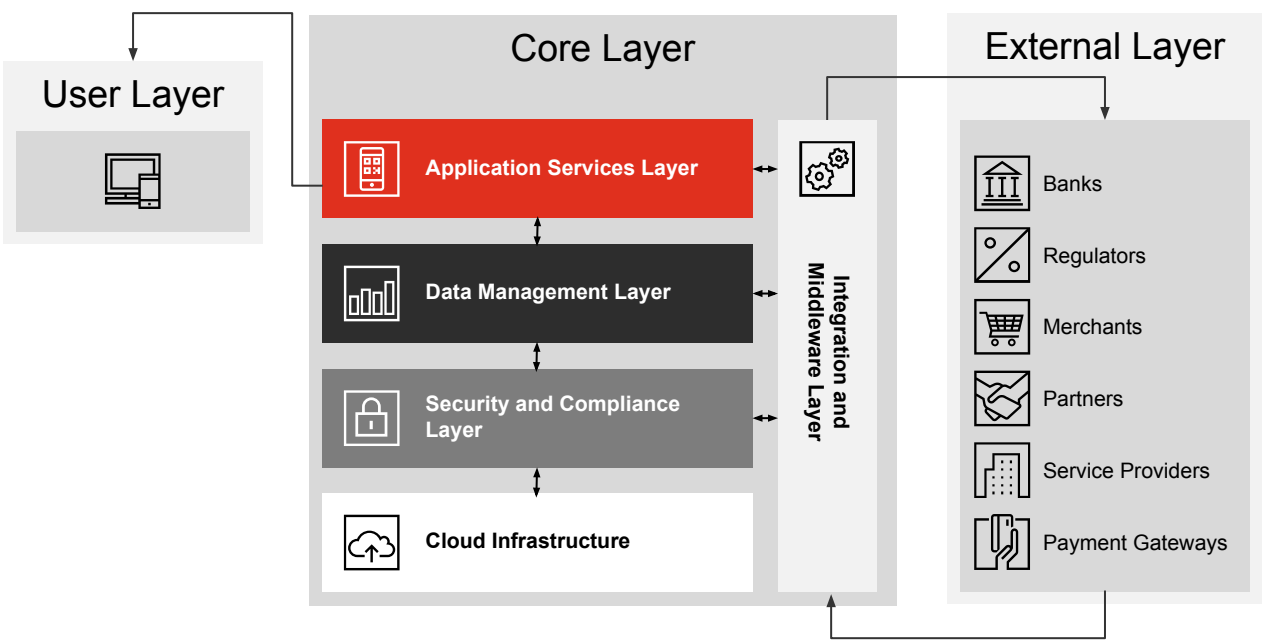


Figure 1.1: Conceptualising a baseline fintech architecture

The layers of the baseline fintech architecture are described in Table 1.1

Description	Components
User layer: The user layer aims to provide a secure, responsive, and user-friendly interface that meets the demands of customers while ensuring a smooth connection to the underlying core systems.	1. **Devices:** Users access fintech services through devices such as smartphones, tablets, and computers. 2. **Interfaces:** Mobile applications, web portals, or other user interfaces that allow users to interact with the system, perform transactions, and access services. 3. **User experience:** This layer is critical for ensuring a seamless and intuitive experience, as it directly impacts user satisfaction and engagement.
Core layer: The core layer forms the backbone of the fintech architecture. It outlines the business logic of the fintech solution, stores and manages data, and includes the cloud infrastructure layer. Cybersecurity solutions and APIs are part of this layer.	1. **Application services layer:** This includes the business logic and applications that provide financial services such as payments, lending, investments, insurance, etc. It also involves the management of user accounts, transaction processing, etc. 2. **Data management layer:** This level handles the storage, processing, and management of data. It includes databases, data warehouses, and big data technologies that store transactional data, user data, and financial records. Data governance, data privacy, and data integrity are vital components of this layer. 3. **Security and compliance layer:** This layer includes security measures such as encryption, authentication, fraud detection, and access controls. Compliance mechanisms are also embedded to adhere to regulatory requirements such as KYC (Know Your Customer), AML (Anti-Money Laundering), and data protection regulations like the KSA PDPL, UAE CPS, and DIFC Data Protection Law. 4. **Cloud infrastructure:** The infrastructure component supports the deployment of the above layers in a cloud environment, allowing scalability, flexibility, and resilience. Cloud infrastructure can include public, private, or hybrid cloud setups, depending on the specific requirements of the fintech platform. 5. **Integration and middleware layer:** This component acts as the glue that connects various systems, services, and external entities. It facilitates communication between different applications, services, and layers within the core architecture and with external entities. Middleware components include APIs, message brokers, and service buses.

[5]https://www.law-middleeast.com/gccs-data-privacy-regulations-decoded/#:~:text=Processing%20personal%20data%20is%20prohibited,whom%20the%20data%20is%20disclosed.

The layers of the baseline fintech architecture are described in Table 1.1

Description	Components
External layer: The external layer comprises external entities that interact with the fintech system. These entities are essential for providing comprehensive financial services and maintaining compliance	1. **Banks:** Banks enable payment processing, hold customer funds, and other services integrated with the fintech platform. 2. **Regulators:** Regulatory bodies oversee compliance with legal and regulatory requirements, such as financial conduct authorities or central banks. 3. **Merchants:** Businesses that use the fintech platform to accept payments, provide services, or engage with customers. 4. **Partners and service providers:** Third-party vendors and partners that offer added functionalities such as fraud prevention, analytics, or additional payment methods. 5. **Payment gateways:** Payment gateways are crucial in enabling the processing of transactions between users and merchants, ensuring that funds are securely transferred in real-time.

Case study: Distilling cybersecurity cruxes from the baseline fintech architecture

While each component in the baseline fintech architecture has specific cybersecurity needs, there are elements critical enough to secure fintech functionality that they warrant regular board-level oversight.

Consider the case of a digital wallet – a platform that stores and manages payment methods for transactions. The MENA digital payments market size is estimated at $226.53 billion in 2024, expected to reach $380.86 billion by 2029.

STC Pay (Saudi Arabia), Payit (UAE), ValU (Egypt), Apple Pay (US), and Google Pay (US) are some of the digital wallets commanding a broad user base in the region.

Consider the case of a user initiating a payment transaction through the digital wallet. Let us delve into the underlying technology architecture and assess the transaction process thereafter.

[8]https://www.verifiedmarketresearch.com/product/digital-wallets-market/#:~:text=Digital%20Wallets%20Market%20Size%20and,forecasted%20period%202024%20to%202030.

Validating the baseline fintech architecture

It is beneficial to start by validating the baseline fintech architecture in the context of a digital wallet. We will analyse the digital wallet by mapping it to the layers of the baseline fintech architecture.

→ User layer:

Users access digital wallets through smartphones, tablets, and wearables. Apple Pay, for instance, is integrated into iOS devices such as iPhones, Apple Watches, and iPads, while Google Wallet is accessible on Android devices.

→ Core layer:

Application services layer:

Payment processing, tokenisation, and transaction management are some of the business processes of the digital wallet that are defined in the application layer.

Data management layer:

User identity data, payment information, transaction histories, and data from integrated apps, among other types, is stored securely in this layer.

Security and compliance layer:

Cybersecurity measures such as encryption, two-factor authentication, and biometric verification are applied across the digital wallet. In the back end, cybersecurity solutions like firewalls, security information and event management (SIEM) solutions, and anti-malware solutions are deployed. Transaction monitoring, device fingerprinting, and geolocation are some of the mechanisms applied to prevent and block fraudulent transactions.

Cloud infrastructure:

The back-end services of the payment application relies on cloud infrastructure – such as Amazon Web Services, Microsoft Azure, and Google Cloud – to offer scalability, flexibility, and high availability services. Depending on the unique outsourcing model with the cloud service provider (CSP), the digital wallet may have an infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), or software-as-a-service (SaaS) cloud deployment. Cloud services such as virtualisation and cloud orchestration are implemented in this layer.

Integration and middleware layer:

Digital wallets connect through APIs with banks, payment networks, and merchants.

- **Bank-specific APIs** allow digital wallets to add new cards, share transaction data, authenticate, and authorise user transactions.
- **Payment network APIs** from the likes of Visa and Mastercard allow digital wallets to process payments with merchants and between users.
- **Merchant-specific APIs** allow vendors to accept payments from the digital wallet on their websites, apps, or physical stores with a card reader (POS terminal).

[7] https://www.microsoft.com/en-us/security/business/security-101/what-is-siem#:~:text=Security%20information%20and%20event%20management,threats%20before%20they%20disrupt%20business.
[8] https://www.redhat.com/en/topics/automation/what-is-cloud-orchestration

Validating the baseline fintech architecture

The digital wallet interfaces with a number of external entities:

External layer:

Banks: Digital wallets connect with banks via APIs to link accounts or cards and authorise payments.

Payment networks: Digital wallets use APIs from payment networks to process transactions and ensure compliance with payment standards, enabling secure payment processing.

Merchants: Digital wallets interface with merchants through APIs to facilitate payment processing, manage transactions, and support customer engagement tools.

Service providers: Digital wallets integrate with third-party service providers through APIs to enhance functionality such as fraud detection, identity verification, and user analytics.

Payment gateways: Digital wallets connect with payment gateways via APIs to securely process transactions and handle payment authorisations.

Regulators: Regulatory reporting to compliance authorities is carried out through relevant APIs.

Figure 1.2 represents the mapping of the digital wallet to the baseline fintech architecture

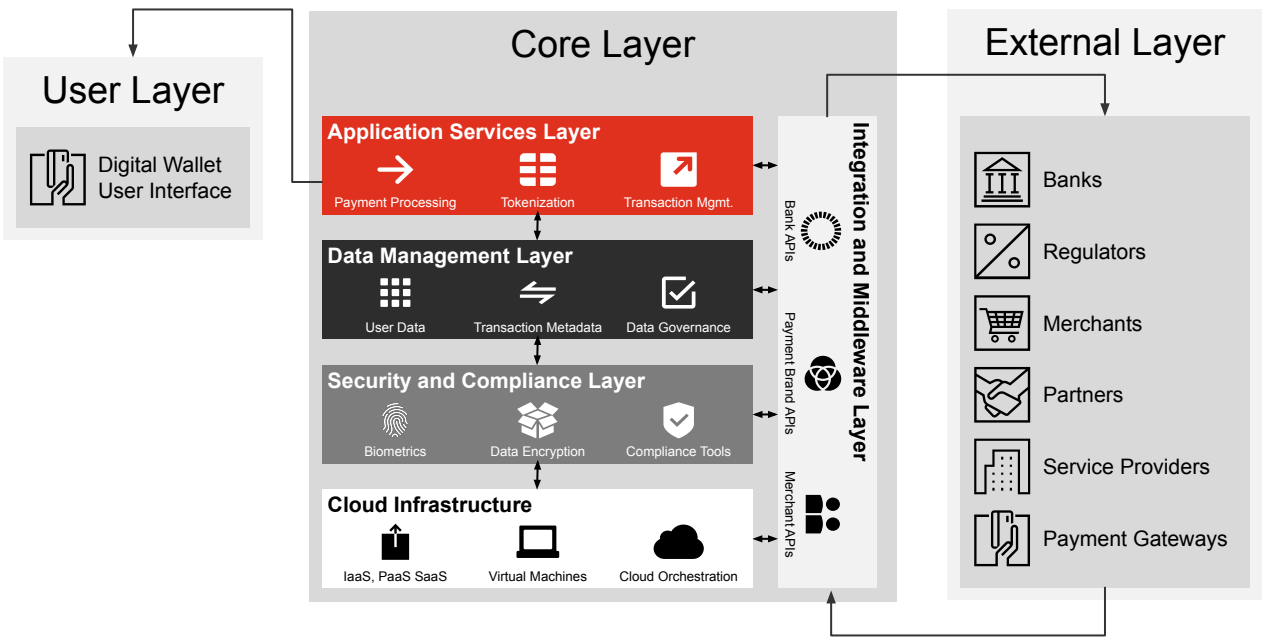


Figure 1.2: Mapping the digital wallet to the baseline fintech architecture

The mapping confirms that the baseline fintech architecture successfully accommodates the various components of a digital wallet.
The next step furthers the analysis by evaluating a payment process in the context of the baseline fintech architecture.

Analyzing a digital wallet transaction against the baseline fintech architecture

Consider a user who wishes to make a payment using a digital wallet. The process involves several steps that span different layers of the fintech architecture:

01

Payment initiation at the user layer:

The user initiates the payment via the digital wallet app installed on their mobile phone (user layer). This step involves the identification, authentication, and authorisation of the user, collecting user inputs (such as which credit card to use), and initiating a request for payment parameters such as the amount to be paid. Biometrics are commonly used to identify and authenticate the user in this step.

02

Payment processing in the core layer:

The payment request is then processed by the digital wallet in the core layer. The application services layer validates the transaction, the data management layer retrieves and verifies user data, and the security and compliance layer ensures that the transaction complies with regulatory requirements. The integration and middleware layer facilitates communication between different components, ensuring the transaction is processed efficiently and securely.

03

Payment completion at the external layer:

The digital wallet communicates with the payment gateway, which in turn communicates with the customer's and merchant's banks to initiate the payment. Necessary APIs are triggered to communicate with banks and payment brands to verify the availability of funds to complete the payment, and to obtain all necessary transaction authorisations. The core system must securely transmit the payment request to these entities, where it is processed and confirmed. Any issues in this final stage could result in failed transactions or security breaches.

The transaction details are consolidated and funds are transferred from the user's account to the merchant's account. Transaction details are updated in the digital wallet, and a payment receipt is issued to the user.

Figure 1.3: Analysing the digital wallet payment process against the generic fintech architecture

Launch and payment initiation

1. User lunches the digital wallet and select payment method (e.g., credit card, and bank account)
2. User is authenticated
3. User selects the merchant or enters payment details
4. User initiates the payment by confirming the amount and payment method

Payment completion

1. Digital wallet receives the transaction status
2. User receives confirmation of payment
3. Funds are transferred from the user account to the merchant
4. Transactions details are updated in the digital wallet
5. User receives a receipt or notification of the completed transaction

Interfacing through payment gateway

1. Digital wallet communicates with the payment gateway
2. Payment gateway sends request to bank of payment network
3. Bank or payment network verifies the transactions details
4. Transaction is authorized or declined based on verification

Establishing the Fintech Fortification Triad

Distilling the cybersecurity cruxes from the Baseline Fintech Architecture

An end-to-end analysis of the transaction process flow reveals three crucial themes that are pivotal to its secure completion, one from each of the three layers of the baseline fintech architecture. Successful compromise of any one of these pillars could have significant consequences that are likely to impact the survival of the fintech solution. These themes, codenamed the Fintech Fortification Triad, constitute a prioritised cyberdefence blueprint for fintech boards:

1. The Gatekeeper
2. The Middle-Man
3. The Treasurer

It is imperative that board members maintain a continued review of the Fintech Fortification Triad in order to sustain and elevate public and regulatory trust in their solutions.

Figure 1.4: The Fintech Fortification Triad that mandates ongoing board-level oversight for sustained cyberdefence

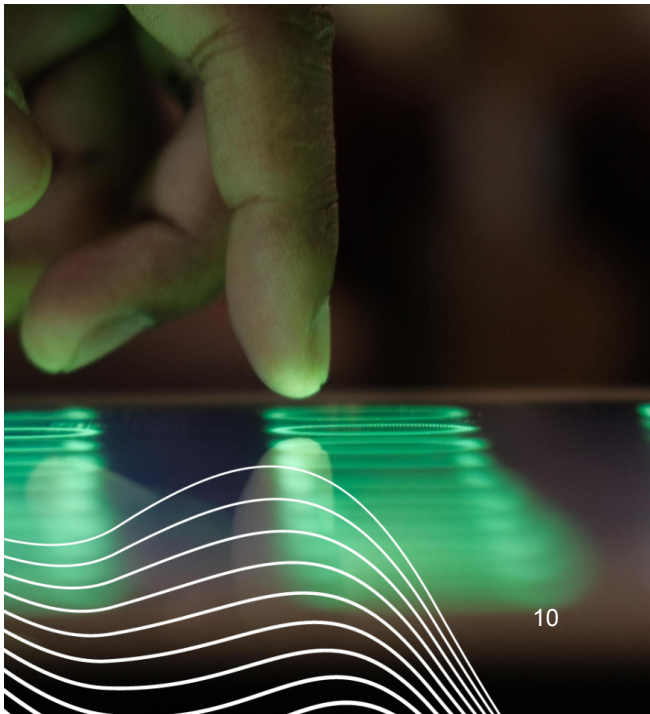
1	**The Gatekeeper** Identity and Access Management	2	**The Middle-Man** Application Programming Interfaces (APIs)	3	**The Treasurer** Payment Gateway Integration

Drawing a board-level blueprint for prioritised cyberdefence

01

The Gatekeeper (user layer) – Identity and access management

The first, most crucial step to secure payment processing is verifying the identity of the user. Identity management serves as the primary defence against unauthorised access and fraud. The integrity of identity management is crucial to fintech's secure functioning. An identity breach could allow malicious actors to impersonate legitimate users, leading to unauthorised transactions, loss of personal data, and significant financial penalties.
Identity management includes mechanisms such as multi-factor authentication (MFA), biometric verification, and secure password protocols.



02

The Middle-Man (core layer) – Application programming interfaces

Application programming interfaces (APIs) are connectors facilitating communication between different components of the fintech ecosystem, both within the core system and with external entities. They enable seamless data exchanges between the user interface, core processing systems, and third-party services such as banks or payment gateways. If compromised, an API can serve as an entry point for attackers to access critical systems, steal data, or disrupt services.

APIs are central to fintech functionality, making them a critical building block to be monitored in the board's prioritised cybersecurity plan.

03

The Treasurer (external layer) – Payment gateway integration

Payment gateways are the final step in the transaction process, where the actual transfer of funds occurs. They interface with banks, credit card processors, payment brands, and other financial service providers to execute transactions. Payment gateway vulnerabilities, if exploited, can lead to severe consequences including fraudulent transactions, financial losses, and damage to the fintech's reputation.

What's next?

This article, the first in PwC Middle East's four-part series, highlights the need for fintech boards to augment business-driven cybersecurity KPIs with a prioritised technical angle. The article identified three crucial cybersecurity pillars that must be overseen by fintech leaders to foster trust and mitigate cyber risks. Codenamed the *Gatekeeper*, the *Middle-Man*, and the *Treasurer*, the article argued that these crucial pillars must be addressed in any board-level report on fintech cybersecurity.

Our upcoming articles in this series will focus on each of the critical pillars, and further decode their role in **fortifying fintech**.

Author

Praveen Joseph Vackayil

Cybersecurity and Digital
Trust Senior Manager

Contributors

Fady Chalhoub

Cybersecurity and Digital
Trust Partner

Samer Omar

Cybersecurity and Digital
Trust Leader

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with nearly 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Established in the Middle East for 40 years, PwC has 24 offices across 12 countries in the region with around 8,000 people. (www.pwc.com/me). PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/ structure for further details.