AUJAS CYBERSECURITY | NSE NSEIT

SECURING THE DIGITAL BANKING ECOSYSTEM WITH API SECURITY & GOVERNANCE

NEED FOR DIGITAL TRANSFORMATION IN FINANCIAL INSTITUTIONS

Digital transformation is not only reshaping global financial institutions but also fundamentally changing the way banking is perceived by the end customers. As per the recent studies, majority of the banking customers are likely to adopt digital financial transactions in the course of next five years. In fact, customers are already in tune with digital technologies in other industry domains such as retail, entertainment, etc. Thus, as soon as a streamlined and user-friendly commercial transaction platform is made available, customer adoptions would take place at a rapid pace and those lacking in efforts for digitisation of the process would be left far behind.

One of the prime reasons for this ongoing transformation is the emergence of digital payment platform providers. These FinTech companies take advantage of customer preference to digital experiences in day to day lives and are free from the legacy systems and manual operating models of traditional banking organisations.

Similarly, transaction cost reduction is also one of the main factors driving the need for this transformation. Since the cost of manual processing is much higher to digital processing, when banks implement the right digital solution to support the transformation, they can realize ROI very quickly.

Compliance is another issue which can be tackled by this transformation. As banking regulations are complex and keep evolving rapidly, legacy banking systems are not able to address these ever-changing requirements. Digital channels make it easier for the banks to keep in line with the regulations and maintain litigation readiness.

TRENDS IN DIGITAL BANKING

Artificial Intelligence (Chat Bots)

Banking industry is adopting artificial intelligence with several applications that makes real impact on banking ecosystem. These applications are used for customer relationship management, identity authentication, fraud detection, anti-money laundering, controlling risk and many operational aspects by the banking organizations. Applications like chat bots, AML pattern detection and fraud detection would revolutionize banking ecosystem.

Robotics

With understanding the unique advantages of robotics like cost efficiency and improving productivity, Banks are exploring to use robotic process automation in their systems for digital transformation.

API Banking

API banking enables banks and other financial organizations to expose their products and services through third party applications. This would help banks to provide services quickly to customers along with the flexibility for product customization. Open APIs play a significant role in providing banking services with high availability through third party service integration.

IOT Enabled Payment Devices

In this era, Internet of Things is attractive for banking and financial organizations to provide advanced payment experience with a variety of payment methods, the use of payment applications, tracking devices, NFC chips and sensors etc. Banks have already started accepting payment using smart devices and are looking at more innovative payment solutions leveraging IOT enabled payments.

BENEFITS OF DIGITAL BANKING INITIATIVES

1 Ease of Banking

Internet connection has enabled banking benefits to one and all. Using Smartphone apps, customers from both urban and rural and locations can check their account balance, transfer funds, check transaction history, raise support issues, etc. Thus, improving customer experience, satisfaction and service.

2 More than Websites

Banks have moved a step further by introducing added features to the websites, apart from the basic banking services, such as financial planning tools, loan calculators, etc.

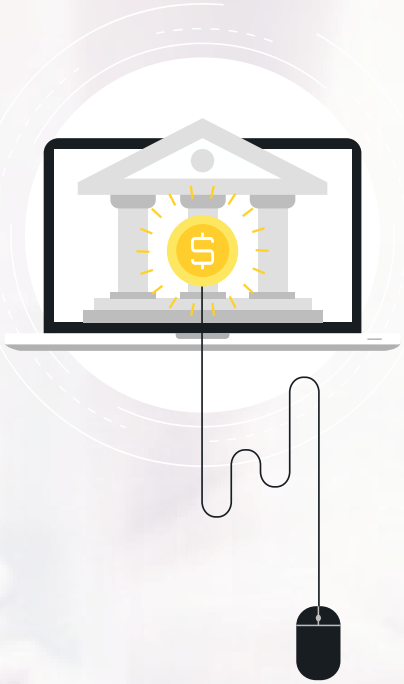
3 Direct Connect with Customers

Reduction in intermediation costs since banks can directly deal with customers, reducing third party service providers. This would help the banks to strengthen the direct relationship with customers and to improve the time to market.

BENEFITS OF DIGITAL BANKING INITIATIVES

4 **Mobility of services**

Ease of Virtual banking for customers, as they have access to Banking services at the tip of their fingers by use of mobile apps/websites thus enabling easier banking operations and services.



5 **Cost effective solution:** With mobility and convenience, costs for banks and customers have reduced, in addition to the less human errors due to automations via online banking.

6 Banks have put in efforts and wisely invested in adopting **Digital Strategies** to compete with the non-banking sectors.

Example: 'Augmented reality' technology, initiative by Common Wealth Bank of Australia, through a mobile app to help inhabitants buy home/property.

7 Banks are helping customers to make informed decisions in their digital journey using **Advanced data analytics** and big data, specifically in Marketing and Channels.

Example: Bank of England uses advanced analytics units to develop and apply advanced analytical techniques

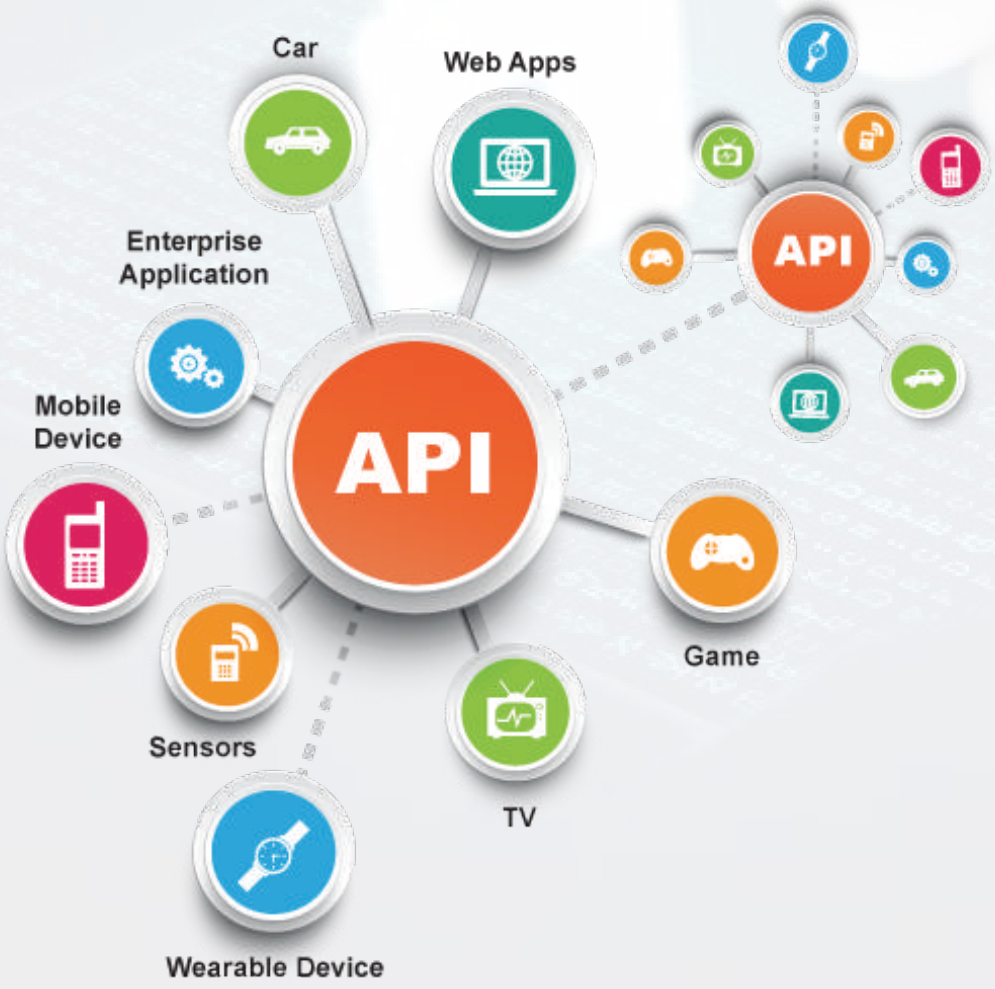
8 **Digital authentication and security**

Improving the user experience overall while enhancing the security against hackers and other threats.

Example: Apple is offering TouchID, a finger print recognition feature; Many banks are working on initiatives to use technologies to replace dependency on passwords.

KEY SECURITY ISSUES

API security is a growing area of concern for banking due to their complex and multi-level integrations. Multilevel integrations require data sharing amongst core banking infrastructure which is highly secured, with APIs which are getting externally exposed. Here security issue is not just what data is being shared, but also data to be explicitly concealed for the dynamic working of the API solution, a much harder issue. Similarly, openness and security are two opposing priorities in API design, and a smart API design would be a balancing act between the two.



RECENT SECURITY INCIDENTS

3.2 Million Debit Cards affected in massive ATM Card Hack affecting Indian Banks, October 2016

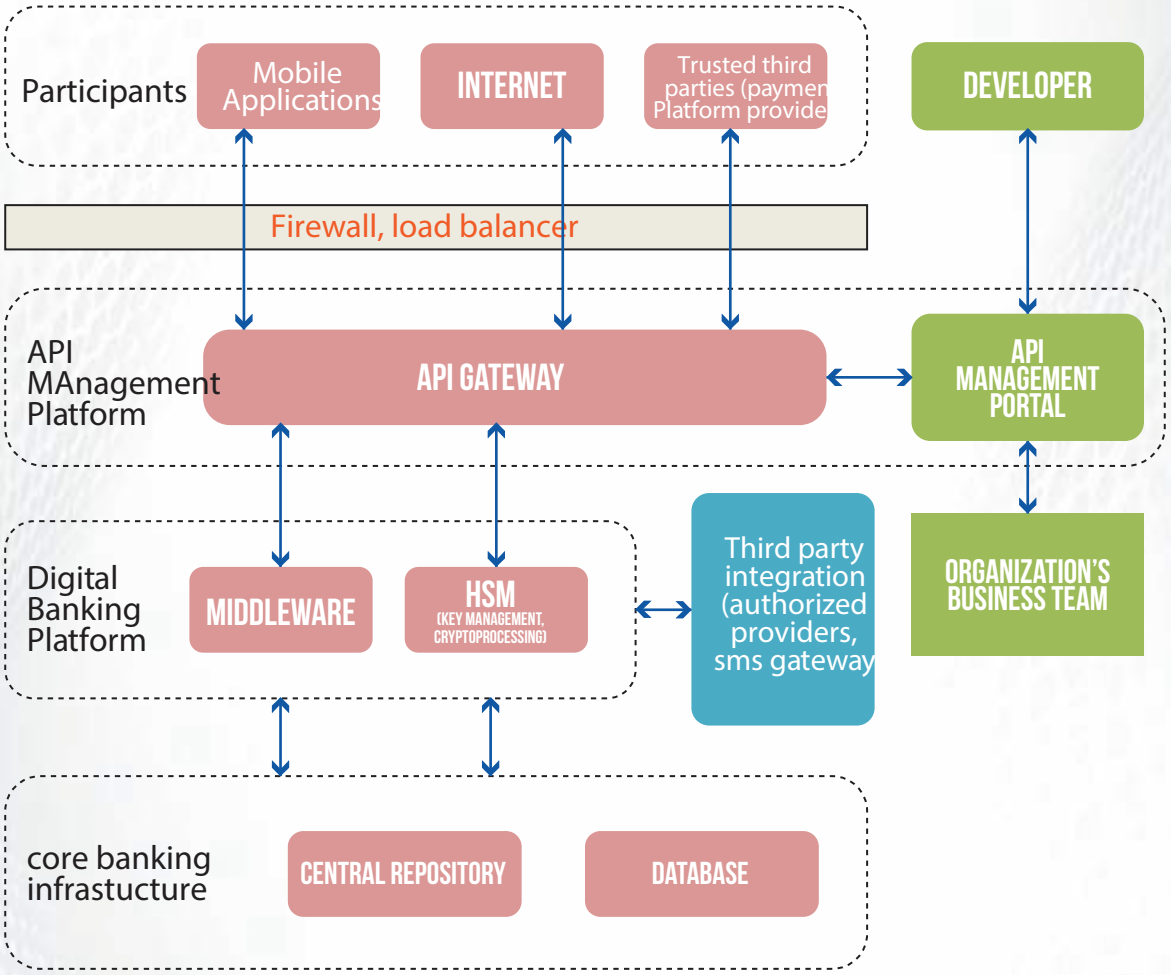
A malware infection in POS solutions enabled hackers to steal critical customer details leading to the retrieval of funds from their accounts. This led to a compromise of 3.2 million debit cards. Unauthorized usages for the leaks lead back to China. Post detection, customers were requested to change their security codes/PIN numbers to prevent further damage.

SWIFT Breach, 2016- 2017

SWIFT, the global messaging network, is on the radar for malware attacks on its network. One of the hacking groups stole US$81 million from a Bangladeshi bank and 2nd attack reported an attempt to steal over US$1 Million from a bank in Vietnam. India recently faced SWIFT attack cases where hackers targeted 3 Indian government owned banks and created fake trade documents. Though no monetary loss was reported, a breach in the bank's systems was clearly identified with this attack.

"API BANKING"

ARCHITECTURE



The above shows the flow of data from originating channels (Mobile apps, TTPs) toward the core banking infrastructure. This end user could be a bank customer or a trusted third party utilizing the services provided by the bank via APIs.

API BANKING ARCHITECTURE

Whenever a consumer entity initiates a request for a service via multiple channels, it first lands on the API management platform. This platform consists of API gateway and a developer portal used by developers for deploying APIs which are consumed by end users. API platform takes care of multiple security as well as management tasks. Hence, the business team from the bank also have some inputs for proper API management from business point of view. These tasks include protection against threats, rate limiting, access control, encryption, API versioning, logging, Commissioning/De-commissioning of service URLs, Monetisation of APIs, etc. In case of third party integrations, API gateway is responsible for providing a uniform platform for communication to take place.

The platform, after verifying the request and identifying the API in consideration, forwards the request to the next hop in the cycle. This could be an SOA, middleware or directly to an application server. If any third-party authenticator is being used, it can be integrated at this level. As most of the banking transactions consist of multiple validations and sub-steps, the device then communicates with multiple core banking systems and a consolidated action is taken.

The response to a request flows back via the same hops in reverse order. Based on the originating request, the gateway decides the valid channel for the response.

TOP 6 SECURITY CONCERNS

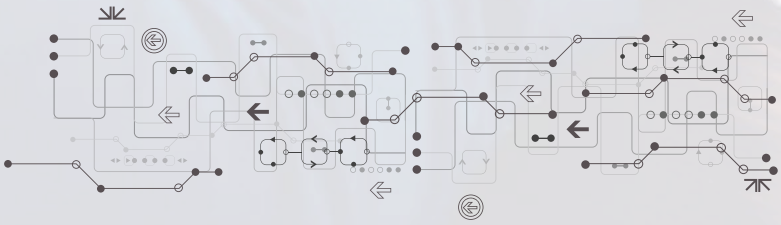
1 Business Logic Attacks (BLA)

Business logic attack exploits the flaws mostly present due to functional level complications and restraints, managing the exchange of information between a user interface and the application's supporting database. Programming flaws may also contribute but due to logical anomalies rather than syntactical errors.

APIs enable business related operations available as procedure calls, making it easier to attack the business logic of a company using an API attack. These attacks include legitimate input values, thus making it difficult to detect the attack. These abuse the functionality of the application.

Examples are:

- Modification of authentication flags and privilege escalations.
- Business constraint exploitation/modification or business logic by-pass to generate fraudulent transactions.
- Parameter modification.
- Cookie tampering and business process/logic bypass.
- Exploiting client side business routines embedded in JavaScript, Flash, or Silverlight.
- Identity or profile extraction.
- LDAP parameter identification and critical infrastructure access.



TOP 6 SECURITY CONCERNS

2 Integration with Third Parties

Third Party APIs would require an environment that might not always be compatible. Additional work would be required to fix these compatibility issues. Additionally, there is less control over the API lifecycle, as these are usually defined by the provider's needs. Working on those aspects might outweigh the benefit of going for third party integration. Also, since the client would be integrating its products with third parties, the security of client's products and services completely rely upon the safeguards and security measures followed by the third party API. There could be inherent incompatibility issues, fixing which on integration would require cost-benefit analysis. Also, integrating third party with client complex legacy system infrastructure needs to be well thought upon, based on feasibility and business functionality.

3 Compliance & Regulatory Issues

APIs are expected to help banks meet new regulatory requirements around the world. The PSD2 Directive introduced compliance requirements for banks and other financial institutions, including the enforcement of new security requirements and interoperability standards aimed at reducing barriers to entry for nonbank card and internet payment providers. APIs are essential for regulation and compliance, and for leveraging big data. Few regions have open regulatory standards, while others mandate regulatory behaviour. Compliance risk has become one of the most significant ongoing concerns in the BFSI domain. Customers and partners prefer to look for moral bankers, failure to abide by the same leads to loss of business, reputational risks, and financial impacts.

TOP 6
SECURITY CONCERNS

4 Data Sharing Issues:

Data exchange should ensure proper authentication and authorization. Unauthorized access and failure to follow required levels of consent may lead to data leakage, and breach of confidential data. For data sharing, access to data must be ensured on access to least privilege. Other unnecessary privileges and data irrelevant for the specific functionality should be later destroyed; else the system functionality would be affected, which would disrupt business processes leading to operational loss.

5 Interfacing with Legacy Core Banking Systems

Considering technical compliance overhead to provide requested responses after customer inputs details, banks need to create TTP-facing, open access front ends, with technical challenges in the back-office integration of legacy core banking systems. If the integration however, fails, it would be of no/little value to banks and banks would fail to leverage hold on the customer data details. Also, if the data held in the database, goes underutilized, ineffective usage of technology, may lead to limited access to refined customer data.

6 Issues in Managing Digital Identities

The pace at which the digital environment is growing, managing digital identities has become a major problem. As multiple agencies are being integrated for providing a service, data sharing and data privacy issues are looming large. Due to high face value, financial data has always been a high-profile target for hackers. As the number of integrations increase, the attack surface also increases exponentially.

TOP 4 MITIGATION STRATEGY

THINGS WHICH WE CAN'T MISS DURING API ECONOMY GOVERNANCE

API Governance should include the following 4 checks:

1 Validate User and App Identity

API key validation is required to be controlled at the management tier. Ensure Authentication and authorization is separately handled. Applying flexible run-time policies and managing these policies from a centralized management console increases the flexibility and control of API provider over these parameters.

2 Integrate a full API lifecycle Management Tool (Efficient Implementation of API gateway)

The API development processes must be approached in a holistic manner with a security mindset. This can be ensured if you consider the below security features

- Implement strong authentication and authorization for access to connected devices across gateway and ensuring strong customer authentication.
- Consider monitoring, logging, and analysing data traffic to track API consumption, and usage as per availability and performance. It could also help in monitoring security incidents/breaches, and errors. Attacks could be prevented by use of features such as whitelisting, managing firewall, considering rate limitation per defined time frame per given app.
- Creation of buffer zones by segregating API servers to mitigate reverse engineering attacks against API's.
- Ensuring strong access control, CIA, threat detection against threats such as data encryption, message validation, traffic management, etc. is essential
- Efficient implementation of API Gateway, using of API keys for rate limitation, QoS, embed multi modal authentication and authorization mechanisms.

TOP 4 MITIGATION STRATEGY

THINGS WHICH WE CAN'T MISS DURING API ECONOMY GOVERNANCE

3 Implement Organization wide Security Policies

Comprehensively define policy-procedure-standard across API lifecycle, i.e. its separate documented policies and their implementation on planning, design, testing, and development stages is required. Instead of individually creating and governing API solution, corporate API security policies and best practices must be enforced at the management level.

4 Encrypt Message Channel

- Provide authentication by digital signatures and use of encryption for data privacy,
- Keys – add to another level security. Keys could be passwords, algorithm generated numbers/code, digital fingerprints, etc. Encryption can be used during communication to avoid attacks if keys are intercepted in transit.
- Encryption - XML encryption to protect data privacy, encrypting message containing sensitive data using strong cipher encryption, encrypting and decrypting content and representing using XML.
- Enabling SSL/TLS encryption – it would help specify type of certificate exchanged between nodes, key messaged authentication, secure key hashing for message authentication code.

CONCLUSION

With the onset of APIs, we are at the cusp of API economy where banks need to embrace openness of APIs and consider the security procedures around it, given the data being explicitly shared and the risks involved. Regardless, the API threats are manageable with a commitment to strong cyber security compliance standpoint. Banks need to strategize their API approach in line with the business decision-making model. Banks need to pace up the approach of securing API conforming to Global risk governance and regulations and utilise the strategic opportunities brought about by API sharing and the revenue that can be raised by them. Banks need to adapt on all the three fronts of cyber security – People, Process and Technology, including their API eco system with a continual improvement approach to align themselves with their strategic and business objectives.

ABOUT AUJAS

Aujas is a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response and Security Engineering services. Our unique products and services help businesses build and transform security postures while mitigating risks. The service focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks, so that you drive change, innovate, and accelerate growth.

For more information, do visit us at **www.aujas.com** or you ou can also write to us at **contact@aujas.com**