TATA CONSULTANCY SERVICES

Building on belief

Cyber Resilience:

The bedrock of next-gen digital banking

Abstract

With great power comes great responsibility — while banks and financial institutions have greatly empowered customers through the provision of digital self-service, the responsibility of ensuring safe, secure, and resilient service still rests with them. Increased adoption of contactless digital service spurred by the ongoing pandemic has created unique opportunities for fraudsters to launch targeted attacks through the same digital channels that end customers use. Small and medium enterprises (SMEs) are particularly vulnerable to payment related fraud as they scramble for ways to improve their cash flow in the prevailing situation. The advent of open banking coupled with rapid customer embrace of innovative financial offerings offered by fintechs and technology giants is likely to expand the attack surface for fraudsters. Developing cyber resilience has thus emerged as a key imperative, especially as banks lean toward the **adaptive distribution** of their partners' offerings through their digital channels. This white paper explores the building blocks of cyber resilience — emerging digital technologies such as artificial intelligence (AI) and machine learning (ML) — and their role in helping banks to evolve into resilient, future-ready, **cognitive enterprises.**[1]

The evolving digital banking threat landscape

Customers are increasingly using desktop and mobile offerings for their routine banking requirements, including point of sale payments. The use of social media channels such as WhatsApp for chat-based banking and Twitter and Facebook for complaints and financial information is also seeing an uptick. But services offered over social channels are not likely to be as secure as those offered by the banks' digital channels. With the advent of Open Banking, banks are actively collaborating with fintechs in order to leverage the wider ecosystem. Banks are leveraging application programming interfaces (APIs) to expose data and business functionalities to ecosystem partners. Products and services offered by ecosystem partners and fintechs will not be protected by the existing security controls offered by the bank's digital platforms, thereby exposing customers to fraud. These developments coupled with shifting customer behavior are creating a threat landscape that mandates a relook at the existing security controls. In our view, banks must perform a comprehensive audit of their security systems and processes, identify deficiencies, and initiate appropriate intelligent technology interventions to address them. The way forward lies in employing AI and data analytics techniques to understand the normal financial engagement behavior of individual customers across all touchpoints. This will enable automatic detection of anomalies in individual customer behavior to prevent fraud in real-time and facilitate personalization **of cybersecurity controls** to fit individual customers.

[1] TCS, Heralding Post COVID Economic Revival through Resilience and Value Leadership, June 2020, Accessed January 2021, https://www.tcs.com/heralding-post-covid-economic-revival-through-resilience-and-value-leadership

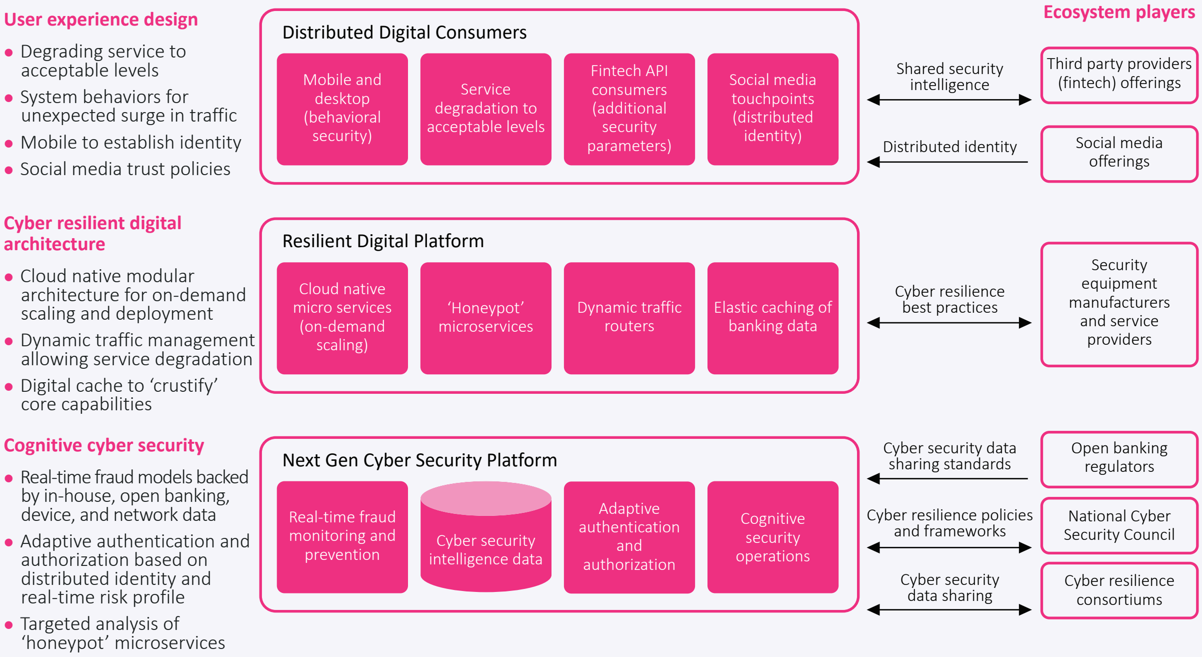
Enhancing security controls for mobile and social channels

Over the years, banks have established multiple layers of security controls in their digital banking channels and offerings at different points in transaction processing (also known as 'defense in depth'). Banks have enhanced their existing security controls by installing mobile-specific security layers. However, with the mobile banking channel set to see explosive growth in the near future, we believe that banks must invest in strategic mobile security suites equipped with intelligent capabilities. Such capabilities could span collecting device profile information through telemetry, detecting devices with compromised operating systems (jail-broken), spotting malware on mobile devices, and alerting customers to these risks besides barring the use of such devices for financial transactions. Real-time transmission of such information to fraud servers will facilitate analytics and enable swift action to prevent fraud. The use of social channels must be limited to non-sensitive journeys, and banks must direct customers to more secure channels for performing banking transactions. Extending security controls available on digital banking platforms to social media touchpoints is crucial to protecting end customers as well as banks' assets. Such protection and controls aimed at cyber resilience must extend beyond banks' own digital offerings to include partner offerings as well.

Larger banks have already invested in such mobile-specific security controls and collected a wealth of device profile information along with data on customer behavior patterns on mobile, desktop, and digital devices. Banks have also invested in real-time fraud prevention systems for card transactions as well as anti-money laundering controls and rules for payments and onboarding systems. However, we observe that such controls are not leveraged effectively across lines of business (LoB) and customer touchpoints. Digital fraud controls such as device profiling, malware detection, and real-time transaction scoring must be leveraged to detect and prevent fraud across LoBs like the SME segment, corporate banking, and wealth management. For instance, when customers set travel indicators to enable the use of their card(s) at international locations, banks must leverage this information to employ security controls in digital and mobile channels as well as the connected small business account (if applicable) while processing high-risk transactions such as payments.

Getting ready for next-gen digital banking

While banks have taken steps to enhance security controls across channels, these measures have been largely incremental as a response to emerging threats without a well-defined strategy in place. As banks tread the future-ready path by adopting purpose-driven ecosystems, enabling contactless banking, embracing adaptive distribution, and deploying new reality products and services, their security responsibilities will further widen. In our view, banks will need to embed future-ready capabilities into their cyber resilience strategy (see Figure 1).



User experience design

- Degrading service to acceptable levels
- System behaviors for unexpected surge in traffic
- Mobile to establish identity
- Social media trust policies

Cyber resilient digital architecture

- Cloud native modular architecture for on-demand scaling and deployment
- Dynamic traffic management allowing service degradation
- Digital cache to 'crustify' core capabilities

Cognitive cyber security

- Real-time fraud models backed by in-house, open banking, device, and network data
- Adaptive authentication and authorization based on distributed identity and real-time risk profile
- Targeted analysis of 'honeypot' microservices

Distributed Digital Consumers
Mobile and desktop (behavioral security)
Service degradation to acceptable levels
Fintech API consumers (additional security parameters)
Social media touchpoints (distributed identity)
Resilient Digital Platform
Cloud native micro services (on-demand scaling)
'Honeypot' microservices
Dynamic traffic routers
Elastic caching of banking data
Next Gen Cyber Security Platform
Real-time fraud monitoring and prevention
Cyber security intelligence data
Adaptive authentication and authorization
Cognitive security operations
Shared security intelligence
Distributed identity
Cyber resilience best practices
Cyber security data sharing standards
Cyber resilience policies and frameworks
Cyber security data sharing
Ecosystem players
Third party providers (fintech) offerings
Social media offerings
Security equipment manufacturers and service providers
Open banking regulators
National Cyber Security Council
Cyber resilience consortiums

Figure 1: Future Ready Cyber Resilience for Next-Gen Digital Banking

Achieving next-gen cyber resilience will mandate defining and executing an effective strategy encompassing all channels, LoBs, functions, partner ecosystems, emerging technologies such as 5G and quantum computing, and connected devices. An effective cyber resilience strategy will need to factor in a few crucial aspects:

Leverage existing fraud controls and cloud computing investments

Some open banking regulators in the UK include optional risk indicators in the API specification. Banks must actively encourage fintechs to collect and share such information through APIs, which will allow banks to take advantage of existing fraud controls. Banks must also offer APIs that can be consumed by fintechs in order to collect additional security parameters as customers consume fintechs' digital offerings.

Specific events such as the Black Friday sale or certain partner offerings often cause unprecedented surge in banking traffic. Banks must embrace cloud technologies to scale and manage the unprecedented surge in banking traffic caused by such events. Degradation of digital banking services to an acceptable level and appropriate caching of banking data must be designed as a part of key user journeys, allowing business-as-usual (BAU) even during system failures or attacks.

Embed cyber resilience into digital platform architecture

Banks must make catering to cyber resilience and security requirements a mandatory part of every IT project and initiative. User experience designers must consider all customer touchpoints, including social media, connected devices, and public wi-fi networks vulnerable to compromise, and incorporate restrictions such as blocking access to all or specific banking functions from such environments while designing the user experience. When customers access digital banking from partially compromised environments, access to all banking services must not be provided. Services must be gracefully degraded and offered at a minimally acceptable level, and this must be taken care of while designing user journeys.

Investments in APIs and microservice architectures are a component of platform modernization initiatives in banks. While banks are employing robust security controls as part of such modernization, the controls are largely tactical or fit-for-purpose, which can be attributed to traditional monolithic architectures. In our view, banks must consider designing ’honeypot’ microservices with the capability to dynamically route customer traffic to such microservices. ‘Honeypot’ microservices are dummy microservices that leverage APIs or web tools to exhibit behavior similar (in terms of banking data or functions) to real microservices but are actually isolated and disconnected from real systems. This empowers security teams to dynamically isolate suspected fraudulent traffic and perform real-time analysis to prevent fraud.

Share cybersecurity data to create exponential value

Though banks have employed sophisticated security defenses and operations monitoring systems, they function in silos. Additionally, banks lack a mechanism to share data on security breach attempts and the associated forensics as well as data collected from monitoring systems with other banks. Banks with the weakest defense are likely to be easy prey to attacks, allowing other banks to ‘hide’ behind vulnerable banks. However, such attacks provide hackers with valuable information and intelligence which can be leveraged to attack ’stronger’ banks.

We recommend that banks across the spectrum come together and establish secure API frameworks to exchange cybersecurity analytics data about individual customers (with the appropriate consents). Banks must leverage data obtained from other banks to enhance their existing AI models and strengthen fraud monitoring and prevention processes. In addition, banks must establish APIs to monitor devices, IP addresses, sim cards, and networks known to be involved in frauds and build up a comprehensive database. Other banks can leverage APIs to access the database and research vital information to protect their customers, thus improving the overall cyber resilience of the financial services industry. Access to fraud analytics insights and database can be offered to fintechs through APIs, thus improving the cyber resilience of fintech offerings as well.

Take the next step

In our view, regulatory agencies must mandate the creation of a common consortium for sharing of data on security breach attempts, forensics, and defense measures and implementations. The Cybersecurity and Infrastructure Security Agency in the US[2] and the National Cyber Security Centre in the UK[3] concentrate on ensuring cyber resilience at a national level — financial services also come under their purview. As part of the holistic restructuring of banks post the pandemic, we envision a broader role for banks in improving the cyber resilience of nations. This will entail building collaborative ecosystems comprising banks and other stakeholders — financial industry regulators, national security agencies, mobile and internet service providers, hardware and software providers, email and chat providers, social networks, and more — to help raise the overall cyber resilience quotient. Such an ecosystem will facilitate sharing of best practices and standards and real-time exchange of vital cybersecurity insights and intelligence among all stakeholders and go a long way in preventing fraud.

A common ecosystem or platform will help IT hardware and software providers to incorporate new security features in their products and services. Educational institutions too can be brought into the ambit — introducing cybersecurity early into the curriculum will improve awareness on safe usage of cyber offerings among next-gen customers. Such an ecosystem will also enable banks to collaborate with internet service and mobile network operators and email, chat, and social network providers to identify financial services related traffic, employ whitelisting techniques, and filter malicious traffic before it reaches banks' networks and assets, thus eliminating denial of service and similar attacks. Achieving such futuristic cyber resilience will mandate differentiated capabilities and require banks to leverage cognitive technologies and cloud-based adaptive distribution models, collaborate actively within the financial services ecosystem, and establish the right partnerships to access the expertise required.

[2] Cybersecurity & Infrastructure Security Agency, Accessed January 2021, https://www.cisa.gov/financial-services-sector

[3] National Cyber Security Center, Annual Review 2020, Accessed January 2021, https://www.ncsc.gov.uk/files/Annual-Review-2020.pdf

TATA
CONSULTANCY
SERVICES

About the author

Prathap Thompson

Prathap Thompson is a chief architect in the Open Banking Strategic Initiatives group with TCS' Banking, Financial Services and Insurance (BFSI) business unit. He has more than 19 years of experience with expertise in open banking compliance, API economy, and next-generation digital propositions. Prathap is also an intrapreneur designing next-gen digital propositions as part of a small digital native team operating as a startup within TCS. He holds a bachelor's degree in Manufacturing Engineering from the College of Engineering, Guindy, Anna University, Chennai, India.

Contact

For more information on TCS' Banking, Financial Services, and Insurance (BFSI) unit,
visit https://www.tcs.com/banking-financial-services or https://www.tcs.com/insurance

Email: bfsi.marketing@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is a purpose-led transformation partner to many of the world's largest businesses. For more than 50 years, it has been collaborating with clients and communities to build a greater future through innovation and collective knowledge.
TCS offers an integrated portfolio of cognitive powered business, technology, and engineering services and solutions. The company's 488,000 consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

Visit **www.tcs.com** and follow TCS news **@TCS_News.**