HOW CAN TELECOM COVER AND SECURE FINANCIAL DATA

airtel
business

Digitisation is changing banks for good. The results are clearly visible: collaboration among branches has improved, service delivery has become more efficient and last-mile connectivity has strengthened. But banks need to do more. Consider the following:

- Nearly 3 billion users will access retail banking services through smartphones, tablets, PCs and smartwatches by 2021, according to Juniper Research
- The number of online banking users in India is expected to reach 150 million by 2020, says a report by Facebook and the Boston Consulting Group (BCG)
- Across the globe, digital-only banks and FinTech start-ups are taking customers away from traditional banks with vertically integrated and product focused business models. The growth story of the big five digital-only banks in Europe (Monzo, N26, TransferWise, Revolut and Starling) is an example
- Individuals under 35 are more than twice as likely to use an online lender compared with those who are older, a PwC survey in the US revealed

GOING DIGITAL, THUS, IS NOT A CHOICE BUT A COMPULSION FOR BANKS.

And that is before we have even considered that digital banking can bring down cost, increase transparency and improve services.

- JPMorgan estimates that the cost of serving a fully digital account is 70 per cent less than a traditional account, while retention rates for mobile banking are 33 per cent higher than non-mobile banking. For cards, the corresponding numbers are 30 per cent and 35 per cent, respectively.

What makes the digital switch even more of a no-brainer is that a significant part of the back-end operations of the major banks are already digital, including settlement of transactions with eco-system partners such as other banks and digital wallets.

But digitisation is a package deal: it comes with the ever-increasing need for data security and privacy, a factor that keeps many banks from realizing the full benefits of digitisation.

CYBER THREATS ARE A CLEAR AND PRESENT DANGER

RBI data shows that between 2008 and 2017, Indian banks faced 130,000 reported cases of cyber fraud involving an estimated Rs 700 crore. In 2016, 3.2 million debit cards got compromised and the worst hit were some of the biggest names in Indian banking. Each of these attacks eroded customer trust, devalued their experience and pegged down revenue.

More than 20 per cent of cyber-attacks that India witnessed last year were on the banking sector and these attacks are becoming more complex by the day. This is not a surprise given that cyber criminals prefer BFSI over other industries. In fact, cybercrime in BFSI is an industry in itself!

The evolving and dynamic threat levels, the vast amounts of data to be protected — data at rest, data on the move, customer identification authentication, for instance — and need to proactively identify potential threats make preventing cybercrime in BFSI such a tough challenge.

And the threat is not limited to an organisation’s apps and websites. Assessing and providing secure payment gateways for e-commerce and other digital transactions is just as important. Banks must also account for the plethora of hardware and software used to access its services. A jailbroken device or a compromised network might trip even the best security arrangements.

HOLISTIC AND SPECIALISED SOLUTIONS

Specialised threats demand specialised responses. The BFSI industry needs experts who are well versed in both data and its security because without understanding data well it is impossible to protect it well.

The BFSI cyber-security framework needs to encompass forensics and incident response. The impact of multi-vector attacks should be assessed in a timely manner using intelligent investigative and analysis tools to evolve an effective incident-response process.

The traditional BFSI threat mitigation processes often rely on prevention and damage control when faced with a breach or attack. What is needed is a holistic approach that not only looks at threat intelligence but also at detection of existing and new threats or intrusions.

In the aftermath of an incident, a specialised service provider is essential for speedy and skilled response to minimise damage and disaster as well as data recovery. This is generally something cyber-security specialists focus on but internal IT teams do not, being bogged down with day-to-day maintenance and technical support.

Device management is critical to eliminate dangers arising from manipulated source code and man-in-the-middle attack. Apps need to have multiple security layers to protect user data and trust.

A robust digital security infrastructure is one that prepares organisations for every stage of the attack/threat lifecycle. It must offer a complete suite of services, starting from helping banks identify and protect critical data assets, network security and DDoS prevention to better compliance and cyber skills development to protect organisations from internal and external assaults. In fact, with the guidance of specialists, security can be built into products at development stage as a preventive measure.

BANKING-TELECOM CONVERGENCE

Banks need to align with the right partners for end-to-end fool-proof cyber security solutions that are preventive as well as reactive.

- Trusted and well-established telecom operators by virtue of their understanding of and decades of experience with large volumes data — they deal with as much data as banks, if not more — as well as state-of-the-art technology like artificial intelligence, machine learning and analytics can deliver that.

- Both BFSI and telecom sectors are bound by strict data rules. The vast amounts of information generated and processed by telecom operators promise insights that could provide BFSI organisations the security boost they need to remain competitive. This synergy also aligns with the trend of greater convergence the BFSI and telecom sectors driven by the rise in the number of customers opting for quick and convenient mobile banking solutions.

- With enterprises increasingly looking for an Opex rather than a Capex-oriented model, key telecom operators have emerged among the top managed security service providers. The reasons are not far to seek. They have long-standing expertise in laying networks for billions and keeping them secure. Airtel, for example, has been consistently warding off cyber-attacks for more than two decades and its cybersecurity services, Airtel Secure, has been enabling enterprises in their cyber security journey.

airtel
business

To know more, email us at airtelforbusiness@airtel.com
or visit http://airtel.in/business/