DIGITAL MONEY IS MAKING THE WORLD GO ROUND p. 26

MAKING IT BIG, AND MANAGING IT TOO p. 54

ALTERNATIVE CLOUD MAKES BETTER SENSE FOR SMBS p. 58

₹100

VOL XXXVIII No 02 | FEBRUARY, 2021

www.dqindia.com

DATAQUEST

CyberMedia

THE BUSINESS OF INFOTECH

DQ 38 YEARS

WHAT NEXT IN FINTECH SAGA?

2020 was a tipping point for fintech players. Question now is where they move next – and how they react to platforms, apps, and incumbents coming to the party

Naveen Jaiswal
maildqindia@cybermedia.co.in

Scaling up UCB cybersecurity practices

Taking the RBI guideline forward, UCBs can draft their own technology vision framework to enhance cybersecurity measures

The banking, financial services and insurance (BFSI) sector has been witnessing dramatic changes in technology. Digitisation of services in banks and insurance organisations has led to accumulation of big data, making the sector a major target for threat actors. The monumental growth in online banking in India and the steady growth of cashless transactions have brought to light the urgency for strengthening cybersecurity postures. Apart from banks, banking consumers are also vulnerable to cyber threats like malware, formulated to steal confidential financial credentials. The increasing need for quicker BFSI transactions, especially the ones dealing with across the border, is under cybercriminals' scanners.

The security threats on BFSI have increased manifold and taken critical turns to affect these organisations. And one of the primary factors is the increasing workload on the cloud, as most of the enterprises have already or are undergoing rapid digital transformation. As per industry estimates, Coronavirus has been blamed for a 238% rise in attacks on banks globally, and if we go by the Kaspersky Security Network (KSN) report, the number of local cyber threats detected and blocked in India from January to March last year is 52,820,874.

The need to rapidly relocate to the Infrastructure as a service (IaaS) cloud ecosystem has brought newer risks that are created from the misconfiguration of access points. Organisations have opted for third-party integrations to sustain the required IT environment to assist online banking. And while deploying multi-vendor solutions, enterprises may sometimes have various vendors stationed across their environment. This obviously leads to integration inadequacy, making enterprises face the unwanted scenario of data forfeiture.

RBI'S FOCUS ON STRENGTHENING UCB CYBERSECURITY

Public sector banks (PSBs) and urban cooperative banks (UCBs) across the board underwent massive centralisation in the past year. However, all of them had to keep pace with the increasing demand for speed and comfort. Unless they followed a strict protocol and focused on security, integration gaps could have left security postures broken and vulnerable.

This is one of the reasons why the RBI introduced a vision framework to enhance the cybersecurity measures

> THE NEED TO RAPIDLY RELOCATE TO THE INFRASTRUCTURE AS A SERVICE (IAAS) CLOUD ECOSYSTEM HAS BROUGHT NEWER RISKS THAT ARE CREATED FROM THE MISCONFIGURATION OF ACCESS POINTS.

of UCBs. It is currently based on a five-pillared strategic approach, GUARD, which focuses on providing an insight into UCB governance, strategies to impart technical skills to manage IT, and raising awareness for all UCBs, regulating the reporting framework and providing appropriate guidance for implementing practices that are secure from the core.

Digitisation of every other business has eventually found its way to banking as well in the form of internet banking, mobile banking, and ATMs. UCBs can, therefore, formulate their technology vision framework that outlines their propositions to include IT solutions in their business operations with complete security. They can also upgrade their IT repository with supported IT infrastructure to ensure that the cyber ecosystem is not vulnerable to risks due to outdated software/hardware.

WHY IS THE GUIDELINE IMPORTANT FOR UCBS?

Cybercrimes continue to expand and are becoming persistent by the minute. Threat actors are getting stealthier and their attacks even more critical to beat. It is time for UCBs to get a grip over their existing security infrastructure and adopt a full-fledged proactive approach. The RBI's objective is to place stricter guidelines and align the current framework with global best practices while keeping in mind the context of the national financial system.

However, the concern whether India's UCBs will be ready on the dot to align with this vision is something that cannot be shelved anymore. The urgency to align with RBI's cybersecurity vision calls for UCBs to buckle up and place their best foot forward through constant reinforcement of global best practices, so as to strengthen the UCB network ecosystem and to stand strong against the emergence of an array of cyber threats. It might sound far-fetched for UCBs to completely align with RBI's vision framework, but with the correct guidance and tenacity, the result will prove far more beneficial that the pain.

PRESCRIPTIVE MEASURES BETTER THAN REACTIVE

Given such a critical security landscape across enterprises, cybersecurity has become the go-to industry for banks for the technology they provide. UCBs can optimise investments to safeguard their network peripheries by heavily investing in systems and people. In order to enhance security posture, the most critical assets that a UCB can own are newer solutions, systems, and people. State-of-the-art technology that includes machine learning (ML), artificial intelligence (AI), and big data must be deployed at the very foundation to effectively detect distrustful transactions. UCBs can, therefore, look at prescriptive measures to scale up their cybersecurity practices. Digitally intelligent technology tools are bringing cybersecurity companies to the forefront and are currently carrying the torch when it comes to securing the bank's assets.

Cybersecurity companies take a proactive security approach that UCBs can deploy as their avant-garde perimeter defence. They are instantly alerted of potential intrusions inside the IT environment, the ones that have already bypassed other security tools. AI and ML algorithms can detect unusual network behavior in real-time, eliminate false positives with its learning capabilities, and enable security practitioners to detect and respond to stealthy attacks.

Companies today are developing solutions that are built to help UCBs maintain stringent compliance with industry regulations as well as provide robust and resilient performance from the day of deployment. Going forward, these companies will play a pivotal role in helping financial institutions scale up and provide seamless services to their consumers.

Jaiswal is a Co-founder and Director, Vehere