CENTRAL BANKING

Technology services: SecurEyes

Indian company has offered integrated suptech/regtech services to help tackle cyber risk

This article is also available at: https://www.centralbanking.com/awards/7954717/technology-services-secureyes

From left: Karmendra Kohli and Seemanta Patnaik, SecurEyes

Cyber security is a growing problem for financial service providers and supervisors alike. Central banks participating in the Risk Management Benchmarks 2022 cited cyber security as both the biggest rising risk last year and the most concerning risk overall – perhaps not surprising given the cost of cyber fraud worldwide is estimated in the multiples of billions of US dollars.

Central banks and supervisors need to address threats to the financial institutions and market infrastructures they oversee to protect financial stability, while at the same time defend themselves and their reputations against the growing, 24/7 risk of cyber fraud. That's where SecurEyes, founded in Bangalore in 2005 by two school friends, Seemanta Patnaik and Karmendra Kohli, comes in. The Indian company has developed an integrated suptech and regtech capability that can help supervisors address cyber risks.

Its SE-RegTrac product was developed to meet the cyber security oversight needs of a central bank, which is responsible for banking, insurance, fintech, financing and payments sectors, on a single platform. "We have full visibility from different angles in a central place," an official from the institution tells Central Banking during a video call.

The system allows for near real-time monitoring of attacks in the financial system, down to individual incidents of cyber fraud.

"We have amalgamated the supervisory technology and regulatory technology into a unified platform and have segregated portals, one for the supervisor and one for the members, with everything hosted within the central bank," Seemanta Patnaik, co-founder, chief technology officer and director, tells Central Banking. "Currently, all local banks in the country have been connected," Patnaik says.

The technology also allows the central bank to perform live and predictive analysis of current and historical data, to provide insight into areas of strengths and weaknesses across the sector. "SE-RegTrac helps the regulator in policy-making decisions," Patnaik says. The central bank can plan ahead by understanding participants' cyber security maturity to pre-empt and respond to threats.

Disaster-recovery activities, data-centre distribution, outsourcing, vendor concentration and workforce distribution are all factors used to build entity risk profiles. The 'supervisory inspection management' feature allows onsite inspection planning and reporting. When an inspection team from the central bank conducts an external supervisory or incident visit, they download the relevant details offline and insert the various key information details while on site. The information gets synched once the team is back at headquarters. "We have an offline model, because this entire system is located within the premises of the central bank," Patnaik says.

Visibility of action plans submitted by regulated entities includes end-to-end workflows with an approval process from the regulator. The platform also facilitates unified communication to all regulated entities. "We have standardised the reporting mechanism and unified compliance frameworks for regulated entities in order for the central bank to have full visibility," Patnaik adds.

The product is based on service-oriented architecture, with application programme interfaces (APIs) available for surrounding systems to consume data from SE-RegTrac. SE-RegTrac can also pull data from surrounding systems via APIs for seamless integration.

Ensuring the quality of data is imperative because this impacts analysis, Patnaik says. "Close monitoring and collaboration with member organisations is very important to make this happen."

SE-RegTrac complies with several internationally recognised security standards for defending systems and data against cyber attacks. These include the OWASP, CIS, OSSTMMl and SANS25. Cross-site request forgery – meaning an attacker gets a user to click on a link to submit unauthorised commands – and insufficiently protected credentials are among the SANS25 list of the most dangerous software vulnerabilities.

"We have seen there is an increase in cyber fraud and scams," SecurEyes' technical director, Alok Rout, tells Central Banking. At the same time, there is a "much, much needed digital transformation that is due in the regtech, suptech and even compliance technology sectors". However, though there is a need today for sectoral overview in near to real time, there are "very few companies that can actually offer this to the central bank, or regulatory authorities beyond central banks and commercial enterprises", he adds.

SecurEyes, which claims its cyber security clients include Goldman Sachs, the Indian Ministry of Defence and the Indian Prime Minister's Office, is currently in conversation with other central banks, notably in the Middle East, about introducing SE-RegTrac in their jurisdictions.

The Central Banking Awards 2023 were written by Christopher Jeffery, Daniel Hinge, Dan Hardie, Joasia Popowicz, Ben Margulies, Riley Steward, Jimmy Choi and Blake Evans-Pritchard.

Central Banking Awards | India Awards
Central Banking Awards 2023
Central Banking staff, 22 Mar 2023