**Banks in India Still Lack Strong Measures Against Cyber Frauds**

With the rise of digital payment apps and subsequent introduction of demonetization concept for conducting transactions, cyber security has become a hot topic for banks and financial institutions to deal with. Still though, security measures adapted by banks are not adequate enough to prevent potential cyber frauds.

According to experts, mobile apps always have a risk of security breaches. If banks are not fully prepared to guard against these risks, even if they are subject to fraud in small transactions at the moment, they could end up having huge financial losses very soon. According to an expert in the cyber-security firm working with financial institutions, “The new apps are evolving, there are incidents happening and they may be low value transactions but if there is a flaw then the losses could run into crores. So the security definitely needs to be beefed up.”

In the past couple of months, multiple apps have been developed as a result of collaboration between National Payments Corporation of India (NPCI) and some banks and wallet companies. Partner, Advisory Services at EY said: “Banks are conducting a lot of audits with new applications including the UPI, BHIM and their own apps. There are still some gaps and banks still have a long way to go. Many smaller banks outsource a lot of security operations to third-party entities. We are also helping many banks in doing the audits and getting the compliance in place.”

According to data released by RBI in Feb, transactions undergone through government initiative Unified Payments Interface (UPI) surpassed in value as compared to those done through digital wallets. Mobile wallets recorded 53.9 million transactions with a worth of Rs. 1,270 crore from Feb 1 to Feb 19 while UPI recorded 2.9 million transactions worth of Rs. 1,310 crores in the same time period.

ICICI Bank in January temporarily suspended its transactions done from Flipkart’s app PhonePe until it resolved its restrictive practices. In the meantime, State Bank of India also blocked all its customers from transferring money into their e-wallets. Chairman of SBI said that a number of recent security breaches were the reason for blocking the service, as advised by the bank committee that foresees security breaches and high risks.

According to an official at Bank of Baroda, banks face new threats every day because of frequent development of new apps. Banks realize that security is now an ongoing process, and they have collaborated with many firms including EY, PwC and Paladion for effective security compliance.

The Indian IT Act does not make it obligatory to notify the regulator in case of breach. But the Reserve Bank of India regulates banks to notify it, the Institute of Development and Research in Banking Technology, or the Computer Emergency Response Team in all cases of security breach.

In October last year, Deputy Governor at RBI SS Mundra said at a public address, “It is important to pay sufficient attention while procuring/implementing any new devices/ solutions… The banks which are big on mobile banking as a service delivery tool must also look to guard against this emerging risk. There is a need to evolve a blueprint of co-ordination between financial institutions and public authorities in such an eventuality.”