DAWN

6th November 2018

Cyber alarm for banks

THE first reported cyber attack on a Pakistani financial institution has just sent alarms bells ringing across the financial sector, and the lessons must be heeded quickly. The amount lost in the attack, which was the handiwork of hackers located abroad, is small — Rs2.6m according to the bank itself — but the figure could have been much larger. More importantly, the attack exposed the vulnerability of Pakistan's financial system to cyber attacks at a time when another similar technology-related breach was reported in the database of the Central Directorate of National Savings that holds up to Rs3.65tr in deposits from individual and institutional investors. The nature of the breach in the two cases is very different, but both have served to highlight the fact that the country's financial system has powerful vulnerabilities that could lead to large-scale damage if not plugged properly.

In the wake of the hacking attack on the bank, it was discovered that the entire security architecture of the financial system is flawed. For example, one would expect that an attack on one institution would trigger an alert for all other institutions so that they can take preventive steps. One would also expect that the alert would be shared with the State Bank and the payment operator in a timely manner so that they can put in place the measures necessary to plug the breach, as well as protect customers. But no such system for generating alerts exists, and individual financial institutions would prefer to bury the news of an attack and cover up its impact in the hope that nobody, save for a few customers who have been affected, will find out, so that they can return to business as usual.

Given the emergence of mobile banking and the fast growth of internet banking, it is all the more important for banks and other financial institutions to focus on cyber security and have industry-wide protocols on how to react when a breach is known to occur. Biometric verification can play a role in this, as it does in mobile banking, as well as real-time monitoring of the IT systems of all financial institutions. The State Bank is leading an effort in this direction, and deserves all the cooperation from the banks. But other institutions, like CDNS and the Central Depository Corporation also need to be brought into this effort, along with brokerages. Perhaps the State Bank can sit down with the management of the Pakistan Stock Exchange and the Securities and Exchange Commission of Pakistan, along with FIA cybercrime experts and private-sector cyber activists, and lead a process to determine the full scope of protections required to safeguard the financial system from future attacks. The threat should not be taken lightly because the next attack could be far bigger.

Editorial