Learning Points – Seminar on "Secur-e-Banking"

As part of its 'Member Education Series', the Indian Institute of Banking & Finance (IIBF), organized a seminar on "Secur-e-Banking" in association with Cyber Society of India on 17th February, 2017, at Hotel Taj Coromandel, 37, Mahatma Gandhi Road, Tirumurthy Nagar, Nungambakkam, Chennai - 600034.

The Key Note address was delivered by Shri Arjun Ram Meghwal – Hon'ble Minister of State for Finance & Corporate Affairs. The seminar commenced with a speech by Dr. C. Sylendra Babu, IPS, Addl DGP, Coastal Security Group, T.N. This was then followed by three thematic sessions delivered by banking and industry experts.

Some of the key learnings from the seminar are:

1. In the digital world, a number of apps are available for download. However, caution need to be exercised at the time of downloading the apps by evaluating the basic need for the app and its purpose. Otherwise, downloading of innumerable apps may lead to extreme selling.

2. When doing a SWOT analysis of e-banking, endeavour should be made to convert the Threats into Opportunities.

3. Preventive steps should be taken to avoid a cyber crime. To mention a few, ATM locations should have CCTV cameras installed.

4. Customer education awareness is of key importance else it will be an uphill the task for banks / government to meet the objective of a digital economy.

5. It is necessary to put in place an approved Board Policy on E-record maintenance. This helps in ensuring retention of digital evidences against cyber crimes committed.

6. Different agencies have collaborated to reduce cyber threats. The Gopalakrishna Committee report of RBI has also taken steps to lay down guidelines for a proper cyber security policy or framework for the setting up of a national security architecture.

7. RBI has also taken many initiatives to bring about awareness like conducting IT examinations, inspecting IT system in banks, setting up of ReBIT, interdisciplinary standing committee for cyber security, working group on financial technology, cyber security laboratory etc.

8. The Board and the top management should ensure that the significance of a cyber security framework is put in place for the organisation and the same percolates down to all the staff in the organisation. In other words, a top down approach need to be followed.

9. Cyber crimes do not leave a crime scene. Also, it involves various jurisdictions and different state laws, thus, making it difficult to bring the perpetrators to book. The agencies concerned should therefore follow a coordinated approach to mitigate cyber crimes.

10. Bankers should take note of Section 43A of the Information Technology Act as it relates to the legal position of digital evidences.

11. Last, but not the least, Cyber security is not merely an IT issue but also a business issue.