ITU Regional Workshop on securing the critical infrastructure for financial Industry

Cairo-Egypt, 14-15 October 2018

AGENDA

Day 1: Understanding cyber threats and security measures for banks October 14th	
09:00 – 09:30	Opening Session ● Welcome remarks ITU ● Welcome remarks Egyptian Banking Institute ● Welcome remarks NTRA Egypt
09:30 – 11:30	Session I: Cyber threats landscape ● Banking information system: Environmental complexity ● Security breaches getting more sophisticated ● New threats and vulnerabilities ● Know your enemy ● Anatomy of an attack: Real cases
11:30 – 12:00	**Coffee break**
12:00 – 14:00	Session II: Cybersecurity needs ● What cybersecurity strategy to secure banks and fight cyberattacks? ● Internal cybersecurity organization ● Importance of compliance: ISO27k, PCI/DSS, etc. ● Operational security
14:00 – 15:00	**Lunch**

Day 2 : Towards a new cybersecurity approach October 15th	
9:00 – 11:00	Session III: Cybersecurity for the financial sector ● Internal CERTs and SOCs for Banks: why and how? ● Information Sharing among the financial sector ● Incident response coordination
11:00 – 11:30	**Coffee Break**
11:30 – 13:30	Session IV: Cyber Exercise Simulations are a new technique that allows managers and decision makers to better understand the issue of cybersecurity and to have a better understanding of the impact that can be generated by cyber-attacks. The aim is also to train them on reaction schemes to deal with different crisis scenarios in relation to cyberattacks and electronic frauds. The exercises help managers realize the importance of involving the various stakeholders within the company, such as the CIO, the Risk Division, the Communication Department, the CISO, the General Management etc. and also the role they can play individually or in a collective and coordinated way. The exercise aim at putting these different actors in simulations to stimulate their reflection by putting them in situations similar to cases of crises they can meet and to proceed then to handle the crisis by the means of coordination, of information sharing and proposal of technical solutions. The simulations will cover scenarios of massive attacks, DDoS, ransomware, phishing, credit card fraud, data leakage, online banking attack, etc.
13:30 – 14:30	**Lunch**