International Seminar on Cyber Risk and Mitigation for banks and FIs was held on September 7-8, 2016, Mumbai

Takeaways from International Seminar on Cyber Risk and Mitigation for banks and FIs

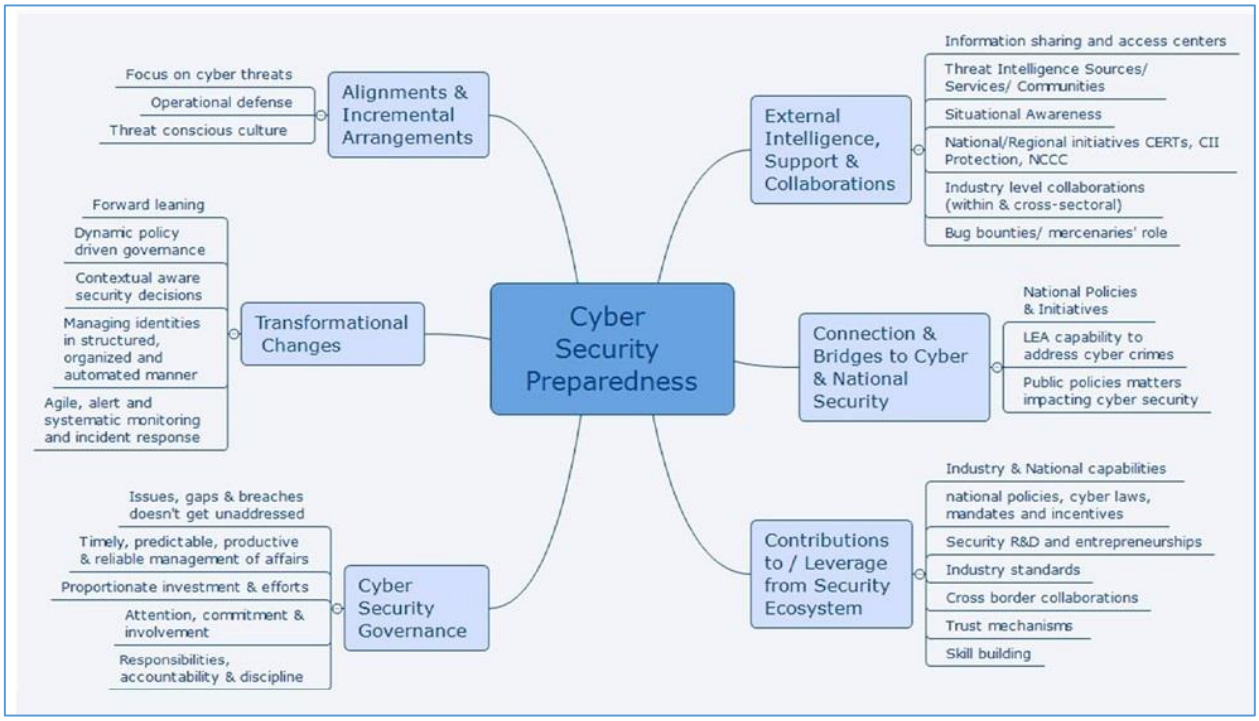
A Brief List of important Takeaways and Suggestions for constructing cyber security mitigation policy of banks, based on the deliberations of the important sessions in the Seminar:

List of select suggestions

1) **Implementing Central Bank Prescriptions:** There is a need for a robust cyber security/resilience framework in view of the low barriers to entry, evolving nature, growing scale/velocity, motivation and resourcefulness of cyber-threats to the banking system.

   RBI as Central Bank has prescribed Cyber Security Framework which entails banks to take action as under;
   (RBI circular /2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16)
   a) Board Approved Cyber Security Policy
   b) Cyber Crisis Management Plan
   c) Continuous surveillance
   d) Cyber security Preparedness Indicators
   e) Conductive IT Architecture
   f) Reporting to RBI
   g) Comprehensive Network and Database security
   h) Organisational arrangements
   i) Protection of customer information
   j) Cyber security awareness

2) **Elements of Cyber Security Preparedness:** Cyber security is difficult to achieve unless a comprehensive policy is at the center of the various actions required to be taken. Various elements of cyber security preparedness are as under;



3) **Implementing Deception technique as innovative and false positive free solution**: Deception Technique for handling cyber security is an effective and forward looking solution and should be used actively. Deception techniques is based on certain premises. Few of them are as under;

   a) Start **"assuming compromise of Information Systems"**
   b) Stop trying to prevent intrusions, **prevent breaches**
   c) Institute **adversarial thinking** in your defence team
   d) Make sure threat intel is **contextual and relevant to you**
   e) Deception is an **effective, false-positive free** way to increase your intelligence and detection capabilities

4) **Learning from J P Morgan's Model Plan of Cyber Security:** J P Morgan's Cyber security strategy and implementation is exemplary. It can be guiding lesson for planning comprehensively by Indian banks.

   JP Morgan's Cybersecurity objective is to ensure that they are able to effectively detect, prevent, and respond to cyber threats against their technology infrastructure. Their scope of Cybersecurity comprises detection and monitoring of threats and vulnerabilities, managing security incidents, and evolving preventive infrastructure

to keep ahead of the threat. They accomplish this through strong information security leadership and active collaboration with line of business partners to provide high quality security solutions and services that are focused on improving the firm's risk posture.

While they make a huge effort to protect their own company in terms of cyber security, they also try to help protect their clients from cyber threats as well. They have extensive fraud and malware detection capabilities that significantly reduce wire fraud on their customers. They have increased client cybersecurity education and awareness programs, having communicated with more than 11,000 corporate customers on this topic and hosting nearly 50 cyber security client events in 2015. They make substantial investments in proactive cyber risk defense measures and capabilities.

5) **Use of Free Tools to Build Cyber Security Solutions:** Microsoft offers lot of free tools which can help in detection and mapping of cyber threats which can be used by banks for cyber security architecture.

6) **For Tackling Next Generation Cyber Threats, Using Big Data, Machine Learning, Big Bounties, Red Teams, Making cyber threats viral etc**: Some options or solutions for handling next generation cyber threats can be use of Big Data Analytics, use of Machine Learning models, use of Open source and cloud, use of Big Bounties, use of Red Team Assessments, Making cyber security go viral and use Deception techniques etc.

   The cyber security product landscape is basically built on weak foundations. Combined with process weakness, it is further worsened by lack of security metrics, cyber security breaches are bound to take place. As Peter Drucker says 'If you cannot measure it, you cannot manage it'. Such innovative tools and techniques can help to go beyond perimeter security.

7) **Using Cyber Insurance:** As cyber breach is unavoidable because of the kill chain and the technology behind the cyber-attacks, mitigation of cyber risk through 'insurance solutions' can be an effective protection mechanism for banks. Insurance solution for banks involves protection against cyber threats, cybercrime, cards crimes, and offer a blanket bond to bankers for burglary, theft, gold adjuster's fraud, cash or premise frauds, cash in transit frauds, other operational frauds etc. Cyber Risk Insurance policy should broadly cover a) Privacy and data liability b) Cyber theft c) Business interruption d) First party expenses.

8) **Factoring Cyber Risk into Legal Risk:** The Legal Risk to banks is further enhanced by Cyber Security breaches, which has to be factored in overall risk management at the banks. Awareness of legal implications of cyber issues need to be improved in banks staff and customers.

9) **During the freewheeling discussion at the conclusion of the Seminar, certain very interesting and important action points were arrived at, which are as under;**

A) **Setting up Banks own SOC:** It may be a feasible idea to think of setting up and running a Security Operations Centre (SOC) by few banks (NPCI like arrangements). This was felt necessary by participating banks in view of the inevitability of relying on the same limited number of private sector players in this field. With their limited stock of experts, these firms/units which may not be able to give best persons to everyone, though they charge for it. Citi Bank SOC could be a good case study.

B) **Setting Up Banks Own IS Audit Entity:** IS Audit or Cyber Security Audit other than RBS as required under Cyber Security Framework is now assigned mostly to the big four like firms. As this excessive reliance may not be good for the banks, it was suggested that banks themselves can create their own common body (like NPCI), which can specialize and conduct Cyber Security Audits.

C) **Building Cyber Security Preparedness Training:** Use of Gaming (like War Games used by Citi) for Building Cyber Security Preparedness Training**.** For building cyber security literacy and protection culture in the bank staff and clients, creation of war-strategizing games and on the lines of those being used by Citi Bank could be adopted by other banks, with required infrastructure build up.

D) **Mapping IDRBT 300 Red Flags with RBI Cyber Security Framework Requirements for Ease of Implementation**: There was a suggestion that the IDRBT 300 Red Flags for cyber security could be grouped and mapped to Cyber Security Framework prescribed by the regulator to create a checklist for assessing cyber frame work in banks. This may help in implementation and monitoring of envisaged cyber security framework.

E) Sharing case studies on CISO platform

F) **Guidelines for Cyber Security Insurance:** Regarding Cyber Insurance, participants felt the need of some regulatory guidelines. It should not turn out to be costlier than the losses expected.

Compiled by Ravi Sangvai, PD, CAFRAL