Annexure A

TLP: AMBER

CERT-Fin Advisory- 201155100308

Advisory for Financial Sector Organisations – RBI and SEBI

Overview

It has been learnt that some of the financial sector institutions are availing or thinking of availing Software as a Service (SaaS) based solution for managing their Governance, Risk & Compliance (GRC) functions so as to improve their cyber security posture. Many a time the risk & compliance data of the institution moves cross border beyond the legal and jurisdictional boundary of India due to the nature of shared cloud SaaS. While SaaS may provide ease of doing business and quick turnaround, it also brings significant risk to the overall health of India's financial sector with respect to data safety and security.

Description

If the following data sets fall in the hands of an adversary/cyber attacker, it may lead to unprecedented increase in the attack surface area and weakening of Indian financial sector infrastructure's overall resilience.

- Credit Risk Data
- Liquidity Risk Data
- Market Risk Data
- System & Sub-System Information
- Internal & Partner IP Schema
- Network Topography & Design
- Audit/Internal Audit Data
- System Configuration Data
- System Vulnerability Information
- Risk Exception Information
- Supplier Information & it's dependencies related Data

Solution

The Financial Sector organisations may be advised to protect such critical data using layered defence approach and seamless protection against external or insider threat. The organisations may also be advised to ensure complete protection & seamless control over their critical system by continuous monitoring through direct control and supervision protocol mechanisms while keeping such critical data within the legal boundary of India.

The organisations may also be requested to report back to their respective regulatory authority regarding compliance to this advisory.

It is requested that you may kindly keep CERT-In informed of the actions taken and periodically provide the updated compliance to this advisory.

(It may be noted that TLP Amber means: Limited disclosure, restricted to participants' organizations.

When should it be used: Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

How may it be shared: Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.)