Comments on

Report of the Working Group for Setting up of Computer Emergency Response Team in the financial sector (CERT-Fin)

Advisory Board for CERT-Fin

The Working Group has recommended that Advisory Board for CERT-Fin may comprise government representatives and it may invite experts for discussion on need basis. It is necessary that Advisory Board has its ear on ground, keeps tab of relevant technological developments, and is aware of consumer concerns. Consequently, it is suggested that few external experts, including consumer representatives, be nominated as members or permanent invitees to meetings of Advisory Board.

Importance of disclosure for consumer empowerment

The Working Group has rightly recommended that the CERT-Fin may do analysis of financial sector cyber incidents, understand the pattern and nuances across financial sectors and also report the cyber security incidents to CERT-In.[1]

However, because CERT-Fin's mandate also includes generating cyber security awareness, the authority should also recognise the importance of public disclosure of information about incidents of breach. Public disclosure would help tackle information asymmetry and will infuse trust in the financial system. It would also enthuse intermediaries and financial institutions to adopt "Security by Design", thereby encouraging institutions to pro-actively check underlying vulnerabilities.

In addition to this, data breach disclosure norms should be framed, with penalties for non-disclosure. This would incentivise financial institutions to swiftly report cyberattacks instead of keeping mum to avoid reputation loss, regulatory intervention and liability.[2]

Balancing regulatory burden with incentives to innovate

[1] The Report, p.69

[2] http://www.livemint.com/Opinion/3tRRZowP1ivg06CQKZ5y8H/Incentivising-financial-sector-cybersecurity.html

Government regulations can have both positive and negative effects on the innovation process.[3] While the CERT-Fin has been empowered to offer policy suggestions for strengthening financial sector cyber security to all stakeholders including Regulators/Government,[4] it should be mindful beforehand, about the effect of its recommendations on innovation and competition in the vibrantly growing financial sector.

To this end, it would be beneficial to recognise the importance of maintaining a certain level of balance between regulations and ensuring incentives to innovate in the market. This would entail recommending optimally stringent security policies which do not over burden stakeholders, thereby chilling innovation and competition. Conducting Regulatory Impact Assessment (RIA) before providing policy recommendations to regulators or the government could be made a necessary prerequisite for CERT-Fin. This would in turn require the necessary additions vis-a-vis building internal capacities of the institution.

Critical infrastructure in financial sector

The Working Group has rightly highlighted the need to identify protected systems/ critical infrastructure in the financial sector. It would have been useful if the Working Group would have provided some indicators from a cyber-security perspective to identify the critical infrastructure.

****

[3] https://www.oecd.org/sti/inno/2102514.pdf
[4] The Report, p.70