Standing Committee Report Summary

Cyber Security and Rising Incidence of Cyber Crimes

- The Standing Committee on Finance (Chair: Mr. Jayant Sinha) submitted its report on 'Cyber Security and Rising Incidence of Cyber/White Collar Crimes' on July 27, 2023. Key observations and recommendations of the Committee include:
- **Regulation of service providers:** The Committee noted that there have been challenges in exerting sufficient control over third-party service providers on cyber security matters. It recommended enhancing regulatory powers to oversee and control such service providers including big tech and telecom companies. It also noted that big tech companies should not disregard inputs from regulators such as the Reserve Bank of India (RBI) to make their systems more secure.
- **Critical payment systems**: Downtime in critical payment systems can disrupt customer services. However, they are not currently regulated. The Committee recommended that such payment systems should work closely with financial institutions to improve uptime and address issues in critical payment systems. This can be done by investing in robust infrastructure, conducting regular security assessments, and establishing incident response mechanisms.
- **Regulatory framework:** The Committee observed that it is important to secure critical financial infrastructure against cyber threats. It emphasised on the need for a comprehensive legal framework involving robust policies, regular risk assessments, and an incident response plan. Such a regulatory framework may be established by: (i) promulgating new rules, (ii) amending the Digital India legal framework to address cyber security matters, or (iii) bringing a new cyber security legislation.
- **Cyber Protection Authority:** The Committee noted that the current regulatory landscape for cyber security involves multiple agencies and bodies. This requires a high level of inter-ministerial coordination. There is no central authority or agency solely dedicated to cyber security. The Committee recommended establishing a centralised Cyber Protection Authority (CPA). The authority would develop and implement robust cyber security policies, guidelines, and best practices in collaboration with states and private sector entities.
- **Challenges faced by smaller financial institutions:** Institutions such as cooperative banks, non-banking financial companies (NBFCs), and other smaller participants have a higher number of cyber security incidents as compared to commercial banks. There is a significant disparity in conducting cyber security audits between cooperative banks and commercial banks. Only 11% of cooperative banks have undertaken such audits. NBFCs, cooperative banks, merchants, and vendors face challenges due to limited manpower and technological capabilities. The Committee recommended that such entities should prioritise investments in cyber security infrastructure, advanced threat detection systems, and secure data storage practices. They should also conduct regular audits and assessments to identify vulnerabilities.
- **Sharing data:** Expanding digital landscapes along with the presence of search engines and big tech companies has increased the vulnerability of digital ecosystems to cybercrime. This requires a clear delineation of responsibilities for search engines and global tech companies. The Committee recommended that application stores should be mandated to share exhaustive metadata and information on all applications that they host on their platform. This data repository will empower regulators to identify potential security vulnerabilities and take needed measures. In addition, tech companies should: (i) regularly update and patch their operating systems and (ii) enforce a stringent vetting process for approvals within their application stores.
- **Central Negative Registry:** The Committee recommended the creation of a Central Negative Registry which would be maintained by the CPA. The registry should consolidate information on fraudsters' accounts. The registry should be made available to banks and NBFCs which would proactively deter and prevent the opening of accounts associated with fraudulent activities.
- **Compensation for frauds:** The existing compensation mechanism for cybercrime victims in the financial sector has limited scope and coverage. The process for filing compensation claims is complex and it places the burden of proof on the victims. The Committee recommended that it should be the financial institution's responsibility to compensate the customer in cases of frauds.
- **Information Technology Act:** The Committee noted that due to inadequate enforcement and the bailable nature of most offences under the Information Technology Act, 2000, fraudulent activity has persisted. It recommended implementing stricter penal provisions, imposing stricter bail conditions, and considering provisions for local surety.

Tushar Chakrabarty
tushar@prsindia.org

July 31, 2023