THE HINDU BusinessLine
FRIDAY, NOVEMBER 8, 2019

Towards transparency

The suggestions on changes to the CIC framework are welcome, but implementation will be the key

It is now fairly obvious that the fast-paced growth in non-bank finance companies over the last few years is partly due to some companies bending the rules and, at times, flouting them as well. The RBI working group under Tapan Ray, that was given the task to review one of the troublespots in the NBFC regulatory framework — core investment companies (CICs) — has made some good suggestions. While the supervision of CICs can improve going ahead, these regulations, if adopted, may not be able to fix the damage already done. The CICs, which hold at least 90 per cent of their net assets as investment in equity, debt or loans in group companies, were under less stringent regulation; it was believed that these entities would be taking lower risk since they have exposure to group entities alone. But the loopholes in the rules have been exploited by some groups, leading to regulatory problems.

Scan & Share

For instance the expanded definition of 'Group' in the regulation — that includes subsidiaries, joint ventures, associates, promoters and related parties — led to CICs dealing with many unregulated entities. Many groups had multiple CICs, and each CIC would raise funds independently to invest in group companies or other CICs. Thus funds were being raised by CICs, step-down CICs as well as by group companies, increasing the group-level gearing. Since some group entities are not governed by any regulator, it was difficult to gauge the extent of leverage in these entities. Also, while CICs are currently restricted to dealing only with group entities on the asset side, there is no such restriction on liabilities. They can borrow from markets, mutual funds and other investors through commercial papers, non-convertible debentures and inter-corporate deposits, for investing in or lending to group companies. The suggestion to restrict the number of layers of CICs in a group to two, will help in multiple ways including reducing leverage, improving transparency and making regulation easier. Stipulating that capital contribution by a CIC in a step-down CIC, over and above 10 per cent of its owned funds, should be deducted from its adjusted networth, will help rein in the borrowings of these entities. The suggestions regarding mandating a group risk management committee, audit committee and nomination and remuneration committee will help improve governance of such groups and ensure that shareholder wealth is protected.

While the changes will certainly help improve governance in CICs, the RBI should be careful about the manner in which the rules are implemented. The glide path of two years given to existing CICs to reduce the adjusted networth and for step-down CICs to stop investing or lending to other CICs may not be enough. Periodic on-site inspection by the RBI is a good idea as is off-site reporting of disclosure relating to leverage at the CIC and the group level. But the RBI should ensure that the changes do not lead to fresh problems.

FROM THE VIEWSROOM

New challenges for Indian techies

Staffing concerns rise as US tightens issue of H-1B visas

Has the software services industry moved quickly enough to avoid getting hurt by the Trump administration's tightening up on H-1B visas? The industry has been preparing for this visa squeeze for several years, especially since Donald Trump amped up his anti-immigrant talk. But now it's crunch time. Visa rejection rates for Indian software services companies have quadrupled since 2015 from about 6 per cent to around 24 per cent, according to a study by a think-tank, the National Foundation for American Policy.

By comparison, American companies like Amazon and Google which are also facing slightly more rejections, are still much better off. Their rejection rates have climbed from 1 per cent to anywhere between 3 per cent and 5 per cent. For Indian companies this means forward planning is suddenly much tougher. If, for instance, they want to send 100 staffers for a project, they face the prospect of only around 75 getting visas, leading to obvious difficulties. That's not all. Even staffers already in the US, who in earlier years could renew their visas easily, now face the prospect of up to 12 per cent of what are called 'continuing employment' visas being refused. That could mean huge upheavals, especially if they've moved there with their families.

The Indian software service giants have been hiring more in the US and even shifting some work to Canada. But the entire software services model is built on the fact that it's cheaper to hire software programmers in India, so there's a limit to how much onsite or near site hiring can be done without affecting costs. All this means uncertainty for software services companies and their employees, most of whom are eager to get coveted foreign postings.

At this rate, the long-term competitiveness of Indian companies could get affected. But the fact remains that US universities don't produce anywhere near enough graduates to feed their hi-tech industry's huge demand for personnel. Indian software engineers can fill the gap — at least for now.

Paran Balakrishnan Editorial Consultant

Is India cyber security ready?

The recent breach at the Kudankulam Nuclear Power plant and the way it was handled leave a lot to be desired

N MADHAVAN

MATTERS OF FACT

Towards end-October, social media was agog with reports of a cyber attack at Kudankulam Nuclear Power plant. The Nuclear Power Corporation of India Ltd (NPCIL), on October 29, denied such a development and said both the reactors were running without 'any operational or safety concerns'.

In a disturbing move, within 24 hours, NPCIL ate its own words and admitted that there indeed was an incident. Computer Emergency Response Team (CERT-In), it said, had noticed a malware attack that breached India's largest nuclear power facility's administrative network on September 4.

Further investigations had revealed that a user had connected a malware infected personal computer to the administrative network.

NPCIL emphasised that the nuclear plant's operational systems were separate (in technical parlance this is called an air-gap) and the administrative network was not connected to it. Hence there was nothing to fear.

Scan & Share

What is more worrying than NPCIL's somersault was its lack of openness (the attack happened almost 55 days earlier), reluctance to share any details about the nature of the malware and, most importantly, obfuscate this grave development by saying that 'any attack on the nuclear power plant control system is not possible' as they are standalone systems.

The malware, DTRACK, was developed by a North Korean hacker group and specialises in extracting information from a system. *The Washington Post* has quoted Virus Total, a virus scanning website owned by Alphabet (Google's parent), saying a large amount of data was stolen during the breach. This, data, the paper added, could be used to plan the next attack more efficiently.

Also, NPCIL's faith on air-gap or an isolated network is laughable. Iran's Nantez Uranium Enrichment facility that was attacked in 2010 was air-gapped. The attack, the world's first use of a digital weapon, destroyed 984 centrifuges thereby setting Iran's covert nuclear weapon programme back by a few years.

The attackers — many point the finger at US and/or Israel — used the Stuxnet worm and chose not to attack Nantez directly but focussed on infecting four companies that were contracted to work in the facility. When one of the workers from these companies used a USB drive at the Nantez facility, the worm was deployed. It destroyed the centrifuges by spinning them at dangerous speeds. Thus air-gapping is not fool-proof as NPCIL would like us to believe.

With India's nuclear facilities located not too far from densely populated areas, fear of a potential nuclear meltdown (the worst outcome of a cyber attack) should make our policymakers paranoid over cyber threats. The way the Kudankulam incident was handled inspires very little confidence.

Lackadaisical approach

The larger issue here is whether India is prepared for cyber attacks which are increasingly seen as the fifth dimension in warfare after air, water, land and space. The threat level is high. According to cyber security major Symantec, India is among the top three countries in the world after the US and China when it comes to phishing and malware attacks.

Not serious India isn't doing enough to protect itself from cyber attacks ISTOCK

Other reports reveal that its share in mobile malware (they enter through apps) is reportedly a high 23.6 per cent. In 2017, there was one security breach every 10 minutes in India. This data has to be taken with a pinch of salt as many cyber security incidents go unreported.

But our approach to this serious issue is, at best, lackadaisical — be it as an individual, corporate or government. Indians still prefer to use pirated software. Hackers exploit vulnerabilities in the software and without the frequent patches the developers send (pirated software user will not get it), the computer will be a sitting duck.

Also, they are contend with just anti-virus which is just one feature of end-point protection. Most companies do not invest in quality people when it comes to manning the IT team. This despite cyber security been considered as an executive-level challenge.

Most companies also lack a proper cyber security framework and standard operating procedures. Even if they have one, there is a need for constant training and awareness.

Not many employees think twice before opening attachments or inserting a USB drive. Weak passwords are a bane and reminders to periodically change them are often met with a frown.

With companies now adopting bring your own device (BYOD) policy, risks have only risen. Under the circumstances, businesses need to constantly test compliance through periodic audits. Those in critical sectors must also do vulnerability testing and even get ethical hackers to test their defences. Very few do this.

Lessons from Estonia

India cannot be cyber security ready unless the issue is taken up on a mission mode and in this Estonia, the northern-most of the three Baltic states, has some lessons for us. When this tiny nation (population 1.3 million) broke away from Soviet Union in 1991, it barely had any infrastructure, physical or digital. Today, it is one of the most digitalised countries in the world. All government services are delivered online. As much as 99.6 per cent of the banking transactions are done digitally. All the schools have been digitised and exams, homework and attendance are available at the click of a mouse. In fact, 28 per cent of people voted online in the last Parliamentary elections in 2018.

In 2007, Estonia was subjected to a brutal cyber warfare (Russia is blamed for it).

The Distributed Denial of Service (DDOS) attack crippled 58 Estonian websites. ATMs did not work. Online banking services failed and media houses could not broadcast news. Estonia adopted a transparent approach to this incident and cut itself off from rest of the Internet. It managed to defend itself well. It was a wake-up call.

It learned from the experience and built a strong intrusion detection and protection systems, created awareness among people, built a strong public-private partnership to tap resources, put in place a central system for monitoring, reporting and resolving cyber incidents and mandated vital service providers to assess and manage their ICT risks regularly.

It also created a voluntary Cyber Defence Unit where experts who work elsewhere chip in to protect when called.

Estonia has also become proactive on cyber security. It ensured that NATO Co-operative Cyber Defence Centre of Excellence was set up in its capital Tallinn. Its annual scenario-based real time network defence exercise, Locked Shields, conducted since 2010 is considered the world's largest and most complex. Today, when it comes to cyber security Estonia is among the top five nations in the world (India is not in the top 20).

Recently, it has offered to help India on this front. We should grab this opportunity with both our hands.

Azadi March in Pakistan, a damp squib

With the Pakistan Army firmly behind Imran Khan and the Opposition divided, Fazlur Rehman's protest will soon fizzle out

D SUBA CHANDRAN

The much hyped 'Azadi March' of Maulana Fazlur Rahman, that started from Karachi on October 28, has entered Islamabad and is making global headlines. But neither will Prime Minister Imran Khan resign nor will elections happen immediately. Despite mobilising thousands of his party cadres, Fazlur will fail in his primary objectives for the following four reasons.

First, does Rahman seriously believe that his Azadi March would force Imran Khan to resign? Rehman is a pragmatic politician, and would know the practicality of his demand. More than Imran's resignation, the Azadi March is meant to keep Rehman politically relevant.

Though the Jamiat Ulema-e-Islam under Fazlur Rehman (JUI-F) was not electorally successful during the last two decades, the 2018 election was the worst, for both the party and Rehman. Following the 2013 elections, the JUI-F had 15 seats in the national Assembly; Rehman had a better equation with Nawaz Sharif. In 2008, he won a Parliamentary seat and the party also did reasonably well. The 2002-08 period was the golden age for both. The JUI-F was a part of the coalition both at the national level and in the KP (Khyber Pakhtunkhwa) and Balochistan provinces.

When compared to the previous three elections, 2018 was a disaster for the JUI-F, as it did not win a single seat for the national Assembly. Rehman suffered a greater blow. The Pakistan Tehreek-e-Insaf (PTI) won both the seats he had contested from, in Dera Ismail Khan, which was supposed to be his political and electoral fort.

Political support

Second, there is not much popular support for Rehman outside his party. Despite the failure in the government's performance, there is no visible public anger that would bring people to the streets and join the Azadi March. Thanks to the JUI-F's biased gender approach, one cannot see women as a part of the march; the upper middle class and those who are not in favour of a mullah narrative within civil society are also not backing the march.

A march for political relevance REUTERS

The Prime Minister has smartly succeeded in diverting the public opinion. Khan's anti-India, anti-Modi and pro-Kashmiri slogans and rhetoric have become the primary policy pursuits of his government. Had it not been for India's new initiatives in Jammu and Kashmir and New Delhi's reluctance to engage Pakistan, Khan could have been facing a serious public outcry.

Though the march started in Karachi and entered Islamabad via Punjab, there is also not much support for Rehman amongst the Pakistani Sindhis and Punjabis.

Third, the opposition is not united behind Rehman. Much to the JUI-F leader's dismay, the two leading parties — the Pakistan Muslim League-Nawaz (PML-N) and the Pakistan Peoples Party (PPP) — are not fully supporting the march. Only the smaller parties at the national and provincial levels have rallied behind Rehman.

The PPP is facing its own demons. Former leader Asif Ali Zardari is unwell and his participation is out of question. Bilawal Bhutto is playing a cat-and-mouse game in taking part in the Azadi March. The PML-N seems to be a divided house. While Nawaz Sharif, the party chief, may be keen to support Rehman, his younger brother Shabaz is not. The latter is aware that the Pakistan Establishment stands behind Imran Khan, and asking for his resignation is akin to banging one's head against the wall.

Military backing

If there are any doubts about where the Establishment stands on the Azadi March, it was cleared by Major-General Asif Ghafoor, the Director General of Pakistan's Inter-Services Public Relations (ISPR). Responding to Rehman's demand that the institutions should remain impartial, Ghafoor commented that the army's support "lies with a democratically elected government." Clearly, the military is with Khan. The Establishment's primary objective is to keep the PPP and PML-N away.

As a result, the Prime Minister will not go. Rehman's march will fizzle out just as Khan's did in 2014. Had it not been for the terrible terrorist attack in Peshawar in December 2014, Khan would not have gotten a face-saving exit from his Azadi March against Nawaz Sharif.

Rehman can stand firm and stay put in Islamabad. But for how long, especially with winter approaching and the PML-N and the PPP not joining in? Without active support from the two parties, Rehman will beat a hasty retreat. In the name of national interest and regional environment, the Establishment may also intervene and ask him to stand down; perhaps by diverting people's attention back to Kashmir.

The writer is a Dean and teaches Global Politics at the National Institute of Advanced Studies, Bengaluru

LETTERS TO THE EDITOR

Send your letters by email to bleditor@thehindu.co.in or by post to 'Letters to the Editor', The Hindu Business Line, Kasturi Buildings, 859-860, Anna Salai, Chennai 600002.

Reviving project finance

This refers to the editorial 'RIP project finance' (November 7). The entire financial sector is passing through a credibility crisis due to accumulation of massive volume of NPAs and frauds surfacing time and again. The uncertainty in terms of movement of interest rates and slowness of the economy have made people/institutions look at short-term goals instead of locking funds long term. This has led to a severe asset-liability mismatch, forcing banks to borrow short and invest in long term projects with gestation period ranging from 20 to 30 years.

The transition of developmental financial institutions (DFIs) like IDBI and ICICI into commercial banks has severely impacted infrastructure funding since the skill sets required for long- and short-term funding are totally different. Also, DFIs found commercial lending more profitable and less tedious is terms of skill sets required and follow-up measures *vis-à-vis* project finance. This had forced banks to adopt a "collateral approach" to project finance as they totally lacked risk-assessment skills required for financing long-term projects. Constraint in capital can also be cited as another reason for banks' refusal to commit to infrastructure funding. Hence to solve the infrastructure financing need of the country, it is time the government set up DFIs exclusively to ensure seamless flow of funds into this sector.

Srinivasan Velamur
Chennai

Long-term lending woes

Though it is unfortunate that institutions are shutting the gate for project finance, the ground reality is that long-term lending comes with a lot of risks. The reasons for the failure of project financing are poor performance of corporates due to lack of demand, humongous NPAs that are created in the process and the Herculean effort needed in liquidating them, money laundering by unscrupulous borrowers, dearth of long term funding sources, and poor skills in appraising a project's viability. The clear message is that commercial banks with short-term funds should not be compelled to enter project financing, as that is one of the main causes of liquidity pressure banks face.

NR Nagarajan
Sivakasi

Funding of realty projects

This refers to 'Centre to open ₹25,000-crore window for stalled realty projects' (November 7). The move is bewildering as most realty projects have come to a standstill owing to demonetisation, indicating that black money was the main source of funding. Second, the protests by home buyers point to non-compliance of the RERA Act, which was implemented mainly to protect the buyers from frauds and delays. Third, there are several real-estate projects which have not been completed for more than a decade, which must be probed. If the government is truly concerned about genuine home buyers, it must analyse the reasons for the slow progress of projects before offering huge amount of funds to developers.

Rajiv N Magal
Bengaluru

Regulating e-commerce

At a time when global e-commerce firms continue to be under the regulatory scanner, it is necessary to encourage only those products/services that are compliant with information security and financial norms. The authorities must act stringently against hackers and improve the rule-based/intelligent surveillance, to safeguard consumer interests. An advanced, tech-enabled mechanism coupled with sufficient user-awareness, can ensure integrity during operations. While the authorities ought to micro-monitor suspicious activities and illicit-content advertised over a host of online portals and social-media platforms, the restrictions should not affect the ease of communication, cost of transactions and pace of digitisation.

Recurring incidents of security violation and potential vulnerabilities posed by spyware/malware and ransomware can cause incalculable damage. Therefore, it is prudent to promote well-regulated alternatives and pre-validate the multi-featured applications before market launch and continually improve the techniques/algorithms used for authentication of underlying data.

Girish Lalwani
New Delhi

Published by N. Ravi at Kasturi Buildings, 859 & 860, Anna Salai, Chennai-600002 on behalf of THG PUBLISHING PVT LTD., and Printed by D. Rajkumar at Plot B-6 & B-7, CMDA Industrial Complex, Maraimalai Nagar, Chengleput Taluk, Kancheepuram Dist., Pin: 603209. Editor: Raghavan Srinivasan (Editor responsible for selection of news under the PRB Act).

ISSN 0971 - 7528