*Targeted Attacks: Protection of Critical Infrastructure of the Country & Capacity Building**

R. Gandhi

I am indeed glad to be present here today as we conclude the deliberations on an important topical area – pertaining to cyber security and protection of critical infrastructure from cyber threats, coupled with capacity building in this crucial area of importance. I must congratulate the organisers on having chosen the theme of this summit, given the concerns emanating from cyber security related incidents.

2. We are at a critical juncture in the world of today which is characterised by rapid advances in the use of Information and Communication Technology (ICT) and where misuse of the facilities results in erosion of public confidence apart from resulting in financial loss and disruption of normal activities. Today's world is witnessing the embedded use of IT in almost all spheres of life; be it in business or financial sector; be it government or household sectors, use of ICT is pervasive; even as mundane as switching a light is today executed by use of ICT; in addition, networked devices are now the norm. New concepts such as centralised processing systems, the internet of things and mobile computing have all made life very easy; but this also has the attendant risks, prime among which is cyber security. The financial system which is at the nerve centre of economic activity is an easy target not only because it is one of the largest users of Information and Communications Technology but also because financial crime results in easy access to money; this also makes it important that cyber security is given its due importance.

3. Recent developments in banking as also payment and settlement systems have resulted in enhanced customer comfort and flexibility in terms of timing, location and choice of channels. These, however, also expose the customers as well as banks to risk of cyber-attacks. While the banks have better resilience in terms of risk mitigation structures and ability to absorb the losses and expenses, the customers may not be so privileged. A relatively small value fraud of a few thousands of rupees may endanger the purchase of basic needs and most customer may be ill-equipped to effectively handle the security features provided with the service. We have also heard of instances, elsewhere in the world, of even as small a value of one penny being robbed off every transaction, misusing the ICT capabilities, which have also resulted in loss of enormous amount of money. While it is recognised that the customer has to protect himself against disclosure of sensitive passwords, PINs *etc.*, they may only have limited ability to distinguish between the genuine customer service calls and fraudulent operators.

Nature of cyber crime

4. Cyber criminals and the attacks they launch on financial sector and its users come with different faces. There are organised criminals who are looking to attack the financial institutions, with a view to siphon away funds, illegally. Then there are those who steal confidential data from financial institutions which may also include customer related information. The latter are more interested in ex-filtration of data, though no loss happens immediately. These stolen data then land in the hands of petty criminals, who defraud the banks directly or by enticing the customers to share more information such as passwords and pins where after actual loss takes place.

* Speech delivered by Shri R. Gandhi, Deputy Governor in the Valedictory Session of the 9th Annual Summit 'CYBER & NETWORK SECURITY' organised by ASSOCHAM along with the Council of Europe, Strasbourg, France on 29th July 2016 in Hotel Hyatt, Bhikaji Cama Place, New Delhi. Assistance provided by Shri S Ganesh Kumar, CGM is gratefully acknowledged.

5. A variation of these attacks is to masquerade as bank officials and extract information from customers, based on random calls to phone numbers obtained from various sources, or even by blind trials which result in at least a few attempts resulting in success.

6. There are other cyber criminals who steal money by putting through fraudulent transactions, or changing the particulars, so that they are able to take large sums away and vanish. In such cases, customer may not be directly contacted, but his particulars are taken through malware or other means. Recent incidents of this type have set the alarm bells ringing. I would like to draw your attention to the recent cyber incident reported by one of our banks, which I am sure all of you would have seen, particularly when similar incident at a central bank in the neighbourhood is still fresh in our memory.

7. Yet another vicious cyber-attack, which we really tread is what is categorised as cyber warfare; this is expected to be of organised attacks, sometimes by backing of large terrorist organisations and often with covert state sponsorship, made against enemy country information assets.

8. The different nature of cyber-crimes naturally require responses which are designed to fight each type of threat, with specifically designed tools and practices. I am sure that during the deliberations of the day, these have all been discussed threadbare so I shall not dwell in details about these. I would, however, outline a set of five commandments which if followed in letter and spirit would mitigate the impact of cyber related risks.

Defence strategies – Protection is better than repenting later on

9. The strategy to build preventive and detective defences depends on the specific link in the asset that one is trying to protect. The ecosystem for financial transaction not only includes banks and their customers, but also network service providers, IT infrastructure providers, providers of managed services such as data centres, software developers, providers of security solutions and providers of the end-point device which is used for accessing the financial service, including the ATMs which may or may not be bank-owned / managed devices.

10. The devices which are used to provide the entire ecosystem produce huge quantity of information and activity logs, which contain crucial information which can throw light on potential attacks, even before the attack takes place. However, the humungous quantity of log data renders it impossible to analyse using conventional outlier detections. Conventional techniques result in considerable false alarms and restrict genuine activity, causing inconvenience and also creating mis-trust among the users about the security products and techniques.

11. Therefore, the focus has now been shifting to techniques which are not rule based, but having ability to identify the normal activity patterns and detect the anomalous and potentially harmful activity. Needless to say, these involve machine learning and soft computing techniques. Application of these techniques is expected to generate better hit-rate in terms of identifying threats, without generating high level of false alarms. As each alarm requires response and is resource intensive in terms of time, money and manpower, the ability of the expert systems to distinguish the malicious behaviour from and casual digressions from the normal activity pattern will determine the value of these tools in the security infrastructure.

12. In addition to the tools, the most important component of the critical infrastructure protection is the skills, experience and alertness of the manpower deployed in this activity. The skill sets required for security are getting diversified from conventional IT skills to investigative skills of criminal investigator,

data scientists having ability to deal with huge data requirements and with innovative minds to stay one step ahead of the cyber-criminal.

13. As the strength of overall security is only as much as the strength of its individual components, it is necessary that all the stakeholders have to work hand in hand to address the threat to the information systems. The forums such as this provide great opportunity to interact and understand the role that each one of us has to play and to also ensure that our actions and plans are complementary and not at cross purposes.

Cyber Security Preparedness – Five Commandments for safety in banking

14. Let me start with a most common requirement. **Thou shall know your customer –** which is my first commandment. All of us are aware of the requirements relating to Know Your Customer or KYC as commonly referred to. Much has been said, discussed and detailed about KYC that I shall not repeat all of them; suffice to say now that it is essential to know our customer well or else we shall have to face the consequences which may be detrimental to our business objectives.

15. The second commandment of mine states that **Thou shall know your employee**. Most of the cyber frauds have some direct or indirect role of an insider, who generally happens to be an employee of the organisation which has been the target of the cyber security attack. There is an urgent need for an organisation to not only perform the antecedent verification of an employee at the time of recruitment, but also continuously monitor employee behaviour, trends in operational usage of the organisational resources, interaction levels with peers and subordinates and the like. Today, IT tools provide a lot of information on employee behaviour and patterns; it is essential that organisations ascribe adequate importance to these aspects.

16. The third commandment reads as follows: **Thou shall keep your IT systems up-to-date and free of all risky components** such as viruses, spams, malware, spoofing software and so on. Today, there are centralised IT system facilities which can ensure that the updates are implemented centrally and also monitored centrally.

17. The fourth commandment is **Thou shall provide for maximum IT Governance**. The broad requirement in this area relates to the need for ensuring good IT practices such as 'maker and checker' for financial transaction processing, a four-eyes principle for IT based operations, regular monitoring of system and operational logs, conduct of regular, periodical and well defined IT system audit followed by suitable corrective action wherever required, and a separate distinct CISO (Chief Information Security Officer) who would continuously monitor the quality and efficacy of IT and IS Security in the organisation.

18. My final commandment is **Thou shall ensure continued Cyber Security Awareness** amongst all players in the chain. The world of cyber related threats is changing very fast and what is current on any day becomes obsolete the very next day. If continued cyber vigil is to be ensured then a continuous process of awareness building, education, re-enforcement, tests, trials and upgradation is a must. It is this area which we generally tend to be rather lax and which is exploited by cyber-baiters.

19. Let me dwell a bit on what the central bank of this country is doing in this regard. In terms of providing a comprehensive framework for IT implementation, we at the Reserve Bank have been proactive and follow an approach of consultation and congruence in the security framework. Right from the early days when the RBI provided guidance on computerisation, we have been conscious of the role that IT plays in meeting the emerging customer needs and the opportunities and challenges of using technology, including cyber related

aspects. I will draw your attention to a few recent initiatives in this regard by the RBI.

20. The Reserve Bank has recently issued on June 2, 2016 a comprehensive set of guidelines for Cyber Security framework in banks. These guidelines built over the earlier work emphasise the importance of having a focussed attention to cyber threats and framework for mitigating the threats and to protect the information assets. I would like to redraw your attention to the recent cyber incident at one of our banks. Apparently there has been no monetary loss in the recent incident. But it is too early to conclude what and how of the incident at this juncture; however, the need for vigil over the sensitive systems like remittances is once again brought to the fore, with particular focus on configuration of the systems and the human aspects in managing the systems. Banks need to put in place preventive measures such as appropriate controls framework around the systems, reconciliation of transactions in on real / near real time basis, controls over the message creation and transmission, applying timely security patches to the interfaces, if any, close monitoring of transactions and disabling USB, and Internet access on the connected nodes. Equally important is the timely detective measures. It is pertinent to prepare ourselves to face such incidents, by having a robust crisis management plan. I am sure the banks are taking earnest steps to comply with the provisions of the Circular as soon as possible. Time has come to scale up the cyber security preparedness to meet the emerging threats.

21. Information dissemination is a key facilitator in combating the menace of cyber related incidents. While the Reserve Bank obtains information from banks on cyber incidents, including those which did not fructify into loss of money or information, such information is also shared amongst the banks along with suggestions aimed at best practises. The Institute for Development and Research in Banking Technology also has a system to collate such information and share the generic aspects amongst the CISOs of banks. All these, I am sure will help the banks in further enhancing their cyber security related capabilities.

22. Let me end with a positive note. The banking sector – similar to other sectors of the Indian economy has always been very responsive to change and has adapted itself very well to meet the challenges which keep emerging frequently. It has also proved that it cannot only adapt well but also quickly so that response times are fast to prevent recurrence of negative incidents. The same fervour, I am sure, will be witnessed in the area of cyber security as well and will leave a mark of confidence in the minds of the customers of banks. This will ensure that banks provide for a safe and secure processing environment when the depositor's money is safe and where all other customers can conduct their banking transactions safely and securely.

23. I am sure that there are many take-aways from today's summit. I am also confident that these would be put to operational use when you all return to your respective organisations. I am grateful to you all for inviting me and for listening to my thoughts and I wish you all safe and secure IT based operations.

24. Thank you.