Committed to
professional excellence

बैंक क्वेस्ट

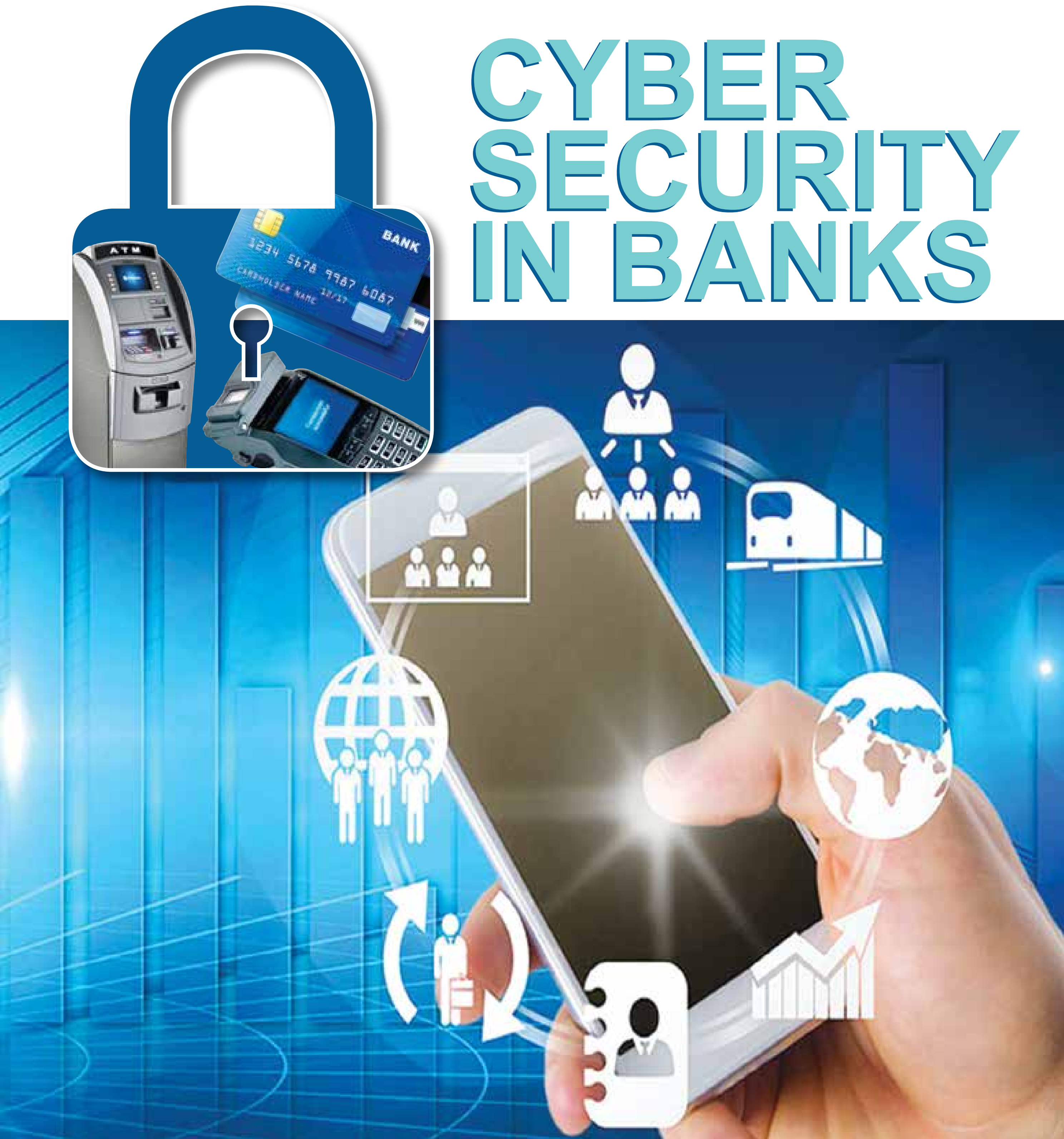
Bank Quest

Rs. 40/-

(ISSN 00194921)

The Journal of Indian Institute of Banking & Finance (ISO 9001:2015 Certified) खंड / Vol 89 / अंक / No 01 जनवरी - मार्च 2018 January - March 2018

CYBER SECURITY IN BANKS



IIBF - PUBLICATION LIST

Sr. No.	Examination	Medium	Name of the Book	Edition	Published By	Price (Rs.)
1	JAIIB / Diploma in Banking & Finance	English	Principles & Practices of Banking	2015	M/s Macmillan India Limited	Rs. 550/-
2	JAIIB / Diploma in Banking & Finance	Hindi	Banking ke Sidhanth Avam Vyavahar	2015	M/s Taxmann Publications Private Ltd.	Rs. 870/-
3	JAIIB / Diploma in Banking & Finance	English	Accounting & Finance for Bankers	2015	M/s Macmillan India Limited	Rs. 440/-
4	JAIIB / Diploma in Banking & Finance	Hindi	Bankeron ke liye Lekhankan Avam Vittya	2015	M/s Taxmann Publications Private Ltd.	Rs. 600/-
5	JAIIB / Diploma in Banking & Finance	English	Legal and Regulatory Aspects of Banking	2015	M/s Macmillan India Limited	Rs. 440/-
6	JAIIB / Diploma in Banking & Finance	Hindi	Banking ke Vidhik Paksh	2015	M/s Taxmann Publications Private Ltd.	Rs. 700/-
7	CAIIB	English	Advanced Bank Management	2017	M/s Macmillan India Limited	Rs. 690/-
8	CAIIB	Hindi	Unnat Bank Prabandhan	2011	M/s Taxmann Publications Pvt. Ltd.	Rs. 575/-
9	CAIIB	English	Bank Financial Management	2018	M/s Macmillan India Limited	Rs. 790/-
10	CAIIB	Hindi	Bank Vittiya Prabandhan	2012	M/s Taxmann Publications Private Ltd.	Rs. 725/-
11	CAIIB	English	Corporate Banking	2010	M/s Macmillan India Limited	Rs. 300/-
12	CAIIB	English	Rural Banking	2010	M/s Macmillan India Limited	Rs. 340/-
13	CAIIB	English	International Banking	2010	M/s Macmillan India Limited	Rs. 275/-
14	CAIIB	English	Retail Banking	2010	M/s Macmillan India Limited	Rs. 300/-
15	CAIIB	Hindi	Khudra Banking	2012	M/s Taxmann Publications Private Ltd.	Rs. 495/-
16	CAIIB	English	Co-operative Banking	2010	M/s Macmillan India Limited	Rs. 425/-
17	CAIIB	English	Financial Advising	2010	M/s Macmillan India Limited	Rs. 325/-
18	CAIIB	Hindi	Vittiya Pramarsh	2013	M/s Taxmann Publication Ltd.	Rs. 450/-
19	CAIIB	English	Human Resources Management	2010	M/s Macmillan India Limited	Rs. 300/-
20	CAIIB	English	Information Technology	2010	M/s Macmillan India Limited	Rs. 300/-
21	CAIIB	Hindi	Suchna Prodhyogiki	2013	M/s Taxmann Publications Pvt. Ltd.	Rs. 510/-
22	CAIIB	English	Central Banking	2010	M/s Macmillan India Limited	Rs. 300/-
23	CAIIB	English	Treasury Management	2010	M/s Macmillan India Limited	Rs. 385 /-
24	CAIIB / Certified Banking Compliance Professional Course / Certificate Examination in Risk in Financial Services -I	English	Risk Management	2010	M/s Macmillan India Limited	Rs. 450/-
25	Certified Banking Compliance Professional Course	English	Compliance in Banks	2017	M/s Taxmann Publications Private Ltd.	Rs. 1,135/-
26	Certificate Examination for Treasury Professional	English	Treasury Management	2010	M/s Macmillan India Limited	Rs. 385/-
27	Certificate Credit Professional	English	Banker's Hand Book on Credit Management	2014	M/s Taxmann Publication Ltd.	Rs. 745/-
28	Certified Bank Trainer Course	English	Trainers' Handbook	2013	M/s Taxmann Publication Ltd.	Rs. 425/-
29	Certificate Examination in Anti-Money Laundering & Know Your Customer	English	Anti-Money Laundering & Know Your Customer	2017	M/s Macmillan India Limited	Rs. 325/-
30	Certificate Examination in Customer Service & Banking Codes and Standards	English	Customer Service & Banking Codes and Standards	2017	M/s Taxmann Publications Pvt. Ltd	Rs. 400/-
31	Certificate Examination in Foreign Exchange Facilities for Individuals	English	Foreign ExchangeFacilities for Individual	2017	M/s Macmillan India Limited	Rs. 473/-
32	Certificate Course for Non-Banking Financial Companies	English	Non-Banking Financial Companies	2017	M/s Taxmann Publications (P) Ltd.	Rs. 615/-
33	Digital Banking	English	Digital Banking	2016	M/s Taxmann Publication Ltd.	Rs. 295/-

CONTENTS

Special Features

Bank Quest

Volume 89, Number : 1

January - March 2018
(ISSN 00194921)

The views expressed in the articles and other features are the personal opinions of the authors. The Institute does not accept any responsibility for them.

लेखों तथा अन्य रचनाओं में व्यक्त किए गए विचार लेखकों के निजी विचार हैं । लेखकों द्वारा व्यक्त किए गए विचारों के लिए संस्थान किसी प्रकार से उत्तरदायी नहीं होगा ।

INDIAN INSTITUTE OF BANKING & FINANCE
Kohinoor City, Commercial-II, Tower-I, 2nd Floor, Kirol Road, Kurla (W), Mumbai - 400 070.
E-mail : admin@iibf.org.in
Website : www.iibf.org.in

MISSION

The mission of the Institute is to develop professionally qualified and competent bankers and finance professionals primarily through a process of education, training, examination, consultancy / counselling and continuing professional development programs.

ध्येय

संस्थान का ध्येय मूलत: शिक्षण, प्रशिक्षण, परीक्षा, परामर्शिता और निरंतर विशेषज्ञता को बढ़ाने वाले कार्यक्रमों के द्वारा सुयोग्य और सक्षम बैंकरों तथा वित्त विशेषज्ञों को विकसित करना है ।

Printed by Shri J. N. Misra, **published by** Shri J. N. Misra on behalf of Indian Institute of Banking & Finance, and **printed at** Onlooker Press 16, Sasoon Dock, Colaba, Mumbai-400 005 and **published from** Indian Institute of Banking & Finance, Kohinoor City, Commercial-II, Tower-I, 2nd Floor, Kirol Road, Kurla (W), Mumbai - 400 070. **Editor** Shri J. N. Misra.

editorial

Dr. J. N. Misra
Chief Executive Officer,
IIBF, Mumbai

Sir Purshotamdas Thakurdas (Sir P. T.) was a distinguished and eminent businessman of India who took keen and active interest in the economic life of the country before and after independence. Sir P. T. was associated with the Indian Institute of Banking & Finance (Formerly Indian Institute of Bankers) as its founding member and served on the Council of the Institute till his death on 4th July 1961. In his memory, Indian Institute of Banking & Finance organises the Sir Purshotamdas Thakurdas Memorial Lecture every year.

The first article of this issue contains the edited extracts of the 34th Sir Purshotamdas Thakurdas Memorial Lecture on "Banking on Governance – Freedom From and Freedom To" delivered by Dr. M. S. Sahoo, Chairperson, Insolvency and Bankruptcy Board of India at SBI Auditorium on 18th December, 2017, under the auspices of the Indian Institute of Banking and Finance. Dr. Sahoo has spoken in detail about Economic freedom to internal freedom in this lecture, besides discussing about the Insolvency & Bankruptcy Code, 2016 & issue of Non Performing Assets (NPAs).

Cyber Security concerns in banking have always been the prime focus area of deliberations. The grave consequences of cyber-crimes have made banks to tighten their cyber security measures. With the objective of creating awareness about Cyber Security in Banks and sharing the knowledge in this area with our readers, we are publishing this issue of Bank Quest with the theme "Cyber Security in Banks".

The second article is penned by Mr. V. Rajendran, Chairman, Digital Security Association of India on "Banking on IT's Security". He has eloquently explained about the technical as well as legal aspects of cyber security, besides elaborating on the importance of Cyber Risk Insurance in this article.

The third article is on "A simple banker into Bank's Cybersecurity : Understanding the task, the role', written by Mr. S Mukhopadhyay, Former General Manager & Chief Information Security Officer, State Bank of India. He has discussed the challenges of Cyber Security & also suggested some preventive measures.

The fourth article is on "Cyber Security in Banks", by Mr. Burra Butchi Babu, Senior Domain Expert, Institute for Development and Research in Banking Technology (IDRBT). Cyber threat is an universal phenomenon and banks are part of the cyber space. Mr. Babu has discussed different aspects of cyber security threats in this article.

The fourth article is on "FATCA-CRS Compliance by Banks - Need for automation in data processing" written by Mr. R. Rajendran, Former Deputy General Manager, Department of Information Technology, Canara Bank. He has discussed the complexities involved in FATCA-CRS compliance in his article.

The sixth article is in Hindi on “साइबर क्राइम्स और उनसे सुरक्षा-एक परिप्रेक्ष्य” is written by Mr. Anand Shrimali, Former Deputy General Manager (Information Technology), Bank of India & presently working as a Faculty, Indian Institute of Banking & Finance. He has elaborated common examples of Cyber-crimes and also suggested the preventive measures to avoid incidents of cyber-crimes.

This issue also contains a Book Review by Mr. V. N. Kulkarni, Former Deputy General Manager and Principal, Management Development Institute of Bank of India, on the book “Credit 360° Appraisal Disbursement Monitoring and Recovery” by Shri Waman Gokhale.

We are also carrying a summary of a Macro Research Report (2014-15) of Dr. Sanjeev Bansal on “The Impact of Technology on the Performance of Indian Banking Industry: An Empirical Study” in this issue. Along with it, this issue also carries summary of Macro Research Report (2014-15) on “Quantifying Basel III’s time varying capital requirements and their impact on macro and financial variables over business and financial cycles” by Dr. Saurabh Ghosh.

We hope that this issue of Bank Quest will stimulate your interest. We thank all the authors for contributing their articles for Bank Quest. We also thank all the readers for showing their positive interest in our Journal.

Dr. J. N. Misra

Banking on Governance - Freedom from and Freedom to

Dr. M. S. Sahoo*

I feel honoured to join you here today to remember a great son of our soil, Sir Purshotamdas Thakurdas, who during his lifetime received several accolades for his values, intellect and leadership. Notably, he received these honours not only from his countrymen, but also from the British, despite being a severe critic of several policies and institutions of the time.

Sir PT, as he is fondly remembered, was a visionary businessman who always put the interests of the State above business and advocated close partnership between business and the State for nation building. He was a champion of free enterprise, and at the same time recognized the need for control and regulation and favoured a sizable public sector. He even served as a member of the National Planning Committee (with Pandit Nehru as Chairman) and co-created a fifteen-year investment plan, popularly known as Bombay Plan. He co-founded Federation of Indian Chambers of Commerce and Industry; blended commercial banking (Imperial Bank of India) with central banking (Reserve Bank of India); and did much more. As a Member of the Royal Commission on Indian Currency and Finance (1926), otherwise known as the Hilton Young Commission that envisioned the Reserve Bank of India, Sir PT strongly opposed demonetisation of sovereign and half-sovereign which were the only gold coins then. That was, of course, demonetisation of a completely different kind! Not surprisingly, this memorial lecture series has attracted a formidable list of eminent speakers.

Business has never been easy, not in the least in the colonial time. During Sir PT's time, business in general encountered several restrictions from the State and other external sources. To address those restrictions, Sir PT espoused a significant role of the State in freeing up firms and building their capacity to utilise the freedom. His vision quite resembled the contemporary policy quest for improving ease of doing business. I thank the Indian Institute of Banking & Finance for providing me with this opportunity to dwell on a key ongoing reform that confers the ultimate freedom on firms while improving ease of doing business.

Freedom From and Freedom To

Economic freedom for a firm is at least as important as civil freedom for an individual and is the foundation of a market economy. There are broadly two types of economic freedom, namely, 'freedom from' and 'freedom to'. The former, usually referred to as external freedom or negative freedom, is granted from outside. It is freedom from external sources that prescribe and prohibit what a business can do and what it can not. Greater external freedom means less restrictions from external sources, particularly from the State. Most economies, including India, as part of economic reforms, have been enhancing external freedom. On the other hand, 'freedom to', otherwise known as internal freedom or positive freedom, is generated within. It is freedom from sources internal to a firm. Many times, the firm self-imposes restrictions on its own freedom. As a result, it does not always perceive in its entirety the freedom that it enjoys or even when it does, restricts its choice set to what it feels comfortable with. This happens mainly because

***Edited extracts of the 34th Sir Purshotamdas Thakurdas Memorial Lecture delivered by Dr. M. S. Sahoo, Chairperson, Insolvency and Bankruptcy Board of India at SBI Auditorium on 18th December, 2017, under the auspices of the Indian Institute of Banking & Finance. Assistance by Mr. Vikash Singh, Consultant, IBBI is gratefully acknowledged.**

the firm does not have the capacity and will to realize the internal freedom. Therefore, at any point of time, while the external freedom is the same for all firms, the internal freedom can vary significantly from firm to firm.

Either of the freedom is not adequate in isolation for a firm; they complement each other in a virtuous circle. While expanding frontiers of external freedom, the State usually builds institutions to incentivise firms to use it and avoid its misuse. A firm, which is long accustomed to living without freedom and consequently not having adequate governance, initially finds external freedom uncomfortable. With a bit of hand-holding, it builds on its governance to generate internal freedom to use the available external freedom and flourishes in a market economy. It then deserves and demands more such freedom, which the State grants and the circle continues. It, however, requires considerable dexterity on the part of the State and the firm to expand the frontiers of external and internal freedom, respectively and to build institutions and governance to use freedom and avoid its misuse.

Freedom and Growth

The mainstream economic thought believes that at any point of time, human wants are unlimited while the resources to satisfy them are limited. The central economic problem, therefore, is inadequacy of resources vis-à-vis unlimited, ever-increasing wants. The mainstream legal thought believes that as a person moves from natural state to an economic state, it loses some degree of freedom. The central legal problem, therefore, is inadequacy of freedom to pursue economic interests meaningfully. Thus, we have twin inadequacies of resources and freedom. Fortunately, there are twin adequacies too, namely, resources have alternate uses and firms pursue their self-interests. An economy thrives if it harnesses the twin adequacies subject to twin inadequacies by allowing self-interested firms to have maximum freedom - external and internal, subject to minimum regulations that address market failure and do no more, to move resources, which can be put to alternate uses, from less efficient uses to more efficient ones continuously and seamlessly. This yields optimum freedom for firms to ensure optimum resource utilisation for optimum economic welfare.

Freedom expands choices for a firm. It allows a firm to undertake any business of its choice in the manner and scale it is comfortable with and thereby allows every firm to participate in the economy. It enables a firm to get in and get out of business with ease, undeterred by honest failures. The greatest success comes from having the freedom to fail.[2] Freedom unleashes and realises the full potential of every firm and every resource in the economy. It is well established that economic freedom and economic performance have very high positive correlation. Countries having high level of economic freedom generally out-perform the countries with not-so-high level of economic freedom. The index of economic freedom[3], which measures the degree to which the policies and institutions of an economy are supportive of economic freedom, has substantially improved for India since the 1990s. The outcome has been astounding; the growth rate since the early 1990s onwards has almost doubled as compared to the Hindu rate of growth in the preceding four decades.

Incentives and Nudges

It is relatively easier to provide external freedom. It, however, requires institutions to put such freedom to use. Institutions incentivise firms to build on governance that generate internal freedom matching external freedom. Acemoglu and Robinson[4] demonstrate that a key differentiator among nations is the quality of their institutions. The institutions define the incentive structure in economies, convert freedom to 'will', ensure voluntary participation of firms, incentivise discretionary efforts in the economic sphere and thereby play a significant role in scripting the economic success of countries. They assert that skills and resources are important inputs to economic

[2] Harvard's 366th Commencement Address, 25th May, 2017, Mark Zukerberg.

[3] 2017 Index of Economic Freedom, The Heritage Foundation.

[4] Why Nations Fail: The Origins of Power, Prosperity, and Poverty, 2012, Daron Acemoglu and James Robinson.

performance, but the determinant input is ‘will’. The State should provide the institutional milieu that (a) provides freedom to pursue a vocation, (b) creates a level playing field for good ideas to replace obsolete ones, and (c) encourages resources to chase the best productive avenues and thereby nurtures ‘will’ to bring out the best from her firms.

Degree of co-ordination necessary to create inclusive policies and institutions on a large scale often eludes all but a central authority, more so in a democracy like ours. The State and its institutions are uniquely bestowed with the mandate and the capacity to prescribe policies that have bearing on economic freedom. They have ended up, mostly by inadvertence and occasionally by design, with rules some of which are prescriptive and hence, restraining, instead of promoting, freedom of choice. Thaler and Sunstein[5] argue for less by the way of government coercion and constraint, and more by the way of freedom to choose. They assert if incentives and nudges replace requirements and bans, Government will be smaller and modest, and it will be easy to do business.

Context and Conduct

Economic freedom is of recent vintage and is evolving; so are the new organs of the State - the regulators and regulatory tribunals - who deal with this. It is yet to acquire the sophistication and sacrosanctity of civil freedom. Further, economic freedom is in a relatively fluid state - it is enhanced or curtailed easily depending on the economic thought and philosophy of the day and sometimes, even regardless. Take the example of right to property which used to be a fundamental right some time ago. It is not so now. Many statutes which restricted, or even denied economic freedom, have been repealed and many others modified in sync with a shift from the command and control regime to a market regime founded on economic freedom. The business, however, needs to remain open to adopt an evolving regime of economic freedom.

Economic freedom is not absolute. It has many shades of grey, probably because it is encapsulated in economic laws, a domain served by both economists and lawyers, who by their multifarious and often conflicting capabilities confuse the rest of us! The determination of an issue relating to economic freedom in each context requires that all possible legal perspectives are considered from all possible economic angles. Let me illustrate this idea with an anecdote. Four persons who had received show cause notices from the competition authority were discussing as to what caused them their predicament. The first person said he charged a price higher than others in the market and has been accused of abuse of market power. The second one said, he charged a price lower than anybody else and has been accused of predatory pricing and hurting competition. The third one said, he charged zero price and has been accused of creating entry barrier. The last one said, he charged the very same price as everybody else and has been accused of cartelisation.

Thus, different conducts invite the same outcome under economic laws while the same conduct may yield different outcomes in different ‘contexts’. So, it is not so much the conduct, as the context - who, why, when, what, where and how - of the conduct that matters. In civil laws, murder is bad irrespective of the context: who, why, when, where, etc. are not relevant. However, the same taxi fare can be bad in the morning and good in the evening under economic laws. Unfair pricing is bad if it is by a dominant enterprise and not otherwise. This is the genesis of the ‘rule of reason’ to guide economic freedom. This has the potential of arriving at either false negatives or false positives sometimes in a context. Further, while no one, not even the State, can encroach upon civil freedom, the State as well the market participants may encroach upon economic freedom in certain contexts for justifiable reasons, and yet not violate the law. The economic laws, therefore, allow greater latitude to businesses, but ascertaining the latitude and using it appropriately requires considerable dexterity on the part of the firm.

[5] Nudge: Improving Decisions about Health, Wealth, and Happiness, 2008, Richard H. Thaler and Cass R. Sunstein.

Ease of Doing Business

Business provides goods and services as well as livelihood to people and consequently determines their economic wellbeing. Better business regulations generally yield more business, which usually translates to higher economic wellbeing. It is, therefore, the endeavour of every economy to have better business regulations with a view to make it easier for its firms to do business.

The World Bank measures and ranks nearly 200 economies in terms of their respective 'ease of doing business', which is nothing but conduciveness of regulations to promote growth. This is done in terms of reforms in ten sets of indicators, which includes resolving insolvency. A couple of years ago, the Government set an ambitious target of being one among the top 50 economies in terms of doing business and towards this end, initiated deep institutional reforms, including an overhaul of insolvency framework. Consequently, India's rank in the ease of doing business improved from 142 in 2015 to 100 in 2018[6]. In terms of insolvency resolution, India moved up from 136th to 103rd position.

It is easy for a firm to do business if it has freedom to do it. A firm needs freedom broadly at three stages of a business - to start a business (free entry), to continue the business (free competition) and to discontinue the business (free exit). The first stage ensures allocation of resources to the potentially most efficient use, the second stage ensures efficient use of resources allocated, and the third stage ensures release of resources from inefficient uses for fresh allocation to competing uses - and consequently the highest possible growth. This enables new firms to emerge continuously. They do business when they are efficient and vacate the space when they are no longer efficient.

External Freedom

As a part of comprehensive economic reforms, India made a decisive paradigm shift in the early 1990s from an economy with largely State provision of goods and services to a market-oriented economy, where the State's role was confined to largely regulations for provision of goods and services. The thrust of the reforms since then has been provision of external freedom and building institutions to promote and secure such freedom and regulate such freedom only to address market failures.

India removed restrictions on freedom to start a business in early 1990s with replacement of discretionary license by registration of any firm that met the pre-specified eligibility requirements. If registration is to be denied, it must be determined by a reasoned order and that order is appealable. Further, this freedom is not much use, if a firm does not have resources of its own to start a business and finds it cumbersome to mobilise resources from others. Accordingly, the securities laws allowed a firm, subject to meeting the pre-specified eligibility requirements, to access the securities markets.

Restrictions on freedom of a firm can come not only from the State, but also from other firms. Ideally, a firm should have freedom to do business, but it must not have freedom to restrain the freedom of others. It restrains freedom of others if it has market power - control over either price and or quantity - and abuses such market power to the detriment of others. For instance, if a firm adopts predatory pricing and has the financial muscle to sustain it, it effectively thwarts the competitors' freedom to do business. With a view to providing freedom at market place from other businesses, reforms in the 2000s proscribed predatory pricing. Further, this freedom does not serve much of a purpose, if the policies and institutions are not neutral to all firms. The competition law accordingly provided the same level playing field to all firms, state owned and private.

A firm that has freedom of entry and freedom to do business may, however, fail to deliver as planned. It is possible that such a firm has a viable business, but

[6] Doing Business 2018: Reforming to Create Jobs 15th edition by The World Bank.

it would deliver if its business is reorganised with or without the existing management, product portfolio, technology or business model. If it is unviable, it needs to be closed with the least cost and disruptions. The Insolvency and Bankruptcy Code, 2016 (Code) provides a market mechanism for orderly resolution of viable, but insolvent firms, and closure of unviable, insolvent firms. It also allows closure of solvent firms if the stakeholders so wish.

Thus, the Indian economy witnessed freedom of entry in the 1990s led primarily by reform in securities laws, and freedom to compete in the 2000s led primarily by reform in competition laws. This decade has witnessed the ultimate economic freedom, the freedom to exit, led primarily by reform in insolvency and bankruptcy framework. It needs to be noted that removal of restrictions is always a work-in-progress and there would never be a situation without any restriction on freedom of entry or freedom to compete at market place. This is because freedom needs to be restricted in certain situations to address market failures or even to protect freedom of others.

Internal Freedom

External freedom may not translate into economic wellbeing, if firms do not have freedom to, otherwise known as internal freedom. The scope of internal freedom depends on the ability and willingness to make the right choice. External freedom may allow a firm to commence a business, but it may not commence that business if it does not have the ability and willingness to take the plunge. A firm, therefore, needs to enhance its internal freedom in sync with external freedom to harness full benefits.

Often a business does not want too much of external freedom, because, it does not have the governance to harness and exercise internal freedom, i.e., it is constrained by its limited maturity and vision of choices available. In a different context, Erich Fromm observes[7]: "freedom from the traditional bonds of medieval society, though giving the individual a new feeling of independence, at the same time made him feel alone and isolated, filled him with doubt and anxiety, and drove him into new submission and into a compulsive and irrational activity". This led him to attempt to escape from freedom that he had gained. Therefore, exercise of internal freedom requires expanded vision and maturity.

If we exclude malfeasance, flawed decisions are mostly due to restricted or limited visibility of available choices. Where a firm is not able to visualise the complete menu of choices available, it takes sub-optimal decisions. Further, it may not always be open to disruptive ideas and may even reject them prima facie. A choice in isolation is very different from a choice relative to options available on the table. If the trade-off between choices are observable, controllable, and measurable; the vision becomes clear. It is for the State to design institutions and policies such that the stakeholders can consider all possible choices and take informed decisions.

Thaler and Sunstein believe that a good system of choice architecture helps people to improve their ability to map and hence, to select options that make them better off. Some of the best nudges use markets; good choice architecture includes close attention to incentives. The reforms and the underlying rules and regulations hence, should focus on a choice structure to 'nudge' people towards a desirable governance structure of the firm. The State needs to be a choice architect and nudge business towards right choices and thereby help the business to visualise the complete horizon of internal freedom.

Sir PT was ahead of his time in envisioning this very contemporary thinking about economic freedom, ease of doing business and governance to use freedom. These basic ingredients have shaped the Code that expands the scope of external freedom and enables firms - debtors, creditors, and resolution applicants – to use such freedom to their advantage.

[7] Escape from Freedom, 1941, Erich Fromm.

The Insolvency and Bankruptcy Code, 2016

Insolvency is an outcome of market process. The Code provides a market process for its resolution. Equity owners have complete control over a firm as long as the firm services its debt obligations. When it fails to service debt, the Code shifts control to the creditors who get a right to decide what to do with the firm. It segregates commercial aspects of insolvency resolution from judicial aspects, while empowering both the stakeholders in the firm and the adjudicating authority to decide matters within their respective domain expeditiously[8] . It provides a time bound and orderly resolution of insolvency, wherever possible, and ease of exit, wherever required, with the least cost and disruption, for maximisation of the value of assets of such persons, to promote entrepreneurship, availability of credit and balance the interests of all the stakeholders.

While competition and innovation contribute to the growth of the economy, they do increase the incidence of firm failure. The failure could also arise from faulty conceptualisation of business, inefficient execution of business and change of business environment. In some rare case, they could be due to malafide intentions too. Irrespective of the reason, it dampens entrepreneurship if it is onerous for an entrepreneur to exit a business in an orderly and predictable manner. The Code reduces incidence of failure in two ways. First, the inevitable consequence of default in terms of insolvency proceedings prompts behavioural changes on the part of debtor to try hard to prevent business failure. Second, it reduces failure by setting in motion a process that rehabilitates failing businesses that are viable. If, however, rehabilitation is not possible, the Code facilitates its closure with the least cost and disruptions. By allowing closure of non-viable firms, wherever required, the Code enables an entrepreneur to get in and get out of business with ease, undeterred by failure (honest failure for business reasons). The Code thus, addresses business failures by reducing the chances of failure, rescuing failing businesses where possible and releasing resources from businesses, where rehabilitation is not possible and thereby promotes entrepreneurship.

Failure usually manifests in a default in repayment obligations. The lenders are unwilling to lend to firms when they face the risk of default. When lenders do not get back their funds, availability of funds at their disposal reduces, limiting their ability to lend to genuinely viable projects. Further, the risk of low and delayed recovery pushes up the cost of funds, and consequently, credit becomes available at a higher cost at which many projects become unviable. The resultant high cost of capital creates a vicious cycle where entrepreneurs with feasible projects are priced-out and lenders end up financing the riskier ventures who are willing to borrow at such high cost. Through provision for resolution and liquidation, the Code enables lenders to recover funds from either future earnings, post-resolution or sale of liquidation assets. On the other hand, the inevitable consequence of a resolution process deters the management and promoter of the firm from committing a default and thereby minimizes the incidence of default. These increase supply of credit, reduce cost of funds, and develop debt market.

Default reflects relative under-performance (inefficiency) of a firm as compared to the most competitive firm in the industry. In other words, the resources at the disposal of a firm may not be optimally utilised. The Code enables the optimum utilisation of resources, all the time, either by (a) preventing use of resources below the optimum potential, (b) ensuring efficient resource use within the firm through resolution of insolvency; or (c) releasing unutilised or under-utilised resources for efficient uses through

[8] When a corporate defaults the threshold amount, a financial creditor, an operational creditor, or the corporate itself may initiate the resolution process. It makes an application before the adjudicating authority (AA) along with the evidence of default. If default is established, the AA admits the application and appoints an interim insolvency professional. The professional runs the operations of corporate as a going concern up to 30 days during which he collects the claims and based on the same, forms a Committee of Creditors (CoC). The corporate moves away from 'debtor-in-possession' to 'creditor-in-control'. The CoC appoints a resolution professional to run the corporate as a going concern and decides what to do with the corporate. The CoC endeavours to resolve insolvency through a resolution plan. The resolutuion professional invites plans from eligible resolution applicants. If it approves a resolution plan within 180 days with 75% majority, the resolution professional submits the plan to the AA for approval. If the AA does not receive a resolution plan within the scheduled time, the corporate is liquidated.

closure of the firm. By liberating the resources stuck up in inefficient and defunct firms for continuous recycling, the Code has granted the ultimate freedom and thereby changed the script from 'Hopeless End' to 'Endless Hope'.

Quest for NPA Solution

I limit my discussion hereafter to banks. It is often asked: Does the Code address the malaise called NPA? Ahluwalia[9] visualises a Sudarshan Chakra with four 'R's, namely, Recognition, Resolution, Recapitalization, and Reforms to tackle the NPA malaise. Clearly, the Code is an essential component of the strategy to deal with NPAs. Ahluwalia finds the Code having some Sudarshan Chakra like qualities, as it offers liquidation as the only alternative to time-bound resolution. It is important to note that first three R's are remedial. If pursued to logical end, they may clean up the books of the banks of NPAs. Further, the Code has the potential to prevent burgeoning of NPAs as a bank is entitled to invoke the Code at the earliest instance of default. However, these three R's do not address emergence of fresh NPA. That requires a *Sudarshan Chakra* on reforms - reform of governance of banks that expands their positive freedom and that accepts a reasonable level of NPAs as cost of doing business where lenders and borrowers, during the natural course of profitable pursuits, will go wrong despite their best efforts.

The Code expands external freedom of banks by adding resolution to the choice set. To make the right choice, a bank needs internal freedom. It may choose between resolution or recovery, but it cannot choose resolution to recover NPAs. It has quite a few choices under the recovery menu; resolution is not an addition to the said menu. Thus, a bank needs to be clear as to what it wishes to achieve from resolution. If it wishes to recover the NPAs, resolution is not a choice. The NCLAT has made[10] it clear that resolution process is not a recovery proceeding to recover the dues of the creditors. In another matter, the NCLT has observed[11] that after the resolution process commences, the nature of proceeding changes to representative suit and the *lis* does not remain only between a creditor and the debtor. In fact, the Code prohibits any action to foreclose, recover or enforce any security interest during resolution period, as recovery yields inequitable distribution of available assets to one or a few aggressive creditors to the detriment of the debtor and other creditors. One creditor after another takes away whatever is available leaving nothing for resolution.

The Code endeavours resolution of insolvency an early stage to prevent it from ballooning to un-resolvable proportions. A stakeholder is entitled to trigger resolution process as soon as there is a default of the threshold amount. It is, however, not obliged to do so at the first available opportunity if it is explicable. This is based on the premise that in early days of default, enterprise value is likely to be higher than the liquidation value and hence, the stakeholders would be motivated to resolve insolvency of the debtor rather than liquidate it. It is thus, not a mechanical exercise for a bank to trigger resolution as soon as there is a default of at least ₹1 lakh. It needs to ascertain the reasons for default and the likelihood of successful resolution under the circumstances and evaluate various options available to it and then choose the best one, from its perspective. If it is interested in recovery, it must not trigger resolution under the Code. In fact, it may find a resolution outside the Code more rewarding. It may find that there is no resolution under the current circumstances. Besides, a trigger of resolution under the Code involves costs to the stakeholders as it derails operations of the debtor to some extent during resolution and brings uncertainty about its future, in addition to the explicit costs of resolution and the possibility of liquidation. A bank needs to take a call whether and when to trigger resolution in case of a default, considering all these aspects. It needs to use the choice, but must not misuse it or wrongly use it, however, must not refrain from using it when required. This requires a very high degree of internal freedom on the part of a bank.

A bank is not the only stakeholder entitled to trigger resolution. An operational creditor, another financial creditor or even the debtor itself may trigger resolution. In that case, the bank has no option but to participate in

[9] A 'Sudarshan Chakra' solution for PSU banks, September 29, 2017, livemint, Montek Singh Ahluwalia.

[10] Prowess International Pvt. Ltd. Vs. Parker Hannifin India Pvt. Ltd. [Company Appeal (AT) (Insol.) No. 89 of 2017].

[11] Parker Hannifin India Private Limited Vs. Prowess International Private Limited [I.A. No. 226/KB/2017].

the resolution. In one case, a bank filed an application under the Recovery of Debts due to Banks and Financial Institutions Act, 1993 before the DRT for recovery of ₹73 crore against a debtor and its guarantors. While the matter was pending before the DRT, the debtor filed an application before NCLT to trigger resolution under the Code. The NCLT admitted the application and declared moratorium till the completion of insolvency resolution process. Thereafter, the DRT stayed the proceeding against the debtor in view of the moratorium. The issue came up whether the proceedings against the guarantors should also be stayed. The High Court[12] observed that until the liabilities of the corporate debtor and guarantor are in a fluid stage and not crystallized, the guarantors cannot be held liable and it cannot allow the creditor to pursue two remedies on the same cause of action. Therefore, it stayed the proceedings before the DRT till the finalization of insolvency resolution process. It is important that a bank takes a decision keeping in view any anticipated moves by other stakeholders so that it does not limit its options.

The Code mandates closure of resolution process in a time bound manner. The enterprise value of the firm reduces exponentially with time, as prolonged uncertainty about its ownership and control and general apprehension surrounding insolvency leads to a flight of customers, vendors, workers, etc. A bank needs to be mindful that if the process does not yield resolution within the timeline, it would end up in liquidation which may not serve its interest. Further, the Code puts the entire process at the disposal of the financial creditors, irrespective of who triggers it. It permits limitless possibilities of market-based resolution plans with or without the existing promoter, management, products, technology or business model. A bank needs to have the ability to engender competitive resolution plans and to evaluate them to choose the best one that maximizes the value of assets of the debtor. More importantly, it needs to handover the corporate to a person who has a credible record and is likely to deliver so that the resolution is sustainable. Traditionally, a bank has capability in matters of credit and certain fee-based services. It now needs the capabilities of a businessman to decipher an appropriate resolution plan or identify a resolution plan that will work.

The Code, thus, presents a choice architecture to stakeholders, where they (a) can see all the policy agnostic options, (b) accurately ascertain the trade-off between different choices, (c) have the freedom to choose the best option, and (d) are nudged towards a solution which balances the interest of all, not just the strongest one. It takes away the excuse of not reacting in time before the problem takes a gigantic proportion. Although the Code adds one more powerful choice for banks, it is not a simple choice. A bank needs capability to evaluate various choices in the menu and trigger resolution at the right time keeping in view choices likely to be exercised by other stakeholders. It is a choice with huge attendant consequences. It may mean acceptance of large losses in some cases. It may even mean liquidation in some other cases. But, not using the choice is not an option. The decision by the bank to make the choice needs to be concluded appropriately and expeditiously. It needs to be used where it is necessary, though its use on a large scale may be inevitable in today's context of legacy issues, and its use must be avoided where it is not necessary. Keeping these in view, it is imperative for a bank to so govern itself that it is not pushed to a point where it has to use resolution and it must have the capability to use resolution appropriately to its advantage.

I have illustrated the internal freedom required to make an effective choice by a creditor keeping in view the external freedom granted by the Code. Other stakeholders, namely, corporate debtor and resolution applicants also need similar internal freedom to use the Code to their advantage. Most often a choice made by a stakeholder limits the choices available to other stakeholders. Coupled with the fact that economic freedom has many shades of grey, a firm needs a much higher order of governance and consequently internal freedom to survive and flourish in a market economy. If, however, it runs away from freedom, the State may have excuses to curb freedom from and hence, freedom to. The State needs to incentivise and nudge the firms to build on their governance.

I thank the Indian Institute of Banking & Finance and its Chief Executive Officer, Dr. Jibendu Misra for this opportunity to speak to you. Thank you very much for your patient hearing.

[12] Sanjeev Shriya Vs. State Bank of India and Ors. (Civil Writ Petition No. 30285 of 2017).

Banking on IT's Security

V. Rajendran*

Banks play a vital role in nation-building, especially in a growing economy like India. Ever since the days of globalization and privatisation in early 1990's, computerisation, and technology in general, has come to stay in banks in India. Until this period, the word "bank" often reminded one of a brick and mortar structure, a building with a Branch Manager and other Officials keeping huge, voluminous ledgers in the counters and with people either in a queue or standing near cash and other counters. Gone are those days. Speak to a modern day youth and utter the word "bank", he does not recollect any building or a person, but just his computer or an ATM or his mobile. Today's banking is associated more with these electronic delivery channels like ATMs, Mobile, PoS Terminals and Online modes than with any physical human being. No wonder, today's customer does not ***know*** his banker, nor does today's banker ***know*** all his customers.

Technology the pre-requisite: Indian Banking is competing with global players in the industry in terms of customer service, efficiency arising out of effective deployment of technology with almost all banks in India exhibiting a paradigm shift in the way banking was perceived earlier. Banking in India is now re-defined with IT becoming the *sine qua non* in banking industry. Much more than focussing on computerisation, banks naturally, had to look at the threats and vulnerabilities associated with computerisation. IT security has become a major concern in banks.

While banks compete with one another in showcasing their technological strength, projecting as the most tech-savvy ones, they are also equally concerned that the race to computerisation and providing ease of use to computers should not make them compromise on the vital aspects of security of customers' money. Gone are the days if a bank-branch in India reports a crime or cash theft or other such loss, the suspect or the criminal would have to be traced within a radius of a few kilometres from the branch. These days, when a fraud is reported, the accused could be geographically in any part of the globe.

Information Asset: Securing banks' assets brings within its realm, protection of not only its physical assets but more significantly and essentially, its information assets too. Nowadays, criminals do not rob banks with guns, or attack the employees with weapons but they attack with more *sophisticated weapons in their arsenal viz. a keyboard, mouse, software program and network* algorithms. And, as it is a Universal phenomenon, the more the banks are prepared to counter the attacks, the more the criminals equip themselves with the latest in technology and thus, they ensure that the banks always keep running -- to learn, to equip and to protect their assets.

With Core Banking Solution (CBS) being a near 100% implementation in the banking industry in India, (exception being a few small-sized co-operative banks and other Non Banking Financial Institutions), bank officials have to re-align themselves with the emerging trends in the way the bank books are maintained, the manner in which a bank record is kept and the methodology in which bank evidences

*** Chairman, Digital Security Association of India.**

are produced, to ensure the underlying compliance of IT Security initiatives and regulations.

Owner of data in CBS: There still seems to be some ambiguity in the way an information asset – to be precise the CBS data - is looked at in a bank. Earlier in the days of physical assets of the bank, the distinct role play of the three stake-holder viz. (i) owner, (ii) custodian and (iii) user of bank's assets was clear. Now, with much of the CBS data and information always on the move and in transit in a huge network of branches and other electronic delivery channels (like ATMs, PCs, PoS Devices and Mobile handsets), many Branch Managers are not clear about who the "owner" of the data is and who the "custodian" is (though aware that who the "user" is). With the advent of CBS, the comfort feeling of the Branch Managers that the physical ledgers and the data are with them, and thus, the data is 'owned' by them and secure, is now gone. Perhaps, it still needs to be vociferously re-iterated that though the bank data is now a huge data (Relational Database Management System (RDBMS) like Oracle) of voluminous amount of tables with rows and columns, the Branch Manager legally is still the 'owner' of the data and thus, responsible for the data which his/her branch has entered and that the CBS Data Centre may be called a 'custodian' only. Unlike the earlier scenario when the branch 'had' the data and 'owned' them, the point is to be driven home now is that bank's data is a huge database of rows and columns out of which every row is owned by the respective official.

Law and Technology: The next area that hugely impacts IT security in banks is how technology is closely aligned to law and how the same technology can be used, misused or abused to make the activity absolutely lawful or unlawful. Denial of Service (DoS), Cyber Squatting, Scavenging, Crypotography, Steganography, Email Spoofing, Mobile Number Spoofing are all sheer technologies which are taught and practised perhaps under the comfort factor that there is nothing *per se* illegal about them. If done with a specific *"mens rea"* i.e. an evil mind or an intention to commit a crime, they become illegal or unlawful activities. Banks should configure their systems effectively and efficiently to ensure that any DoS attempt, spoofing attempt or other forms of Phishing websites etc, is immediately shown as a systemic alert and the preventive controls are immediately put in place. In fact, failure to have such controls in place, may be even legally construed as a non-compliance issue and banks may be accused of not following "reasonable security practices and procedures" as enshrined in the IT Amendment Act, 2008 in Section 43-A and may be taken as non-observance of due diligence as per Section 79 of the Act.

Due Diligence is itself a major area of debate and banks have to give serious attention to it especially to showcase its prowess on the security front and exhibit its cyber law compliance. For instance, a mail with unlawful content in individual name through a mail provider like Gmail or Yahoo! and another with the same content, from the bank's email id like sender@ xxxbank.com, have entirely different ramifications and banks cannot feign ignorance and escape culpability in the latter scenario, taking a defence that the sender alone is responsible and not the bank. The bank is also equally responsible for such mails and can be proceeded against, treating its lack of supervision and monitoring as non observance of reasonable security practices.

Not just protecting the bank from attackers, protection of its customers, protection of its own officials, protection of the nation's financial data etc. all come under the areas of what is to be protected. As an intermediary handling third party data, how the bank protects itself or how the CISO (Chief Information Security Officer) protects the bank in the event of a threat, is a matter of not just law but an issue of society and an assurance to customers.

Cyber Crime as a Service! With technology so intertwined with today's banking, no surprise that customers are often as tech-savvy as, and most often more than, an average bank official. Typically, when a customer reports a problem, say in their remittance or a statement, or an Account View etc. banks cannot get away with the normal routine remark or the oft-repeated cliché, like "it is a computer problem" or "a software issue" or "a technological failure". Customer no doubt, knows better. Quite often, a customer compares the internet banking of Bank X with that of Bank Y and questions why that feature is not introduced. There are scores of websites available for access in public viewing which compare the administrative, legal, technological and customer-service issues of various banks like comparing the loan interest rates, service charges etc. Interestingly, there are occasions when tech-savvy, (sometimes misguided) youth commit the misadventure of hacking into the bank's system or otherwise observe some existing vulnerabilities in the system and misuse them or sometimes from a positive perspective, even bring it to the knowledge of the IT team in the bank expecting some recognition for the services rendered.

There are often reports in the Press, about cases of banks becoming targets of attacks like hacking taking advantages of existing vulnerabilities in the system. The recent attack called "Wannacry" is neither the beginning, certainly nor the end in this game. Such attacks will only increase day by day and banks' spending on Information Security should be much higher and **not just higher but should also be transparent** and conspicuous to drive the criminals away deterring them from embarking on any such misadventure of attacking the bank data.

E-Record Maintenance Policy and e-evidences: With the wide-spread knowledge about the Information Technology Act and its Amendment Act, 2008, which recognise maintenance of records in electronic format and the amendment that the ITA 2000 brought in Bankers' Books Evidence Act recognising computer data as valid records, there is an increased necessity on the part of banks to ensure proper retrieval of old data and information stored some times in diverse computer systems. Many of the banks in India still do not have a comprehensive Board approved e-records Maintenance Policy (like the earlier Records Maintenance Policy applicable for physical records and registers) that would clearly define the scope, periodicity, methodology, process of storage and retrieval of all e-records. Absence of documented and approved policy with due compliance will expose the bank to a greater risk of non-compliance of IT Act provisions besides making the banks liable to face evidentiary issues, in the event of any legal dispute. Such a policy should address challenges like change over from an earlier technology to a newer one on the software, hardware replacements, software upgrades, Change Management, Retrieval issue in CCTV footages, period of preservation of all kinds of electronic data, including especially the customers' instructions that may be received by phone (which too are saved and stored by some banks for record purposes).

Blockchain technology (a decentraised technology with a global network of computers jointly managing the database which records crypto currencies like Bitcoins) is an emerging method of global payments. It is considered as an incorruptible digital ledger of economic transactions which records all financial transactions and is transparent among its members, **with no regulator and no monitoring and not under the control of any** particular nation or entity or body.

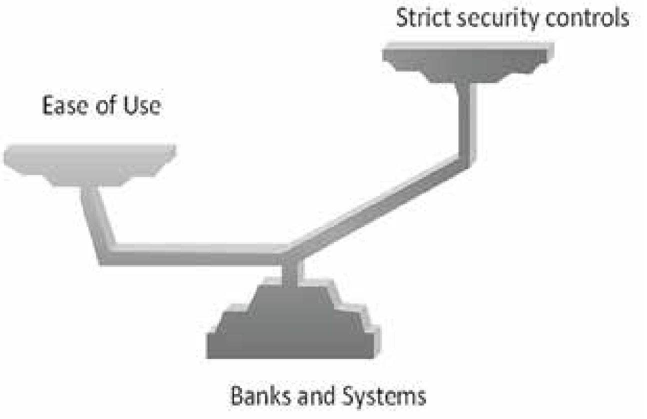
Some Economists even say that blockchains are the future and have the potential to even substitute regular banking itself as an industry. Under such circumstances, if banking has to survive the onslaught of such competitions like blockchain, mode of payments like Payment Wallets etc. as an industry, banking has to give the users namely the customers a comfort of security, safety of transactions besides a legal and formalized structure of grievance redress. Information Security is one area wherein banks can make the customers feel comfortable and draw them.

Panel of Cyber Law Advocates: Perhaps the time is ripe for banks in India to go in for a separate panel of Advocates called "Cyber Law Advocates Panel" just like banks have their own panel lawyers to take care of NPA related suits like DRT etc., customer service like consumer court cases etc. In fact, most of the bank related disputes in future may have to be in some form or another treated like a cyber crime case.

User Awareness: Digitisation is disruptive innovation and naturally, time has come for the banks to increase the level of awareness of not just their own officials but the banking public. Words of caution like "Do not reveal your PIN... never part with your card... never click a bank website as a link received in an email... Avoid using public WiFi for Internet Banking" etc. may just be not enough. In the days to come, banks may have to educate their own staff members and the customers on the significance of biometric authentication, multi layered approach to security and other security initiatives, security concerns in WiFi and Internet of Things (IoT). Digitization need not be considered to be a threat to traditional banking but has to be welcome, as an opportunity to serve the customers better and of course, safer.

Cyber Risk Insurance A discussion on IT Security and Cyber Crime in Banks can never be complete without a reference to cyber risk insurance. This is a topic being spoken about for almost a decade now, with even the RBI's Gopalakrishna Working Group strongly batting for it way back in April 2011, itself advising banks to go in for cyber crime insurance policy, vide **RBI/2010-11/494 DBS.CO.ITC.BC.No. 6/31.02.008/2010-11 dated 29 April 2011.**

(Ref: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=6366&Mode=0). Other than the regulator-driven insurance policy protecting the banks (and not the customers directly) on card transactions as a mandate of Payment Card Industry Data Security Standard (PCI-DSS), banks still are shy about taking a cyber crime insurance policy. Only now in the recent past, some insurance companies in India have come out with cyber crime insurance policies (which may be considered as Version 1) and perhaps depending upon the coverage, usage, claims-acceptance and claims-refusal, investigation etc. the cyber crime insurance will gain in popularity. Banks and insurance companies may have to sit together and discuss the issues in all its reach and ramifications taking into account factors like amount (maximum coverage), technological issues, own loss vs. third party loss, global attacks, randomised attacks vs. specific targeted attacks etc. Sure, the debate is going to be interesting.



With so much competition, banks these days cannot simply afford to introduce stricter controls. If the controls are tougher and many in number, that itself would scare the customers and drive them away. On the other hand, if the bank keeps the system too loose and user friendly, it exposes itself to a high level of undesirable and avoidable risks.

Hence, banks may always strike a proper balance between factors like ease of use, user-friendly systems, simple procedures etc. on the one side and safety of customer's money, security and compliance with regulatory guidelines on the other.

Indian Cyber Crime Coordination Centre: If a criminal attacks a bank's website or customer successfully and gains illegal money, there is every possibility that the criminal will deploy the same tactics and try to attack more banks (unless the victim bank shares the knowledge including the modus operandi how it lost money and thereby cautions other bank/s). This issue of co-ordination and exchange of views among the Chief Information Security Officers too, is one of the recommendations of Gopalakrishna Working Group in 2011, referred to above.

Focusing on Cyber Security in banks, the regulator RBI has issued detailed guidelines and directions to banks vide circular No. RBI/2015-16/418.DBS.CO/CSITE/BC.11/33.01.001/2015-16 dated 2 June 2016, which speaks about arrangement for continuous surveillance, the need to comprehensively address network and database security, need to evolve a Cyber Crisis Management Plan and other related issues laying emphasis on sharing of information on cyber-security incidents with RBI, adding that "banks are hesitant to share cyber-incidents faced by them". On a national level in this issue, Indian Cyber Crime Coordination Centre (IC4) has already been conceptualized and set up paving the way for utmost co-ordination among all the agencies (not just banks) like investigators, police etc. for sharing of information about cyber crime attacks on the critical infrastructure in the nation.

To conclude, it does not need a seer to say that growing technology in banks is an indicator that the traditional multilayered defence that banks already have is not adequate. Globally, not a day passes with no news of some data breach, and cyber crime incident in banks. Understandably, most often, banks will be reticent to reveal the news for fear of adverse publicity and its impact on public confidence the bank enjoys. As stated above, RBI as the regulator has a much larger role to play, than just an enabler of e-commerce, facilitator of online banking but additionally as an 'assurer' to the public in the electronic era of banking.

☯

Sachet Portal

The Reserve Bank of India launched a mobile friendly portal Sachet (sachet.rbi.org.in) on August 4, 2016 to help the public as well as regulators to ensure that only regulated entities accept deposits from the public. The portal can be used by the public to share information including through uploading photographs of advertisements/publicity material, raise queries on any fund raising/investment schemes that they come across and lodge and track complaints. The portal has links to all regulators and the public can easily access information on lists of regulated entities. The portal has a section for a closed user group – the State Level Coordination Committees (SLCCs), inter-regulatory forums for exchange of information and coordinated action on unauthorised deposit collection and financial activities. It will help in enhancing coordination among regulators and state government agencies and will serve as a useful source of information for early detection and curbing of unauthorised acceptance of deposits. The portal is designed to place the entire proceedings of SLCCs on an IT platform. It facilitates comprehensive MIS with respect to complaints received, Referred to regulators/law enforcement agencies and for monitoring the progress in redressal of such complaints. Complaints relating to unauthorised deposit collection and financial activities that have been lodged in Sachet have been taken up expeditiously with respective regulators for resolution.

Source: RBI Annual Report, 2016 -17

A simple banker into Bank's Cybersecurity: understanding the task, the role

S. Mukhopadhyay*

1. Cybersecurity is being looked at as a distinct domain than being subsumed within overall Information Security (IS). However, the overall security considerations and components of IS will apply to Cybersecurity, with specific focus on system access/delivery through internet. Incidentally, exchanges through public domain internet with external world outside the Banking system is not the only area to look to, as, access from other parts of the Bank system over internet protocol through in-house webpages will have about the same risks as external webpages. So, the cybersecurity risks are out there in the big bad world, as also within our house though we may not know it before a problem happens.

2. How challenging our days are getting? The answer has been the same over the past year or past decade or so on. Threats and risks are getting bigger and bigger, wider and wider, and a look-up into a few sites can provide you and me with huge details of all these. The nature of the tool of attack, the area of the system where the attack happens, the type of system malfunction or misuse that is attempted – all these go on changing all the time. Generally, after a problem happens, often a patch, a workaround, etc. follow after some lag, and we go on patching, updating, repairing, as also correcting some data or re-do some other routines to keep our data acceptably business-worthy.

As the nature and area of attacks go on changing, for example one day it will be 'wannacry' the other day it will be 'meltdown', or, one day the weakness leveraged will be of an Intel chip, another day it can be of Windows OS, or another time it can be human mind's credulity (say for Phishing or Social Engineering – a human gets to err and divulge valid non-sharable data).

3. We are not discussing here some names / cases or instances of attacks / domains or their fixes, to save space. These information galore in literature and the reader can conveniently look up in the web and get informed. One needs no prior knowledge or background to do this. Overall, as mentioned above, we may remain with the understanding that the frequency, variety and operating domains of cyberattacks or problems always increase.

4. This poses a great challenge to a banker. Bankers are not supposed to be IT experts or security experts. Often a CISO or Risk Manager has not been there for a lifetime in that role, so that acquisition of functional knowledge and expertise also remains a difficult task for them. However, as IT organisations or scientific organisations also got such problems at least at sometimes, we can take it that Info Security is always like this. IT develops something. Usage brings in some baseline securities. Attack frontiers widen and so the security baseline also gets reinforced and widened. This dynamic iteratively goes on.

5. So, how therefore we approach this cybersecurity challenge to keep floating? And what specific pieces seem more useful now? This is a question all information security persons ask. The approach has multiple steps, as it has been so far.

*** Former General Manager & Chief Information Security Officer, State Bank of India.**

6. An oversimplified example of an organisation can be, say, your physical office building. You may have a boundary wall, a gate that can be opened and closed – locked and unlocked, the house proper thereafter, with the main door for entrance, an employee or a card reader and lock mechanism to verify the person entering or exiting and then allow. After one comes in office, he may meet you in visitor area, or come into your meeting room or office room or even your Board Room depending on what the person is allowed by your office. Similar things we do in the systems by controlling the access rights very finely. The access controls are controlled at who can or cannot enter, what all resources, data or programs the person is allowed to access and, then, what action at the accessed point is allowed for this person - like he can read or copy or delete or view or change, he can create or delete a user or modify rights of a user, etc. This control can be done in a fine-grained manner. However, all of these attempts may get quite regularly defeated. Insiders i.e., our own employees or users and known regular business visitors can manage to steal the keys (just as one of your in-house staff can steal a key, make a duplicate) and take away or delete/change our data. Outsiders also can scale the walls, steal or copy somebody's ID card, cheat or impersonate to enter the main door and inner doors to different areas of office, and then break open / unlock your cabinets to access valuables. How entities can break all these multi-level barriers (this multi-level barriers to challenge and verify the incoming entity, is normally called 'defence – in-depth' or 'protection in layers', etc. – the spirit is if one deterrent fails even, – all will not fall together) needs a digression to discussions on types of attacks and their methods.

7. Attacks from external entities may happen in many ways and at many places of our network. Usually bank's computer systems are networked, i.e., all the computers are linked. This networking is managed by a specialised system to manage a network - which means managing to add or remove workstations, control which part or workstation of a network can have what sort of set-up or exchanges with which other part of network, etc. A server with a specific software for this is maintained to do this job on a regular basis. We may call it the network server. Computers in a network are connected to its neighbouring or a central computer by wire or wireless (Wi-fi, even Bluetooth). They can be connected directly, or between two computers an intermediate piece of hardware can be used. These are just connection boxes (like we see for telephone land lines, at some road side) having slots to terminate wires. Computers are connected through these. There are a few types of these connection boxes, called - hub, switch, router, bridge, etc., depending on capabilities. Often a part of a bigger network - say a whole office - at a specific locality or logical unit will be networked (say a bank branch with 50 workstations or 5 workstations), and then this network will have a central computer (say the branch server in our example of a branch) through which this set-up will get further connected to a bigger unit as a part (say in our example of a bank branch, the branch is then connected to a Zonal Office or a Central Office). This whole connected set of computers form our network. Employees will work at some or other workstation in this, and software allows us to control and configure if an employee can work at one machine, more than one machine, etc., at various levels. So long as we all are coming to office to work, and working from inside our offices from one or other of these workstations, we are all inside the network. Physically however, the employees may be spread over distances - say one working at a branch of Bank A at Ludhiana and another working from a branch of Bank A at Thiruvanantapuram. However, another person, say a customer sitting at waiting lobby at the Ludhiana branch of Bank A, remitting money from his account in Bank A to a third branch of Bank A / or to a different bank, is in our network, having entered as an external user through internet or mobile banking gateway. However, this customer, can do now an online remittance from a different Bank B to an account of a third Bank C. This time,

he is not presently in the network of Bank A (though physically present there), but is connected to the network of Bank B (through mobile data connection to his mobile network provider company's network) which may be very far away, say in Mumbai. This way, we remain/enter in a network and work there, despite being physically widespread. We may consider all the employees working at the bank branch workstations as 'insiders' - our own employees. In our network, we have connected computers at locations (branches/offices) among themselves and then connected this cluster with other parts of the cluster. Anybody coming from outside (like our customer who is in the network of bank B with his mobile phone) needs a place in the bank's network, which is like a permitted entry door, where his exchanges he has to direct and request an entry. And, the bank will have to examine if this customer is allowed to come in, and also, use which banking activity software (remittance, or, balance enquiry, etc.). The gate the bank has provided for customers to come in, may be called a gateway in our bank's network for people to come from outside the network. All entities coming in from outside the network of the bank, can be thought of as 'outsiders', irrespective of the fact that the person can be physically inside the bank.

8. A banking application (core banking) sits in a server system centrally. This is housed and maintained very securely, because the customer data and business data are here only. All branches are connected to this, and so, all the branch workstations are. All these workstations are entry points to the bank's network, the in-house entry points for a bank. The number of such points and their users are quite large. So, to keep our internal entry points safe, we shall need to protect so many PCs or laptops or whatever other devices are there (can be a mobile, i-Pad or Tab also).

There are other systems for specific activities, e.g. ATM, Internet Banking, Telephone banking, kiosk banking, etc. These systems sit on different specific servers at the central location (the data centre), with their own software, giving their specific functionalities, as also distribution channel. Let us take the example of ATM. All ATMs these days are connected, like branches, to a separate central server – let us call it the ATM Switch. This is a multi-part system. It exchanges data with ATMs as we operate them, in real time, i.e., as soon as it happens, so that card ownership and ATM transaction request details can be verified and transaction requests can be sent to the account maintaining system (i.e., Core banking sitting behind the ATM switch) and again instructions can be sent back to ATM to dispense cash or refuse, etc. These ATMs are entry points for customers, so that, all the ATMs can be considered as external entry points, i.e., entry points at outer extremities of our, network.

Similar is the situation with Internet banking, telebanking, etc.

Banks therefore, have large networks with many entry points from inside, to be used by employees to enter data as per customer transaction requests, and run routines required to provide customer service even if the customer is not standing across the counter (like, say, running routines to send out clearing cheques data to the clearing house, or, for internal accounting jobs). Mistakes, misdeeds and wilful undesirable activities of employees can create serious problems for the bank's technical systems. Introduction of a malware in the system, data theft, and many other problems can happen, without any external attack.

The users in a bank are the employees that insert, extract or operate on customer data. These users are ordinary users for the system, and their rights of access in the system are restricted on a 'need-to-know' basis, to minimise chances of fraud loss to banks.

There are another types of users in the banks or in all systems. These are the people who maintain and operate the technical systems at various stages. The first level behind the customer-facing users are such 'technical' employees of bank or vendor, who may be, managing the ATM switch, or the Internet Banking

Server etc., or the daily operations of Core Banking. A part of job is to run programs already residing in the systems as part of specific routines which may be having various routines or can be need-based. The other part will be to maintain various parameters – say an interest rate, or a loan demand calendar, number of login failures till forced log-out of customer, etc., for example. These users have special rights higher than the standard users. We call them privileged users. Some privileged users are enabled to create users, delete users, change the rights of the users, etc. These users are quite important to monitor to prevent fraud or system misuse. Basically these privileged users are mostly not able to change the system or delete or damage it, but can misuse it or put the system to stress or overload, and, obviously undertake frauds create mistakes and customer discontent.

One further higher group of privileged users are those who develop programs and can install, change or copy software or data. Mostly they are not configured to have access in the operating business software, so that they may not 'post' data in the system like an employee in a branch office. However, these separations do not practically mean these highly knowledgeable set of backend people (more of vendor employees presently) cannot really have means to damage the system or cause/enable data loss or malfunctions.

9. So, we are having a big network with thousands of doors inside and outside, for people from both sides, known and unknown, to enter the system to the extent permitted or technically able. These people are handling technology that run processes, all of them being very intricate. Most people run the processes by selecting valid routines, and then, if the system is compromised (have a wrong program inside), without the knowledge of the person operating, undesired damages can happen. This problem is much larger than it sounds so briefly, and can bring in remote problems into the bank even accidentally. For example, if a customer's PC is affected by some malware and that travels to bank system (i.e. The bank's internet gateway is unable to stop or sense it) even without customer's knowledge or bank's knowledge some damage may get done. Whatever malfunction it causes will only be known when found, which may not be easy. By then the problem might have spread to many computers at diverse geographies/ locations, of many people or organisations without knowledge of the bank or its vendors, through internet/message exchanges / file exchanges / file sharing.

10.Our systems have computers, computer programs, other devices like router, switch, firewall etc., as also laptops, mobiles, i-Pads (for mobile staff or customers through internet, threat horizon will include Apps on his/her mobile phone also), etc. The computers work on Operating Systems (OS), chips, RAMs, storage disks or devices, and above all, the programmes stored already or fired from outside. These systems are accessed through direct keypad based entry (like for branch staff), or, operations at ATMs or kiosks or POS, or further, by sending files or messages from a second business connected system like internet or NEFT operations by another bank, etc. A malware file designed to do some damage or exploit vulnerability of any of our components - say a chip, or an OS like Windows, or some databases or files, a firewall, a program etc., has to reach the component to do the damage. We need to protect all of these IT assets then. These are technically different items and technical methods to be employed therefore may be diverse. Control procedures also will be diverse. Do we lose track of them or get overwhelmed? Not really. As technologies evolved or new products kept on coming, their protection practices also evolved.

11. As the spectrum of vulnerable IT components is quite wide, for each of them piecemeal and specific technical solutions are required. Our job is then to be with the original vendors of all these parts and get solutions or defence methods for them and apply them, on a regular basis. However, many other considerations dictate actual work in the field.

Take for example some vulnerability in computer Chips, which are miniature (size can be like a mobile phone SIM card, but thicker somewhat) Integrated Circuits of thousands of semiconductors and capacitors, resistors, etc., that in old days could fill up a big table or filing cabinet. Thousands of chips can be in a server array that we use for banking data processing. If a Chip is reported to have been exploited for a vulnerability, the malware delivering or exploiting such vulnerability can any day crumble our system. If we did not know it before and our vendors could not solve and release a solution, then we head for a catastrophe. There can be a need of taking stock and see if some critical work can be managed otherwise than using these chips or after these chips are affected, how to recover and reorganise data to make business run as usual. This may need a lot of work and involve learning at the operational levels, confusions and mistakes. But if the solution has been developed and delivered, we could apply the same to all such Chips, may be we can be safe till the next attack. But, do we really know where how many Chips are there to handle? Or, what to do if any problem arises by applying the solution? Really not, at least at the outset. So, we take the solution, get programmes written by another vendor partners to load it on top of our system/or to each affected component, - as the solution demands. Chipmakers release updates or 'patches' to be applied to take care of the chips deployed, if reported to have been compromised. A technical partner has to apply the solution as we are not technically so skilled. For us, the job will be to get hold of the technical solution as early as possible and apply it to the machines that have such chips. Does it go so straight and fast really? May not be. For example, after the recent 'meltdown' malware, Intel Corporation has released such patches. The patches are free in the industry by all providers. However, as this patch slows down chips (reportedly 6 %) and servers use hundreds of them, some trend of orders shifting from Intel to AMD chips are already getting reported. The end user banker may ill afford to change all Intel Chips or computers as such, and tomorrow another problem around the replacement chip may prove the decision to be wrong. It is this unstable equilibrium that is a constant factor in Information Security, there is no panacea that solves all the problems for good to allow us to take rest. Right now the media reports suggest that banks (not in India, this report is on Europe) have not patched mobile phones and pads to any reasonable extent for 'meltdown' but PCs, servers and Laptops have been attended to more, which anyway remains risky because mobile devices are used in operations and transactions by employees also, banks having many roving employees. Also it is getting reported that all chips cannot be so patched, the patch works on a particular chip version and above. This problem is much more accentuated for software – both system SW (those that helps systems to operate – OS, Firmware, etc.) and Application SW (those that make programs run for specific business purpose – like the internet banking application sitting on the internet banking switch server, or the Core Banking Software). Applications are often released and maintained for a specific version and patch level of the OS; for example, your Core Banking could have been tested and perfected for Windows 7 Professional upto a specific patch number. If we change the basic OS by patching, it has to be checked that the Core Banking works correctly in all details. If not, this basic update patch itself will be a problem. On top of it, if there are additional patches required due to some problems or malware attack, we need to see if existing core banking will correctly work after patching. So, the rectification patch for the current problem can better be applied only after our software vendors have touched up the Application, tested the Application Software and cleared it. This will take some time though, while the desire in case of a malware attack will be to solve it as early as possible. From this discussion, we may have an idea that, in real activity, the complications have many more dimensions and may need workarounds, and need be managed through, for a longer time than we thought. Overall process and business management issues come in, and the case does not remain to be a technology patch – some person running a CD and the case gets ‘solved’.

We discussed around chips mostly so far. There can be many other different domains like OS, App SW, and other specific attacks on firewall, databases etc. Solutions, issues and practices there offer us practical learning to cope with the ongoing attempts of breaches and their counter measures.

12. By these nature of the problems and their counter-measures, now, the industry has developed a few approaches.

Chips develop and keep coming. The platform to operate goes through evolution and expansion – from minicomputers to PCs to Laptops, I-Pads, Tablets, mobiles, other microprocessor enabled machines - which includes refrigerators, or cameras, or like saving medical equipments, vehicle and aeroplane engines, to CCTVs, door locking systems, to what-not! Incidentally, this last set of things therefore can be standardised on common data format exchange standards to some extents, apart from wireless connectivity capabilities (wi-fi, Bluetooth, NFC all are of this class) and therefore, one of these can be made to operate on receipt of specific incidence based signals/messages from another (and we shall call them Internet-of-Things, or IoT!). So now, instead of a hacker, a mechanised doll or an air refreshing system can help and organise to loot your system!

Operating Systems keep developing with new platforms (I-Pad, Mobile, etc.), or new way of doing things in computer, and Database or other constructs also develop (for Big Data, say).

Even networking devices go through evolutions.

So, all these ever changing members of these diverse domains, will continue to offer gaps or weaknesses for hackers etc., to exploit, expanding the universe of technical challenges continuously.

Secondly, the methods of trying to steal data will also go through changes including how the insider humans can be tricked to share data or grant access, even unknowingly. If I click an innocent looking link received in my mobile phone from a friend registered and stored in my phone itself, I may learn later at a cost that such message was generated without my friend’s knowledge and after doing so, my phone remains very slow, use excessive of RAM, and occasionally feels warmer than expected, it will be beyond my competence to check if somebody else is running some programmes using my phone and the same is for , may be attacking other machines, or doing tasks of some questionable business of some unknown person. But, how do I decide whether to open the link or not, differentiate between the genuine and a fake?

As we cannot hope to be on technically and psychologically on top of the problem creators in real time, we have come to some usage norms and behavioural norms, to survive. These are like a driver’s guide in a city street, no need to know the intricacies of an engine, but, always drive safely. What we do is –

i. Ensure we always buy and use hardware, OS, Application Software, known to be devoid of weakness or risk discovered but unresolved.

ii. Ensure to do ‘hardening’ for all hardware and OS, - i.e., configuring to set parameters to safe ranges for proposed use, and shut off unnecessary services available in a general purpose product. For example – PCs come with a ‘remote desktop’ facility whereby we may enable one PC to enter and operate on another PC, but say in a banking scenario, we have no reason to keep this enabled to ensure safety of each workstation and operator.

iii. Test all Application SW as also OS against bugs, common weaknesses where some instruction statements in the program code leave some gaps where one can come in and ‘inject’ some other command that will create a trouble. Good programming practices therefore properly logically close all command lines or codes so that it is not possible to add anything – but then, we want more changes, demand changes without a long term vision so that in a few months we want change again upsetting the planned order, we want fast and cheap solutions but users do not really participate in thinking and designing details and post-development testing. The result is, most of the App SW leave a lot of weaknesses. The answer is, test for App vulnerabilities; automated tools are available to try inject some codes, or otherwise mimic an attack and see the result in-house.

iv. Ensure to have fall back plans in case of system unavailability or impairment, to help the critical parts of the business run, and recover within agreed plans.

v. Continuously check all applications, hardware, devices, networks, gateways etc., against malware, wrong configuration, etc.

vi. Control all access (physical, logical), review all system changes, segregate duties and accesses in such a manner that no system change or operational parameter/process change can be singly done by any person. (this is facing challenges of business convenience, as people desire 'single window' clearance, or automated service delivery in many areas). Control vendor access and vendor people access, strictly.

vii. Put in administrative measures – penalties, deterrents for carelessness, and, more for wilful mishandling.

viii.Check all exit points, and content of data to the extent possible both incoming and outgoing. This has got huge technical involvement.

ix. AND, continuously communicate and help awareness development of humans. People are the most diverse, most unpredictable and fluid part of a system. If sincere, aware and enabled, people can stand up and control if machines or systems malfunction. But, if not, people commit fraud, destructive acts, careless mistakes, revengeful damages, misinformation etc., which are not easy to discover and more so, very hard to rectify on a permanent basis.

x. Finally, always keep informed and seek support from Top Management, as otherwise, it is not possible to continue doing all of the above that will surely displease many colleagues and partners.

The above steps, in elaboration with specific system and organisation related workable details, in the shape of Policy, Standard, Procedure, etc., will expand to perhaps somewhat voluminous official documents for an organisation. However, as this world is, like IT, heavy with special terms and a bit abstract sort of lingo, it is important to keep understanding and procedures simple and straight, clean and unequivocal.

This, in my observation is briefly the philosophy that has come in place in the Info. Security Practices. We may observe that we have not talked much of specific technologies or malware names or technical issues. Our IT assets, as discussed above, are in an ever expanding and evolving mode. Technical specific knowledge piles up in these areas is an exploding huge; these gets used by developers, operators, servicing personnel in respective areas. For the job of maintaining Cybersecurity we need information about a specific problem as faced, and get to know what all fixes are available and their implications. The specifics will continuously come and go. We need ability to understand systems on a macro and broader basis to be able to understand these discussions, look for solutions and evaluate options. A thorough technical background will not be the need but an aroused common sense, an agile mind and willingness to continuously update current knowledge about these risks, developments, solutions, etc., in the industry – will be a desirable trait in any security person. Security also involves technical checking and testing of things, and to that extent security will involve some support people with technical grounding on network security etc.

13. As Cybersecurity is a bit specific to security against possible problems from the internet based access of the world into us (when I go to the external world over internet, I can bring in all these problems into my system without appreciating that it is happening so), it may be useful to note that access from outside happens through our systems put at the periphery to accept inward internet access requests. Also our insiders go out in the web through this, to various sites, which may bring back attacks. Our internet access providers service this set up. We receive requests from many IP addresses across the globe. If problem is traced to a site, we may move (through agencies) to authorities to 'take down', i.e., close an undesirable site. Global co-ordinations managed by some security providers regularly list known bad sources, which can be blacklisted at this gateway so that access to them is denied. We also whitelist desirable sites at this set up, which means our people from inside can visit only such sites and nothing else. These steps sound manageably administrative in nature. However, the attackers change their site names or provide new sites, and therefore, like other steps these also will be candidates for regular review and update.

14. While all these sound to be repetitive and expanding in coverage, what are the new things that become important at any point of time? As the nature and area of attacks changes, the newness mainly are two-fold – learning and handling the new attack vector of the time, and trying to see things incrementally in a different way. The first one will make us look at do-ables for 'Wannacry' at a time, "Meltdown" at another, for example. The second one will be from trying to react to attacks as was done so far, regularly create attacks in test-bed and manage it involving IT, Security, and business (vulnerability tests, ethical hacking, repeated Disaster Recovery, BC planning, etc.), and then, further into proactive attempt to guess what may be next attack agent and its domain (need very big set-up, modelling, analytics, etc. to make such guesses and try to fortify defence at that area , selectively do in-house attacks and testing to improve). As of now this last piece is more of a shared thought and efficient working models are awaited it seems.

15. Altogether, challenges in terms of IT knowledge and skill seems lesser, challenges in terms of regular checking and preparedness prove to be more demanding, challenges in steering the mind-set of the security person and the users are high, and thereafter luck is also important –as, for the same vulnerability not that all persons having it in his system will get attacked and halted. God bless! But we learn more, try harder, and keep standing.

☯

Bank Quest Articles - Honorarium for the Contributors

S.No.	Particulars	Honorarium Payable
1	Invited Articles	₹7000
2	Walk-in Articles	₹4000
3	Book Review	₹1000
4	Legal Decisions Affecting Bankers	₹1000

Cyber Security in Banks

Burra Butchi Babu*

1. Introduction

Cyber security in Banks has gained paramount importance as banks have opened up their IT platforms to customers in the name of digitisation, competition from peers, customer experience, reduction of transaction cost. Massive amounts of confidential data reside in Bank's data Centres and also flows through Bank's servers and various networks and devices. To protect the IT systems, confidential data of bank's as well as customers either in rest or in motion, and to ensure continuity of business a Cyber Security Policy and a Cyber Security Framework are required for every bank.

Government's encouragement since demonetisation in November 2016 has brought unprecedented spurt in new digital Banking customers and Digital Payments have registered a record growth. Banks have scrambled to implement various new mobile banking technologies like Wallets, Utility Bill Payments, 24x7 money transfers etc. Lot of mobile applications were developed by banks and most of the new digital users were new to digital banking. This called for greater focus for revamping of cybersecurity in Banks and Financial Institutions.

As Cyber-attacks are carried out continuously on various organisations, banks became the favourite destination, for such attacks. The volume and sophistication of cyber-attacks is ever increasing and evolving. Innovation, sophistication, organization of Cyber Criminals is producing ominous results for banks. This has led to cybersecurity rising to the top agenda for banks top Management.

2. What is Cyber Security?

Cyber Security in banks involves measures to protect the computer assets, information and networks from unauthorised users and preparedness to business continuity and Disaster Recovery. It encompasses Information Security, Application Security and Network Security and Disaster Recovery.

For over many years, information security has held confidentiality, integrity and availability (known as the CIA triad) to be the core principles. However, other principles such as authenticity, non-repudiation and accountability are also now becoming key considerations.

Some of the common threats faced by the Banks are Malware, Ransomware, Phishing, Spear Phishing/ Whaling, SQL injection Attack, Cross site Scripting, Denial of Service (DoS), Social Engineering, Website Defacement etc.

3. Risks of Cyber presence

The impact of a cyberattack on banks can be devastating in various ways which include financial loss, critical data loss, business disruption/loss, dip in brand image, legal battles, regulatory penalties etc.

As the banks moved from branch banking to any where 24x7 banking, they were required to expose a

* Senior Domain Expert, Institute for Development and Research in Banking Technology (IDRBT).

segment of their network to the customers accessing their web based, mobile based applications like Internet Banking and Mobile Banking. Cyber adversaries are exploiting the vulnerabilities in the network, servers to commit frauds, data theft, business disruption etc.

Worldwide, organizations are concerned about cybercrime, as they are worried about the technically combating cyber incidents, business disruption, public perception and loss of clientele. Understanding the technical implications of an attack are incredibly important. That's why many organizations employ incident response teams. Analysis of an attack and restoring business operations is key to ensuring that organizations do not fall prey to the same attack or similar attacker.

In the wake of a cyber incident, while technical issues can be resolved quickly it takes much longer to restore the public brand perception and customer retention

4. Cyber Threat Landscape in India for Banks

Banks are exposed and susceptible to various types of cybercrime and online frauds. Cyber criminals have become more sophisticated and organised and they are continuously carrying attacks in volume, frequency and severity. Malware perpetrators are inventing and inflicting various types of malware attacks. Distributed Denial of Service (DDOS) activity is ever increasing and evolving as they are using IOT (Internet of Things) devices as platform to conduct such attacks.

As per the information collected by India's Computer Emergency Response Team (CERT-in), 44,679, 49,455 and 50,362 cyber security incidents took place in India during the years 2014, 2015 and 2016, respectively. These incidents include phishing, website intrusions and defacements, virus and denial of service attacks amongst others.

There is manifold increase in credit and debit card frauds on account of skimming, Malware attacks, compromise of credentials by insiders etc. Skimming at ATMs has become very common and laxity of security at switch or any bank's ATM will impact many banks and the losses extend to all banks in the eco system. Banks provide mobile banking to customers and the applications run on various platforms and devices. Often banks cannot visualise all the vulnerabilities and they are utilised by the criminals. Over 40% of banking transactions are happening through mobile devices. Software vulnerabilities in the banks' mobile applications are being exploited and aadhar based account frauds by some business correspondents also surfaced.

There is rise in misuse of bank's SWIFT systems credentials for transfer of funds or letters of understanding/comfort through unlawful access to the bank's SWIFT Systems for cross-border transactions. Recently Reserve Bank of India has advised banks to stop issuing LOUs and LOCs.

E-mail became the carrier for cybercrime and novice/innocent e-mail users are falling prey to phishing attacks. e-mail became a tool for stealing confidential credentials of customers like login details. Business e-mail Compromise (BEC) scams, are draining huge money from customer's accounts.

According to Symantec report Cyber criminals caused unprecedented levels of disruption of IT services with relatively simple IT tools and cloud services. Governments are targeted for cyberattacks and the focus is shifting from economic espionage to politically motivated sabotage and subversion. The cloud has become a dangerous place and vulnerabilities in cloud infrastructure provide the next frontier for cybercrime.

Banks have strengthened their perimeter security by managing or outsourcing Security Operation Centres and the following tools are used:

1. SIEM (Security Information and Event Management).
2. Vulnerability Management.
3. NBAD (Network Behaviour Anomaly Detection).
4. Anti-APT (Anti Advanced Persistent Threat).
5. DDOS (Distributed Denial of Service).
6. Anti-Phishing, Malware Monitoring .
7. PIM (Privilege Identity Management).
8. FIM (File Integrity Management).
9. WAF (Web Application Filtering.

Cybersecurity has extended beyond Data Centre perimeter, to end points, the cloud and using analytics, IP profiling to outwit the cyber adversaries. The attackers take advantage of endpoint vulnerabilities and poor security controls and have been changing the pattern of attacks to escape detection.

5. Challenges of Cyber Security

Security is a response to risk. Identity is a response to a need, and unless that need is clearly understood, and actually expressed as something that the business wants to address the banks will be at great loss.

Many cyber criminals are exploiting the known network vulnerabilities of organisations who have not even implemented baseline cyber security defence. The cyber adversaries keep scanning all the connected systems/devices in the cyber space for easy targets who are laggards in cyber security implementation.

While assessing cyber risk of an organisation the critical phase is identifying critical assets, valuable information, threats and risks associated with that information, and outlining the risk of breach of such information. Many a times it is observed that there are shadow IT systems which are not covered under the cyber security purview.

Customer privacy violation can take place in many ways; stolen card data, leakage of personal data due to improper security measures, unauthorized data sharing by third parties. Cyber threat with the growth of technology, cyber-attacks also took new shapes in the form of next-generation ransomware, web attacks etc.

For majority of the cyber criminals the motive is money and banks and financial institutions are the favourite targets. Ransomware is rampant and became an easy method of extortion of funds from individuals to organisations. Also stealing of credentials through phishing mails and syphoning of funds through whaling is increasing.

Consumers access the banking services from a wide range of devices and yet they want the assurance from the bank that their personal data will be protected, regardless of the devices they use for access. Managing threats from multiple variety of points of access by customers is a challenge.

Lack of awareness of Cyber threats and their serious implications by bank's staff and customers is a major challenge for banks.

Managing and adhering to the regulatory compliance in India and also abroad has become extremely challenging for the banks. The volume of regulations has increased dramatically over the past few years and all banks are required to fulfil the regulatory obligations

Government and Regulatory Support and Supervision

There are significant ongoing efforts by Reserve Bank of India, MEITY, CERT-IN, IBCART, NCIIP in setting Cyber Security Frame works, guiding, warning and monitoring of cyber-attacks.

Reserve Bank of India had, provided guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds through its

Circular DBS.CO.ITC.BC. No.6/31.02.008/2010-11 dated April 29, 2011, wherein it was indicated that the measures suggested for implementation cannot be static and banks need to pro-actively create/fine-tune/modify their policies, procedures and technologies based on new developments and emerging concerns.

Reserve Bank of India issued a comprehensive Circular on June 2, 2016, underlining the urgent need to put in place a robust cyber security/resilience framework at banks and to ensure adequate cyber-security preparedness among banks on a continuous basis. The salient features are:

- Banks to have a Board approved Cyber-Security Policy which is distinct from the broader IT policy / IS Security Policy of a bank.
- Banks to establish cyber risks in real time through SOC (Security Operations Centre) and make arrangement for continuous surveillance to monitor and manage cyber threats.
- A minimum baseline cyber security and resilience framework is given to be implemented by the banks.
- A Cyber Crisis Management Plan (CCMP) should be immediately evolved which should be a part of the overall Board approved strategy.
- Banks should share information on cyber-security incidents with RBI.
- Banks to bring Cyber-security awareness among stakeholders / Top Management / Board.

RBI had created a cyber-cell under the Department of Banking Supervision and conducted a separate IT audit of banks covering each bank for separate cyber-security and IT audit. RBI is also has done a gap analysis on the basis of the reports and asked banks to bridge the gaps.

IB-CART, CERT-IN, NCIIP help Banks in disseminating and foster sharing information associated with physical and cyber events (incidents/threats/vulnerabilities) and resolution or solutions associated with the bank's critical infrastructures and technologies.

Information Technology Act 2000, and subsequent amendments focused on Digital Signatures, E-Governance, Justice Delivery System, Offences and Penalties. There is a need to enhance the scope and definitions of the Act in the light of ever changing cyber space and attacks.

6. Involvement of top management

The impact cyber threats on banking system should be well understood by the top management and managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This will require a high level of awareness among staff at all levels. Top Management and Board should also have a fair degree of awareness of the fine nuances of the threats and appropriate familiarisation may be organized. Banks should proactively promote, among their customers, vendors, service providers and other relevant stakeholders an understanding of the bank’s cyber resilience objectives, and require and ensure appropriate action to support their synchronised implementation and testing.

7. Customer / staff awareness

Cybersecurity cannot be fought by CIOs and CISOs alone without involvement of all stake holders including staff, customers and MSPs. Security awareness should be built into the culture of the bank and this should start from the day an employee is recruited. As part of training of staff, banks may include simulation of cyber-attacks so that the staff can understand the Threats they are likely to face and are equipped to react to Cyber Incidents.

Staff should be encouraged through competitions quizzes and incentives for Cyber Security related courses. Often encouraging an employee for reputed Cyber Security Certification empowers him better than an in-house training.

8. Way Ahead

Cyber threat is a universal phenomenon and banks are part of the cyber space. Being in the ecosystem every organisation needs to ensure security as any cyber security compromise on one organisation can expose other entities in the eco-system. The cyber security mechanism should be dynamic and ensure defence resilience and assurance. information security can help banks to mitigate risks before they turn into security breaches. There is no single strategy which guarantees prevention of cyber security incidents.

Indian banking industry has successfully enabled mobile banking for large customer bases. Many banks offer Internet Banking also with varied capabilities to their Customers. As customers are free for anywhere, anytime banking, it became necessary that strong controls are put in place for mobile browsing as well as the apps by the security managers and experts.

New technologies are always targeted by cyber criminals and hence new products mainly web facing need to be launched after proper testing and security should be built in to the application development process. Regulatory or qualified third party sand boxing will help the Banks to reduce the risks.

Data Theft/Data Breach

Worldwide including in India, many data breach incidents have occurred and confidential data of millions of customers were exposed or stolen and misused. Organisations had to shell out lot of money in bridging the breaches as well as cost of litigation in law suits. Latest examples of such data breaches inflicted were on Equifax, Facebook, Yahoo, Uber etc. where millions of records of personal data of customers were stolen.

Hackers are targeting banks and customers for stealing theft like customer information, e-mail accounts, banking logins etc. A proper Data Leakage Prevention policy enforcing Data Leak Prevention should be in place for all systems. E-mails are still a major source of Data Leakage and Ransomware threat. Staff and Customer education helps to mitigate the treats. Data in rest or in transit should be encrypted and app. data should be able to move through bank owned VPN connections. Banks should make data available to the staff and vendors only on need to know basis and monitor and block various type of structured and un-structured data against data theft/ leakage.

All these years we never seriously suspected the vulnerabilities of the CPU architecture like leaking of information and the likely abuse. Spectre and Meltdown incidents brought hardware architecture security into serious reckoning.

Spectre, which is known to impact virtually all modern processors, is a class of micro-architectural attacks that abuse the way processors perform branch prediction through speculative computation to read confidential information from a process. Perhaps the most shocking revelation of Spectre is that the researchers were able to create a side channel to leak memory from a chrome browser process via JavaScript.

Meltdown, which at this time is only known to impact Intel-based CPUs, exploits out-of-order execution to gain unrestricted read access to system memory. This has particularly devastating impacts for systems relying on isolation techniques like containerization or para virtualization for security since, an attacker can break through the isolation to read from co-located instances

Identity Management

Risk based **multifactor authentication** and transaction limits may be built into mobile and internet banking applications. Also security controls like multi factor authentication, creation of strong passwords, adaptive authentication, image authentication, etc. can be considered. Banks will adopt biometrics authentication and other variable risk access control models for mobile and internet banking. Banks will integrate, standardize and automate real-time enterprise security, fraud and controls. API Security, Mobile Security and Identity Frauds will dominate and replace older ATM skimming, Web and cheque frauds.

Many banks have started providing the customers mobile utility to control the transaction limits including disabling of transactions from their ATM Cards and mobile banking. A customer at his will can enable or disable transactions through his mobile or an ATM Card. This will help reduce the skimming frauds.

To prevent misuse of Aadhar credentials UIDAI has proactively introduced Aadhar Biometric Locking System which enables residents to lock and temporarily unlock their biometrics.

In the light of ever increasing insider threats and third party threats bank may adopt Zero policy or Trust but, verify policy where every user or a vendor is treated like an outsider in terms of cyber security checks.

Transaction Monitoring

It is observed that cyber heists take longer to detect and the damage would have happened by the time it is noticed. While focussing on cyber security, banks should not forget to monitor the transactions through FRM (Fraud Risk Management) solutions to identify fraudulent transactions on the fly. Banks should build some scenarios under which fraudulent transactions can take place and build alert mechanism for monitoring such online transactions.

In a Banking system millions of transactions are processed and it is always a good practice to monitor high value and high risk transactions to ascertain the legitimacy of those transactions. Also advising the customer through e-mail or sms and wherever possible taking approval for such transactions helps mitigating the quantum of Bank's risk.

Linking of all payment and financial messaging systems with core banking is essential. This helps centralised monitoring and escalation of suspicious events to the monitoring officials. In a maker checker scenario in Core Banking two officials can cause intentional or unintentional damage to the bank while authorising transactions. Many core banking systems have some default limits at the time of implementation. These limits on various type of transactions should be reviewed and incorporated in the core Banking Systems. Any exceptional high risk transaction should be approved at a central level. Banks should continue to make core banking access through biometric access only.

Social Media Threats and policy

Indiscriminate sharing of official data like circulars, internal communications over social media is on the rise and every bank should have a Social Media Policy describing and discouraging acts and the consequences.

Cyber Threats

Threat Prevention automatically stops vulnerability exploits with IPS capabilities, offers in-line malware protection, and blocks outbound command-and control-traffic. When combined with Wildfire and URL Filtering, organizations are protected at every stage of the attack lifecycle, including both known and zero-day threats.

DDOS will be a persistent a threat to web facing systems / networks, only the methods of attack may change. If banks and other stakeholders like ISPs, MSPs, connected entities can collectively block and disrupt the DDOS activities.

Bank's need to understand that Cyber Security is an ongoing battle. Adding new IT infra structure like new digital assets, new applications, networks mechanisms for accessing them needs utmost care and should be integrated with the cyber security plans.

Ensuring compliance with bank's policies or regulator guidelines is not the equivalent of protecting the bank against cyber-attacks. Focus on evolving cyber trends, threat vectors and new vulnerabilities, new exploits will help the banks to build and refresh resilient cyber security strategies. As part of cyber readiness, banks are conducting simulated cyberattacks to identify vulnerabilities and educating and gearing of the staff for facing and mitigating cyber-attacks. Other banks may follow suit.

Standards and Best Practices

Accreditation/adoption of International IT standards bring some best practices in the organisation and brings discipline in to the stake holders. Banks may adopt Standards/Certifications like PCIDSS, ISO 27001, COBIT, ISO22301 which will help in mitigating IT risk.

Latest Technologies like AI, Analytics RPA and Block chain may help in tackling Cyber Security. But, the flip side is the cyber criminals may be able to make better use of such Tools.

Manpower and Budget

With the growing number of cyber-attacks, IT security budget constraints, and the challenge of finding people with the necessary cyber security skills, banks may look for managed security services (MSSPs) to guide implementations and help respond to attacks. Banks need to allocate sufficient IT budgets in tackling the growing cyber risk. Also manpower issues in Cyber Security Department should be addressed. New Cyber Security Talent is required to be recruited and the existing to be trained and retained.

Cyber insurance is yet to fully mature being offered in India for Customers as well as Banks. Once, the ecosystem develops banks can contemplate to transfer some cyber risks as per their risk appetite and insurers also will be more encouraged to make the insurance schemes attractive.

The Government may encourage forming of larger body of stakeholders, including banks, fin-tech start-ups, cybersecurity companies, and academic institutions who can jointly fund advanced research and even incubate cybersecurity solutions on a co-creation basis. Also, the threat incidents and intelligence should be shared among them to combat cybercrimes collectively.

Acknowledgements

www.rapid7.com

www.paloaltonetworks.com

http://whatis.techtarget.com

https://economictimes.indiatimes.com

www.skyboxsecurity.com

http://www.zdnet.com

www.webopedia.com

https://meltdownattack.com/

www.rbi.og.in

FATCA-CRS Compliance by Banks - Need for automation in data processing

R. Rajendran*

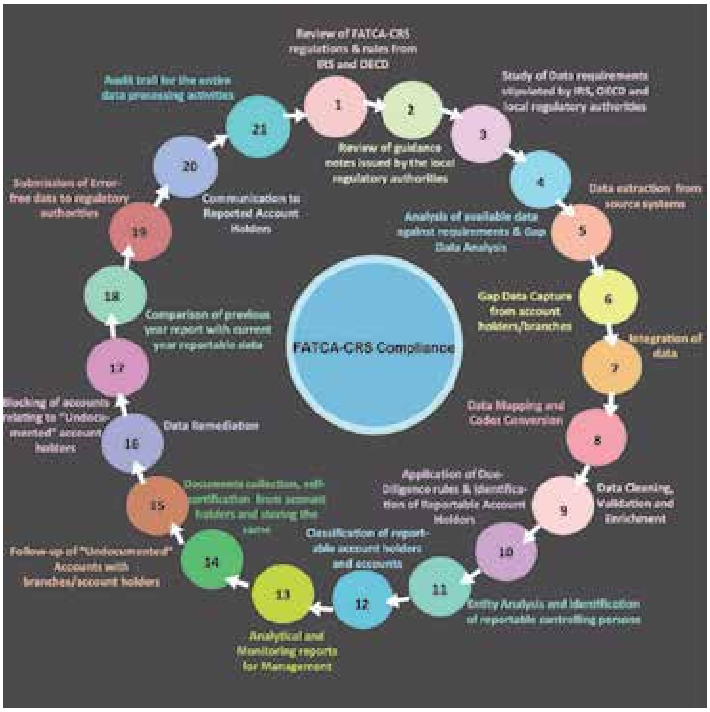
Advent of Technology resulted in Big Data Analytics thanks to technocrats who made it a reality. But a big question is whether Financial Institutions (FIs) have the required data for ensuring compliance of regulatory requirements. The answer is a big "NO". This is because our financial institutions have evolved from legacy systems to automated systems; further, the data requirements keep on changing from time to time and FIs are not fully equipped to handle/ integrate data flowing through social media.

One of the latest additions to the regulatory requirements is FATCA-CRS Compliance. Though, it may look simple to report the data on account holders, who are tax residents outside the domestic country, it is a complex process involving application of various rules for reporting the account holder and the accounts.

This paper aims to bring out the complexities involved in data compilation, at every stage, right from the identification of products till final submission of data and discusses the action points to follow so as to ensure error-free submission of final data to the regulatory authorities.

Though FATCA and CRS rules appear similar in many aspects there are subtle differences which have to be taken care of, while framing "rule engine" and processing data, before arriving at the reportable status of the account holders.

The following diagram provides a fair view of the complexity involved in FATCA-CRS compliance:


FATCA-CRS Compliance
1
Review of FATCA-CRS regulations & rules from IRS and OECD
2
Review of guidance notes issued by the local regulatory authorities
3
Study of Data requirements stipulated by IRS, OECD and local regulatory authorities
4
Data extraction from source systems
5
Analysis of available data against requirements & Gap Data Analysis
6
Gap Data Capture from account holders/branches
7
Integration of data
8
Data Mapping and Codes Conversion
9
Data Cleaning, Validation and Enrichment
10
Application of Due-Diligence rules & identification of Reportable Account Holders
11
Entity Analysis and identification of reportable controlling persons
12
Classification of reportable account holders and accounts
13
Analytical and Monitoring reports for Management
14
Follow-up of "Undocumented" Accounts with branches/account holders
15
Documents collection, self-certification from account holders and storing the same
16
Data Remediation
17
Blocking of accounts relating to "Undocumented" account holders
18
Comparison of previous year report with current year reportable data
19
Communication to Reported Account Holders
20
Submission of Error-free data to regulatory authorities
21
Audit trail for the entire data processing activities

* Deputy General Manager (Retired), Department of Information Technology, Canara Bank.

The data requirements for FATCA-CRS Compliance broadly cover the Name, Address, Date_of_Birth, Birth Place, Birth Country, Citizenship, Hold_mail_address, Resident Country, Tax Residency Countries, Account Status, Branch Code, Account Balance, Document Details, Self-certification, Country of incorporation, power of attorney holder's individual details, Controlling persons' details, account standing instructions details, balances in various accounts, interest paid/credited, sale proceeds of securities, etc.

As many of the countries have entered into Governmental level agreements, the data will be exchanged between Government authorities. This added a new complexity, as local regulatory authorities seek additional data from Reporting Financial Institutions (RFI) during annual reporting of data. For instance, CBDT of India requires all RFIs to provide additional data like Father's Name, Spouse Name, Gender, Occupation etc., for Individuals and Place of Incorporation, Constitution Type, Business Code, Address State Code etc., for Entities. For Accounts, FIs have to report account type, IFSC Number of the Branch, Branch Address to CBDT.

The data available in the source system may not be in the desired format of requirements and it may need proper mapping & conversion. Many Banks attempt this exercise by using manual processes and some of them use XL Utilities & scripts to match and merge data. As the data require multiple processing during the data remediation stage, adhoc utilities can be of use only to a limited extent and this is also dependent on an individual's way of handling processing of data. Such manual interventions (in the absence of any standard operating procedure) may result in omitting some of the reportable accounts not being extracted or some accounts extracted/identified wrongly as reportable accounts. [e.g.: An IT official of a bank may forget to include a liability product or product of an SBU while aggregating/reporting.]

When the complexities increase, the challenges for the Compliance officer of the RFI also multiply in extracting the existing data, collating the same with the required data, collecting the gap data [e.g. birth place/country], processing the same against the FATCA-CRS due-diligence rules and ensuring accuracy of the data submission.

Data volume is high especially for large financial institutions like a Bank. Therefore, inclusion of reportable account holders and elimination of non-reportable account holders from such large database (but with limited/incorrect data elements) is a herculean task. RFI is answerable to the regulatory authority if any of the reportable accounts is omitted in data submission or an account holder is reported wrongly. In such incorrect reporting, an FI faces legal consequences including payment of penalty to Regulatory Authority, as also reputational risk.

As the data volume is large and the tasks are numerous, it is imperative for the RFI either to develop or outsource an automated solution which should take care of majority of the data volume handling processes, if not 100% end-to-end solution.

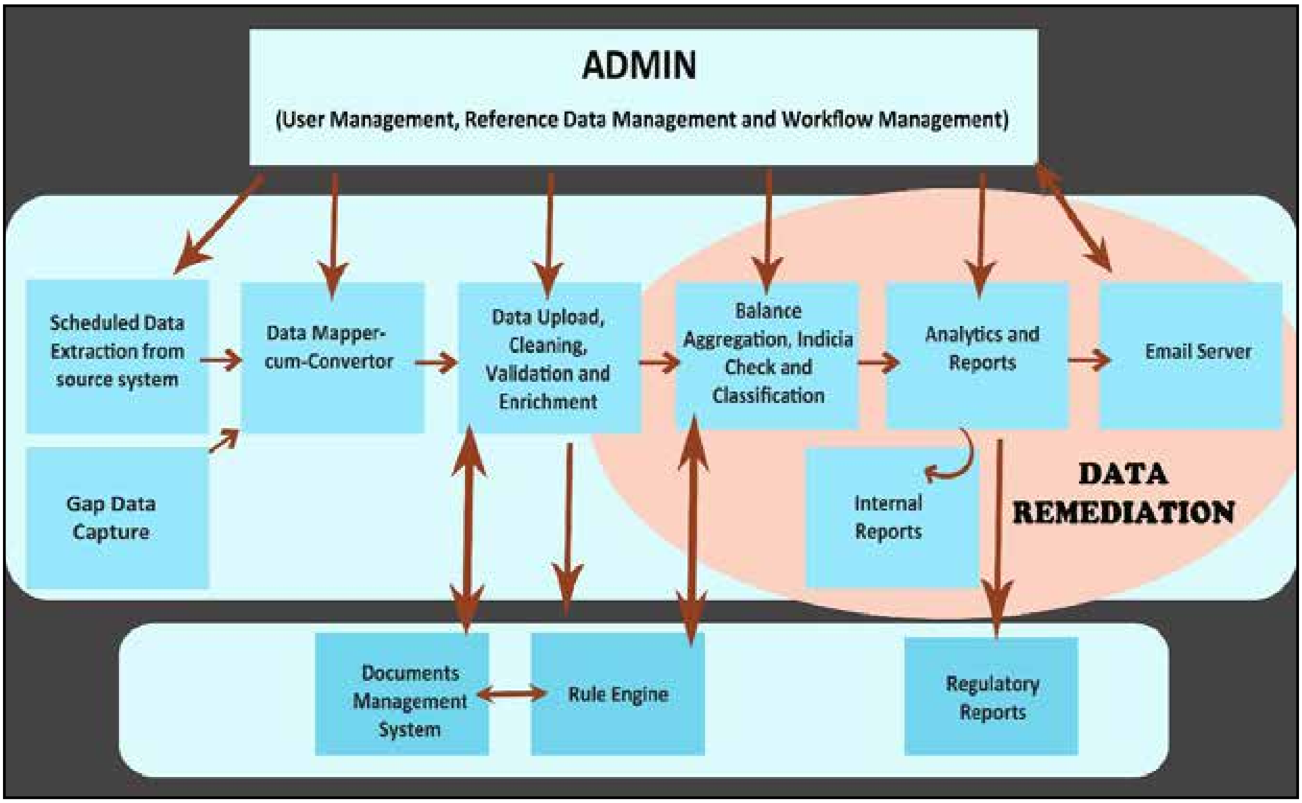
A question arises whether it is the core activity of a Banker/Financial Institution to indulge in software development, data collection/extraction, processing, following up documents with customers and remediating the data for accurate submission of report to regulatory authority. The answer is "No".

The tasks are techno-functional in nature and hence identification of resources and development/implementation of the compliance program would take long time besides huge efforts & costs for the Institution. Further, such internal resources keep moving "in" and "out" due to transfers, promotions, resignations, etc.

Hence it is prudent for the Banker to explore outsourcing this task to a competent agency experienced in this space at a reasonable cost instead of developing a customized solution/ procedure without compromising on data privacy and data security and the same is also permitted by the regulatory authorities.

Such automated solution should mainly contain a work flow framework covering configuration of compliance rules through a well-defined rule engine, scheduled data extraction from source systems, Gap Data capture utility, Integration of gap data with source data, Code Mapper & Converter, Indicia Finder, FATCA-CRS Classifier, Data Integration with Document Management System (DMS)/Case Tool, Data remediation handling, generation of periodic Monitoring reports for Management, a communication strategy (with operating units/ account holders) for completing due diligence/ data remediation and generation of final Data to the regulatory authorities.

Proposed architecture for the automated solution


ADMIN
(User Management, Reference Data Management and Workflow Management)
Scheduled Data Extraction from source system
Data Mapper-cum-Convertor
Data Upload, Cleaning, Validation and Enrichment
Balance Aggregation, Indicia Check and Classification
Analytics and Reports
Email Server
Gap Data Capture
Internal Reports
DATA REMEDIATION
Documents Management System
Rule Engine
Regulatory Reports

The automated application would function as per a Standard Operating Procedure and will take care of main challenges like communication with account holders in seeking additional data, self-certifications, follow-up communications, document storage during the Data Remediation and other pitfalls in manual data extractions, mapping and data conversion. ☯

साइबर क्राइम्स और उनसे सुरक्षा-एक परिप्रेक्ष्य

आनंद श्रीमाली*

सूचना तकनीक एवं दूरसंचार में उन्नति ने हमारे जीवन और दैनंदिनी पर पर्याप्त प्रभाव डाला है। हम टेलीविज़न, मोबाइल और कंप्यूटर पर दिन के 24 घंटे में से काफी समय गुजारते हैं। सोशल नेटवर्किंग साइट्स, इ-कॉमर्स क्रांति, और तो और हमारे बैंकिंग के कामकाज तथा अन्य सर्विसेज और सुविधाओं का उपयोग यथा यात्रा, मनोरंजन, कार्यस्थल आदि सभी में आमूलचूल परिवर्तन आ गया है। किन्तु इसके साथ ही हमें उनके खतरों के प्रभाव पर ध्यान देना अनिवार्य हो गया है। इनसे अनभिज्ञता हमारे जीवन या आर्थिक स्थिति में पर्याप्त नुकसान पहुंचा सकती है। अगर हम आजकल के न्यूज़ पेपर्स, टीवी चैनल्स तथा रोज़मर्रा की घटनाओं पर नजर डालें तो इससे एक आम दृष्टिकोण का अंदाजा होता है, कि क्यों बार-बार चेतावनी दिए जाने के बाद भी ऐसी घटनाएँ सामान्य सी हो गयी हैं।

हम कुछ विभिन्न उदाहरणों पर निगाह डालते हैं जो की आजकल काफी चर्चा में हैं:

1) आप कल्पना कीजिये की आपको एक फोन आता है या ऐसे फ़ोन के बारे में आपके मित्र आपको बताते हैं। "हम एस बी डी बैंक से बोल रहे हैं। आपका एटीएम कार्ड बैंक की कार्यवाही पूरी नहीं होने के कारण ब्लॉक होने जा रहा है। इसे ब्लॉक होने से बचाने के लिए आपका केवाईसी दोबारा करना होगा। इसे चालू रखने के लिए हमें आपसे कुछ डिटेल्स चाहिये जिससे आपका कार्ड चालू रखा जा सकेगा। आपके पास मास्टर या वीसा का एटीएम कार्ड है। कृपया कन्फर्म कीजिये कि यह मास्टर कार्ड है या वीसा कार्ड है। आप अपने कार्ड का नंबर (या अंतिम आठ अंक) बताइये। (आपके बैंक के नाम, मास्टर/वीसा तथा क्रेडिट/डेबिट से प्रारंभिक नंबर जाने जा सकते हैं)। इस कार्ड की वैलिडिटी तुरंत समाप्त हो सकती है। बताइए - अभी क्या एक्सपायरी डेट है? अब आपके कार्ड के पीछे 3 अंकों का नंबर होगा उसे पढ़िए। अब आपको एक एसएमएस आया होगा। मोबाइल चेक कर उसे पढ़िए" और इसके साथ ही भोले-भाले और पढ़े-लिखे लोग अनजाने में ही वह सब जानकारी दे देते हैं। जो कि किसी भी ट्रैंजैक्शन को इ-कॉमर्स साइट पर पेमेंट पूरा करने के लिए आवश्यक है। यह जानकारी कॉल करने वाले व्यक्ति के पास पहुँचते ही धड़ाधड़ नए एसएमएस खाताधारक के पास पहुँचते हैं कि आपका खाता दी गयी राशि से डेबिट किया गया है। कॉल करने वाले व्यक्ति के साथ ही उसके टीम के अन्य व्यक्ति भी बताई गयी जानकारी, कंप्यूटर पर एंटर (प्रविष्ठी) करके ट्रैंजैक्शन पूरा करने में सेकण्ड्स भी नहीं लगाते और खाते को साफ़ होने में देर नहीं लगती।

2) आप अपने मेल बॉक्स में एक मेल प्राप्त करते हैं – "मेरे पति एक देश के पूर्व राष्ट्रपति थे। उनकी मृत्यु के बाद उनके नाम से अरबों डॉलरों की सम्पति बैंक के खातों में जमा हैं। इसको सुरक्षित रूप से आपके देश में ट्रांस्फर करने के लिये मुझे आपकी सहायता चाहिये। इस मदद के लिये आपको बैलेंस का 50% राशि आपके बैंक खाते में ट्रांस्फर (अंतरण) की जायेगी। इसके लिए आपको अपने बैंक डिटेल्स भेजने होंगे" बैंक डिटेल्स भेजने के पश्चात् आपसे हैंडलिंग चार्जेस के नाम से कुछ राशि जमा करने को कहा जाएगा। फिर कुछ राशि कमीशन के तौर पर जमा करने को कहा जाएगा। तब तक आप कुछ हजार या लाख राशि से अपनी जेब ढीली कर लेंगे तब अचानक आपका संवाद उस धोखेबाज छलकर्ता (फ्रॉडस्टर) से बंद हो जाएगा और आपकी मेल या फोन का कोई जवाब नहीं आएगा। जब तक आपको इसमें दाल में काला नज़र आयेगा तब तक बहुत देर हो चुकी होगी।

*पूर्व उप महाप्रबंधक (सूचना प्रौद्योगिकी) बैंक ऑफ़ इण्डिया, वर्त्तमान संकाय सदस्य (रिटेनर बेसिस), आई आई बी एफ, मुम्बई।

3) आपको एक अन्य मेल प्राप्त होता है कि “रीडर्स डाइजेस्ट ने आपके नाम से 20 बिलियन पौंड की लॉटरी खोली है। इस राशि को प्राप्त करने के लिए आपको बैंक डिटेल्स शेयर करने होंगे।” फिर उपरोक्त अनुसार हैंडलिंग चार्जेस, कमीशन, पोस्टेज, कूरियर आदि नाम से आपसे इंस्टालमेंट्स में राशि कलेक्ट कर आपको उस 20 बिलियन राशि के लालच में लाख दो लाख का चूना लग जाएगा। यह राशि 10-20 लाख या अधिक भी हो सकती हैं जो कि पीडित व्यक्ति की, आर्थिक क्षमता और उसके भोलेपन तथा लालच के अनुसार अधिक हो सकती है।

4) आपको वेब सर्फिंग के दौरान कुछ विज्ञापन आकर्षित करते हैं जो आपको कुछ मनोरंजन के साधन, सर्विस, दवाइयां आदि पहले मुफ्त तथा तत्पश्चात मामूली राशि या भारी डिस्काउंट पर खरीदने के ऑफर देते हैं। राशि बहुत छोटी, जैसे 50 रुपये या 10 डॉलर, होने के कारण आप उसे क्रय कर लेते हैं। इसके लिए आप अपने कार्ड या बैंक खाते का उपयोग करते हैं। तत्पश्चात इन जालसाज वेबसाइट के माध्यम से आपके कार्ड या बैंक डिटेल्स छलकर्ता (फ्रॉडस्टर) प्राप्त कर उपयुक्त समय पर आपके खाते को खाली करते हैं या अन्य जालसाज ग्रुप्स को ये जानकारी बेच दी जाती है। आज के इ-कॉमर्स के जमाने में कई बार आप जान ही नहीं पाते की आपने किस वेबसाइट या पेमेंट गेटवे पर अपने महत्वपूर्ण और गोपनीय या व्यक्तिगत डिटेल्स शेयर किये हैं। इस माध्यम से आपके न केवल बैंक या कार्ड डिटेल्स, अपितु आपका ईमेल, मोबाइल नंबर, जन्मतिथि, पैन नंबर, आधार नंबर, घर/ऑफिस एड्रेस, पासवर्ड एवं पासवर्ड रिकवरी आदि गोपनीय जानकारी एकत्र की जा सकती है और आपके अन्य वेब खातों को हैक किया जाता है।

5) फेसबुक पर आपको फ्रेंड रिक्वेस्ट (मित्र अनुरोध) प्राप्त होती है। आप बिना कुछ सोचे समझे अपने मित्रों की संख्या बढाने के चक्कर में इसे एक्सेप्ट (मंजूर) करते हैं। कुछ संदेशों के आदान-प्रदान के बाद ही आपका कथित मित्र आपसे घनिष्ठता बढाता है और आपके बारे में अधिक जानकारी एकत्रित करता है। फिर यही जानकारी विभिन्न तरीकों से आपको नुकसान पहुंचाने के लिए काम में लायी जाती है। जैसे आपकी आर्थिक स्थिती के अनुसार आपसे राशि वसूलने के लिए आपका मित्र किसी परेशानी की कहानी गढ़ कर आपसे रुपया पहुँचाने के लिए अनुरोध कर सकता है। आपकी आर्थिक स्थिति के अनुसार विवाह का अनुरोध भेज कर मिलने का बहाना कर आपको धोका देने की कोशिश कर सकता है। किशोरों और बच्चों को, विशेष कर लड़कियों को फेसबुक मित्र से वास्तविक मित्र बना कर ब्लैक मेलिंग से पैसा वसूलने और अन्य तरह से हानि, क्षति या अहित पहुंचाने का मायाजाल फैलाकर पीडित किया जाता है।

6) एक अन्य तरीके में आपको मेल के द्वारा कंप्यूटर वायरस आदि भेजकर आपके कंप्यूटर का कण्ट्रोल, या उस पर रखी गई व्यक्तिगत और गोपनीय जानकारियां एकत्रित की जाती हैं। इसमें आपको फ्री क्रेडिट रेटिंग्स, सस्ते लोन पात्रता, इनकम टैक्स नोटिस या बैंक खाता/बीमा पॉलिसी विवरण आदि के नाम से उक्त मैलवेयर अटैचमेंट्स पहुंचाए जाते हैं जिन्हें क्लिक करते ही आपके कंप्यूटर में ये मैलवेयर प्रविष्ठ हो जाते हैं। तत्पश्चात आपके कार्ड यूजेस, इन्टरनेट बैंकिंग साईट यूजेस और अन्य व्यक्तिगत जानकारियां आसानी से इन जालसाजों के पास पहुँचती रहती है, जो कि उपयुक्त समय पर आपको नुकसान पहुँचाने के लिए उपयोग की जाती है। न केवल आर्थिक क्षति के लिए बल्कि अक्सर आपके कंप्यूटर के माध्यम से अन्य कंप्यूटरों और सर्वरों पर हैकिंग आदि क्राइम करने के उद्देश्य की भी पूर्ति की जाती है, जिससे वे क्रिमिनल क़ानून की पहुँच से दूर हो जाते हैं, और कानूनी एजेंसीज आपके कंप्यूटर के मेलिशियस उपयोग या दुरुपयोग के कारण आपको दोषी ठहरा सकता हैं।

7) उपरोक्त तरीकों से ही आपके कंप्यूटर को हैक कर उस पर रेंसमवेयर वायरस आपके कंप्यूटर में डाल कर आपसे कंप्यूटर को पुन: खोलने के लिए राशि वसूल की जाती है। रेंसमवेयर एक तरह का मैलवेयर सॉफ्टवेयर है जो आपके कंप्यूटर पर सन्चित (stored) फाइल्स या सूचना को एन्क्रिप्ट कर देता है, जिसे आप खोल या पढ़ नहीं पाते हैं। फाइल्स को पुन: सही स्थिति में लाने के लिए ‘डीक्रिप्शन की या कुन्जी’ (decryption key) की आवश्यकता होती है जिसके लिए यह जालसाज आपसे रेंसम राशि की मांग करते हैं। यह रेंसमवेयर राशि कंप्यूटर पर स्टोर्ड जानकारी की जरुरत और महत्व के अनुसार कम या अधिक होती है। इसमें अधिकतया कॉर्पोरेट जगत, बिजनेसमैन, कंपनी सीक्रेट्स आदि के केस में रेंसमवेयर इंस्टाल कर तत्पश्चात कंप्यूटर को खोलने के लिए अधिक से अधिक राशि वसूलने की कोशिश की जाती है।

8) क्या आप अनजान लोगों से मुफ्त गिफ्ट्स प्राप्त करते हैं? क्या आप अपने बच्चों को अनजान लोगों से चॉकलेट आदि खाने- पीने की वस्तुएं लेने से मना करते हैं? उसी तरह आप अनजान लोगों या कंपनियों के सॉफ्टवेयर कंप्यूटर या मोबाइल में लगाकर मुसीबतों को निमंत्रण दे सकते हैं। इन्टरनेट पर हर व्यक्ति सज्जन मानव होगा या वह कंपनी धर्मादाय कार्य कर रही है, इसकी संभावनाएं कम या बहुत कम होती हैं।

उपरोक्त उदाहरणों से हम कई प्रकार के कंप्यूटर दुरुपयोगों तथा क्राइम्स के बारे में अवगत होते हैं। वास्तव में, हम प्रतिदिन न्यूज़ पेपर्स, टीवी और अन्य साधनों से नए-नए क्राइम्स के बारे में अवगत होते हैं। पर अक्सर हमारे मन में यही विचार ज्यादा मजबूत होता है की हम सुरक्षित हैं और हमें चिंता करने की कोई वजह नहीं है। यह बेरुखी और असावधानी ही दिन-प्रतिदिन नए क्राइम्स को जन्म देती है। क्रिमिनल अपने बुरे कार्यकलापों में सफल हो पाते हैं और नई क्राइम कहानियां उत्पन्न होती जाती हैं।

तो क्या इन सबसे बचाव संभव है? बचाव के क्या तरीके हो सकते हैं? आइये हम कुछ महत्वपूर्ण बातों को समझने की कोशिश करते हैं।

1) क्या आप घर से बाहर जाते समय चप्पल या जूतों का उपयोग करते है? क्यों? ताकि आप अपने पावों की सुरक्षा कर सकें। क्या आप टू व्हीलर पर हेलमेट या कार में सीट बेल्ट का उपयोग करते हैं ... अपने बचाव के लिए ही ना। तब क्यों नहीं हम यह तय करें की हम कंप्यूटर में बिना एन्टी वायरस के उसे नहीं चलायेंगे या इन्टरनेट, ईमेल, पेन ड्राइव, डीवीडी आदि के लिए उपयोग नहीं करेंगे।

2) क्या आप घर छोड़ते समय घर के दरवाजे खिड़कियाँ आदि ध्यान से बंद करते हैं? क्या आप पंखे, बिजली के उपकरण, नल आदि बंद करने का ध्यान रखते हैं? क्या आप बाहर जाते समय घर के लॉकर्स, कबड्र्स आदि पर ताला लगाते हैं? क्या आप अपनी ज्वेलरी व बेशकीमती वस्तुओं को बैंक लॉकर में ले जाकर रखते हैं? बाहर जाते समय या प्रयोग न होने की स्थिति में अपने कंप्यूटर को बंद करना ना भूलें। हम अक्सर इन्टरनेट राऊटर/मॉडेम आदि को हमेशा चालू छोड़ देते हैं। बाहर जाते समय आप इन्हें भी पॉवर ऑफ़ करना न भूलें क्योंकि यह आपके वर्चुअल वर्ल्ड के मुख्य द्वार हैं।

3) क्या आपने रामायण में लक्ष्मण रेखा द्वारा सुरक्षाचक्र का विवरण सुना है? क्या आप जिस सोसाइटी में रहते हैं उस गेट पर सिक्यूरिटी चौकीदार रखे गए हैं? क्या आप के दरवाजे, सोसाइटी परिसर, मेन गेट आदि सेंसिटिव स्थानों पर सीसीटीवी कैमरा, अलार्म आदि सुरक्षा साधन लगाये गए हैं? आपके कंप्यूटर में पर्सनल फ़ायरवॉल या विंडोज फ़ायरवॉल भी उसी तरह काम करती है। जिस प्रकार उक्त सिक्यूरिटी प्रकल्प (सिस्टम) सोसाइटी के रहवासियों, आपके परिचितों, तथा नियमित काम पर आने वाले कर्मचारियों पर ध्यान रखता है। कोई भी अनजान व्यक्ति के आने पर सिक्यूरिटी द्वारा आपसे इण्टरकॉम पर पुष्टि की जाती है। उसी तरह ही यह फ़ायरवॉल सुरक्षा दरवाजे का काम करती है और अवांछित डाटा व सूचना के आवागमन पर ध्यान रखती है तथा उसे अवरोधित करती है।

4) क्या आप मॉल, थियेटर आदि में प्रवेश के समय अपनी सुरक्षा जांच से गुजरते हैं? क्या आपने एअरपोर्ट पर सुरक्षा जांच तथा विशेष सुरक्षा जांच का अनुभव किया है या विवरण सुना/पढ़ा है? फ्रिस्किंग शब्द से भी हम काफी कुछ परिचित हो गए हैं। कॉर्पोरेट नेटवर्क, महत्वपूर्ण शासकीय दफ्तरों में सुरक्षा जांच, भौतिक जांच पड़ताल, सामान की एक्सरे मशीन से जांच, प्रवेश और निर्गम के लिए गेटपास का उपयोग आदि से भी हम अवगत हैं। इसी प्रकार कॉर्पोरेट, सरकारी, बैंक या सेना आदि के नेटवर्क में फ़ायरवॉल, आइ. डी. एस. (इंट्रुजन डिटेक्शन सिस्टम – घुसपेठ खोज प्रणाली), एन. आइ. डी. एस. (नेटवर्क इंट्रुजन डिटेक्शन सिस्टम – नेटवर्क घुसपेठ खोज प्रणाली) तथा आइ. पी. एस. (इंट्रुजन प्रिवेंशन सिस्टम - घुसपेठ निरोधक प्रणाली) कुछ इसी तरह के साधन (हार्डवेयर तथा सॉफ्टवेयर सिस्टम) हैं जो इन नेटवर्क को बाहरी तथा आंतरिक हमलों से बचाती हैं। यह सिस्टम कंप्यूटर, सर्वर या नेटवर्क में कोई नए प्रोग्राम

या डाटा की प्रविष्ठी या बाहर ले जाने को परीक्षण कर अनुमति प्रदान करती है तथा उनका रिकॉर्ड भी रखती है। एन्टी वायरस की तरह इन प्रणालियों का नियमित अपडेशन एक जरुरी आवश्यकता होती है। एस. ओ. सी. (सिक्यूरिटी ऑपरेशन सेंटर) एक तरह से फिजिकल सिक्यूरिटी कण्ट्रोल रूम का ही काम करता है, जो हर आने-जाने वाले (डाटा, प्रोग्राम, सूचना, सूचना पैकेट आदि) पर निगाह रखता है।

5) मोबाइल के ब्लू-टूथ और हॉटस्पॉट के साथ भी उक्त बाते लागू होती हैं। साथ ही ब्लू-टूथ की (पासवर्ड) शेयर करना तथा ओपन हॉटस्पॉट और ओपन वाई-फाई यूज़ करना या मोबाइल में चालू रखना भी आपके घर के दरवाजे खिड़कियाँ अनजान लोगों के लिए खुली रखने के समान ही है।

6) क्या आप अपने मोबाइल को इन्टरनेट या मोबाइल बैंकिंग के लिए उपयोग करते हैं? क्या आप मोबाइल को फेसबुक, व्हाट्सएप्स, ईमेल आदि के लिए इस्तेमाल करते हैं? यदि आपका उत्तर हाँ में है तो जरूर ही आपने अपने मोबाइल को खोलने के लिए पिन या पासवर्ड या पैटर्न सेट किया होगा। या आपका फ़ोन फिंगर सेंसर या रेटिना या फेस रिकग्निशन से युक्त है और केवल आपके द्वारा ही उसे खोला जा सकता है। यदि आप इन प्रावधानों का उपयोग करते हैं तो आपने फ़ोन की सिक्यूरिटी प्रणाली का उपयोग किया है। अन्यथा आपको इनका उपयोग तुरंत शुरू करना चाहिये। शायद आपको यह भी पता होगा - मोबाइल खोने की स्थिति में आप अपनी सेंसिटिव जानकारियों को किसी अवांछित व्यक्ति के हाथों में पड़ने से बचाने के लिए फ़ोन को रिमोटली या दूरनियंत्रित कर फॉर्मेट या फैक्ट्री रिसेट कर सकते हैं। इस प्रकार की कई व्यवस्थाओं द्वारा आप अपनी फ़ोन पर सन्चित जानकारी अधिक सुरक्षित कर सकते हैं।

7) हम अक्सर बहुतसे एप्स अनजाने में इंस्टाल करते हैं, जो की हमारे मोबाइल पर सन्चित बहुत-सी जानकारी को चुरा कर या हमारे जाने-अनजाने में ही औरों से शेयर करती हैं। इनमें आपकी फ़ोन डायरेक्टरी, एस एम एस, एसडी कार्ड, कैमरा, यूजर आईडी, पासवर्ड आदि सम्मिलित हैं। इनसे बचाव का तरीका क्या हो सकता है? आप पी. एन. आर. जांच के लिए आई. आर. सी. टी. सी. या एयरलाइन की अधिकृत वेबसाइट और एप्लीकेशन का ही उपयोग करें, जिससे आप वह जानकारी किसी अन्य के साथ शेयर नहीं करेंगे। बैंक मिस्ड कॉल सर्विस या यू. पी. आई. आदि के लिए बैंक की अधिकृत एप्लीकेशन का ही उपयोग करें, जिससे आप अपने बैंक खाते, आईडी आदि को थर्ड पार्टी एप्लीकेशन के माध्यम से किसी अन्य के साथ शेयर नहीं करेंगे।

8) एंड्राइड फोन्स के नवीन ऑपरेटिंग सिस्टम्स (वर्जन 6/7/8 मार्शमेलो/नौगाट/ओरियो) में आप विभिन्न भाग, जैसे कॉन्टैक्ट बुक, मेसेजेस, कैमरा, एसडी कार्ड, स्टोरेज आदि की अनुमति (Permission) को निर्धारित या नियंत्रित कर सकते हैं तथा अवांछित अनुमति को बंद कर सकते हैं। यह आपको उन एप्लीकेशन को नियंत्रित करने में मदद कर सकता है, जिन्हें आप उपयोग तो करना चाहते हैं, पर उनके साथ केवल आवश्यक जानकारी ही शेयर करना चाहते हैं, या उन एप्लीकेशन को निकाल (अनइंस्टाल कर) सकते हैं।

इस प्रकार हम देखते हैं की जहाँ सूचना प्रौद्योगिकी विविध सुविधा प्रदान कराती हैं, उसके साथ ही हमें अवांछित खतरों का भी ज्ञान होना अतिआवश्यक है। इसी के साथ हमें जरुरी सुरक्षा के लिए कदम उठाना आवश्यक है। कहते हैं कि 100% सुरक्षा एक अवधारणा है, पर इसकी प्राप्ति के लिए हमें हमेशा सजग रहना जरुरी है। साथ ही विभिन्न घटनाओं के अनुभव से सीख लेना हमेशा हितकर होता है। इससे हम रिस्क मिटिगेशन द्वारा क्षति को न्यूनतम कर सकते हैं।

यदि हम सुरक्षा को अनिवार्यता की बजाय आदत में शुमार कर लेते हैं तो हमें यह एक अड़चन या व्यवधान न लग कर एक सुखद अनुभव प्रदान करता है और काफी हद तक हम साइबर क्रिमिनल्स की आसान पहुँच से अपने आप को बाहर रख सकते हैं। ☯

Author: Shri. Waman Gokhale

Reviewed by: Mr. V. N. Kulkarni Ex. Dy. General Manager and Principal, Management Development Institute of Bank of India.

Credit 360°Appraisal Disbursement Monitoring and Recovery

Credit management by commercial banks is a part of banking activities of normal course where banks constitute as a largest group of financial intermediaries. Banks' credit has to be productive and must contribute to the generation of the borrower's income and also towards increasing the rate of growth of the economy as a whole. Towards this end banks have to strive hard to maintain the asset quality. Maintaining the asset quality is a challenging task for the bankers demanding stringent credit monitoring and recovery management efforts. Non-Performing Assets (NPAs) are a key concern for banks in India. They are the best indicator of the health of the banking industry. To improve the efficiency and profitability of banks, NPAs need to be reduced and controlled. At the same time understanding of the legal implication and significance of documentation in the loan department of banks can hardly be overemphasized.

With ever increasing new entrants in banking industry, there is a need for good reference book which will not only meet the theoretical knowledge, but also, the practical part. This is where a book written by Shri Waman Gokhale bridges the gap. Shri Gokhale has varied experience in banking having worked with Central Bank of India for nearly four decades.

The book comprises of 14 Chapters with 116 lessons & covers practical aspects. For the new entrants to the credit department, readers can learn the basic principles while handling the credit portfolio, right from interviewing the borrower etc. Chapter 7 of the book has a real life case of interviewing the borrower.

Through the subsequent chapters the reader can assimilate various financial aspects such as understanding Balance Sheet, Ratio Analysis and their interpretation, the concepts such as Working Capital Assessment, Term Loan Appraisal, Assessment of non-fund based facilities, export finance has been discussed threadbare to have crystal clear understanding. The banking industry is concentrating more on Retail and MSME lending and the book covers these aspects including lending to priority sectors. These chapters will be useful to the youngsters who will be dealing with these types of advances in the initial years. Apart from understanding the processing part, documentation is also an important aspect and Chapter 11 covers it elaborately. The Chapter on documentation, covers step by step; selecting proper set of documents, stamping of documents,

BOOK REVIEW

execution, registration, limitation & renewal etc.

The most crucial part in credit department is credit monitoring and follow-up action for recovery of dues. The book elaborately covers various aspects of credit monitoring including handling of stressed assets, non legal & legal methods of recovery. The restructuring discussed will surely help the bankers to tackle stressed MSME loans.

What is more interesting about this book is coverage of live case studies. This chapter should definitely of use to the youngsters and those who are new to the credit in understanding the various aspects that need to be looked in to while preparing a credit proposal. Author, who has varied experience of more than 4 decades, has done well by adding this chapter which will solve the problems of the youngsters while preparing a comprehensive proposal. To the experienced bankers it will definitely help to sharpen their appraisal skills. The Author has covered various concepts like Ratio Analysis, QIS, FFR, along with various legal terminologies in a simple way. The book contains appraisal of BG & LC proposals and their monitoring which again is a very important facet of lending. In short various aspects of credit ranging from Credit Appraisal to Monitoring and ultimately Recovery are lucidly explained. The chapter on documentation gives an insight about the process of documentation more particularly on 'General aspects about Execution of Documents' tackling various situations during the process so as to protect Banks interests.

Chapter 14 of the book will be of great use to the new entrants handling credit portfolio not only about preparation of a credit proposal but in presenting it before various authorities. This chapter covers what a proposal should contain by way of bullet points followed by live examples of handling MSME proposal, agro products proposal and also a large consortium proposal. Reader will get insight in to the practical aspects of preparation and presentation of a credit proposal.

The new entrants to the banking industry as well as those bankers who did not have exposure in handling credit portfolio so far will find this Book very practical and useful. This book will help the Banker to build up requisite knowledge base to face the day to day challenges while working in Credit Department.

The book has been forwarded by former CMD of Central Bank of India and former Chief Executive of Indian Bank's Association. Similarly, the book is appreciated by present CMD of Union Bank of India, (then E.D of Oriental Bank of Commerce) and Ex-E.D. of Indian Overseas Bank.

Lastly, I pen off by saying that not only the youngsters in the bank as well as those who did not have exposure in handling credit portfolio, but also, the Credit Appraisers should possess this book as a readymade handy guide.

Summary of Macro Research Project

Title of the Macro Research Project: The impact of technology on the perfomance of Indian Banking Industry: An Empirical study

Researcher: Dr. Sanjeev Bansal, Professor & Chairman, Department of Economics, Kurukshetra University.

Year of Study: 2014-2015

With intense competition both from domestic sector and international players and explosive growth in information technology, the way in which commercial banks conduct business has changed considerably. In order to survive and adapt to the changing environment, banks are putting in more efforts on understanding the drivers to generate better financial performance. The role of information technology in performance of an organization is still a paradox. The technology is not a panacea rather it is a tool to enhance efficiency and its implementation requires prudent planning, organizational capabilities, managerial skills, and entrepreneurship. In the age of competition, the contribution of information technology to the performance of an organization is being questioned. In this context, the study is an attempt to analyze the effect of information technology on the performance of Indian Banking Industry.

Review of Literature

The enduring magnitudes of investment in information technology have drawn attention of researchers and policy makers to analyze the impact of information technology on growth and productivity. The expectation was that increased investment in information technology would naturally lead to an increase in performance of organization but despite massive investment in information technology, its impact on performance continued to be questioned. Despite hundreds of studies carried out, opinion of the experts is solidly divided on the information technology-productivity debate. The debate is divided into two groups: (a) productivity paradox; and (b) productivity pays-offs. A good quantum of literature defends the idea of 'Solow Paradox' in concluding that information technology may affect negatively on bank's efficiency and may reduce productivity. Conversely there are many works, approving the positive impact of information technology on business value.

Such studies have used firm level evidence and have concluded that productivity paradox has disappeared. The difficulty in measuring and evaluating the benefits of information technology has generated an extensive literature, both on quantitative and qualitative plane. There are very few studies that quantitatively index both, 'information technology' and the 'performance' of a service organization and relate the two. In this respect, the lack of good quantitative measure for the output and value created by information technology has made the studies on justifying information technology investment, particularly difficult. In this setting of argument, this work is an attempt to fill this research gap by investigating the relationship between information technology investments and performance in the Indian Banking Sector.

Objectives of the Study

The present study has the following objectives:

1. To evaluate the status of technology implementation in Indian Banking Sector.
2. To analyze the impact of information technology adoption on the performance of Indian Banking Sector.
3. To estimate the relative efficiency and productivity of Indian Banking Sector in pre and post e-banking revolution period.
4. To draw some policy implications based on the findings emanated from the study.

Data and Methodology

The present study is based upon the time-series data from 1999-2000 to 2014-15. The time period has been deliberately selected because the information technology has been introduced only during this time period and many private sector banks have got their licenses from RBI only during this period. The data have been obtained from the public data sources on bank's financial statements and income expenses reports. The secondary data and information have been collected from the publications of the Reserve Bank of India: 'Report on Trend and Progress of Banking in India', 'Handbook of Statistics on Indian Economy'.

'RBI Bulletin (Monthly)', Annual Reports of respective banks and other valuable publications of public sector banks, private and foreign banks in India. Various websites have also been used for the data mining. Data published by Indian Banking Association in monthly bulletins, in special issues and annual publications on 'Performance Highlights of Banks' have also been used. For present research work, various journals, magazines and newspapers like 'Indian Journal of Commerce', 'Economic Survey of India', 'Economic and Political Weekly', 'Financial Express', 'Economic Times' have also been considered. To make the work manageable and effective, it has been confined to 31 banks only. The sample represents all categories of banks: State Bank of India and its associates; nationalized banks; old private banks; new private banks; and foreign banks. By using a meaningful denominator, technology parameters have been normalized. To derive the overall technology parameter, a technology index has been derived using the discrete technology parameters. Performance analysis has been done by computing a performance index which takes into consideration different variables. The relation of technology index and performance index has been analyzed by using correlation and regression technique on both time series and panel data. Wherever needed, appropriate price adjustments have been made. The study makes an attempt to study the efficiency and productivity aspects of Indian Banking Industry at a disaggregated level. To measure efficiency of bank groups and individual banks, DEA has been used and to measure the productivity, Malmquist Index has been used.

Main Conclusion of the Study

The overall conclusion that emerges from the analysis is that in banking industry, performance is a positive function of information technology. The findings confirm that contribution of technology to bank's performance has a differential behavior. Information technology led performance is a promising strategy for many banks to accelerate the development process. However, it does not guarantee success for all banks, as their backgrounds and capabilities to produce and use information technology differs. This is what explains the productivity paradox in service sector in general, and in banking sector in particular.

Main Recommendation of the Study

The information technology expenditure data for new private banks suggest that banking industry has been engaged in arbitrary information technology budgeting during the period under study. Over budgeting of information technology spending is noticeable among banks, suggesting managements' eagerness to approve information technology budget irrespective of its contribution to performance. The results of current study show that there is no relationship between information technology budget and performance of new private sector banks and foreign banks. The banks' management and information technology practitioners need to focus on higher information technology resources utilization and efficiency. Information technology budgeting should focus on planning, monitoring and controlling future operation. The results of current study suggest evidence of information technology productivity paradox in the Indian Banking Industry, evidence that could fade if information technology solution aligns well with business strategies. The existence of productivity paradox indicates the need for information technology managers and organization leaders to justify their information technology spending in terms of performance. ☯

Summary of Macro Research Project

Title of Macro Research Project: Quantifying Basel III's time varying capital requirements and their impact on macro and financial variables over business and financial cycles

Researcher : Dr. Saurabh Ghosh, Reserve Bank of India.

Year of Study: 2014-15

1. The collapse of Lehman Brothers in September 2008, and the ushering of the global financial crisis brought to the fore several regulatory gaps that could have long lasting financial, real and spillover effects. At the heart of the banking crisis was the pro-cyclicality of risk based banking regulations, which led to a credit boom and then its bust. The ill-effects of the financial downturn and its impact on the business cycle affected economics across Pacific and the Atlantic, causing massive economic disruptions.

2. With the quantum of loses mounting to an all-time high, multilateral bodies like G-20, IMF, BIS and FSB initiated several policy actions aimed at bridging gaps in the banking policy domain. Some of the major initiatives in this regard aimed at improving the quality and quantity of banking capital and introducing elements of countercyclicality in banking operations.

3. Since its inception in 1974, the Basel Committee has strived for stability in the banking system and it has made major changes, including risk based capital requirements in Basel II published in 2004. GFC and a plethora of academic and policy debates following this made BCBS to rethink banking regulations. A new set of regulations were initiated in a discussion paper and there final versions were published as Basel III in 2010. The capital and liquidity reforms called for higher banking capital holdings in the form of Tier-I capital, the most subordinate claim being in the case of bankruptcy. The liquidity ratios included LCR for short-term stressed market liquidity demand and NSFR for long-term asset liability matching. It also included two buffers, the conservation buffer and the countercyclical capital buffer to make credit smooth and banking countercyclical.

4. While the debate surrounding the adequacy a 4.5 per cent risk weighted capital as Tier-I is yet to be settled, some more controversial issues have surfaced in the academia and policy domain. One of these is related to the cost of increased capital and liquidity requirements in terms of credit deceleration and output sacrifice for more resilient banking systems and financial stability. This is especially so at this juncture when some economies are showing signs of recovery and some of the emerging markets that were considered as engine of growth are signalling tapering in output growth.

5. A quick review of theoretical and empirical literature in this context suggests that in a frictionless MM-world the liability side of a bank's balance sheet should not affect its asset side. However, with tax transactions and agency cost financial markets are far from frictional less and therefore, subsequent literature has also documented the importance of bank size, capital and liquidity in deciphering monetary policy, deposit or other financial shocks. A bank attempting to raise capital could do so by retained earnings, raising capital from the market, a stake sale by majority holders or by infusion of capital from owners. The capital adequacy ratio, on the other hand, can be improved either by increasing capital or by changing the risk profile of the bank's asset side so that the risk weighted assets (denominator of the ratio) of the bank decline.

6. There is ample evidence in literature that banks attempting to raise capital generally witness an

increase in their lending spreads to cover the costs of additional capital. If raising capital is costly because of asymmetric information and debt overhang problems, especially during a downturn, a bank may choose to ration lending, especially to risky ventures, to match the target capital adequacy. In a bank finance dominated economy, this in turn affects output and gives rise to a trade-off - the cost of macro-prudential policies vis-a-vis its benefit in terms of avoiding output loss due to a crisis.

7. With the emphasis on the quantity and quality of bank capital in the Basel III accord, a debate has erupted on the quantum of output sacrifices for achieving financial stability and their short-run and long-run characteristics. Several multilateral organizations, think tanks and industry representatives have estimated the magnitude of the trade-off. To refer to a few, BIS's Macroeconomic Assessment Group estimated the impact of Basel III implementation on GDP to be relatively small and short lived, whereas the Institute of International Finance estimated much higher costs (in terms of decline in GDP) for implementing Basel-III. While, the estimated models and their assumptions differ, the trade-off depends on the timing and initial conditions (for example, the level of capitalization of banks or present interest rate cycles) in the underlying economy.

8. The Basel-III measures of strengthening capital in the banking system were endorsed by the G-20 Banking Summit in November 2010. The Regulatory Consistency Assessment Programme (RCAP) indicates that while some countries have already completed implementing capital regulations, others have made progress depending on their stages of development. There are four Asian emerging market economies (China, India, Indonesia and South Korea) that are G-20 signatories and will be implementing Basel-III by 2019. This analysis with the real GDP growth rate and capital adequacy ratio indicates a negative relationship between the two for China, Indonesia and South Korea. A dynamic panel regression also supports a negative relationship between banking capital adequacy and GDP growth for these countries. It may be mentioned here that most of these countries have policy rates higher than near zero rates in advanced economics, and therefore, an increase in capital could have a larger impact on GDP growths as compared with those estimated by the MAG (BIS) study or by the IMF study, even after allowing for global spillovers.

9. In India, the banking system plays a dominant role as a source of finance to the private sector. India has started implementing Basel-III recommendations. The RCAP assessment in 2015 found India to be compliant with all 14 components of the Basel framework. Indian banks are presently adequately capitalized with significant portions of Tier-1 capital being contributed by Common Equity (CET1). However, to meet all Basel III requirements by 2019, it is estimated that the Indian banking sector will require huge capital infusions.

10. With the Reserve Bank and the Government of India attempting policy measures for a smooth transition to the Basel-III capital framework, we made an attempt to estimate the impact of such large capital infusions on changes in lending spreads, banks' credit off-takes and risk taking and their consequent impact on GDP growth using historic data from 1996 to 2015 (quarterly) from different publicly available sources.

11. A correlation between banks' capital and lending rates generally indicates that banks' lending rates increase with a growth in bank capital. A stronger result holds between a bank's lending spread (lending rate minus call rate) and growth in bank capital. In a multivariate framework, the bank lending spread is found to be positively and significantly related to changes in the capital adequacy ratio (CRAR) after controlling for growth cycle, inflation, change in non-performing assets (NPAs) and a crisis period.

GDP growth (and also output gap) has a positive (significant) coefficient indicating an increase in the spread during an economic boom, while changes in GNPA have a negative co-efficient indicating decline in the spread with an increase in bad assets in the banking sector. Among the bank groups, changes in public sector banks' (PSBs) CRAR have the maximum and most significant impact on spreads, which is expected, as public sector banks dominate the Indian Banking arena.

12. Correlation results indicate that there are positive and significant correlations between an increase in banks' capital and deposit mobilization by the banks. There has been considerable debate on the negative relation between an increase in the banking sector's capital and credit growth. We attempted to evaluate the relationship between bank capital and credit growth after controlling for demand side factors affecting credit. The findings suggest that during the sample period, there existed a negative relationship between an increase in CRAR and credit off-take. This relationship held after controlling for an output-gap, stock index returns, lending rate and persistence in the credit off-take (AR(1)) coefficient. The output gap had a positive coefficient indicating a pro-cyclical increase in credit off-take, while the lending rate reported a negative coefficient. These results hold for year-on-year (y-o-y) as well as quarter-on-quarter (q-o-q) variations. However, some of these lagged changes in CRAR coefficients were weekly statistically significant.

13. There is debate surrounding the factors that influence a bank's risk taking, with a school of thought claiming that a bank's investments in risky assets declines with an increase in capital. In this study we took banks' investments in G-secs with zero risk weight and banks' investments in housing loans, with risk weights depending on the loan size. This analysis indicate that as capital requirements increase the contemporaneous (correlation) relationship shows an increase in banks' investments in G-secs and a decline in their investments in housing. This indicates that higher capital requirements reduce banks' investments in risky segments.

14. In a multivariate analysis, we controlled for other demand side factors (GDP growth, interest rate, stock returns and change in SLR) and attempted to evaluate the impact of changes in CRAR (and its lags) on the growth rates of housing credit and G-secs investments. Empirical results support our earlier findings and indicate that with an increase in banks' capital requirements they park their funds in safer investments (G-secs). Stock returns had a positive and statistically significant coefficient for an increase in a bank's investments in housing while the co-efficient was negative and significant for bank's investments in G-secs, indicating banks' risk taking behaviour during an upturn in the financial cycle and/ or market perceptions.

15. The relationship between bank capital and output is unlikely to be contemporaneous. This is also supported by our correlation results using different measures of output (quarterly GDP growth, IIP growth and core IIP growth and their components). These suggest the absence of contemporaneous relationship between an increase in the banking sector's capital and output growth.

16. To evaluate the impact of a shock to bank capital on major macro-variables, we followed existing literature and estimated an endogenous set of equations in a Vector Auto-regression framework suggested by Sims. To address the a-theoretic nature of this model, taking cue from theoretical literature and ordered these variables. We then evaluated the effect of a structural shock to a change in a bank's capital adequacy ratio on other macro-variables by analysing impulse response functions, accumulated impulse response functions and variance decompositions. To test the robustness of our results we used: a) generalized impulse responses which are indifferent

to the ordering of the variables, as established by Pesaran, and b) a different set of variables (proxy) for output growth and/or gap. Since, quarterly data was used and there is evidence of seasonality, growth rates in the macro-variables were adjusted for seasonal fluctuations.

17. Researcher started with the momentum measure, that is, q-o-q changes in four variables namely CRAR, bank lending spread, bank credit growth (SA) and the q-o-q growth rate of GDP. The results indicated weak evidence of increase in spread, decline of bank credit growth and decline in quarterly GDP growth. These results were consistent when generalized impulse responses were generated. The variance decomposition of q-o-q growth indicates that a small portion of the variation in quarterly GDP growth was explained by a change in CRAR, while change in the lending spread explained much more variations.

18. Using the same VAR framework after replacing q-o-q variations by annual variation (y-o-y) we got a statistically significant result of increase in lending spread and decline in GDP due to a shock to CRAR changes, which is robust to changes in variable ordering. However, it may be mentioned here that the magnitude of such an effect was small which reverted to the baseline within a short period. A shock to a bank's lending spread had a similar effect on output decline. These findings are in line with BIS's findings on the impact on GDP. Most of the literature surveyed in this field also claims that the new banking regulations could have a cost in terms of sacrificing GDP in the short-run. However, such cost is likely to be short lived and small compared to the output loss in case of a financial crisis.

19. In 2014, the Central Statistical Organization (CSO) released a new series for real output, the gross value added at basic prices (GVABP) which incorporates several welcoming features. In view of having an estimate with the new series, the series was spliced appropriately and a series for historic data was derived. Using this as a proxy for output in the VAR model, the effect of a shock to a CRAR change and bank spread was calculated. The impulse responses were indicated a decline in bank credit to commercial sectors and to the GVABP growth rate. However, in line with earlier observations, such a decline was short lived and the effect tapered off over six to eight quarters.

20. One of the measures introduced in Basel-III refers to a countercyclical buffer with an objective of reducing pro-cyclicality in the banking system. This was considered to be one of the major evils flaring up GFC. However, there are debates surrounding the effectiveness of such measures on business and financial cycles. More precisely a school of thought led by Saurina et. al. believes that countercyclical policies based on a credit-to-GDP gap could actually result in aggravating the cycle's amplitude. In an attempt to evaluate the effect of an increase in banking capital requirements on the cycle, we evaluated cyclical variations in GVABC using different methods of estimating output gaps (HP, Bandpass filters). Then the same VAR system after replacing the estimated output gap as a proxy for an output variable was used. The impulse responses clearly indicated a decline in the output gap due to a shock in banks' CRAR. This finding notes the stabilizing impact of buffer policies in the Indian context; besides macro-prudential features of a capital buffer, an increase in bank capital during an economic boom is likely to stabilize positive outputs and thereby contribute to economic stability.

21. To have a focused approach on the impact of an increase in bank capital on manufacturing sector, seasonally adjusted IIP growth as a proxy for output growth and estimated the VAR system and impulse responses was considered. The impulse responses indicated a decline in responses to the manufacturing sector's output. However, it seemed to be short lived as compared with a decline in other measures of output.

22. Infrastructure plays a dominant role in sustaining long term growth in emerging market economies. Considering its strategic importance, we tried to evaluate how change in banks' CRAR impacts core (infrastructure) IIP. To do so, researcher replaced the last variable(output gap) by the seasonally adjusted core IIP growth rate and estimated the VAR model. The impulse responses using both unrestricted and generalized VAR gave a different prospective for core IIP growth, as there was no initial decline and these impulse reactions were not statistically significant.

23. Intrigued with this result, we estimated impulse responses for seasonal IIP growth rates of each of the eight sectors (electricity, fertilizer, cement, coal, crude, natural gas, petroleum and refinery and steel) that are included separately in the VAR framework. Impulse responses for each of these to a one standard deviation shock to the bank capital adequacy ratio indicated no immediate sign of a decline and most of these were statistically insignificant. It could be the case that long term loan contracts and active policy measures and monitoring for these sectors resulted in such difference in results.

24. After an extensive literature survey, considering a battery empirical techniques to evaluate lending spreads and discussing credit flow and its impact on output (using a set of proxy) it may be concluded that the new banking regulations could have a small cost in the short run as compared to already documented measures of huge losses due to financial instability. The increase in capital during an economic expansion could achieve the macro-prudential goals as well as being an automatic economic stabilizer. Experience with the infrastructure sector was an exception to this finding. These results are robust to the introduction of a new GVA and changes in impulse generating techniques. On the issue of what could be the exact magnitude of the shock, it may be mentioned that lending spreads of banks play a stronger role in deciding the impact of capital shocks on banks' credit disbursements and their subsequent impact on output. Therefore, if CRAR changes takes place during a time when lending spreads are low, then CRAR's impact on changes in credit disbursements or quarterly output growth could be far less as compared to periods when the lending spread is already high. In a cross-country framework, countries with higher interest rates could have a significantly higher impact on bank credit or GDP growth as compared to countries that have low, near zero or negative deposit rates.

25. In this research, researcher have empirically evaluated possible impact of an increase in banking sector capital on output. The natural progression to this could be a dynamic stochastic general equilibrium (DSGE) model incorporating financial sector that would allow us to have counter-factual set of experiments in banking sector in India. The second extension of this study could be by introducing the impact of increase in global banking sector capital on Indian economy that could attempt to quantify such spillover impact on Indian GDP and banking sector.

☯

Bank Quest Articles - Guidelines For Contributors

Contributing articles to the Bank Quest : (English/Hindi)

Articles submitted to the Bank Quest should be original contributions by the author/s. Articles will only be considered for publication if they have not been published, or accepted for publication elsewhere.

Articles should be sent to:

The Editor: Bank Quest

Indian Institute of Banking & Finance,

Kohinoor City, Commercial-II, Tower-1,2nd Floor,
Kirol Rd., Kurla (W), Mumbai - 400 070, INDIA.

Objectives:

The primary objective of Bank Quest is to present the theory, practice, analysis, views and research findings on issues / developments, which have relevance for current and future of banking and finance industry. The aim is to provide a platform for Continuing Professional Development (CPD) of the members.

Vetting of manuscripts:

Every article submitted to the Bank Quest is first reviewed by the Editor for general suitabillty. The article may then be vetted by a subject matter expert. Based on the expert's recommendation, the Editor decides whether the article should be accepted as it is, modified or rejected. The modifictions suggested, if any, by the expert will be conveyed to the author for incorporation in case the article is considered for selection. The author should modify the article and re-submit the same for the final decision o the Editor. **The Editor has the discretion to vary this procedure**.

Features and formats required of authors :

Authors should carefully note the following before submitting any articles:

1) *Word length:*

   Articles should generally be around 2000-3000 words in length.

2) *Title:*

   A title of, preferably, ten words or less should be provided.

3) Autobiographical note and photograph:

   A brief autobiographical note should be supplied including full name, designation, name of organization, telephone and fax numbers, and e-mail address (if any), or last position held, in case of retired persons. Passport size photograph should also be sent along with the submission.

4) *Format:*

   The article, should be submitted in MS Word, Times New Roman, Font Size 12 with 1½ line spacing. A soft copy of the article should be sent by e-mail to publications@iibf.org.in

5) *Figures, charts and diagrams:*

   Essential figures, charts and diagrams should be referred to as 'Figures' and they should be numbered consecutively using Arabic numerals. Each figure should have brief title. Diagrams should be kept as simple as possible. in the text, the position of the figure should be shown by indicating on a separate line with the words: 'Insert figure 1'.

6) *Tables:*

   Use of tables, wherever essential, should be printed or typed on a separate sheet of paper and numbered consecutively using Arabic numerals (e.g. Table-1) and contain a brief title. In the body of the article, the position of the table should be indicated on a separate line with the words 'Insert Table 1'.

7) *Picture / photos/ illustrations:*

   The reproduction of any photos, illustration or drawings will be at the Editor's discretion. Sources should be explicitly acknowledged by way of footnote, all computer-generated printouts should be clear and sharp, and should not be folded.

8) *Emphasis:*

   Words to be emphasised should be limited in number and italicised. Capital letters should be used only at the start of the sentences or for proper names.

Copyright:

It is important that authors submitting articles should declare that the work is original and does not infringe on any existing copyright. He/ she should undertake to indemnify the Institute against any breach of such warranty and consequential financial and other damages. Copyright of published article will vest with publisher (Institute).

DECLARATION FORM

The Editor,
Bank Quest,
Indian Institute of Banking & Finance,
Kohinoor City, Commercial II,
Tower I, 2nd Floor, Kirol Road,
Kurla (W), Mumbai - 400 070.

Dear Sir / Madam,

Re : Publication of my article

I have submitted an article "____" for publication at your quarterly journal Bank Quest.

In this connection this is to declare and undertake that the said article is my original work and that I am the author of the same. No part of the said article either infringes or violates any existing copyright or any rules there under.

Further, I hereby agree and undertake without any demur: to indemnify and keep the Institute (IIBF) indemnified against all actions, suits, proceedings, claims, demands, damages, legal fees and costs incurred by the Institute arising out of infringement of any copyright /IPR violation.

Yours faithfully,

(______________________________)

Author

____

Name : ____

Designation : ____

Organisation : ____

Address : ____

Tel. No. : ____

E-mail ID : ____

Signature : ____

Date : ____

Subscription for Bank Quest and IIBF VISION

Since 1st July 2016 Institute has started to accept subscription for Bank Quest and IIBF VISION in online mode through SBI Collect and discontinued to accept subscription through Demand Draft. Domestic subscribers are requested to visit "Apply now" at home page of IIBF Website - www.iibf.org.in for payment of subscription in online mode and also note:

1. Subscription will be accepted only for one year.
2. Third party payment would not be accepted.
3. Institute will dispatch the Bank Quest and IIBF VISION to domestic subscribers through Book-Post.
4. Foreign subscribers may write to Publication Department at Publications@iibf.org.in for subscription application form.

Annual Subscriptions rates for Bank Quest and IIBF VISION are as under: Subscription Rate for Bank Quest:

Period	One year
No. of Issues	4
Annual Subscription Rate inclusive of postage (In India) (₹)	160/-
GST* (₹)	Nil
Total Subscription inclusive of postage (In India) (₹)	160/-
Total Subscription inclusive of postage (Foreign) (US $)	10

*GSTN-27AAATT3309D1ZS

Subscription Rate for IIBF VISION:

Period	One year
No. of Issues	12
Annual Subscription Rate inclusive of postage (In India) (₹)	40/-
GST* (₹)	Nil
Total Subscription inclusive of postage (In India) ((₹)	40/-

*GSTN-27AAATT3309D1ZS

STATEMENT ABOUT OWNERSHIP AND OTHER PARTICULARS OF BANK QUEST, THE JOURNAL OF INDIAN INSTITUTE OF BANKING & FINANCE

1.	Place of Publication	:	Mumbai
2.	Periodicity of Publication	:	Quarterly
3.	Publisher’s Name	:	Dr. Jibendu Narayan Misra
	Nationality	:	Indian
	Address	:	Indian Institute of Banking & Finance Kohinoor City, Commercial-II, Tower-1, Kirol Road, Kurla (W), Mumbai-400 070.
4.	Editor’s Name	:	Dr. Jibendu Narayan Misra
	Nationality	:	Indian
	Address	:	Indian Institute of Banking & Finance Kohinoor City, Commercial-II, Tower-1, Kirol Road, Kurla (W), Mumbai-400 070.
5.	Name of Printing Press	:	Onlooker Press, 16 Sasoon Dock, Colaba Mumbai - 400 005.
6.	The name and Address of the Owners	:	Indian Institute of Banking & Finance Kohinoor City, Commercial-II, Tower-1, Kirol Road, Kurla (W), Mumbai-400 070.

I, Dr. J. N. Misra, hereby declare that the particulars given above are true to the best of my knowledge and belief.

01.01.2018

Dr. J. N. Misra
Signature of Publisher

Standing Committee on Cyber Security

In the wake of exponential growth of digitalisation in banks, cyber risks have emerged as a major area of concern. Conscious of the rising threats to the cyber infrastructure in its regulated entities, the Reserve Bank of India has taken a number of measures, particularly over the last two years.

Based on the recommendations of the Expert Panel on Cyber Security and Information Technology Examination (Chairperson: Smt. Meena Hemchandra), guidelines were issued to banks in June 2016, mandating cyber security preparedness. Banks’ progress in strengthening their cyber resilience and response is being monitored. Recognising the increasing frequency and complexity of cyber security incidents, the monetary policy statement of February 8, 2017 announced that an Inter-disciplinary Standing Committee will be set up to conduct an ongoing review of the cyber security landscape and emerging threats.

The remit of the committee, inter alia, includes reviewing the threats inherent in existing/emerging technology; studying adoption of various security standards/protocols; interfacing with stakeholders; and suggesting appropriate policy interventions to strengthen cyber security and resilience.

The committee was constituted on February 28, 2017 (Chairperson: Smt. Meena Hemchandra, Executive Director). Members of the committee include experts on cyber security in the Reserve Bank as well as from outside. The committee is meeting regularly and, as per its recommendations, subgroups have been formed on certain focus areas for an indepth examination.

Source: RBI Annual Report, 2016 -17

IIBF - PUBLICATION LIST

Sr. No.	Examination	Medium	Name of the Book	Edition	Published By	Price (Rs.)
34	Certificate Examination in MSME Finance for Bankers	English	Micro Small & Medium Enterprises in India	2017	M/s Taxmann Publications Private Ltd.	Rs. 375/-
35	Certificate Examination in International Trade Finance	English	International Trade Finance	2017	M/s Taxmann Publications Private Ltd.	Rs. 255/-
36	Certificate examination in IT Security	English	Certificate Examination in IT Security	2017	M/s Taxmann Publications Private Ltd.	Rs. 425/-
37	Certificate Examination in Prevention of Cyber Crimes & Fraud Management	English	Prevention of Cyber Crimes & Fraud Management	2017	M/s Macmillan India Limited	Rs. 245/--
38	Certificate examination in Micro Finance	English	Micro-finance Perspectives & operation	2014	M/s Macmillan India Limited	Rs. 365/-
39	Certificate Examination in Rural Banking Operations	English	Rural Banking Operation	2017	M/s Taxmann Publications Private Ltd.	Rs.545/-
40	Certificate examination in Information System Banker	English	Information System for Banks	2017	M/s Taxmann Publications Private Ltd.	Rs. 645/-
41	Advanced Wealth Management Course	English	Introduction to Financial Planning	2017	M/s Taxmann Publications Private Ltd.	Rs.390/-
42	Advanced Wealth Management	English	Risk Analysis, Insurance and Retirement Planning	2017	M/s Taxmann Publications Private Ltd.	Rs. 240/-
43	Advanced Wealth Management Course	English	Investment Planning, Tax Planning & Estate Planing	2017	M/s Taxmann Publications Private Ltd.	Rs. 420/-
44	Diploma in Treasury, Investment and Risk Management	English	Treasury, Investment and Risk Management	2017	M/s Taxmann Publications Private Ltd.	Rs. 595/-
45	Diploma in International Banking & Finance	English	International Banking Operations	2017	M/s Macmillan India Ltd.	Rs. 285/-
46	Diploma in International Banking & Finance	English	International Corporate Finance	2017	M/s Macmillan India Limited	Rs. 290/-
47	Diploma in International Banking & Finance	English	International Banking-Legal & Regulatory Aspects	2017	M/s Macmillan India Limited	Rs. 245/-
48	Diploma in Cooperative Banking	Englishi	Cooperative Banking-Principles, Laws & Practcies	2017	M/s Macmillan India Limited	Rs. 315/-
49	Diploma in Cooperative Banking	English	Management and Operations of co-operative Banks	2017	M/s Macmillan India Limited	Rs. 445/-
50	Diploma in Banking Technology	English	Information Technology, DataCommunication & Electronic Banking	2017	M/s Macmillan India Limited	Rs. 435/-
51	Diploma in Retail Banking	English	Retail Assets Product & Other Related Services	2017	M/s Macmillan India Limited	Rs. 360/-
52	Diploma in Retail Banking	English	Retail Liability Product & Other Related Services	2017	M/s Macmillan India Ltd.	Rs. 380/-
53	Diploma in Banking Technology	English	Design, Development & Implementation of Information System	2017	M/s Macmillan India Limited	Rs. 338/-
54	Diploma in Banking Technology	English	Security in Electronic Banking	2017	M/s Macmillan India Limited	Rs. 314/-
55	Business Facilitator / Correspondence	English	Inclusive Banking Thro' Business Correspondents	2018	M/s Taxmann Publications Pvt. Ltd	Rs. 275/-
56	Certificate Examination for Debt Recovery Agents	English	Hand Book on Debt Recovery	2017	M/s Taxmann Publication	Rs 325/-
57	Certificate Examinations for Employees of I.T. and BPO Companies	Hindi	Banking : Ek Parichay	2006	M/s Taxmann Publications Private Ltd.	Rs. 140/-
58	Certificate Examinations for Employees of I.T. and BPO Companies	English	Basics of Banking (Know Your Banking – I)	2015	M/s Taxmann Publications Private Ltd.	Rs. 140/-
59	Certificate Examinations for Employees of I.T. and BPO Companies	English	Credit Cards (Know Your Banking – II)	2013	M/s Taxmann Publications Private Ltd.	Rs. 140/-
60	Banking An Introduction	Hindi	Banking An Introduction	2016	M/s Taxmann Publication Ltd.	Rs. 235/-
61	Banking An Introduction	English	Banking An Introduction	2016	M/s Taxmann Publication Ltd.	Rs. 195/-