8

General Aspects of Risk Management

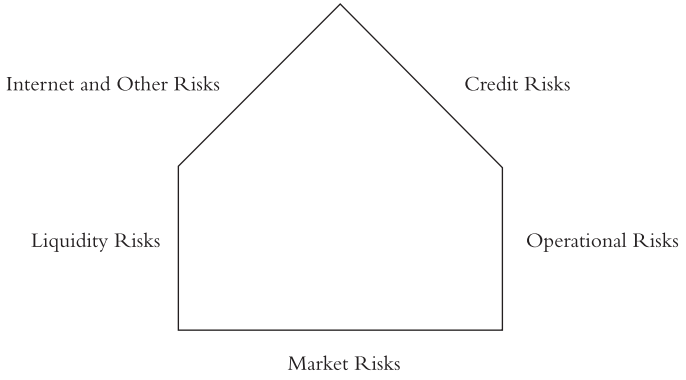
Risk is the probability or likelihood of injury, damage or loss in some specific environment and over some stated period of time. It involves two elements:

- Probability.
- Loss amount.

Risks arise on account of a number of factors. Figure 8.1 indicates very broadly the various factors that have to be taken into account while dealing with risk management. It indicates the factors that impinge on risk assessment and consequently on management; the task of risk management is highly complex and equally demanding. It also provides a brief representation of the most common risks encountered by any financial institution. The list is by no means complete. It is only indicative.

It would be pertinent to mention that a failure in one area could lead to other risks also. An increase in non-performing assets could bring in other risks also. Perhaps, the hexagonal representation gives a better idea about the interconnectivity of risks. For a more detailed review of risk assessment, techniques and their management refer to *Managing Indian Banks* (Joshi and Joshi 2009). Additionally, one has also to look at the risks undertaken by banks on the investments made. We have dealt with these aspects, including the Value at Risk Approach, in *Managing Indian Banks*. The treatment was somewhat elementary as we had noticed that even these introductory aspects were found to be somewhat difficult by a number of participants/readers at seminars who probably had not dealt with these areas.

Figure 8.1 Interrelations of Risks



At this stage it is, absolutely necessary to highlight a very important aspect which has now occupied centre stage and is currently being examined by various authorities, academicians and regulators. The broad range of policy changes could be discerned by a brief look at the recommendations made by Lord Turner (2009) in his review paper submitted to the Chancellor of the Exchequer. Some of these aspects have been discussed in the chapter on regulation. Suffice it to say that at this point in time these are mere suggestions and it would be quite some time before they are implemented globally.

- The quality and quantity of overall capital in the global banking system should be increased so that this results in minimum regulatory requirements, significantly above existing Basel rules.
- The transition to future rules should be carefully phased given the importance of maintaining bank lending in the current macroeconomic climate.
- Capital required against trading book activities should be increased significantly (for example, several times) and a fundamental review of the market risk capital regime (for example, reliance on VAR measures for regulatory purposes) should be launched.
- Regulators should take immediate action to ensure that the implementation of the current Basel II capital regime does not create unnecessary procyclicality. This can be achieved by using 'through the cycle' rather than 'point in time' measures of probabilities of default.

- A counter-cyclical capital adequacy regime should be introduced, with capital buffers, which increases in economic upswings and decreases in recessions.
- Published accounts should also include buffers, which anticipate potential future losses, through, for instance, the creation of an 'Economic Cycle Reserve'.
- A maximum gross leverage ratio should be introduced as a backstop discipline against excessive growth in absolute balance sheet size.
- Liquidity regulation and supervision should be recognized as of equal importance to capital regulation.
    - More intense and dedicated supervision of individual banks' liquidity positions should be introduced, including the use of stress tests defined by regulators and covering system-wide risks.
    - Introduction of a 'core funding ratio' to ensure sustainable funding of balance sheet growth should be considered.

Institutional and Geographic Coverage of Regulation

- Regulatory and supervisory coverage should follow the principle of economic substance not legal form.
- Authorities should have the power to gather information on all significant unregulated financial institutions (for example, hedge funds) to allow assessment of overall system-wide risks. Regulators should have the power to extend prudential regulation of capital and liquidity or impose other restrictions if any institution or group of institutions develops bank-like features that threaten financial stability and/or, otherwise, become systemically significant.
- Offshore financial centres should be covered by global agreements on regulatory standards.

It is absolutely clear that the whole gamut of financial institutions' working is under critical evaluation. However the limited aspects pertaining to internet security are a matter of concern and in this chapter the discussion would merely touch on the broader questions. Basically, the questions pertain to the assumptions on which the predictive models were based and their limitations. There was a time when these models were recommended for adoption by various regulators, including the RBI and what we are now witnessing is a retreat from the so-called 'market would

take care' approach. It is true that some of the fault lies with the way these models were used to derive conclusions. It would not be wrong to say that lust for profits and bonuses (a part of remuneration policy) did lead to a gross misuse of these techniques for prediction. It needs to emphasized that the conclusions have to be tempered with experience (grey hair has a unique place in financial institutions) and reviews at appropriate levels.

However, part of the blame lies with the regulators. Institutions like the IMF and the World Bank put too much faith in the market mechanism and encouraged similar fundamentalist policies for adoption which, but for such dogmatic beliefs, could not have been easily adopted.

This chapter focusses on nature of additional risks faced by banks/financial institutions when they are using online channels. The banks, brokers or financial institutions need to take note of all the aspects mentioned earlier and in addition to that deal with risks specific to the relevant aspects of an electronic environment, which would include transaction speed, geographic reach and user anonymity. One of the major problems is to integrate the newer techniques with legacy systems. It is necessary to emphasize that risk management is an ongoing process of identifying, measuring, monitoring and managing all significant operational, legal and reputation risks.

It has been noticed that many institutions are somewhat indifferent to the aspects of internet risk management and look on these aspects as part apart. These are not yet an integral part of activities. Therefore, we need to start the discussion from the basic requirements of any such programme. A good starting point is to look at the measures suggested by the Federal Deposit Insurance Corporation (FDIC) in USA.

Following the FDIC guidelines, these areas can be divided into the following broad areas:

- General areas: Planning, policies and procedures. Distribution of duties, accountability and delegation of authorities, regulatory compliance and audits, and so on.
- Transaction processing: User authentication, information integrity, and non-repudiation of transactions and data confidentiality.
- Systems administration: Resource requirements, system security, contingency planning, outsourcing policies, and so on.

The results of this process need to be integrated into the following:

- Strategic planning and feasibility analysis.
- Management supervision and control.
- Operating policies and procedures.

- System audit, administration and testing.
- Physical and transaction system security.
- Incident response and preparedness plans.

These techniques are also applicable to traditional risk management methods. Risks peculiar to the electronic systems must now be considered because these areas are the ones, which would be areas of concern for the regulators. Financial institutions would henceforth be evaluated, not only in terms of their 'Risk Management Systems', but probably on a much wider scale as highlighted by Turner (2009). It is, no doubt, in the institution's own interest to have systems which would safeguard its own and the interests of its customers.

Electronic System Risks

Conceptually, these risks can be broadly classified into two broad groups. There are risks, which can lead to disabling the system from functioning properly. The other group includes risks relating to data tampering and misuse. In the first category hacking can be included, which is done either to show off one's technical abilities (ethical hackers in the age group of 15–18) or with malicious intent (carried out by 'black' hackers).

The other area pertains to fraudulent data misuse in order to have access to sensitive information for some personal gain. It is worth noting that in 70 per cent of the cases it is the staff, which is found to have been responsible for the mischief. Chapter 11 deals with network security in greater detail. Authors like Ankit Fadia or Yogesh Barua and Prateek Dayal have explored these areas thoroughly and both the technical and non-technical readers would find these of great use (see Barua 2005, Dayal 2008, Fadia 2009). It must be pointed out, however, that there are bound to be technological advances and today's methods could be quite outmoded tomorrow. Thieves try to be two jumps ahead of the authorities.

A review of data protection techniques is discussed in the next section. The material has been largely drawn from FDIC circulars and those issued by other regulatory bodies.

Preventive Measures

Preventive measures include sound security policies, well-designed system architecture and properly configured firewalls. Additionally, two more

measures viz. assessment tools and penetration analysis are also discussed. Some of these aspects have been discussed in the chapter on regulation as well. At this point in time these are mere suggestions but they may be implemented at a later date.

Vulnerability assessment tools generally involve running scans on a system to proactively find out vulnerabilities, flaws and bugs in software and hardware. These tools can also detect the loopholes that allow unauthorized access to a network or insiders to misuse the system. Penetration analysis involves an independent party (internal or external) testing an institution's information system security to identify (and possibly exploit) vulnerabilities in the system and surrounding processes. Using vulnerability assessment and performing regular penetration analyses will assist an institution in determining what security weaknesses exist in its information systems. Detection measures involve analyzing available information to determine if an information system has been compromised, misused or accessed by unauthorized individuals. Detection measures may be enhanced by the use of intrusion detection systems (IDSs) that act as a burglar alarm, alerting the banker, service provider to potential external break-ins or internal misuse of the system(s) being monitored. Another key area involves preparing a response programme to handle suspected intrusions and system misuse once they are detected. Institutions should have an effective incident response programme outline in a security policy that prioritizes incidents, discusses appropriate responses to incidents and establishes reporting requirements. Before implementing some or all of these measures, an institution should perform an information security risk assessment. Depending on the risk assessment, certain risk assessment tools and practices discussed in this section may be appropriate. However, use of these measures should not result in decreased emphasis on information security or the need for human expertize.

Risk Assessment/Management

A thorough and proactive risk assessment is the first step in establishing a sound security programme. This is the ongoing process of evaluating threats and vulnerabilities, and establishing an appropriate risk management programme to mitigate potential monetary losses and harm to an institution's reputation. Threats have the potential to harm an institution, while vulnerabilities are weaknesses that can be exploited. The extent of the information security programme should be commensurate with the degree of risk associated with the institution's systems, networks and information

assets. For example, compared to an information-only website, institutions offering transactional internet-banking activities are exposed to greater risks. Further, real-time funds transfers generally pose greater risks than delayed or batch-processed transactions because the items are processed immediately. The extent to which an institution contracts with third-party vendors will also affect the nature of the risk assessment programme.

Performing the Risk Assessment and Determining Vulnerabilities

Performing a sound risk assessment is critical to establishing an effective information security programme. The risk assessment provides a framework for establishing policy guidelines and identifying the risk assessment tools and practices that may be appropriate for an institution. Institutions still should have a written information security policy, sound security policy guidelines and well-designed system architecture, as well as provide for physical security, employee education and testing, as part of an effective programme. When institutions contract with third-party providers for information system services, they should have a sound oversight programme. At a minimum, the security-related clauses of a written contract should define the responsibilities of both parties with respect to data confidentiality, system security and notification procedures in the event of data or system compromise. The institution needs to conduct a sufficient analysis of the provider's security programme, including how the provider uses available risk assessment tools and practices. Institutions also should obtain copies of independent penetration tests run against the provider's system.

When assessing information security products, management should be aware that many products offer a combination of risk assessment features, and can cover single or multiple operating systems. Several organizations provide independent assessments and certifications of the adequacy of computer security products (for example, firewalls). While the underlying product may be certified, banks should realize that the manner, in which the products are configured and ultimately used, is an integral part of the products' effectiveness. In relying on the certification, banks should understand the certification process used by the organization certifying the security product. Other examples of items to consider in the risk assessment process include identifying mission-critical information systems and determining the effectiveness of current information security programmes. For example, a vulnerability might involve critical systems that are not

reasonably isolated from the internet and external access via a modem. Having up-to-date inventory listings of hardware and software, as well as system topologies, is important in this process. Assessing the importance and sensitivity of information, and the likelihood of outside break-ins (for example, by hackers) and insider misuse of information, is equally important. For example, if a large depositor list is made public, that disclosure can expose the bank to reputation risk and the potential loss of deposits. Further, the institution can be harmed if human resource data (like salaries and personnel files) are made public. The assessment should identify systems that allow the transfer of funds, other assets or sensitive data/confidential information, and review the appropriateness of access controls and other security policy settings. Assessing the risks posed by electronic connections with business partners has to be an integral part of such an exercise. The other entity may have poor access controls that could potentially lead to an indirect compromise of the bank's system. Another example involves vendors that may be allowed to access the bank's system without proper security safeguards, such as firewalls. This could result in open access to critical information that the vendor may have 'no need to know'. Determining legal implications and contingent liability concerns associated with any of the aforementioned scenarios is also necessary. For example, if hackers successfully access a bank's system and use it to subsequently attack others, the bank may be liable for damages incurred by the party that is attacked.

Potential Threats to Consider

Serious hackers, interested computer novices, dishonest vendors or competitors, disgruntled current or former employees, organized criminals, or even agents of espionage pose a potential threat to an institution's computer security. The internet provides a wealth of information to banks and hackers alike on known security flaws in hardware and software. Using almost any search engine, average internet users can quickly find information describing how to break into various systems by exploiting known security flaws and software bugs. Hackers also may breach security by misusing vulnerability assessment tools to probe network systems, then exploiting any identified weaknesses to gain unauthorized access to a system. Internal misuse of information systems remains an ever-present security threat. Many break-ins or insider misuses of information occur due to poor security programmes. Hackers often exploit well-known weaknesses and security defects in operating systems that have not been appropriately addressed by

the institution. Inadequate maintenance and improper system design may also allow hackers to exploit a security system. New security risks arise from evolving attack methods or newly detected holes and bugs in existing software and hardware. Also, new risks may be introduced as systems are altered or upgraded, or through the improper set-up of available security-related tools. An institution needs to stay abreast of new security threats and vulnerabilities. It is equally important to keep abreast of the latest security patches and version upgrades that are available to fix security flaws and bugs. Information security and relevant vendor websites contain much of this information. Systems can be vulnerable to a variety of threats, including the misuse or theft of passwords. Hackers may use password-cracking programmes to decode poorly selected passwords. The passwords may then be used to access other parts of the system. By monitoring network traffic, unauthorized users can easily steal unencrypted passwords. The theft of passwords is more difficult if they are encrypted. Employees or hackers may also attempt to compromise system administrator access (root access), tamper with critical files, read confidential email or initiate unauthorized emails or transactions. Hackers may also use 'social engineering', a scheme using social technique to obtain technical information required to access a system. A hacker may claim to be someone authorized to access the system, such as an employee or a certain vendor or contractor. The hacker may then attempt to get a real employee to reveal user names or passwords, or even create new computer accounts. Another threat involves the practice of 'wardialing', in which hackers use a programme that automatically dials telephone numbers and searches for modem lines that bypass network firewalls and other security measures. A few other common forms of system attack include denial of service (system failure), which is any action preventing a system from operating as intended. It may be the unauthorized destruction, modification or delay of service. For example, in a 'SYN Flood' attack, a system can be flooded with requests to establish a connection, leaving the system with more open connections than it can support. Thus, legitimate users of the system being attacked are not allowed to connect until the open connections are closed or can time out. Internet Protocol (IP) spoofing allows an intruder via the internet to effectively impersonate a local system's IP address in an attempt to gain access to that system. If other local systems perform session authentication based on a connection's IP address, those systems may misinterpret incoming connections from the intruder as originating from a local trusted host and not require a password.

Trojan horses are programmes that contain additional (hidden) functions that usually allow malicious or unintended activities. A Trojan horse

programme generally performs unintended functions that may include replacing programmes, or collecting, falsifying and destroying data. Trojan horses can be attached to emails and may create a 'back door' that allows unrestricted access to a system. The programmes may automatically exclude logging and other information that would allow the intruder to be traced. Viruses are computer programmes that may be embedded in other code and can be self-replicated. Once active, they may take unwanted and unexpected actions that can result in either nondestructive or destructive outcomes in the host computer programmes. The virus programme may also move into multiple platforms, data files or devices on a system and spread through multiple systems in a network. Virus programmes may be contained in an email attachment and become active when the attachment is opened.

BIS had drawn out a set of 14 principles for a proper development of a mechanism for risk management. It is necessary to say that prescribing principles should not turn out to be counter productive. Each bank's risk profile is different and requires a tailored approach for risk mitigating efforts appropriate for the scale of e-banking operations, the materiality of risks present and the institute's willingness and ability to manage the risks. This does imply that 'one-size fits all' approach to e-banking risk management may not be appropriate. It would be useful to bring out the guidelines brought out by BIS and also by FDIC for the use of bank examiners.

A combination of prescriptive measures suggested by the BIS and examination techniques proposed by FDIC are a good starting point. There is considerable unanimity about the proposals made and one is on a safe wicket in adopting them.

The existing risk-management principles must be tailored, adapted and in some cases extended to address specific risk management challenges created by the peculiar characteristics of e-banking activities. The RBI can extend the policies enunciated in 1998 (RBI Circulars dealing with Asset/Liability Management and Risk Management: *(a)* DBOD no. BP.BC.94/21.04.098/98 and *(b)* DBOD no. BPsc.BC.98/21.04.103/99) and make it mandatory for banks broadly to adopt the suggestions made by BIS in its report on 'Risk Management Principles for Electronic Banking' in consultation with RBI. BIS is quite right in asserting that setting detailed risk management requirements must not be counter productive. Each bank's risk profile is different and requires a tailored approach for risk mitigation appropriate for the scale of e-banking operations, the materiality of risks present and the institute's willingness and ability to manage the risks. This does imply that one-size fits all approach to e-banking risk management may not be quite suited.

Broadly, the risk management efforts fall into three groups.

Management Oversight

Effective management oversight of the risks associated with e-banking needs to be in place and risk management should be integrated with overall risk management. There must be an explicit, informed and documented strategic decision, covering specific accountabilities, policies and controls, to address risks. Key aspects of security control process must be covered.

Due Diligence

This includes comprehensive due diligence and management oversight processes for outsourcing relations and third party dependencies.

Security Controls

This includes:

- Authentication of e-banking customers.
- Non-repudiation and accountability for e-banking transactions.
- Appropriate measures for segregation of duties.
- Data integrity of e-banking transactions, records and information.
- Establishment of clear audit trails for e-banking transactions.
- Confidentiality of key banking transactions.
- Legal and reputational risk management principles.
- Appropriate disclosures for e-banking services.
- Privacy of customer information.
- Capacity and business continuity.
- Contingency planning to ensure availability of e-banking services.
- Indent response planning.

Against the backdrop of preceding information, the Basel Committee on Risks for Electronic Banking has developed the following 14 key risk management principles:

- Management of outsourcing and third party dependencies.
- Segregation of duties.

- Proper authorization measures and controls.
- Clear audit trails.
- Authentication of all entities, counterparts and data.
- Non-repudiation of e-banking transactions.
- Comprehensive security.
- Integrity of banking transactions, records and information.
- Appropriate disclosure for e-banking services.
- Confidentiality and privacy of customer information.
- Business continuity and contingency planning.
- Incident response planning.
- Role of supervisors.

These suggestions need to be supplemented with a report prepared by FDIC for bank examiners. The summarized version is in two parts. The standards represent performance objectives to ensure that bank operates in a safe and sound manner and that the bank's objectives are carried out. Associated risks represent potential threats because of failure to adhere to such standards.

There are problems associated with other e-finance activities like broking, alternate systems of trading, foreign exchange transactions, and so on. These would be taken up in the chapter on regulation.

It is important for financial institutions to develop and implement appropriate information security programmes. Whether systems are maintained in-house or by third-part vendors, appropriate security controls and risk management techniques must be employed. A security programme includes effective security policies and system architecture, which may be supported by the risk assessment tools and practices discussed earlier. Information security threats and vulnerabilities, as well as their countermeasures, will continue to evolve. As such institutions should have a proactive risk assessment process that identifies emerging threats and vulnerabilities to information systems.

A sound information security policy identifies prevention, detection and response measures. Preventive measures may include regularly using vulnerability assessment tools and conducting periodic penetration analyses. Intrusion detection tools can be effective in detecting potential intrusions or system misuse. Institutions should also develop a response programme to effectively handle any information security breaches that may occur.

It would be important to indicate here the part played by technology in the risk management process and the way to select the appropriate system. While selecting the appropriate system it would be useful to:

- Establish clear goals for the risk management system.
- Identify each operation's needs.
- Survey available technology.
- Never trust a demo model.
- Take everything with a pinch of salt.

It would at this stage be useful to highlight the relationship between key business risks and activities undertaken.

- Poor loan quality credit risk.
- High funding costs interest risk.
- Asset/liability management, yield curve/cash-flow risks.
- Poor controls operational risks.
- Frauds legal/reputational risks.

The term technology refers to two distinct aspects: *(a)* The physical components of technology that are required for a risk management system and *(b)* the software that drives the application. It needs to be mentioned here that after the crisis, serious doubts are raised about the software used and the work done by the rating agencies. It would not be wrong to say that a number of accepted arrangements for risk assessment and management are in the melting pot and it would require a strong regulator and the strong finance ministry to undertake the kind of changes, which are required to be taken on an urgent basis.

Outsourcing

Very often organizations outsource e-banking systems and services. Obviously great care has to be exercised in dealing with such system. A brief outline of the practices to be adopted for risk management when such systems are outsourced is given in the next section. This aspect has been dealt with in some detail in the chapter on Network Security. These would have to be borne in mind while dealing with risk management systems.

Risks beyond the Organizational Control

The management of risks at the organizational level has been discussed so far in a somewhat abstract way. But there are areas where the organization may suffer losses on account of factors beyond its control. Following is

a case where services required were not available when they were most needed.

Hurricane Ivan illustrated a need for new forms of internet business risk management when it damaged an undersea cable and disconnected the Cayman Islands. The disconnection lasted more than two days and is an example of a risk beyond the control of the enterprise or the telecommunications carrier: a force *majeure* risk, or act of God. No amount of firewalls, intrusion detection or patches would have prevented it. Another undersea cable running to the Cayman Islands might have minimized the downtime, but at some point, the expense becomes greater than the risk or at least greater than the cost of insurance for the risk.

On the internet, physical risks such as hurricanes, floods and earthquakes are not the only force *majeure* risks, and not the most economically significant ones. Hurricanes are constrained in geographical scope. Worms, denial-of-service attacks and terrorism are not so constrained, and could cause even more aggregate damage than a hurricane. Put another way, offshore content caching may help prevent an outrage due to a hurricane, but will not necessarily avoid a worm.

To conclude it can be said that organizations must be proactive, read the signs on the wall and start initiating steps which the current crisis demands. Only then would it be possible to restore the confidence.