9

Risk Management for E-banking and E-insurance

Chapter 8 discussed and examined some of the general tools for assessment and management of risks on the internet. This chapter specifically considers insurance and banking industries' attempts at controlling and managing these risks. In particular, two features will be highlighted. These industry groups are usually reluctant to disclose any intrusions into their systems. This stems from fears about further attacks and about adverse publicity, which could lead to panic reactions amongst clients.

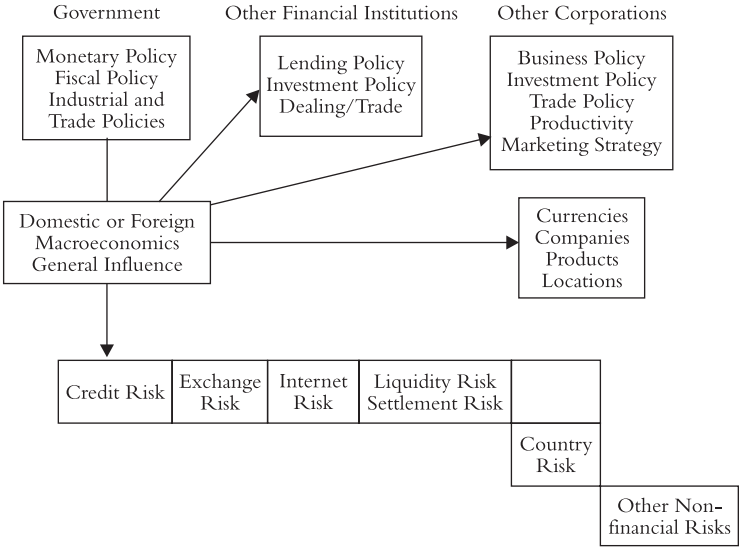
The South-East Asian crisis and the Barings Bank debacle were perhaps the immediate causes for banks and the supervisors to work together to evolve sound policies for this vital area of management for the financial services industry. It is indeed heartening that the problem is being analysed globally and that most countries are not only examining these issues, but are also concerned with developing appropriate strategies suited to their conditions. A particularly encouraging feature is that whenever there are differences of views amongst central regulators, they are aired and even made available on their websites for comments. Further, the organizations, which have framed these rules, do not claim that these are 'model' rules and that they need to be copied *in toto*.

Figure 9.1 describes the various forces that have to be taken into consideration.

BIS Recommendations

A summary of recommendations made by Bank for International Settlement (BIS) has been discussed in the following paragraphs. These are part of

Figure 9.1 Analysis of Risk



Source: Prepared by the author.

the total set of recommendations for risk management and need to be viewed in that context. A bank or financial institute developing the e-trade channel must be equally careful about the total apparatus it has for the risk management function. E-banking must be a part of that scheme. Further, organizations like the Federal Deposit Insurance Corporation in the US also provide specific guidelines which organizations could take advantage of.

The recommendations are summarized in the next section. BIS is quite right in asserting that fulfilling detailed risk management requirements must not be counter productive. Each bank's risk profile is different and a tailored approach is required 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 suitable.

As explained in Chapter 8, the risk management efforts broadly fall into three groups:

1. Management Oversight.
2. Due Diligence.
3. Security Controls.

Against the backdrop of the preceding information, the Basel Committee on Risks for Electronic Banking has developed 14 key risk management principles, as elaborated in Chapter 8.

The Insurance Sector

Some of the principles enunciated by the International Association of Insurance Supervisors are discussed in this section. Companies must be more conscious of strategic risks associated with an internet strategy. These risks are critical and would be more so when new products designed for sale on the Internet reach the market. The new underwriting opportunities that would become available must be kept in mind. A critical aspect to be examined relates to the risks posed by e-commerce that are new or different in scale or impact from traditional business conducted through other distribution channels. Reputations are at stake as mistakes can multiply and spread quickly.

Strategic Risks

These risks arise when a company engaging in new business strategy, does not analyse the implications that decision on electronic commerce will have on other parts of the organization or the company as a whole. Without such a plan, the risk of mistakes occurring increases and the chances of the strategy succeeding decrease.

The impact on the solvency should be the overreaching consideration in the analysis. In addition the company should be wary of the following factors:

- The global nature and rapid development and growth of e-commerce will put pressure on its planning and implementation of online operations, in particular, product design and technological applications.
- The Internet is an efficient way of doing business, but it is far from being cost free. System costs and maintaining customer awareness of the website may involve significant advertising costs.
- Brand loyalty may evaporate in the face of competition. Customers could switch their business from one to the other company.

- There is a danger of some customers being neglected. There is an equal danger that research, product innovation, data security and even risk management may be neglected.
- The speed of processing may complicate management of information.
- The dangers of adverse selection could increase and there could be inadequate disclosure by the customers.
- It is the responsibility of the Board to choose strategies that reflect the company's desired risk profile, functional capabilities and solvency. It must decide how its internet strategy will influence the company's philosophy, the way it conducts business and its financial situation.

Without a well thought out strategy, the decision to engage in e-commerce may result in an unwarranted increase in risks at the operational level and an unproductive drain on resources.

Operational Risks

These relate to risks that arise as a result of a failure or default in the IT infrastructure. There could even be deficiencies in the structure available. It may not

- have the capacity to handle increased traffic, process transaction and volume;
- be scalable;
- be accessible all the time due to a lack of fault tolerant technology;
- be secure from internal and external disruption;
- be accessible, compatible or interoperable in every market;
- have appropriate policies and controls in place for third-party vendors; and have adequate scrutiny of the service provider's operational viability, financial liquidity and project management skills.

Transaction Risks

Transaction risks arise on account of an unauthorized alteration or modification to texts, information or data transmitted over the computer network between an insurer and the client or vice versa. In e-commerce these risks

arise mainly on account of technology. This risk also includes information, which is hosted on the server or website of a 'partner' third party.

Data Security Risks

These risks arise due to losses, unintentional changes or leaks of information or data in computer systems. These could be broadly divided into two categories. Incompatibility of the data systems or part of the data system information leaks or information loss may be the cause for such risks. The external links could lead to data breaks. A customer's personal data may be illegally accessed. These could complicate and in some cases, negate the company's ability to authenticate information and data. Information concerning an insurance contract may be changed without authorization after the system has been broken into. Thus, a company's reputation may suffer.

Connectivity Risks

Failure in one part of the system may impact all or other parts of the system. If any part of the internet's operational system is damaged as a result of intentional or negligent actions, the company may fail to provide service to clients.

Conduct of Business Risks

The laws and regulations are developed with the view that business will be conducted on a person to person basis, with proper documentation. E-commerce poses new issues with attendant risks, such as:

- Authenticating the identity of a customer.
- Verifying and maintaining the security of electronic documents and signatures.
- Notification of contract-related information to safeguard the interests of the client and the company.
- Format and presentations wherein disclosure and disclaimer requirements are met.
- Providing policyholders with a proof acceptable to regulators or other third parties.

- Acceptance of electronic payments in lieu of cheques, drafts or cash.
- Meeting record retention requirements.

Supervisors apprehend that a host of legal issues, including the status of the insurer, the applicable laws, location of the company and, therefore, by whom and how it would be supervised, would sooner or later arise. They are also afraid that the clients may not be aware of all the risks involved and when and if a problem arises it may be too late even for a proper remedy to be found.

Alternate Systems of Trading

The Securities and Exchange Board of India (SEBI) has specifically indicated the use of appropriate technology for risk management. Following is a summary of their major conclusions:

- Exchanges must ensure that brokers have a system-based control on the trading limits of clients, and their exposures. There must be predefined limits on the exposure and turnover of each client.
- The systems should be such that client risks could be immediately assessed and that the client would be informed within a reasonable time frame.
- The reports on margin requirements, payment and delivery, should be made known to the client through the system.
- Contract notes must be issued within 24 hours or as per existing rules.
- No cross trades should be undertaken.
- The other rules applicable to brokers should, no doubt, continue to operate.
- Documents should be authenticated through digital signature, electronic certification, and so on.

The following security measures are mandatory for all internet-based trading systems:

- User ID, first-level passwords, automatic expiry of passwords and reinitializing access on entering fresh passwords.
- All transaction logs with proper audit trails and facilities to be maintained.

- Suitable firewalls between trading set-up connected to the exchange system and the internet trading system.
- Secured socket-level security for server access through internet.

The SEBI has gone a step further and recommended the following: *(a)* microprocessor-based smart cards; *(b)* dynamic password; *(c)* 64bit/128 bit encryption and finally *(d)* second-level password.

Standards for interface between the brokers and clients have also been prescribed. The rules also give detailed instructions to brokers to use the same logic or priorities used by exchanges to treat client orders. Brokers are also to maintain all activities/alerts log with audit trail facility. A unique numbering system, which is internally generated, is also mandatory. There is a considerable overlap of the risk management suggestions of various sectors. Many suggestions by insurance regulators would, therefore, be equally applicable to banking/broking.

Conclusion

Many of the requirements can be taken care of by technology. The book refrains from going into these in great details as management would have to take these decisions themselves depending on their specific requirements. Further, the developments are so fast that the suggestions could be outmoded before they are made. While some of the aspects on security are covered in Chapter 8, the details on computer crimes in the next chapter drive home the message for greater attention to risk management.