RESULTANT INFORMATION TECHNOLOGY RISK FROM A PARADIGM SHIFT IN THE BANKING INDUSTRY

Niroshana Seneviratne *FCA, FIB, CISA, MSc(Management)*

1. Information Technology (IT) – the Driving Force

The paradigm shift in the banking sector is undoubtedly capitalizing on the development in the information technology. The right technology in place for a bank not only helps its operations to be up and running, but also improves its services to customers, its profitability for shareholders and its support for the community.

Increased responsiveness to customers is becoming even more important as the financial service providers respond to the pressures of globalization, as well as regulatory and compliance requirements. Financial institutions must satisfy requests for information from their customers, as well as from regulators. International banks are using technology to serve their customers effectively over longer distances, and we are still only at the beginning of the revolution in technology.

2. Back to Centralization

It is interesting to note the circular movement in the banking operations in Sri Lanka. Each bank in the industry started its banking operations with a single office located in Colombo catering to an affluent client base with a centralized process. With the development of the industry, the need to reach out to other areas led the banks to open-up branches in other cities, yet continuing with a centralized operation with most of the decisions being taken at Head offices located in Colombo.

Pressure for quick decision making at the branches, to cater to their clients better, compelled the banks to decentralize the decision making through regional offices and finally to the branch directly. Authority limits for approval had been delegated to branches offices, and the branch managers were made accountable for their actions. Decentralized decision making had been looked upon as one of the best practices to facilitate and make the customer service more effective. Almost all the banks embraced this practice until the late 80's, when the new technology revolutionized and reversed the practice back to centralization.

Today, the banks are increasingly, but with much struggle, attempting to centralize their decision making process through implementing core banking information systems. Opening accounts, keeping custody of mandates, processing cheque books, effecting standing orders etc which processes have been originally centralized, traditionally decentralized, are now increasingly being centralized.

The recent move from decentralization to centralization has posed many a risk that otherwise would have been less. For instance, the base deposit interest rate would be maintained in a central file with respective variance percentages, where, inadvertent mistake in modifying this rate would have a global impact on the deposit interest rates in the whole bank as it is now centrally maintained and updated. Similarly, security compromises on the central database would lead to significant damages to the operation and the very existence of the business.

3. Use of IT, has it really helped ?

The revolution in the Information Technology industry has tremendously influenced and continue to influence, the direction of the banking industry. A successful implementation of an effective information system should drastically reduce the transaction cost for a bank, which in my view, we are yet to experience.

Theoretically, "anytime one can eliminate a piece of paper, the transaction should get cheaper."

In my view, it is an exercise worthy of investigation whether use of IT has really helped banks to minimize cost, for the benefit of individual banks, the industry and the economy as a whole.

Having embraced information technology, how successful have we been in eliminating "paper" from our processes to enhance efficiency and reduce transaction cost. For instance, have we managed to use Information Technology to eliminate, the traditional internal memo system, staff and operational circulars, credit and other approval processes that essentially depended heavily on paper which invariably delay the customer service and lead to cost .

Additionally, the banks are now burdened with significant capital cost in acquiring and maintaining information systems that escalate cost leading to negative impact on the profitability. Abuse of internet facilities, and e-mails facilities that get loaded with junk mail would probably result in a drop in efficiency.

Moreover, heavy dependent on Information Technology has forced the bankers to number of risks that we have little knowledge of. It is in this context the writer is trying to identify the risks that the bankers are exposed to when depending on Information Technology.

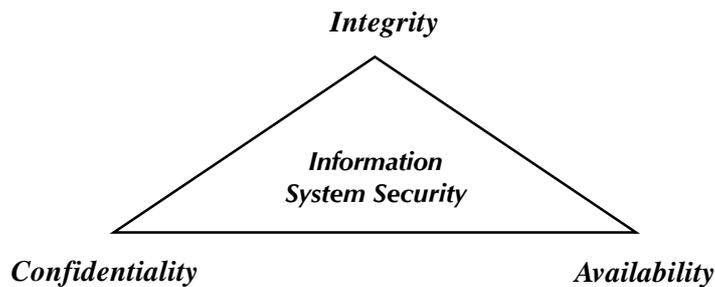## 4. Information System Security

Bank's sensitive information resides in equipments such as servers, client systems, storage devices or it could be in transit on telecommunication lines and devices. Information system (IS) technologies such as networking and databases enable greater reach and access to information by multiple users. However these technologies also present challenges like restricting access on selective basis to different categories of users, protection of information etc. Hence, the need to secure banks information, systems and other IS resources.

For instance, Internet banking poses number of threats to the bank with regard to access restrictions, protection of confidential customer information, providing 24/7 access to information etc.

Information and information systems are susceptible to plethora of threats and vulnerabilities, exploitation of which may result in partial or total loss, or compromise of information.

As per the ISO 17799 Standard on Information Security Management, information security refers to the preservation of **Confidentiality, Integrity** and **Availability of Information**. It is also referred to as the Pyramid of Information Security.

Confidentiality refers to the fact that the information should be accessible only by the authorized persons. Protection from unauthorized modifications to information is covered under **integrity**. **Availability** insists that the information should be available as and when required for authorized purposes.

Integrity

**Information
System Security**

Confidentiality   *Availability*

5. Loss from Information Security Breaches

The 2005 CSI/FBI Computer Crime and Security Survey results on 700 computer security practitioners indicate that organizations worldwide are burdened with security threats on their information systems. The report identified that $ 42.8 Mn has been lost through virus and related attacks whereas $ 62Mn has been lost resulting from unauthorized access and theft of information. The table below, highlights the financial losses incurred under each category.
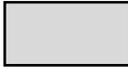
Financial Losses Due to System Security Threats in 2005	
Type of System Security Breach	Amount of Losses
Virus	$42,787,767
Unauthorized access to information	31,233,100
Theft of proprietary information	30,903,000
Denial of service	7,310,325
Insider abuse of Internet access	6,856,450
Laptop theft	4,107,300
Financial fraud	2,565,000
Misuse of public Web applications	2,227,500
System penetration	841,400
Abuse of wireless network	544,700
Sabotage	340,600
Telecom fraud	242,000
Website defacement	115,000

Source: 2006 CSI/FBI Computer Crime and Security Survey

6. Information System Threats

Threat to information systems could be broadly classified under,
- Human related
- Physical and Environmental related
- Logical Accesses related
- Technology related

6.1 Human Related Threats

International survey results suggest that most of the frauds that take place are through the exploitation of human related vulnerabilities. It seems to be the easiest to manipulate due to issues of integrity and discipline. Results also indicate that around 70% of such frauds have taken place with the involvement of the internal staff.

6.1.1 Impersonations
Impersonations are threats that often become stepping stones for other threats. Impersonation for physical access could include misuse of badges, key cards, Personal Identification Numbers (PIN), etc. Impersonation for electronic or system access could include use of another's identification and authentication.

In the context of our banking system, impersonation, popularly known as sharing of passwords, possesses the highest threat. Most of the recent frauds in our banking sector had been a direct result of compromise of passwords. The reason being, the simplicity in exploiting this vulnerability. Most of the bank employees have taken the use of User ID's and passwords for granted without understanding what it exposes them to.

There were instances of using common passwords, swipe cards with passwords being freely used among operational staff, usage of easily guessable passwords, leaving active workstation sessions unattended, usage of common impersonal User IDs and recording passwords in places that has access to others to name a few.

6.1.2 Data Entry Errors/Omissiions

Data entry errors and omissions are mistakes when keying in data or oversight of key data, which could affect system resources and the safeguards that are protecting other system resources. This include inadvertent acts and carelessness of staff that would result from lack of supervision.

Such errors and omissions could be eliminated to a reasonable extent by exercising dual control and segregation of duties with effective supervision.

6.1.3 Sabortage/Vandalism

Theft, sabotage, vandalism, or physical intrusions are deliberate malicious acts that could cause damage, destruction, or loss of system assets. Disgruntled employees could create both mischief and sabotage of system data. Deletion or corruption of data could occur through acts of vandalism.

6.1.4. Shoulder Surfing

Shoulder Surfing is the deliberate attempt to gain knowledge of protected information by observing. The unauthorized disclosure of protected information leads to information misuse (identity theft), or such information could be used to gain additional access or information.

Failure to protect a User ID and Password from observation by others during logon could allow unauthorized users to capture sensitive information.

6.1.5 Espionage

Espionage is the overt act of spying through copying, reproducing, recording, photographing, interception, etc., to obtain information.

Most of the human related threats could be managed through awareness, discipline and appropriate guidance with top management sponsorship.

6.2 Physical and Environmental Related Threats

6.2.1 Power Failure
Power Fluctuation is a disruption in the primary power source (power spike, surge, and blackout) that results in either insufficient or excessive power.

Use of uninterrupted power supplies with stabilizer could minimize the damage to information from power failures and drops.

6.2.2 Natural Disaster
Natural disasters, such as earthquakes, fire and floods could result in damage or destruction of system hardware or software assets. Any of these potential threats could lead to a partial or total outage.

An effective business continuity and disaster management plan with tested results could minimize the damage in such an event.

6.3 Logical Accesses

6.3.1 Viruses
A virus attack unlike most of other threats, are easy to carry out and posses threats to all three pillars: confidentiality, integrity and availability.

A computer virus is a software code that can multiply and propagate itself. A virus can spread into another computer via e-mail, downloading files from the Internet, or opening a contaminated file. It is almost impossible to completely protect a network computer from virus attacks; the CSI/FBI survey indicated that virus attacks were the most widespread attack for six straight years since 2000.
Viruses are just one of several programmed threats or malicious codes (malware) in today's interconnected system environment. Programmed threats are computer programmes that can create a nuisance, alter or damage data, steal information, or cripple system functions. Programmed threats include, computer viruses, Trojan horses, logic bombs, worms, spam, spyware, and adware.

- Introduction of network worms, such as Code Red worm, W32/Leaves worm, and power worm could damage the system and associated data.

- Trojan Horse applications could be inserted into authorized software. Some examples are Sub Seven Trojan, Barok, Kuang2, pSender Full, Sesame, and Deep Throat. This could result in system damage and data compromise.

- Virus code, such as W97M.Mailissa, MerryXMAS or Independence Day, could be inserted into authorized software resulting insystem damage and data compromise.

- Logic bombs again is a malicious software that activate on meeting certain conditions, such as date or time.

  Adopting an effective IT policy restricting the use of mobile devices such as diskettes, CDs and pen drives etc would minimize the damage, while an effective and updated virus guards could act as preventive mechanism.

6.3.2 Intrusion or Unauthorized Access
Gaining unauthorized access to system resources mostly refers to a third party without any authority trying to penetrate into the system that is popularly known as hacking. The intent could be malicious or non malicious.

Installation of intrusion detective systems that are capable of identifying the system access traffic with effective monitoring would probably minimize such shock. Firewall software also could be effectively used for the purpose.

6.4 Technology Related

6.4.1 Hardware /Equipment Failure
Equipment Failure is the unexpected loss or malfunctioning of operational hardware asset.

Effective preventive maintenance agreements with hardware vendors and backup equipments supported by a disaster recovery plan would enable the bank to minimize such risk.

6.4.2 Eavesdropping
Eavesdropping is the deliberate attempt to gain knowledge of protected information. TheUnauthorized disclosure of protected information leads to information misuse (identity theft), or such information could be used to gain additional access to information.

Eavesdropping devices, such as Electronic Bugs could capture system activities and keystroke recording software could transmit every keystroke so that all user input could be reproduced.

These devices are popularly used at ATMs by the fraudsters to create skimming cards.

6.4.3 Jamming
Jamming is the deliberate radiation, re radiation, or reflection of electromagnetic energy, which could cause communications, degrading communication, or total loss of the system.

It is an increasing trend to outsource most of the business processes and IT related activities that would expose the bank to unknown shocks that would impact confidentiality, integrity and availability of information due to security and control compromises at outsourced sites.

7. Remedial Action

The above is just a few threats and not an exhaustive list. Having said that, there is a bit of good news too for a sigh of relief for bankers.

7.1 Declining Trend

Firstly , the research statistics published by the same organization (CSI/FBI Computer Crime and Security Survey) for 2005 reveals that the losses from the security threats are drastically coming down internationally. May be, due to secure information systems with preventive action taken by the corporates or diversion of attention of the fraudsters or hackers due to corporate transparency.
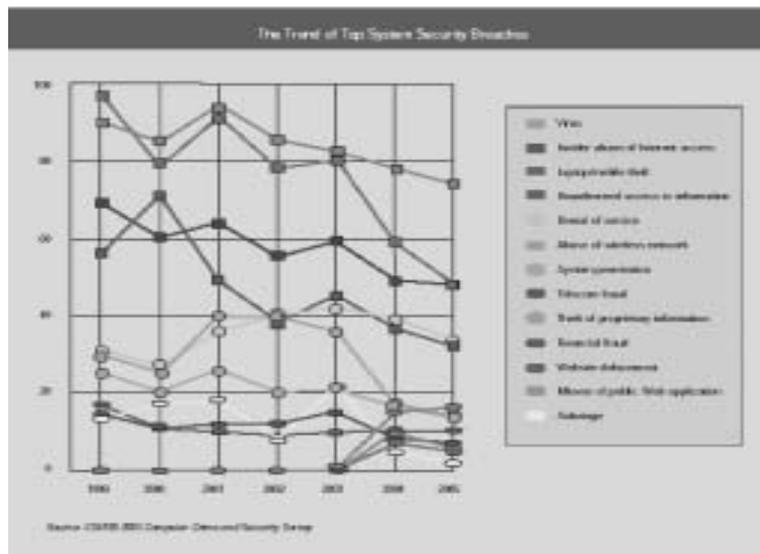

7.2 Internal controls

Secondly, those threats we have identified could be effectively managed to minimize the related exposure. There are Information system security professionals who are specialized to provide advice on how best we can manage such risk.

The latest research results published by Ernst & Young International (9th Global Fraud Survey, Ernst & Young 30th June 2006) suggest that in emerging markets most effective preventive mechanisms have been implementation of Internal Controls with a 75% confirmation and Internal Audit with 65% response. Internal education and management sponsorship also has effectively contributed in minimizing the threats to information systems.

Key to Fraud Prevention
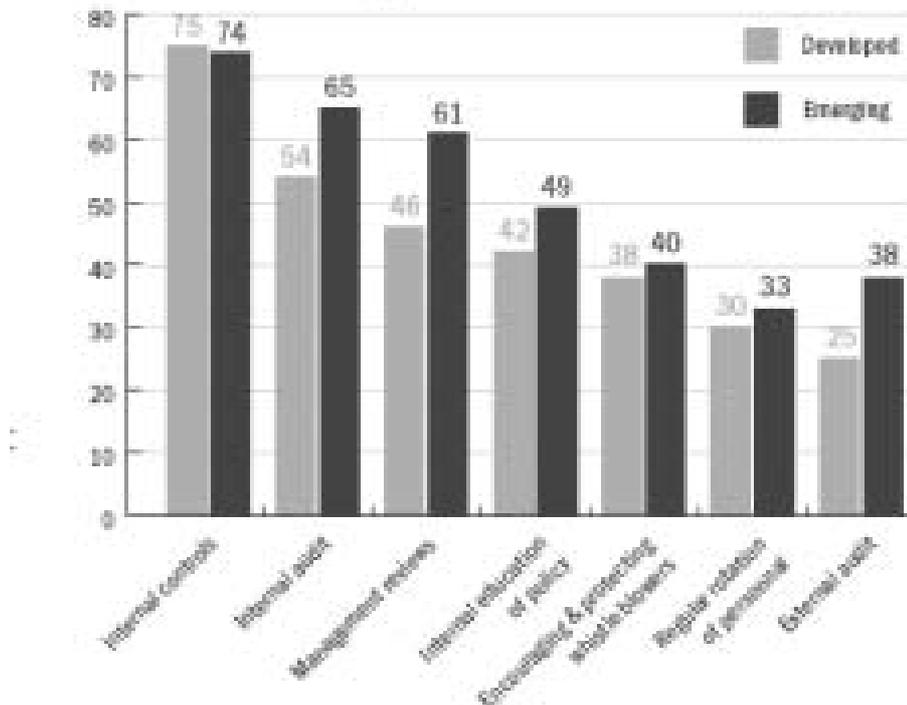
8. Conclusion

The paradigm shift in the banking industry has made it inevitable for banks to depend heavily on the development of the Information Technology. The rapid development in IT industry has itself posed the banks with a significant threat, to keep pace with, to prevent others from outsmarting the banks. The IT related exposure is tremendous and the bankers ought to prioritize their preventive actions and for this we are still not too late.

References,

1. The Certified Practising Accounts (CPA) Journal, July 2006,

2. 9th Global Fraud Survey, Ernst & Young 30th June 2006

3. http://www.nsscpa.org

BLANK