सुरक्षा र न्याय अध्ययन केन्द्र
CENTRE FOR SECURITY AND JUSTICE STUDIES

SEMINAR PAPER

BANKING INFORMATION SECURITY IN NEPAL

MAHESH SINGH KATHAYAT
DEPUTY INSPECTOR GENERAL OF POLICE
NEPAL POLICE

PROGRAM SUPPORTED BY THE ASIA FOUNDATION

Seminar on Banking Information Security: Challenges and Solutions'. This seminar was jointly hosted by Centre for Security and Justice Studies (CSJS) and National Banking Training Institute (NBTI) on May 9, 2014 at NBTI. This program was supported by The Asia Foundation, Nepal.

Banking Information Security: Challenges and Solutions

Er. M.S.Kathayat, ME, MBA
Senior Computer Engineer

Introduction

The banking industry has changed the way they provide services to their customers and process information in recent years. Information and Communication Technology (ICT) has brought about this historic transformation. Security of Information for a financial institution has therefore gained much importance, and it is vital for CEO/CIO to ensure that the risks are properly identified and managed. Moreover, ICT systems are essential assets for the banks as well as for their customers and stakeholders. Information assets are critical to the services provided by the banks and FIs to their customers. Protection and maintenance of these assets are critical to the organizations' existence, sustainability and growth. Banks must take the responsibility of protecting the information from unauthorized access, modification, disclosure and destruction. Bank has to develop a Guideline for ICT Security to be used as a minimum requirement and as appropriate to the level of computerization of their operations and management.

As we all know Information is at the heart of today's business, and the all-pervasive impact of information technology in harnessing, arranging and processing huge volumes of information is ultimate. In this scenario, the need for ensuring that information is kept confidential adhering to accepted norms of privacy and making it available to authorized users at the appropriate time assumes great significance. This is particularly valid for the banking sector where day-to-day operations are centered on information and information processing, which in turn is highly dependent on technology. Banking as a business involves the management of risks based on a repository of trust extended by the customers. If this objective has to be accomplished, it becomes essential for all security concerns especially customer sensitive data to be addressed in an effective way so as to ensure that the trust levels are well preserved and information assets perform the role that they are supposed to.

In addition, banking is hovering to be universal through facilities such as 'Anywhere and Anytime Banking', proliferation of services offered through ATM networks, IT enabled instant remittances across banks, customer payments, mobile payments and many more. The giant project of ICT-supported financial inclusion is all set to change the face of Nepalese banking by making banking services fully comprehensive. The last decade witnessed a seismic change in the way banking services are made available to customers. With the interlinking of ATMs, the customer has been further transformed into constituent of the financial sector rather than a bank.

Seminar on Banking Information Security: Challenges and Solutions'. This seminar was jointly hosted by Centre for Security and Justice Studies (CSJS) and National Banking Training Institute (NBTI) on May 9, 2014 at NBTI. This program was supported by The Asia Foundation, Nepal.

The time is now appropriate to review the adequacy of the measures taken by banks. As the banks and ICT industry came up with layers of protection for their systems, fraudsters, hackers and a bewildering variety of other such entities made big attempts at breaking the security layers.

Technically when the application layer was fortified, the attention was on to break the network layer. When the network equipment manufacturers hardwired the security protocol making it extremely difficult to break them, the attack switched over to the internet servers. Activities like phishing require customers and bankers to migrate to the higher levels of security. While these examples relate to Internet-based banking, the latest dimension relates to security for mobile banking.

It is to be recognized that information security has two important dimensions, namely:

- Protection of investment in information systems and to the actual information (data) thereon, and,
- Availability of information systems for use whenever and wherever required.

It is necessary to address basic concerns relating to safety and security of information and communication technology (ICT) assets, to data and to information pertaining to the bank as a whole and the customer in particular. Against this background, it would be appropriate to define a set of best practices which would enhance the value of ICT security in finical sectors.

Challenges:

1Human factor (employees and customers) must be consideredfor the ICTsystems security in the organization.

2. ICT security throughout the organization must in the top priority.

3. Clear ICT security policies and procedures for the organization must develop and implemented.

4. ICT Security related action must be executed at the appropriate time.

5. Adequate resource capability must be provided for ICT security.

6. Best possible business process re-engineeringmust be executed at the fixed interval of time frame.

7 Must audit obsolescence issues for ICT securityat the fixed interval of time.

Seminar on Banking Information Security: Challenges and Solutions'. This seminar was jointly hosted by Centre for Security and Justice Studies (CSJS) and National Banking Training Institute (NBTI) on May 9, 2014 at NBTI. This program was supported by The Asia Foundation, Nepal.

8. Must develop and provide a framework for ICT security incident management.

9. Must take care of data quality, integrity and security as part of business processing system.

Solutions:

CEO/CIO must take adequate care of the human factor in ICT implementation

IT security is more often than not a people related aspect than a technical issue. This is applicable to both insiders and customers of banks as well. There is a need to be vigilant against an insider who may know more than what is required and when aided with unregulated access, could wreak havoc on the bank concerned.

Equally important is a customer who exploits technology loop holes for malaises intentions. It is thus essential that IT Security parameters provide adequate focus on the set of people directly related to the systems in addition to the targeted audience as well. In this connection, communication in a language understood by these stakeholders assumes critical importance.

2. CEO/CIO mustensure access of ICT security throughout the organization

World over, it has been recognized and accepted that ICT security is optimal if the implementation is top driven. The indication for this is that the top management of banks need to provide a missionary keenness for implementing ICT security; their efforts would automatically ensure that the IT security related procedures are effectively implemented across all levels in the banks.

3. CEO/CIO must develop well defined ICT security policies and procedures for the organization.

One of the main characteristics of banking in Nepal relates to the existence of well documented policies and procedures pertaining to their areas of operation. The ICT security domain, however, cannot possess of a similar level of compliance. Well laid down processes and procedures not only enhance employee efficiency but also aid a great deal in ensuring that there is clarity of objective apart from acting as a genuine guide to the conduct of operations in a safe and secure manner. It is also crucial that these procedural requirements are fully disseminated to all sections of the staff for their steady compliance at all times.

4. CEO/CIO must take action about ICT security incidents at the appropriate time

Seminar on Banking Information Security: Challenges and Solutions'. This seminar was jointly hosted by Centre for Security and Justice Studies (CSJS) and National Banking Training Institute (NBTI) on May 9, 2014 at NBTI. This program was supported by The Asia Foundation, Nepal.

It is almost impossible to achieve complete IT security in any organization. Addressing IT security related concerns and breaches thus assume significance. The watch word here is timeliness; it is only those banks which take quick corrective action which can survive the attack of security breaches.

Such prompt action is possible only if the banks have already put in place well defined systems and procedures. The need to focus on attempted security violations also needs to be taken care of since these offer themselves as excellent early warning signals which, if left unattended or improperly attended, may result in substantial losses and a small lapse often becomes a mega event due to lack of right decision at the right time.

5. CEO/CIO must ensure that adequate resource capability is provided for the ICT security.

An effective IT security structure cannot be implemented in isolation. It is vital that all resources which facilitate the accomplishment of this objective are adequately provided for. These include adequate personnel, effective and efficient ICT systems, good vendor management policies, and sound ICT Audit mechanisms. Costs are certainly associated with these but the benefits accruing on account of reduced impact of ICT security breaches more than compensates for the costs incurred in this regard.

6. CEO/CIO must provide for optimal business process re-engineering at fixed interval of time.

Most ICT implementations in the Nepalese Banking scenario are replicas of the manual work processes which have been only tweaked to perform in an ICT-enabled environment. The result is the existence of unnecessary processes and loss of efficiency. Business process re-engineering leads to cost savings, better work flows, improved efficiency and better customer service levels as business process systems are cross-functional, i.e. the system boundary is not within a single function but actually goes across boundary lines.

7. CEO/CIO must take care of obsolescence issues for ICT security at the fixed time frame.

Perhaps the only industry in today's world where advancements are very rapid and every advancement brings in its wake reduced costs for adoption is the ICT industry.

Network based communication has reached rock-bottom levels as far as costs are concerned while the prices of ICT systems have exponentially reduced.

Seminar on Banking Information Security: Challenges and Solutions'. This seminar was jointly hosted by Centre for Security and Justice Studies (CSJS) and National Banking Training Institute (NBTI) on May 9, 2014 at NBTI. This program was supported by The Asia Foundation, Nepal.

The rapid degree of product and feature obsolescence in the ICT industry is a terrible challenge for banks. Such obsolescence needs to be tackled in a systematic and proactive manner for mutual benefit of the banks and their customers.

Care needs to be, taken in such a way that upgradation to take care of technology obsolescence is performed in a scientific manner and on a need-to-upgrade basis. This would help banks avoid falling into the technology-obsolescence trap requiring huge sums of money for to come out.

8. CEO/CIO must provide a framework for incident management of ICT security incidents.

Security related incidents cannot be wished away. The best tool towards an effective ICT security framework would thus be one which acknowledges such security instances and provides for a framework for appropriate incident reporting within the organization and to the regulators.

Such a mechanism would provide insights into the security violations and other such attempts, but the single largest beneficial factor would be the development of a set of knowledge workers who hold the key to success of any ICT based initiative by banks in a country which can boast of some of the best ICT companies runs by effective ICT Big houses.

9. CIO/CEO must take care of data quality, integrity and security as part of business processing system.

The most vital component of ICT security is the data which forms part of the ICT enables business processing system. Data is hard to get or create, easy for misuse and is tough to be channeled towards beneficial interpretation resulting in meaningful analysis.

To this end, banks need to work out effective standards aimed at high levels of data quality and integrity. At this juncture of a book called *Database Nation* written by S.Garfinkel which outlines the death of privacy in the twenty-first century. The author skillfully explained the various facets governing data piracy while concluding that the owner of one's own private information is not himself! Banks cannot afford to fall into this category and data refinement is one approach which would facilitate good data management with adequate levels of protective covers.

Conclusion

Seminar on Banking Information Security: Challenges and Solutions'. This seminar was jointly hosted by Centre for Security and Justice Studies (CSJS) and National Banking Training Institute (NBTI) on May 9, 2014 at NBTI. This program was supported by The Asia Foundation, Nepal.

We all should understand ICT security cannot be viewed in isolation; neither can it be implemented in fits and starts. Examples of good ICT security implementation reveal that good ICT security features are fulfilled as essential requirements in a normal way of life. As banks, we need to absorb the security culture in our normal day-to-day activities. This is a challenging and discouraging task since the normal human mind is more used to towards an easy, *laissez faire* approach towards reduced security so as to enhance convenience. ICT security does add on to inconvenience as it does towards increased costs, but it is economical in the long run. While there have been conscious efforts on the part of the regulator as well as regulated entities, we still feel there is considerable scope in working towards having a uniformly accepted standards and practices for operational risks especially information security risks across all financial institutions. It is in this context that we need totry to set out the standards for ICT security. That in the world of today where only the fittest have any chances of survival, our banks will not only survive but also grow in prosperity and mature as well, using the best of information and communication technology.

Seminar on Banking Information Security: Challenges and Solutions'. This seminar was jointly hosted by Centre for Security and Justice Studies (CSJS) and National Banking Training Institute (NBTI) on May 9, 2014 at NBTI. This program was supported by The Asia Foundation, Nepal.

Glossary and Acronyms

ICT Information Communication Technology

IT Information Technology

CEO Chief Executive Officer

CIO Chief Information Officer

AMT Automatic Teller Machine.

Seminar on Banking Information Security: Challenges and Solutions'. This seminar was jointly hosted by Centre for Security and Justice Studies (CSJS) and National Banking Training Institute (NBTI) on May 9, 2014 at NBTI. This program was supported by The Asia Foundation, Nepal.

References

1. Cronin, Mary J. (1997). Banking and Finance on the Internet, John Wiley and Sons.
2. Security Testing Handbook for Banking Applicationsby ArvindDoraiswamy), SangitaPakala , Nilesh Kapoor.
3. Accurate and realistic for banking applications By HonBlue on January 6, 2013
4. "The Home Banking Dilemma".
5. "Computer Giants Giving a Major Boost to Increased Use of Corporate Videotex". Communications News. 1984"Stanford Federal Credit Union Pioneers Online Financial Services." (Press release). 1995-06-21.
6. NSW Government Digital Information Security Policy,Version: 1.0, November 2012, Australia
7. Determining the Impact of Information and Communication Technology on Decent Work in Nepal,International Labour Organization, Regional Office for Asia & Pacific (ILO/ROAP), Bangkok Prepared by Nepal Foundation for Advanced Studies (NEFAS) Tekusi, Balkhu, Kathmandu, Nepal.March-2004
8. Guideline on ICT Security For Scheduled Banks and Financial Institutions,By Bangladesh Bank.
9. ICT for Greater Development Impact World Bank Group Strategy for Information and Communication Technology 2012-2015.