Security in Information Systems :

The identification of risks in selected electronic banking applications

A thesis presented in partial fulfilment
of the requirements for the degree of

Master of Business Studies in Information Systems

at

Massey University

Elizabeth A. Kemp

February, 1988

Acknowledgements

In presenting this thesis, I would like to take the opportunity to express my thanks to the following people for their help and support :

Firstly, my supervisor, Richard Hayward, for his guidance, criticism and encouragement throughout the course of the project.

Secondly, Professor Rae Weston for her invaluable suggestions and comments about security issues in banking.

Finally, I would like to thank my family, Raymond, Rebecca and Stephen, for all the support they have given me in so many ways during the completion of this thesis.

Abstract

This thesis considers the security threats associated with the introduction of electronic banking. In electronic banking services the paper based instructions for the movement of money are replaced by the electronic transmission of data. Since electronic banking relies heavily on advanced information technology (the use of computers and communications), security is a matter of grave concern. This thesis identifies the principle risks to security in five electronic applications : Automated Teller Machines (ATMs), Electronic Funds Transfer, Point-of-Sale (EFTPOS), credit cards, home banking and wire transfers. Both the information technology used and the applications are described. The major threats to each element of the computer system, hardware, software, data, communications and the environment are identified and related to the appropriate service. Five major risk categories are described : disaster, accident, error, computer abuse and sabotage. These headings are used as the starting point for the analysis of risks to each component of the system.

Table of Contents

Figures

Tables

Chapter 1

Introduction

1.1 The banking industry and information technology

With the introduction by the finance industry of applications based on advanced information technology (the use of computers and communications), it has become apparent that the security of such systems is a matter of grave concern. Both banks and customers stand to lose from the weaknesses endemic in the technology. The purpose of this thesis is to identify the principle risks to security in five applications that are central to electronic banking: Automated Teller Machines (ATMs), Electronic Funds Transfer, Point-of-Sale (EFTPOS), credit cards, home banking and wire transfers. Both the information technology used and the applications are described. The major threats to hardware, software, data, communications and the environment are then analysed in terms of the principle risks : disaster, accident, error, crime and sabotage.

In the past few years financial institutions all over the world have chosen to offer a wide range of services to their customers that depend upon computing technology. These include Automated Teller Machines (ATMs), bank credit and debit cards, Electronic Funds Transfer Point-of-Sale services (EFTPOS), Automated Clearing House Services, home banking, cash management and wire transfers. Not all of these are new services, wire transfers, for example, but in their present form they all rely heavily on computing technology. These services are often referred to as electronic funds transfer (EFT) applications since paper based instructions for the movement of money are replaced by the electronic transmission of such data. A more meaningful term also used to describe such services is electronic banking. This seems more appropriate than electronic funds transfer in the present climate where banks deliver not only money but also financial information and transaction services to the customer as required. Banks, therefore, have become very dependent upon the entry of data and its manipulation by the computer since it represents both information and money.

Various factors have led to this expansion of services. Bankers themselves identified three principle forces that currently shape payment systems, technology, cost revenue relations and competition (De Mattia, 1985). Computer technology and associated advances in telecommunications make it possible for banks to transfer and act upon messages from their customers very quickly. Payments made at the point of sale as well as small incoming and outgoing payments can easily be automated. Banks can also process and settle high value payments in one day. The use of computer technology to add value to products and services has become widespread. The large and sophisticated systems needed to support such processing can be developed using an effective information systems strategy which enables an organisation to plan its application, technology and management policies to achieve its business goals. The costs associated with such a system are rapidly decreasing; the reduction in the price of hardware (mainframes and terminals) as well as cheap rates for data transmission on packet-switching networks have made possible great economies in scale.

Cost revenue relations have become particularly important in view of two developments. In the first place banks need to replace their lowered profits from interest income by earning fees from the various services that they offer their customers. Retail banks have found that lending out the deposits has proved less and less profitable as the competitive environment has had the effect of significantly increasing the cost of collecting the deposits in the first place. These costs are difficult to recoup so there has to be some means of reducing operating costs (Bailey,1986). Secondly, bank payment systems throughout the world are having to handle an increasing numbers of cheques. There appears, unfortunately, for the banks, to be a trend to use cheques for lower value payments (Read,1983). Replacing the cumbersome and relatively costly processing of cheques by alternative services such as ATMs and EFTPOS should help reduce costs for the banks. Figures provided by Lipis (1985) indicate that the cost of a teller transaction is well above the average ATM transaction cost.

Various competitive forces have compelled banks to making increasing use of information technology. Financial deregulation in many countries of the world has made it possible for non-banks to carry out functions once the sole prerogative of banks. These institutions have been able to make use of this opportunity because of the lowered barriers to entry. Technological changes mean that there is no longer any necessity, for example, to have a large number of branch outlets in order to meet the needs of the customer effectively. In order to survive banks have to use the same technology as their competitors. Their reasons for providing an attractive range of services include all or some of the following : generating new and profitable accounts, higher retention of present accounts, enhanced image of the organisation, competitive advantage and expansion of geographic coverage at considerably less cost than traditional branch activities (Bennet,1976). It is not only on the domestic front that banks have to act. The internationalisation of the finance industry is another reason why banks have had to adapt their competitive strategies. With a system of international markets, increasing trade between the subsidiaries of transnational corporations and an international spread of corporate related services, the banks are having to integrate their operations on a global basis (Langdale,1985). Again, it is computer technology that makes this possible.

Banks are currently in a transitional phase. Once they held a legal monopoly on the payment system, now they have been forced to respond to economic and technological forces to ensure their survival. They have done this by making available electronic banking services that are offered off-premises as well as on. A survey carried out by Louis Harris and Associates (1985) on behalf of Coopers and Lybrand revealed that most of the large banks which offered these technology-enhanced or technology-dependent products believed that these applications were on the "cutting edge", that is relatively new and untried. They felt committed to such a course of action in order to keep up with the competition. The speed at which changes have been introduced is causing some concern not least from a security point of view. As early as 1983, Miller noted that "with the concentration of more and more operating functions in computer systems, characteristics

of threats change, exposures to loss increase greatly." He listed nineteen possible exposures that could result from a threat, the principle of which are loss of assets, the cost of litigation, the loss of business and increased insurance fees.

Banks not only have to worry about the financial losses they could sustain but are also particularly vulnerable to a loss of confidence on the part of their customers. Any threat to their reputation can lead to a "run-on the bank" by their customers, resulting very quickly in bankruptcy. In order to avoid such a contingency and to minimize monetary losses, many banks have instituted a risk management programme. The first stage of this process provides for the identification of threats to security. Once this has been carried out, a bank can decide how much to spend on measures to reduce the risks. Both the likelihood of a threat materialising and the consequent losses have to be taken into account. If the risk management procedure is carried out properly management can reduce the overall level of risk in the system. Moreover, substantial savings in insurance costs can be achieved since premiums are related to the effectiveness of the controls in place. At a time when insurance fees are rising rapidly, this gives financial institutions a great incentive to make a realistic appraisal of weaknesses in the services they offer and implement suitable controls. The most important stage in this exercise is the initial identification of the principle risks.

1.2 Scope of the thesis

The author is unaware of a comprehensive survey of risks associated with the introduction of electronic banking. This study attempts to address this by identifying the major security risks in five important applications. At a time when more and more financial institutions are bringing technology-dependent products on to the market, it is important to analyse the applications in order to determine the major security threats. This should prove helpful not only to those working in this area but also to the general public whose interests have to be safeguarded. The scope of the study is limited to five electronic banking services : Automated Teller Machines, Electronic Funds Transfer Point-of-Sale,

bank credit cards, home banking and wire transfer systems. The first four of these are applications that are currently or, banks would like like to see, well-patronised by the general public. Wire transfer systems, on the other hand, are more often used by corporations. They involve the movement of huge sums of money daily and are crucial to the economies of the west. Whether the application is a matter of private or public interest, however, customer and bank monies are at risk. The five applications selected are described in some detail prior to the analysis of risks. This is an integral part of the thesis since the risks identified have to be related to a specific environment.

The principle risks consequent upon the use of computer technology are identified and described. Real-world examples, taken mainly but not solely from the banking industry, are included to illustrate the dangers. Each application is not the subject of a separate chapter since this would involve a great deal of duplication. Many risks (for example fire at a computer installation) are common to all the electronic banking services. Instead, the threats to each element of the computer system : hardware, software, data, communications and environment, are identified and related to the appropriate service.

Five major risk categories have been identified from the study of the literature : disaster, accident, error, computer abuse and sabotage. These are used as the starting point for the analysis of the risks to each component of the system. A threat can be seen from many perspectives. To take an example, a transaction can be altered when transmitted along communication lines. This is classified as the unauthorised modification of data in chapter 7 but as an active wire tap in chapter 8. It is essential to view an action from these different angles. Not only does this approach provide a double check so that no major risk is overlooked but makes it easier to provide appropriate solutions as it often identifies the method of attack. Finally, many risks arise from a combination of circumstances and have to be categorised in more than one place.

There are three sources for the material in this thesis; firstly published material, the books and articles written by security professionals, handbooks published by banking organisations, international and national standards, working documents of organisations involved with setting up banking applications and press reports (including the electronic mail journal "Risks-List"); secondly, discussions with EDP auditors, data security staff and university colleagues to clarify the issues involved; lastly, the application of the principles derived from the previous two sources.

The structure of the thesis is as follows:

Chapter 2

An introduction to the problem of security in computer systems with a discussion of the model that has been used as the basis of risk analysis.

Chapter 3

A description of the technology used in electronic banking

Chapter 4

A description of the electronic banking applications selected. Sufficient detail is given to enable examples in the body of the text to be comprehensible.

Chapter 5

The risks associated with hardware

Chapter 6

The risks associated with software

Chapter 7

The risks associated with data

Chapter 8

The risks associated with communications

Chapter 9

The risks associated with the environment

Chapter 10

This chapter contains the conclusion