2005

Information Security in the Caribbean Banks

Hongjiang Xu
Butler University, hxu@butler.edu

Pierre Bowrin

INFORMATION SECURITY IN THE CARIBBEAN BANKS

Dr. Hongjiang Xu, Central Michigan University, xu1h@cmich.edu
Pierre Bowrin, Central Michigan University

ABSTRACT

Information security is a crucial issue for organizations, especially for banking and financial institutions. However, not many studies have considered the perspectives of end users in developing countries' banking industry, for which the challenges of competing globally are greater due to a lack of technical, human and financial resources. Therefore, this study examines how end users of local, regional, and international banks in St. Kitts (a Caribbean country) perceive information security. The study will provide financial institutions in developing countries with more efficient security measures that would facilitate their success in the global community.

Keywords: information security, developing countries, banking and finance

INTRODUCTION

Traditionally, the burden to ensure the security of information is borne by various information technology specialists such as security manager or systems manager [11]. However, Vyskoc and Fibikova [9] argue that these individuals create only the basic security framework to facilitate a secure operational environment and that real security can be achieved only when end users collaborate and behave in a manner that does not open security holes or render security safeguards inefficient. The perspective of the end user is, therefore, a critical indicator to consider in assessing the information security measures employed by financial institutions.

Studies by Adams and Sasse [1], Vyskoc and Fibikova [9] and Brostoff and Sasse [2] focused on the perspectives of end users in an attempt to argue that information security designs need to consider more than technical elements and that narrow technical design perspectives produce security mechanisms that are less effective than generally assumed to be. The economy of every nation—industrialized or not, developed or not, western or not—plays its part in the success or failure of the world economy [7]. It may be more important to assess the perspective of end users of less developed or developing nations such as the islands of the Caribbean region that are constantly struggling to combat the savage and inhumane forces of globalization [5]. Such activities will assist in improving the activities of agricultural, manufacturing, and financial institutions and thus improve the economies of these nations and also the world.

There are no known studies that consider the perspectives on end users in less developed countries for whom the challenges of competing globally are greater due to a lack of technical, human and financial resources. Therefore, in an effort to add depth to the existing body of knowledge on Information Technology, this study examines how end users of a sample of local, regional, and international banks in St. Kitts perceive information security with the hope that such an instigation will provide insights into the usefulness and effectiveness of current information security measures. With this assessment, financial institutions will be more equipped

to create and implement more efficient security measures that will facilitate the success of businesses and economy in St. Kitts and the global community.

BACKGROUND

Information Security

One of the fundamental elements for a successful enterprise is security. Whitman and Mattord [10] define security as the quality or state of being secure. The National Security Telecommunications and Information Security Committee (NSTISSC) define information security as the protection of information and the systems and hardware that use, store and transmit that information. Businesses are secured from harm by implementing mechanisms that aim at impeding possible data loss and misuse. Whitman and Mattord [10] recommend layers of physical, personal, operational, communications, and network security to be employed to achieve maximum protection. However, to protect the information and its related systems, a suitable and, to an extent, tried and tested model is needed. One of the most referenced security guidelines is the Information technology—Code of practice for Information Security Management, which was originally published as the British standard BS 7799 [10]. In 2000 it was adopted as an international standard by the International Standard for Organization (ISO) and the International Electro-technical Commission (IEC) as ISO/IEC 17799 [10]. It is this internationally tested and accepted benchmark, against which the findings of the study will be gauged. Instead of using the ISO/IEC 17799 to measure the technical elements and design of a security system, the researcher will utilize its ten (10) security points of standard (discussed later) to determine user acceptance of information security measures.

Users' Perspective of Information Security

The effect of globalization continues to ravage Caribbean economies. The Honorable Dr. Denzil Douglas, current Prime Minister of St.Kitts and Nevis, highlights in his 2004 budget address the challenges that incessantly plague the island and the wider Caribbean region as they struggle to survive in the global economy [4, 8].

From early colonial occupation, St. Kitts and Nevis survived as a mono-agricultural twin island federation, with sugar cane as its primary and reliable source of foreign exchange. However, the fruitful years of "King Sugar" are only a memory. Sugar production in 2002 declined by 4.8% after experiencing a 24.5% growth in 2001 [3]. Today, the sugar cane fields that continue to sparsely blanket the islands produce barely enough for export. This decline in the production and exportation of sugar from the island is due primarily to the influence of the North American Free Trade Agreement (NAFTA), World Trade Organization (WTO) and General Agreement on Tariffs and Trade (GATT) as they strive to promote "free trade." The decision of these industrialized co-operations stripped St. Kitts and other Caribbean islands of the preferential treatments once afforded by the European Union (EU). This preferential treatment provided the islands of the region a guaranteed opportunity to sell their produce in the global market that is already monopolized by a few powerful developed countries with subsidized production.

Caribbean people have long been known for their resilience. When face to face with the snarling jaws of despair, they bite down and with "Plan B" in hand, attempt another approach. For the

past few years, a viable alternative ("Plan B") has been to further develop the tourism product and the private business sector. Participants of both public and private sectors continue to develop viable business enterprises aimed at producing a region that is self-sufficient and an overall stable economy. However, Caribbean businesses are continuously battling the effects of globalization. In search of a more "leveled" ground upon which to compete, the region has embraced new technologies such as client/server technology and the Internet, which allow for quicker access to relevant information, more equitable competition on the global market, and other services. Although such strides are welcomed, it is important to be aware of accompanying dangers. However small, Caribbean businesses cannot afford not to employ the necessary precautions to safeguard against inefficient handling of data. The region cannot risk being further behind in the global market game; therefore, adequate effort must be invested to create a secure environment in which businesses can efficiently operate.

When deploying information security systems in business in the Caribbean or any region, the perspective of prior end users must be considered in selecting the information security measures [6] to be employed. This assessment of prior end users also helps security specialists project future users' acceptance and support.

Research Objective

This study aims to determine how end users perceive the information security measures of business enterprises by identifying the perceptions of end users in developing nations such as St. Kitts. The investigation also aims to create an awareness of issues pertaining to the development of information security systems in the Caribbean region in an effort to enrich the contributions that already existing in the body of literature. The study will specifically explore the following:

> *The perception of end users of the effectiveness of information security measures at banks in St. Kitts*.

METHODOLOGY

To explain the research question, the case study approach was selected as the research design. Yin [12] credits the case study approach for its ability to balance adaptiveness with rigor. The study focuses on end users from three banks that operate in the federation of St. Kitts and Nevis. For the purposes of this study, the banks will be referred to as Bank A, Bank B and Bank C and those banks are classified as local, national and international, respectively. This selection of case study banks was designed to include all levels of banks, which allows us to investigate whether there are any differences between different sized banks, as well as have a complete representation of the entire range of banks in the country.

The individual directly responsible for the implementation and operation of information security measures was interviewed in person. The most senior IT person was interviewed in each of the three (3) organizations studied. The three-part interviews consisted of (1) a description of the study and a clarification of terms; (2) a request for demographic data about the respondents and their firms; and (3) the collection of data relevant to the study protocol area of questions. Telephone interviews were later conducted with two end users in each of the three participating

organizations. These end users all held middle management positions and were randomly selected.

Face-to-face and telephone interviews were conducted with the middle management in the three case study banks. The respondents responded to the ten security points of standard covered by the ISO/IEC 17799 information security standard. The perspectives of the users were sought to assess the information security measures employed and to gauge their acceptance and support.

This first stage was limited by the number of case study participants. In the second stage of the study, a more representative assessment of end user perspectives will be investigated by a large scale survey design based on the analysis of the case studies from the first stage.

Data Collection

Three case studies were conducted for the first phase of this research project that focused on the banking sector. The protocol for conducting the case studies consisted of semi-structured interviews with information technology and middle managerial personnel discussing the information security measures with which they work, as well as the collection of secondary documentation accumulated on each company. The Case Study Interview Protocol (CSIP) used in the interview process was based on the ten security points of standard (outlined by the ISO/IEC 17799 information security standard) to extract specific and, as much as possible, comparable information about aspects of the information security measures employed. The CSIP addressed ten areas of information security: business continuity planning, system access control, system development and maintenance, physical and environmental security, compliance, security organization, security policy, computer and operations management, asset classification and control and security policy. Most interviews were tape-recorded and were approximately thirty minutes in duration. In analyzing the case study, the aim was to identify themes arising from the perceptions expressed by middle management personnel (end users). The report does not attempt, however, to apply to the data any quantitative techniques such as analysis of frequencies of terms related to the ten security areas discussed.

RESEARCH FINDINGS AND DISCUSSIONS

Case study interviews collected data about the organizations, their information security systems and the respondents' backgrounds. The companies studied are geographically centralized. Only the banking industry is represented. The participating banks vary in size, provision of services and assets under management. One category of the case study participants were information systems mangers who were directly responsible for information security: they had from three to ten years working experience. The experience level of the middle management respondents ranged from three months to fifteen years. However, the perspectives provided by these respondents did not reflect their time with the company.

Business Continuity Planning Theme

A key theme that emerged in this section was that the acknowledged reliance on manual reports in the eventual loss of the computer system inhibited normal business continuity. Middle

management from all three banks expressed confidence in their ability to continue. Apparently, this area was developed in preparation for hurricanes which frequent this side of the Caribbean. One respondent boldly noted:

> *"Yes … we do have a contingency plan in place that is documented and rehearsed about on a bi-annual basis."*

However, no voluntarily mention was made of the obvious time delay in service that would exist. This question will be further explored during the second phase of this research.

System Access Control Theme

The objective of this section was to obtain perspectives on security measures in place to prevent unauthorized access to information systems. Respondents from Bank B and Bank C articulated confidence in their systems' ability to maintain access control. However, discussions with respondents from Bank A expressed the occurrences of events in which unauthorized transactions were made and being investigated. No details were supplied. The system manager from Bank A did admit to security breach that had occurred in the past year.

System Development and Maintenance Theme

The system managers noted that efforts to prevent data loss, modification or misuse of user data in application systems were reliant on application security features and on the computer network. Respondents from all banks agreed that measures in place were adequate and that they worked. According to a respondent from Bank B:*"I think it's really secure … I mean… not everything is available to everybody … I honest take it for granted because those guys are always on top of things."*

Physical and Environment Security Theme

The objective of this section was to obtain perspectives on security measures in place to primarily prevent damage of assets and the theft of information and information processing facilities. Systems managers indicated that efforts to secure corporate assets included alarm systems and external monitoring systems. Middle management respondents also verified the existence of these measures. However, a filed police report that was verified by the researcher noted a robbery that occurred approximately four years ago at Bank A. Obviously, additional measures in this regard must be put in place at Bank A. Perhaps the constant reference to the fact that the new headquarter of Bank A will provide better facilities will assist these shortcomings.

Compliance Theme

It is interesting to note that there were no efforts or requirements to achieve any international compliance standards. Responses with regard to compliance issues were in reference to banking procedures. However, the system manager of Bank B noted current ongoing efforts to adhere to aspects of the U.S. Patriot Act. This was a "request" made by a company that conducts business with Bank B. The system manager noted *" … that U.S. Patriot Act is a pain …"*

Personnel Security Theme

General efforts to reduce risks of human error are reliant on application measures and an audit system. Respondents from Bank B and Bank C indicated the presence of an internal audit department that reviews data entry reports for errors. Discussions with Bank A respondents revealed the absence of an internal auditor but noted that the review role was performed by the department head. The audit function was referred to as "double check." One respondent from Bank A noted:"*… we should be able to flag it in the double check … because it has to be reviewed by the head of the department."*

Security Organization Theme

The objective of this section was to obtain perspectives on security measures in place to manage information security within the company. Discussions with all respondents revealed that all efforts to maintain security were done in consultations with overseas consultants. This suggests a lack of or confidence in local expertise.

Computer and Operations Management Theme

The objective of this section was to obtain perspectives on security measures in place to ensure the correct and secure operation of information processing facilities. Respondents from Bank B and Bank C gave high marks to the measures in place at their work place. However, improvement was subtly hinted at by a respondent from Bank A.

CONCLUSION

To understand the end users' perspectives is important in developed nations, as it can help with the determination of users' acceptance and support for the security measures employed. It is even more important for security specialists in small developing countries such as the islands of the Caribbean, who constantly struggle to combat the forces of globalization. From the findings of this study, it is clear that smaller institutions like Bank A struggle to provide information security at a level commensurate with the other banks. In this regard, more must be done to assist the smaller companies to implement more rigorous security measures. The Caribbean needs to pay more attention to its smaller institutions as they too are contributors to its success. The larger financial institutions appear to have a stronger grasp on implementing measures that are required to ensure a secure environment. Real security is incumbent on the users that use the system and a viable framework can be strengthened by incorporating end users' perceptions and viewpoints.

REFERENCES

1. Adams, A. & Sasse, M. A (1999) Users are not the enemy. *Communications of the ACM, 42*(12), 40-46
2. Brostoff, S. & Sasse, M. A (2001) Safe and sound: a safety-critical approach to security. *Proceedings of the 2001 workshop on New security paradigms*, 41-50.
3. Caribbean Development Bank. (nd.) *Caribbean Development Bank: 2002 Annual Report*, http://www.caribank.org/, accessed January 25 2004.

4. Douglas, D. (2004). *The 2004 Budget Address* by St. Kitts and Nevis Prime Minister and Minister of Finance.
5. Kaarst-Brown, M. L. & Wang, C. (2003). Doing business in paradise: How small, information intensive firms cope with uncertain infrastructure in a developing island nation (TCI). *Journal of Global Information Management*, *11*(4), 37.
6. Landwehr, C. E. (1981). Formal Models for Computing Security. *Communications of the ACM*, *13*(3), 247-278
7. Proudlock, M.J., Phelps, B. & Gamble, P. L. (1998). IS decision making: A study of information-intensive firms. *Journal of Information Technology*, *13*(1), 55-66
8. The Official web-site of the Government of St. Kitts & Nevis, St. Kitts & Nevis 2004 Budget Address, http://www.stkittsnevis.net/news-budget2004.html, accessed February 10, 2004.
9. Vyskoc, J. & Fibikova, L. (2001) IT Users' Perception of Information Security. *Proceedings, IFIP WG9.6/11.7 conference. Security and Control of IT in Society - SCITS-II*, June 15-16, 2001, Bratislava.
10. Whitman, M. & Mattord, H. (2003). *Principles of Information Security*, Course Technology.
11. Whitson, G. (2003). Computer security: Theory, process and management. *Communications of the ACM*, 57-65.
12. Yin, R. K. (1994). *Case Study Research: Designs and Methods*, *5*, SAGE Publications.