Chapter II
Enhancing Cyber Risk Management with the Framework of ERM and Basel II

Junji Hiwatashi
Bank of Japan, Japan

ABSTRACT

How is it possible to enhance efficiency of management and to control cyber risk at the same time so that sustainable growth is achieved? Possible solutions were found in ERM and Basel II. First, a newly introduced ERM is a tool not only for defense against loss but also for a formidable weapon to seek sustainable returns. Appropriate coordination and cooperation in implementing risk management on a firm-wide basis encourages firms to identify, analyze, measure and control all material risks such as cyber risk, and to provide a sound base to make strategic decision on the balance of risk and return, or risk adjusted return on equity. Second, in Basel II, operational risk such as cyber risk is explicitly introduced. The author proposes a practical framework based on ERM and Basel II. It consists of policies and structure, and five steps. This framework is based on the practices of financial institutions but could be applied and expanded to firms in general.

INTRODUCTION

Information technology (IT) has been rapidly developed to provide financial services with customers by the Internet. This service is available 24 hours a day, 7 days a week beyond the boundary. On the other hand, technology-oriented financial services may face various cyber risks such as disruption caused by natural disaster and terrorist attack, impersonation, and other events stemming from unauthorized access, and theft or alternation of data. Once these events occur, they could affect not only companies such as financial institutions but also their stakeholders...
such as customers and financial stability. These events lead to indirect effects such as lawsuits and bad reputation losing sound customer base immediately. Thus, it is critical to enhance cyber risk management in advance before the nightmare in order to enjoy the benefits of IT. This chapter introduces the practical methods of enhancing cyber risk management efficiently and effectively with the framework of Enterprise Risk Management (ERM) and Basel Accord II (Basel II). It aims to learn how to enhance cyber risk management effectively and efficiency so that sustainable growth is achieved with the balance between risk and return, or risk-adjusted return on equity.

LESSONS LEARNT FROM THE PAST

We are in the new age of information revolution. For example, owing to unprecedented IT development, we could tremendously save both the time and the cost of exchanging information. The current information revolution is said to be the fourth in the human history. Based on Drucker (1999), three revolutions are reviewed as follows: The first was writing 5,000 to 6,000 years ago in Mesopotamia. The second was the invention of written books first in China, perhaps as early as 1300 BC. The third was the innovation set off by Gutenberg in terms of printing press and movable type between 1450 and 1455. What was the impact? Before the third revolution, well trained and disciplined monks could protect their positions by showing their skills of copying books by hand, but by 1500, these monks became unemployed after this innovation of printing press (Drucker, 1990). In the fourth revolution, computer networks are used for huge amounts of financial payments and settlements on a daily basis as well as exchanging information. For example, the Federal Reserve Board operates Fed-wire, a computerized network system of money transfer, in Japan. SWIFT is used for cross border settlement among internationally active banks. It is recognized why critical cyber risk management is essential based on the following three lessons learnt from the past large events.

The Shadow of IT

The history of computer development is said to be that of security. Computer users are diversified from limited ones such as computer specialists in universities, research centers, big firms, and financial institutions to unlimited ones including their general staff and individuals. At first, computer system was developed to execute a huge number of transactions for payments of customers among financial institutions. These computer systems are called “closed network systems” in the sense that these transactions were accessed to computer and operation staff of financial institutions. In the closed system, the control methods of cyber risk were limited to those such as the entry and exit control of staff in main computer center. They used limited measures such as security video for monitoring and telecommunication protocol.

In the latter half of 1990s, open network systems such as the Internet, became very popular and used for financial services of individuals. On the other hand, it became easier to invade into computer network systems and get valuable information without permission. It is not rare to become victims of having privacy information stolen at the age of open network systems. For example, the privacy information such as names, addresses, and telephone numbers of users of an Internet connection service provider, was leaked twice, in June 2003 and January 2004. The event affected around 4.6 million users of this provider. Later, its operating company apologized to them for leaking these kinds of information and voluntarily sent a gift certificate of 500 yen or approximately U.S. $4 to each customer concerned. In May 2006, the Court in Osaka judged that its
Related Content

A Typology of Interorganizational Relationships: A Marriage, a Fling, or Something in Between
[www.igi-global.com/article/typology-interorganizational-relationships/1856?camid=4v1a](www.igi-global.com/article/typology-interorganizational-relationships/1856?camid=4v1a)

[www.igi-global.com/chapter/nibbling-sniping-role-uncertainty-second/9364?camid=4v1a](www.igi-global.com/chapter/nibbling-sniping-role-uncertainty-second/9364?camid=4v1a)

Games-Based E-Learning: Implications and Challenges for Higher Education and Training
[www.igi-global.com/chapter/games-based-learning/9327?camid=4v1a](www.igi-global.com/chapter/games-based-learning/9327?camid=4v1a)

An Empirical Study of the Impact of Brand Name on Personal Customers’ Adoption of Internet Banking in Hong Kong
[www.igi-global.com/article/empirical-study-impact-brand-name/38957?camid=4v1a](www.igi-global.com/article/empirical-study-impact-brand-name/38957?camid=4v1a)