FACTORS INFLUENCING ELECTRONIC PERSONAL DATA PROTECTION MANAGEMENT AND DEVELOPMENT OF FINANCIAL INSTITUTES IN THAI BANKING ASSOCIATION.

Thawat Sairahu
Graduate School, Suan Sunandha Rajabhat University, Bangkok, Thailand
Email: thawat.sa@ssru.ac.th

ABSTRACT

The research objectives represented 1) to study electronic personal data protection management and development of financial institutes in Thai Banking Association 2) to study the factors influencing electronic personal data protection management and development of financial institutes in Thai Banking Association. This research represented qualitative approach on the in-depth and focus group on interviewing, the population consisted of financial institutes, financial association and the head of government agencies. The sample represented purposive sampling of ten agencies, the participants who were the head of government agencies, financial institute and financial association executives. The interviewing data were obtained from executives of selected agencies and then synthesized to be specified information for research answering.

The finding found government agencies paid attention to the personal data protection by issuing the legislation on electronic transactions including personal data access in addition, factors influencing the electronic personal data protection management and development of financial institutions in the Thai Banking Association consisted of 1) the governmental policies consisted of the guidelines of legislation on personal data and privacy protection 2) the public participation consisted of the technological capability and 2) technological capability.

INTRODUCTION

The electronic communication and transaction expanded increasingly at the present due to the spread of internet using exclusively the internet application on portable devices or called mobile internet that contributed to easily access the electronic contents in anywhere, anytime and borderless and also absolutely differed from the past. At the present the data were easily stored, transferred, accessed and diffused, for this reason, the strengths of today's internet systems were widely applied with the various businesses performing in the internet and digital era and developed from the paper work to electronic contents, the financial institutes in the Thai Banking Association were not exemption. At the present, the financial institutes adapted their information strategies to accommodate the lifestyle's needs of customers in the term of dissemination, storage and transaction or other customers' activities and the participants of financial institutes with electronic online through the website, program and applications on portable devices of financial institutes.

Even if the change made the convenience, cost saving and rapid in operations to financial institutes in Thai Banking Association and clients including tracking back and back up for data security, however the disadvantage of electronic online application represented the leakage of personal and transaction data during transferring or hacking by hackers. For this reason, online transactions were doubtful among many people inside and outside the country. The security of personal data that might be used in the misconduct by fraud, this reason, government and financial institutes on Thai Banking Association needed to build trust and confidence in online transactions.

One thing that was important to build credibility and confidence for the people and clients of financial institutions in Thai Banking Association represented policies formulation and legislative control by the government. However, the dealing with the government by proposing the Act of privacy protection for many years but still be unapproved to the present day. If this law was approved, the personal information protection law would be valid and would substitute the tortious law on the general or the human rights on constitutional law in the past, In addition, this new law also protected users against the storage of personal information of organizations or agencies to storage data without approval or outbound authorized usage that caused the slow growth of electronic commerce in Thailand in the past.

The mentioned above, the research prioritized and focused to study factors influencing electronic personal data protection management and development of financial institutes in Thai Banking Association.

The research questions were obtained as following.

1. How did the electronic personal data protection management and development of financial institutes in Thai Banking Association?

2. Which factors did influence to the electronic personal data protection management and development of financial institutes in Thai Banking Association?

The research objectives as following:

1) to study electronic personal data protection management and development of financial institutes in Thai Banking Association

2) to study the factors influencing electronic personal data protection management and development of financial institutes in Thai Banking Association.

LITERATURE REVIEW

Government policies

The guidelines for legislation in personal data protection, the personal data protection law, privacy represented the right to privacy that expressed the fundamental human right and was prioritized by social in almost countries and endorsed this principle in the Constitution or even if some countries did not perform that but it also enacted provisions in specific laws. All of the human right, the privacy was one of the most difficult to define the meaning because of the environmental considering in social contents, culture and relevant behaviors. Some countries the concept of privacy included the personal data protection which interpreted to personal data management, however the term of privacy represented the broad definition and referred to many rights as following:

1. The data privacy represented the personal data protection through establishing regulations regarding the collection and management of personal data.

2. The personhood privacy represented the protection of substantial body that would be unacted in anyway and invasion the privacy like genetic testing, drug testing, etc.

3. The communication privacy represented the protection in safely and privacy of the letter, telephone, e-mail and any communication methods that no one could know.

4. The territorial privacy represented the boundary or limitation that any person invaded to personal place including the surveillance and identification checking.

However, although there were many aspects of privacy, but the privacy that was prioritized by many countries due to the rapid development of information technology meant the privacy in personal data, because the advancements in computers influenced the communication and dissemination of information can be transmitted and linked without the limitation of time and place longer, contributed the processing, storage or disclosure of personal data to be done easily, conveniently, and quickly. On the other hand, these technologies might be embraced in invasion to others.

The privacy protection policies

The privacy concept was accepted for a long time such as many parts of the Bible described the privacy, Jewish, Greece or Chinese also accepted the concept of privacy in addition the most wide recognized and referenced concept of privacy represented the privacy concept of Samuel D. Warren and Louis D. Brandeis in 1890, which explained that privacy meant "the right to be let alone" as legal concept at the first time, but later the development of information technology especially via communication network made the idea of "privacy" meant "the right to be let alone" was not enough because a tort in privacy could be easily performed. Therefore, the effort of defining the meaning of privacy in accordance with modern society by Alan F. Westin, who gave the definition of "privacy" in the book "Privacy and Freedom", which meant to "the rights of individuals, groups, or organizations was disclosed to others whether when and how. At the present this concept was widely accepted although this unclear issue, that the privacy of the group or organization should also be protected or not.

Public participation

The technology capability

At the present the people possessed more technological ability; a study found that search engine like Google accessed the first webpage of many financial institutes in Thai Banking Association, Standard Chartered Bank, Government Housing Bank and Bank for Agriculture and Agricultural Cooperatives with privacy policy recognition. While others financial institutes in Thai Banking Association did not show the privacy policy on their websites or other sentences that was not “personal data protection” of financial institutes in Thai Banking Association.

The survey of Thai Netizen Network on the online personal torts in Thai society in 2013 found that abused things were names, surnames, identification numbers, addresses, photos, emails, telephone numbers, fax number, workplace, travel details, position, academic performance, especially the account number, financial institutes in the Thai Banking Association and credit card numbers related to the financial institutes in the Thai Banking Association directly. In addition, financial institutes in The Thai Banking Association remained the number one source of electronic transactions beyond the online purchasing, in addition, the survey found that financial institutes in the Thai Banking Association obtained the personal data for mutual benefit like insurance companies. In addition, the survey found some problems were caused by the inaccuracy of financial institutes in Thai Banking Association, for example, the verified question system was extremely easy or tried to do only a low standard.

The technology usage

At the present, hackers not only aimed to penetrate the banking network or online service providers for customer's privacy but also to inexperienced internet users that was easier and wide to access. Sometime the internet users tried to download programs or some information that hackers published on popular websites, some programs was attractive on the name like porn clips, acceleration programs, cracking serial number programs, game programs, etc. When users were obsessed with downloading such programs to install on their device, there might be attached hidden malware on file causing the users to be a victim of fraud.

The general users’ aspects, threats protection with awareness and self-controlled behavior on internet usage in the personal computer, no downloading with unsafe feeling, operate the computer with updated protection software, setting a strong password.

The service providers' aspect, although service providers designed the network so well that it was hardy for hackers to penetrate the system, hackers could hack through users as popular method. For this reason, in addition to providing convenience to customers, service providers also prioritized the user identification technology, data security and how to utilize it when customers had to carry out transactions via the internet, as well as educating customers to keep up with the danger current threat. There were three types of authentication technology used for electronic transactions: 1) Something you have, like door keys, electronic cards, or tokens. 2) Something you recognize represented a password or a unique set of numbers. 3) Something you are represented biometric authentication, like fingerprints, voice recognition systems and iris scanning system, etc.

For electronic transactions, the single-factor authentication might not be enough to provide electronic transactions which tended to expand along with the higher risk as well, it was worthiest to implement two-factor authentication. A prominent example was an ATM that handled a plastic card (what you have) with a unique four digit number (what you know) compared to network authentication is the use of a combination of tokens and passwords. This method skipped the security, and users could not deny responsibility for their transactions which efficient system contributed strengthen the security structure and reduce the problems of fraud.

For internet transaction service providers via a web application that had not yet designed a two-factor system, there should be remained the login to the webpage to find out who represented the user on the service, to promote security for customers, as well as surveillance cameras that monitored ATMs, the service provider would also keep login accordance with the Computer Crime Act. In addition, the survey found that people wanted financial institutes in the Thai Banking Association maintained a transparent process for collecting and managing personal information according to global standards and done urgently jointly with legislation to regulate due to the privacy torts situation in Thailand.

RESEARCH METHODOLOGY

This research represented qualitative approach on the in-depth and focus group on interviewing, the population consisted of financial institutes, financial association and the head of government agencies. The sample represented purposive sampling of ten agencies, the participants who were the head of government agencies, financial institute and financial association executives. The interviewing data were obtained from executives of selected agencies and then synthesized to be specified information for research answering.

RESULTS

The finding found government agencies paid attention to the personal data protection by issuing the legislation on electronic transactions including personal data access in addition, factors influencing the electronic personal data protection management and development of financial institutions in the Thai Banking Association consisted of 1) the governmental policies consisted of the guidelines of legislation on personal data and privacy protection 2) the public participation consisted of the technological capability and 3) technological capability.

REFERENCES

[1] Alongi. A. Elizabeth. (2004). Has the U.S. Canned Spam. Arizona Law Review, (46), 263–290.

[2] Andrew Hotaling. (2008). Protecting Personally Identifiable Information on the Internet: Notice and Consent the Age of Behavioral Targeting. Common Law Conspectus: Journal of Communications Law and Technology Policy, 23(16), 529–565.

[3] Ann Black & Gary F. Bell. (2011). Law and Legal Institutions of Asia. New York : Cambridge university press

[4] Charles, R., Beitz. (2012). The History of the Idea of Human Right. Oxford: Oxford University press.

[5] Ferdinand, D., & Schoeman. (2011). Philosophical Dimensions of privacy: An Anthology. New York: Cambridge University Press.

[6] Greenleaf Graham & Sinta Dewi (2013). Indonesia's data protection regulation 2012: A brief code with data breach notification. Privacy Laws & Business International Report, 122(36), 24–27.

[7] Greenleaf Graham & Livingston Scott. (December 2016). China's New Cyber security Law– Also a Data Privacy Law? Privacy Laws & Business International Report 1–7; UNSW Law Research Paper, 14(19), 2–11.

[8] Ministry of Information and Communication. (2005). International Personal Data Transferring. Bangkok: