Eurasia Business and Economics Society
www.ebesweb.org - ebes@ebesweb.org

29th EBES CONFERENCE – LISBON

PROCEEDINGS VOLUME 1

October 10-12, 2019 / LISBON, PORTUGAL

Hosted by

ISCTE IUL
Instituto Universitário de Lisboa

ebes@ebesweb.org

www.ebesweb.org

ADVISORY BOARD

SCIENTIFIC COMMITTEE

- **Sagi Akron**, *University of Haifa*, Israel
- **Hasan Fehmi Baklaci**, *Izmir University of Economics*, Turkey
- **Adam P. Balcerzak**, *Nicolaus Copernicus University*, Poland
- **Marco Bisogno**, *University of Salerno*, Italy
- **Gabor Bota**, *Budapest University of Technology and Economics*, Hungary
- **Laura Brancu**, *West University of Timisoara*, Romania
- **Taufiq Choudhry**, *University of Southampton*, UK
- **Joel I. Deichmann**, *Bentley University*, USA
- **Ivana Dražić Lutilsky**, *University of Zagreb*, Croatia
- **Irene Fafaliou**, *University of Piraeus*, Greece
- **Clara García**, *Universidad Complutense de Madrid*, Spain
- **Tamara Jovanov**, *University Goce Delcev - Shtip*, Macedonia
- **Alexander M. Karminsky**, *National Research University*, Russia
- **Ashraf A. Khallaf**, *American University of Sharjah,* UAE
- **Tipparat Laohavichien**, *Kasetsart University*, Thailand
- **Gregory Lee**, *University of the Witwatersrand*, South Africa
- **Roman Mentlik**, *University of Finance and Administration*, Czech Republic
- **Veljko M. Mijušković**, *University of Belgrade*, Serbia
- **Alexander Redlein**, *Vienna University of Technology*, Austria
- **Nives Botica Redmayne**, *Massey University*, New Zealand
- **Liza Rybina**, *KIMEP University*, Kazakhstan
- **Hunik Sri Runing Sawitri**, *Universitas Sebelas Maret*, Indonesia
- **Irina Sennikova**, *RISEBA University*, Latvia
- **Pekka Tuominen**, *University of Tampere*, Finland
- **Manuela Tvaronavičienė**, *Vilnius Gediminas Technical University*, Lithuania
- **Sofia de Sousa Vale**, *ISCTE Business School*, Portugal

Determinant factors Affecting cyber risk of Thailand commercial bank

Tidathip Panrod

Faculty of Management Science, Silpakorn University, Phetchaburi, Thailand

Corresponding author: tidathip@ms.su.ac.th.

Abstract

At present, Internet technology is increasingly being used, especially in financial institutions. However, sometime Internet technology adoption inevitably lead to cyber risk. This research purposed to study determinant factors that effect to cyber risk of commercial bank and to study the correlation between cyber risk and cyber risk management of commercial bank. The samples used in this study were employees who have an experience in working with commercial bank in Bangkok, Thailand. Data was analyzed by using multiple Regression Analysis and Pearson's correlation coefficient in hypotheses testing.

The research found that Business environment factors affected the cyber risk of commercial bank, technology was the most effective factor. Management factors affected the cyber risk of commercial bank, man was the most effective factor. Cyber risk correlated with the cyber risk management of commercial bank. The suggestion of this research was commercial bank should concern about upgrading required skills and knowledge of their staffs in working with digital transformation technology.

Keywords: determinant factors, risk management, cyber risk, commercial bank

Introduction

Increasing interconnectivity, globalization and "commercialization" of cyber-crime are driving greater frequency and severity of cyber incidents, including data breaches. Data privacy and protection is one of the key cyber risks and related legislation will toughen globally. More notifications of, and significant fines for, data breaches can be expected in future. Legislation has already become much tougher in the US, Hong Kong, Singapore and Australia, while the European Union is looking to agree pan-European data protection rules. Tougher guidelines on a country-by-country basis can be expected.

Attacks by hackers dominate the headlines but there are many "gateways" through which a business can be impacted by cyber risk. Impact of business interruption triggered by technical failure is frequently underestimated compared with cyber-attacks. Vulnerability of industrial control systems (ICS) to attack poses a significant threat. To date there have been accounts of centrifuges and power plants being manipulated. However, the damage could be much higher from security sensitive facilities such as nuclear power plants, laboratories, water suppliers or large hospitals.

Cyber-crime in Thailand is still increasing every year. And the impact that has occurred on large corporations, despite the high total damage value is lower than those of smaller organizations. Moreover all business or industry was unable to escape from cyber-crime. Businesses related to energy and utilities, as well as businesses that provide financial services. For example, banks are often important targets for attacks each year. (Ponemon Institute, 2014) Cyber security is very important for protecting corporate resources. Therefore, the safety of information technology, there must be a good risk management process consisting of Identifying Risk, Risk Assessment, Risk Management Planning, Monitoring and Controlling Risk, and Conclusion and Reviewing Risk. (Rattanapongpinyo, 2017)

As mentioned it above, the researcher would like to study the determinant factors affecting cyber risk of commercial bank by the views of information technology users. This study concentrated in management factors and external factors, the important factors that result in cyber risk, including how to manage cyber risk as it happens actually for maintaining security from being threatened and overall efficiency operations.

Research Objectives

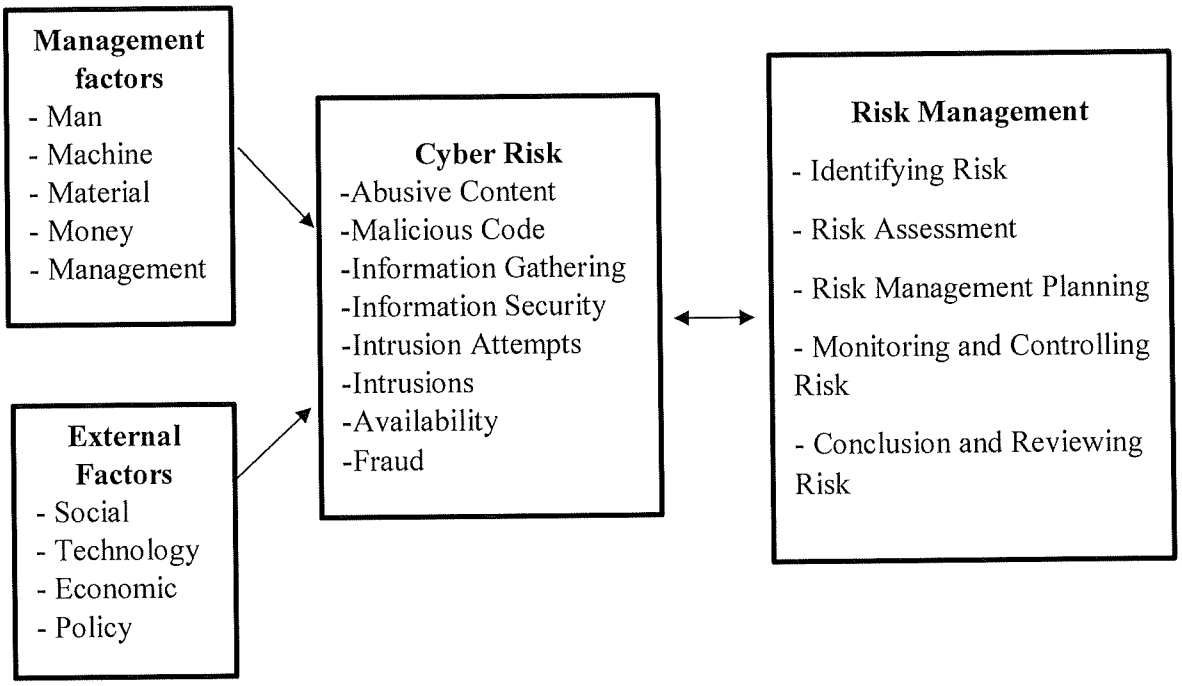
1. To study determinant factors that effect to cyber risk of commercial bank

2. To study the correlation between cyber risk and cyber risk management of commercial bank.

Conceptual framework of the study

Learning from the related Literature review, it can conclude and determine the Conceptual framework like the following figures.

Figure 1: The conceptual framework



Literature Review

Rattanapongpinyo Taninrat. (2017) identified risk management process consisting of Identifying Risk, Risk Assessment, Risk Management Planning, Monitoring and Controlling Risk, and Conclusion and Reviewing Risk.

Radanliev Petar. et.al. (2018) studied Future developments in cyber risk assessment for the internet of things. This article is focused on the economic impact assessment of internet of Things (IoT) and its associated cyber risk vectors and vertices – a reinterpretation of IoT verticals.

Cheang Sopheak (2009) studied Conceptual Model for Cybersecurity Readiness Assessement for Public Institutions in Developing Country: Cambodia. The result shown that combination of various sub-indicators, so the policymaker could realize the issue in detail

before the countering measures could be established. In this study, we perform detail analysis on how the readiness index can be constructed and what area it could be employed. We measure the cybersecurity preparedness of public institutions on three dimensions including, Human Resource, Infrastructure, and Environment. These three categories are the combination of 46 indicators aggregated by using Factor Analysis/Principal Component Analysis as multivariate and weighting method with linear additive aggregation.

Research Methodology

Area selection: This study was a quantitative research. It was studied in the form of survey research. The sample group was selected from the officers of commercial bank or those with experience in working in relation to commercial bank in Bangkok Thailand.

Source of information: This research didn't know the population so, that determined the sample sizes by Cochran's approach (Cochran, 1977) about 400 samples. The data collection used questionnaire to gather primary source information.

Research Tools

The researcher used questionnaire and research guideline as a tool to collect data from the officers of commercial bank. In the questionnaire structure, it divided to 6 parts that composed of Personal data, Management factors, External factors, Cyber Risk, Risk Management and the other related suggestions for the open-end part. This questionnaire and research guideline developed from the related researches and tested by 30 officers of commercial bank in Kanchanaburi. In addition, the return research tools were calculated by Cronbach's Alpha Coefficient (Cronbach, 1970), the outcome was 0.87 for confidence interval of overall questionnaire parts.

Data Analysis

All of questionnaire data were calculated by the SPSS, the results were analyzed and shown in the forms of percentage, mean and standard deviation for descriptive statistics. This research had hypothesis testing: firstly, for Management factors and External factors affected

to cyber risk of commercial bank was tested with Multiple regression, and secondly for Cyber risk related to Risk management was tested with Pearson's correlation coefficients.

Research Results

1. To study determinant factors that effect to cyber risk of commercial bank

Table 1. Multiple Regression Analysis for determinant factors that effect to cyber risk.

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	-1.068	.281		-3.798	.000
	Management factors	.726	.103	.527	7.034	.000
	External Factors	.582	.109	.399	5.328	.000
a. Dependent Variable: cyber risk **b.** $F = 140.676$, Adjusted R Square = 0.738 , $P < 0.05$, Sig. = 0.05						

In over all, Management factors and External factors affected to cyber risk of commercial bank by R^2 adj. = 0.738 at significance level 0.05. Management factors have influenced to cyber risk more than External factors by Coefficients 0.726 and 0.582 consecutively.

Table 2. Mean and standard deviation of Management and External factors.

Management factors	$\bar{x}$	S.D.
Man	3.6533	.46401
Money	3.3200	.42947
Machine	3.4350	.36345
Material	3.4233	.35724
Management	3.4925	.46392
External factors	$\bar{x}$	S.D.
Social	3.3667	.34976
Technology	3.8267	.47962
Economy	3.4500	.61340
Politics	3.4167	.47467

It revealed that Management factors: Man is the highest factor ($\bar{x} = 3.65$, S.D. = 0.46). For external factors: Technology is the highest factor ($\bar{x} = 3.83$, S.D. = 0.48).

2. To study the correlation between cyber risk and cyber risk management of commercial bank.

The research shown that cyber risk related to cyber risk management on 0.862 with Pearson's correlation coefficients at 0.05 significant levels.

Research Discussion

The finding of determinant factors that effect to cyber risk of commercial bank that demonstrated Management factors have influenced to cyber risk more than External factors. It conformed to the research of Waithaka Samuel (2016) that mentioned about internal organizational factors affecting cyber security were identified as lack of management support in implementation and adherence of cyber security strategy and standards, and employees' systems exploitation for personal gains. Lack of management support in implementation of cyber security is a major contributor to poor cyber security.

For the issue of correlation between cyber risk and cyber risk management of commercial bank, Antonucci Domentic (2017) explained in his paper "The Cyber Risk" that composed of four steps: Determine the cyber risk profile, Treating cyber risk, Alignment of cyber risk treatment and Practicing cyber risk treatment. It could compare with how to cope with cyber risk management when risk manager can identify cyber risk category by sources.

Conclusion and Recommendation

The research results displayed that Management factors and External factors affected to cyber risk of commercial bank. Internal factors: Leader is the highest factor, like Technology from external factor. Moreover, cyber risk related to cyber risk management.

The suggestion of this research was commercial bank should concern about upgrading required skills and knowledge of their staffs in working with digital transformation technology. Another useful recommendation was risk manager must take an integrated approach to deal with cyber risk management. This holistic application method should be the important topic for the next research too.

Reference

Antonucci Domentic. (2017). ***The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities.*** USA., New Jersey, John Wiley & Sons, Inc.

Cheange, S. (2009). Conceptual Model for Cybersecurity Readiness Assessement for Public Institutions In Developing Country: Cambodia, *IEEE Computer Society*: 1411 - 1418

Cochran, W.G. (1977). ***Sampling Techniques***. (3rd Ed). USA., New York: John Wiley and Sons, Inc.

Cronbach, L.J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16 (3): 297-334.

Dorfman, Mark S. (1997). ***Introduction to Risk Management and Insurance***. *(6th Ed)*, Prentice Hall.

Ponemon Institute. (2014). ***Global Report on the Cost of Cyber Crime 2014***. (https://www.octree.co.uk/Documents/2014- Global-Report-on-the-Costof)

Thai Reinsurance Public Co., Ltd. (2015).***Cyber Insurance Potential in Thailand***. (https://www.thaire.co.th/thaire_backend/upload/ourservices/publict_201512161 11050.pdf)

Radanliev P. et.al. (2018) Future developments in cyber risk assessment for the internet of things. *Computers in Industry,* 102: 14-22.

Rattanapongpinyo T. (2017) ***Fundamental of Risk Management*** *(2nd Ed)*. Bangkok, Thailand: P.A. Living Co., Ltd.

Waithaka Samuel. (2016). ***Factors Affecting Cyber Security in National Government Ministries in Kenya.*** Thesis of Master of Business Administration, Management of Information Systems, School of Business, University of Nairobi, Kenya.