CYBER RISK INSURANCE POLICY
A PROPOSED FRAMEWORK FOR
E-BUSINESS IN MALAYSIA

LEE SIOK HWEE

UNIVERSITI TEKNOLOGI MALAYSIA

CYBER RISK INSURANCE POLICY
A PROPOSED FRAMEWORK FOR
E-BUSINESS IN MALAYSIA

LEE SIOK HWEE

A dissertation submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

APRIL 2009

To my beloved family members and friends.

ACKNOWLEDGEMENT

I would like to express my gratitude to the people who have contributed to the successful completion of this project, especially my supervisor, Dr. Rabiah Ahmad, for her advices and guidance toward the accomplishment of this project. Without her guidance, my project would not be perfectly completed. Besides that, I would like to thank Dr. Zuraini Ismail and Dr. Maslin Masrom (panel of examiners) for their reviews, assessments and comments, which are significant in contributing toward the betterment of this project.

I am grateful to the online questionnaires and case study participants who shared their experience and valuable insights with me. I also wish to thank all those who supported this project with helpful suggestions, expertise and information.

I would like to express my gratitude to my sponsor, Tunku Abdul Rahman College (TARCollege), who has not only funded my studies but also provided me unlimited resources and understanding throughout the project period.

Last but not least, I am grateful to my beloved family members and friends who supported me unconditionally both physically and emotionally throughout the completion of this project.

ABSTRACT

Security risks can significantly affect the e-business company's reputation as well as the financial performance. Due to the increasing rate of the security breaches in Malaysia, the impacts should be handled with care to prevent the company from exposing to major financial and legal liabilities. E-business companies can manage their security risks by reducing it using technology like firewall, intrusion prevention tools, reducing the financial risk through insurance or maintaining the risk at an acceptable level. This research is aimed to propose an insurance procurement framework for both the insurer and the insured companies to promote a greater understanding of the alternatives of managing cyber risks. The research will study on the security structures and flows of the e-business in Malaysia context, review on the Internet computer crime and security issues locally and internationally, analyse on the international cyber-risk e-business and individual insurance policies and alternative solutions. A preliminary investigation was conducted on current business and individual insurance policy across various insurance companies in Malaysia. A survey on sample users for e-business and insurance companies in Malaysia on the effectiveness of the solution was done. Finally this research proposed a cyber-risk insurance policy framework to provide useful insights for policy formulation.

ABSTRAK

Risiko keselamatan boleh menyebabkan reputasi dan perlaksanaan kewangan sebuah syarikat terancam. Disebabkan kadar peningkatan pelanggaran keselamatan di Malaysia semakin tinggi, implikasinya haruslah ditangani dengan berhati-hati untuk mengelakkan syarikat tersebut daripada terlibat dengan liabiliti kewangan dan undang-undang. Syarikat e-bisnes boleh mengurus risiko keselamatan mereka dengan meggurangkannya dengan menggunakan teknologi seperti firewall, alat pengelakan penceroboh; mengurangkan risiko kewangan melalui insuran atau mengekalkan risiko pada tahap yang boleh diterima. Penyelidikan ini bertujuan mencadangkan sebuah rangka perolehan insuran kepada syarikat yang memberi dan yang membeli insuran supaya boleh menggalakkan pemahaman yang lebih kepada alternatif pengurusan risiko siber. Penyelidikan ini akan mengkaji struktur e-bisnes di dalam konteks Malaysia, mengkaji jenayah internet dan isu-isu keselamatan tempatan mahupun luar negara, menganalisi polisi insuran risiko siber untuk e-bisnes di luar negara dan tempatan. Satu tinjauan keberkesanan insuran siber terhadap sampel pengguna internet, e-bisnes dan syarikat insuran di Malaysia telah dilaksanakan. Akhirnya, penyelidikan ini menghasilkan sebuah cadangan rangka polisi insuran risiko siber supaya boleh membantu di dalam pembinaan polisi.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

This project discusses the needs to mitigate e-business financial loses to the insurance companies in Malaysia. The outcome of this project is to propose a cyber-risk insurance procurement framework for a greater understanding of the alternatives of managing cyber-risk attacks for the insurer as well as the insured.

This chapter describes the background problems of this project which in details shown the growth of e-business in Malaysia, cyber security breaches in Malaysia and the United States and the growing demands for cyber insurance worldwide. This chapter also describes the problem statements, objectives, scopes, requirements and plans of this project.

1.2 Problems Background

Internet has long been an important tool as the second life of people today. Many organizations and individuals agreed that it is a place of convenience, easy and within finger tips for business and daily activities. Yet it can vulnerable a company to information theft, vandalism and denial of service attacks. Computer breach has constantly growth without rest worldwide and soon to Malaysia since the Internet has become more popular locally.

E-business is defined as the use of networks and information technology to electronically design, market, buy, sell and deliver products and services worldwide (Turban, 2008). All businesses operate in a climate of insecurity, be that financial or otherwise. With the speed at which e-business is developing, "trust is becoming increasingly harder to establish and maintain" (Turban, 2008). The lack of face-to-face interaction in transactions and the anonymity of the Internet result in an impersonal style of business where trust must be implied but is not necessarily there. Turban (2008) notes that deliberately falsified information are also more difficult to detect. Some examples of the risks of doing e-business in Malaysia are sending rumours and defamatory messages to sending mails to unsuspecting banking customers and luring them to give out personal details to the more direct crimes, including transferring money from others' accounts, stealing critical information, etc. (Foo, 2004) and 26 cases of internet banking fraud and Keystroke Logging Trojans amounting to RM 200,000 were reported in 2005 (the Star).

Many of the companies who deal with internet business transaction have not covered with any cyber-risk insurance for reducing the risk of financial losses over the Internet as most of the Insurance companies in Malaysia cover only life, health, accident and physical business lost.

Though there are many security policies to serve as a guideline for employee to follow and practise and powerful protection, detection and correction systems are available for risk management, they might still be exposed to threats that could cause their organisation to loss severely from security breach. Therefore the risk should be transferred to third party company that is insurance to reduce their loss.

1.2.1 The growth of e-business in Malaysia

Online business in Malaysia is growing rapidly despite of the low demand for online products which has reported by the Small and Medium-sized Industries Association of Malaysia in the late 2005 (Internet#1) and its many problems like Internet security concerns, low broadband penetration rate and the absence of local consumer-protection laws.

This might be due to the strong support given by the Malaysia government on online business as we can see in its Ninth Malaysia Plan that has allocated RM12.9 billion for information and communication technology (ICT) programmes; RM5.7 billion is earmarked to computerise government ministries and agencies (Internet#2).

In the 2005 Economist Intelligence Unit e-readiness survey, Malaysia ranked 35th out of 65 countries, with a score of 5.43 out of 10. Malaysia ranked ahead of Thailand, Indonesia, India and China but behind Singapore, Hong Kong, South Korea and Taiwan (Internet#3). The survey measures how amenable a market is to Internet-based opportunities.

To help companies tap into electronic global supply networks, the 2002 budget granted RM5 millions for the development of RosettaNet (Internet#4), an

internationally standardised supply-chain-management platform, and extended income tax deductions for expenses incurred to implement it in Malaysia. RosettaNet itself launched its Asia engineering centre in northern Penang state in February 2004. Costs of developing websites have been deductible for income taxes since 2003, at 20% annually for five years.

A number of B2B Internet hubs have emerged, most centred on specific industries. Tradenex.com, the B2B electronic marketplace of the Federation of Malaysian Manufacturers, had enrolled more than 3,400 members in 28 different sectors by April 2006. Tradenex also takes part in the TIGeR (Technology, Industry and Government for the e-Economic Revolution) initiative to link Malaysian companies to global buyers and to roll out secure e-commerce services to manufacturing companies.

IDC Malaysia, a leading industry forecaster, estimates that local B2B e-commerce was worth RM28.5 billion in 2005. This marks a growth of 88% on the 2004, and IDC Malaysia forecasts expansion of the market by 77% in 2006 (Internet#5).

The Ministry of Agriculture and the Malaysian Institute of Microelectronics Systems (MIMOS), a government-linked information-technology firm, launched the AgriBazaar.com.my website on January 1st 2004. AgriBazaar enables the buying and selling of farm produce via the Internet. More than 10,000 participants had signed on by April 2006. MIMOS is also involved, along with the Ministry of Plantation Industries and Commodities, Multimedia Development Corp, Malaysian Palm Oil Association, Ministry of Science, Technology and Innovation, and others, in the Oilpalmworld.com website, which was launched on August 9th 2005. The site aims to become the main electronic exchange for all commerce functions of the global palm-oil industry, including trading. Malaysia is the world’s largest producer of palm oil. A total of 531 companies from 62 countries had signed up by April 2006.

Though eBay, a giant US Internet auction site, expanded its operations into Malaysia in December 2004, a domestic auctioneer, Lelong, remained the leading domestic auction site in April 2006.

Dagang Net operates the national Electronic Data Interchange (EDI) system and provides other electronic trade-facilitation services. All major sea- and airports now use the EDI system, and in April 2006 Dagang Net was in the process of implementing its e-Permit Project, which would see all 24 permit-issuing government agencies issue their permits electronically. Dagang Net, 60% owned by Time Engineering (a major Malaysian telecoms provider), expects a 16% rise in revenue in 2006, to RM58 million, from RM50 million in 2005 (Internet#6).

MASkargo, the cargo arm of Malaysian Airline System, the national flag carrier, launched three new e-commerce initiatives in December 2004: an enhanced website; an electronic-sales facility; and an electronic billing, presentment and payment system. The website (www.maskargo.com) allows a user to check schedules as well as to track online shipments, and it also features improved navigation and access. The electronic-sales facility lets MASkargo market its products proactively via e-mails and text messages to targeted customers. Among the available products is one that offers customers discounts on selected routes and another that sends text messages and e-mails to customers informing them of available discounted flights packages. The payment system supports interbank fund transfers using Bank Negara Malaysia's Financial Processing Exchange, which manages and facilitates online payments for e-commerce transactions.

The Small and Medium Industries Development Corp (SMIDEC), a government agency, estimates that only about 20% of Malaysia's 100,000 manufacturers have an online presence (Internet#7). Through SMIDEC, small and medium-sized enterprises can apply for soft loans of up to RM250,000 to use information and communications technology to improve competitiveness, efficiency and productivity. In general, eligible companies must have annual sales of less than

RM25 million, employ fewer than 150 persons and be at least 60% Malaysian owned to qualify for SMIDEC loans and grants. SMIDEC also administers grants to implement RosettaNet.

Nearly all of Malaysia's banks offer online banking services. Maybank, the nation's largest, became the first to offer electronic banking to retail customers in June 2000, with its portal Maybank2u.com. The site has since expanded to offer services to both individuals and businesses. Customers can use the site to open accounts, pay bills to more than 100 companies, check balances, buy and sell shares, renew insurance policies and conduct many other financial-services transactions. On April 6th 2006 Maybank and Celcom, a mobile-phone company, launched a service to conduct banking transactions via mobile phone. Foreign banks have been allowed to offer online services since January 1st 2002; HSBC (UK), Citibank (US), OCBC and UOB (both of Singapore) offer electronic banking.

The Malaysian Communications and Multimedia Commission (MCMC), established in 1998, reported 11 million Internet users at end-2005, up by 11% from 9.9 million a year earlier and representing more than 40% of the population. There were 490,630 broadband subscriptions at end-2005, compared with 252,500 a year earlier. The number of dial-up connections rose by 11.5% in 2005, to 3.7m by year-end (Internet#8).

According to a mid-2005 survey by the MCMC, only 9.3% of Internet users had purchased products or services through the Internet during the preceding three months. Among those who did so, airline tickets were the most popular items (43.8%) followed by books (15.6%) and music (6.8%). Amounts spent on these items were small, however, with 57.7% of transactions worth less than M$500.

IDC Malaysia, a leading industry forecaster, estimates that IT spending on software, hardware and services reached RM13.3 billion in 2005, up from RM10.3

billion the previous year. Spending is expected to come mainly from telecommunications and manufacturing. Expenditures are forecast to grow by 12% in 2006. This IDC study analyses Malaysia's total broadband services market that is anticipated to grow to 3.3 million subscribers by 2012. The national telecom regulator MCMC is entrusted to push the Broadband Plan specifically for Klang Valley (KVB90) initiatives, which aims to proliferate up to 90% household broadband penetration by 2010 in the Klang Valley (Internet#8).

Since the government plans to foster growth in electronic communications mainly through private enterprise, the MCMC's major practical responsibilities are licensing and regulation. By April 2006 the commission had granted 62 licences for application service providers (ASPs), 64 for network service providers (NSPs) and 58 to network facilities providers (NFPs) (Internet#9).

Six companies, including the government-run Malaysian Institute of Microelectronics Systems (MIMOS), have licences to operate as Internet service providers (ISPs), though two control the market: MIMOS, through Jaring; and Telekom Malaysia, through TMnet. Celcom Net, Time Net, Digi Net and Maxis Net are other, much smaller, ISPs. Though all ISPs offer broadband connections, the market still consists mainly of dial-up connections.

There were 11,821 registrations of Malaysian Internet domain names (that is, carrying .my as part of their URL) in 2005, compared with 10,248 in 2004, according to the Malaysian Network Information Centre (MYNIC) (Internet#10). There were 641,015 Malaysian Internet domain names at end-2008; nearly all of those (61,427) were .com.my domains. MYNIC, which has its offices at MIMOS, administers registration of domain names in Malaysia. MYNIC also offers a domain-name dispute-resolution service; if disputes over a .my domain cannot be resolved through negotiations, complaints can be filed with the Regional Centre for Arbitration in Kuala Lumpur.

1.2.2 Cyber Security Breaches in Malaysia

The growth of e-business in Malaysia has lead to problems like cyber security breaches which causes the company to suffer from great financial losses. According to data extracted from Cyber Security Malaysia, the trend of total security breach in Malaysia is increasing every year and it shown a drastic flight after 2005. There are nine most significant threats reported which are Mailbomb, Harrassment, Fraud, Hack Threat, Virus, Denial of Service, Destruction, Intrusion and Spam in august, 2008. The top four threats reported are Spam that alone booms rapidly and recorded 36, 425 cases in year 2008, followed by Intrusion, 355 cases; Fraud, 464 cases and Virus 197 cases (see Appendix I).

1.2.3 Cyber Security Breaches in the United States

Cyber security breaches had not only occurs widely in Malaysia but also happened in the United States and other countries far long ago. The earliest event is when the Microsoft Hotmail Web site was defaced and customer accounts were accessed (see Appendix J). Other events include hacking of the Staples.com site and the more malicious attack on the Internet music store eUniverse, when a supposed Russian hacker stole over 300,000 customer credit card numbers. Later, some of the biggest icons of the Internet, such as Amazon, Yahoo, CNN and eBay were attacked by denial of service where they suffered a deluge of service request, a magnitude greater than its normal volume that has crippled the site. Burger King and British Telecom who were outside of the United States also affected by having their Web sites defaced.

These attacks showed the true vulnerabilities of the Internet and increased awareness on the financial impacts of security breaches, including the lost revenue

due to downtime, systems recovery costs and damage to brand reputation and customer perception.

1.2.4 Growing Demand for Cyber-Insurance

The growing cyber-threat is highlighting the need for risk mitigation strategies such as cyber-risk insurance. Currently, none of the insurance company in Malaysia covers cyber-risk insurance. However, in 2002, at least two dozen insurance companies in the United States have already offered cyber-policies, like Chubb, Lloyd's of London, Zurich North America, and American International Group. Cyber-risk insurance policies often have higher premiums and deductibles because of the uncertainties in assessing cyber-risk (Kolodzinski, 2002). USA Today (Swartz, 2003) reported that the average cost for cyber-insurance ranges from $5,000 to $30,000 per year for $1 million in coverage.

After only three years in the market, network risk insurance or "hacker insurance" coverage reached about $100 million in 2002 and was expected to reach $2.5 billion by 2005, according to insurance industry projections (Keating, 2003). The United States' National Strategy to Secure Cyberspace report recommends insurance "as a means of transferring risk and providing for business continuity" (Internet#11). The 2001 Code Red Worm incident cost its victims and insurance companies an estimated $2 billion in damage. The research organization Computer Economics estimates that damages caused by The Love Bug, Melissa, Code Red, and other incidents have exceeded $54 billion in downtime, removal expenses, and repairs (Geralds, 2003). A survey of 500 U.S. companies showed an increase in reported financial losses of 21%, or $455.8 million, in 2002. In addition, those losses are increasingly the result of organized, planned cyber-attacks (Internet#12). According to Ernst and Young, security occurrences can cost companies between $17 and $28 million per incident (Garg *et al.*, 2003). There are hundreds of millions

of Internet-connected computers worldwide, nearly two billion Internet-enabled mobile devices, and one billion users of Internet messaging. These growing numbers suggest that companies will have a host of new security concerns (Gross, 2003). As cyber-related incidents continue, demand for insurance to cover losses related to electronic theft, vandalism, and extortion will likely increase.

1.3 Problem Statements

(a) Security breach will likely occur even with the best security management system.

(b) There is a need to reduce the cyber-risk financial lost to the minimal acceptable value.

(c) There is no insurance policy coverage for securing e-business in Malaysia.

(d) There is no available cyber-risk insurance policy framework for insurance company's references in Malaysia.

1.4 Project Objectives

(a) To identify the need of insurance as a new form of cyber risk solution in Malaysia.

(b) To identify the preparedness level of security management system over the Internet business in Malaysia.

(c) To propose an insurance policy framework for cyber-risk mitigation in securing e-business in Malaysia.

1.5 Project Scope

(a) This project reviewed the security structures and flows of e-banking and e-shopping in Malaysia.

(b) There are three insurance, two e-banking and five e-shopping companies involved in the interview.

(c) This project proposed cyber risk insurance policy framework.

(d) This project recommended cyber risk insurance policy coverage.

1.6 Summary

This chapter provides an overview on the purposes and needs to develop this project. The importance of securing e-business was highlights through the analysis of cyber security breach statistics and the growth of e-business in Malaysia. In the next chapter, literature review on four cyber risk insurance policy frameworks will be discussed.

REFERENCES

Bohme, R. (2005). Cyber-Insurance Revisited, *Workshop on the Economics of Information Security (WEIS) 2005, USA.*

Creswell, J. W. (2008). Research Design: *Qualitative, Quantitative, and Mixed Methods Approaches*, Sage Publications, Inc; 3rd edition

Drouin, D. (2004). Cyber Risk Insurance, *A Discourse and Preparatory Guide*, February 9, 2004, GIAC Security Essentials Certification, SANS Institute 2004.

Foo E. J. (2004). Cybercrime Activities on the Rise *22nd November 2004 (Computimes)*, CyberSecurity News 2004.

Garg, A., Curtis, J., and Halper, H. (2003). The Financial Impact of IT Security Breaches: What do Investors Think? *Information Systems Security*, *12*(1), 22–34.

Geralds, J. (2003). Hacker insurance set to rocket - Value of hacker policies still unclear though, warn analysts, *Silicon Valley*, 14 Feb 2003; *http://www.vnunet.com/vnunet/news/2121538/hacker-insurance-set-rocket*

Gordon, L., Martin, p.L., and Sohail, T., (2003). A Framework for Using Insurance for Cyber-Risk Management, March 2003/vol. 46, no. 3 *Communications of the ACM*.

Gross, G. (2003). Net Attacks Down but Sophistication Is Up. *IDG News Service*, January 30.

Iarossi, G. (2006). The Power of Survey Design: *A User's Guide for Managing Surveys, Interpreting Results, and Influencing Respondents,* World Bank Publications; 1st edition.

ISO/IEC FDIS 17799: 2005-02-11: Information technology — Security techniques — Code of practice for information security management (2nd edition).

Keating, G. (2003). Hacker Insurance Market Boosted by Cyberattacks. *Reuters,* January 27.

Kenneth, J. and William, R. (2006). Cyber-Warefare Threatens Corporations: *Expansion into commercial environments*, www.ism.journal.com, Spring 2006.

Kolodzinski, O. (2002). Cyber-Insurance Issues: Managing Risk by Tying Network Security to Business Goals.

Lerdorf, R. and Tatroe, K. (2002). Programming PHP, O'Reilly Media, Inc.

Lallmahamood, M. (2007). An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of This and Their Intention to use E-commerce: Using an Extension of the Technology Acceptance Model, *Journal of Internet Banking and Commerce, December 2007, vol.12, no. 3.*

Mukhopadhya, A., Chatterjee, S., Roy, R., Saha, D., Mahanti, A., and Sadhukhan, S. K. (2007). Insuring big losses due to security breaches through Insurance: A business model, *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, IEEE.

Prasanna (2006). Security of IT Assets and the Diffusion of Cyber Insurance.

Swartz, J. (2003). Firms' hacking-related insurance costs soar, *USA TODAY*; *http://www.usatoday.com/money/industries/technology/2003-02-09-hacker_x.htm*

Turban, E., King, D., McKay, D., Marshall, P., Lee, J., and Viehland, D. (2008). Electronic Commerce 2008, *A Managerial Perspective,* Pearson Education, Inc.

Internet#1 Small and Medium-sized Industries Association of Malaysia official website; *http://www.smisme.com/index.php*

Internet#2 Federal government development allocation and expenditure by sector, 2001-2010; *http://www.epu.jpm.my/RM9/english/allocation1.pdf*

Internet#3 Technopreneur Development Division Portal; *http://www.technopreneurdevelopment.net.my*

Internet#4 Official Portal of Ministry of International Trade and Industry Malaysia; *http://portal.miti.gov.my/*

Internet#5 *www.mida.gov.my/beta/pdf/press_report2005.pdf*

Internet#6 Dagang Net; *http://www.dagangnet.com/*

Internet#7 *www.undp.org.my/uploads/UNDP_SME_Publication.pdf*

Internet#8 The Malaysian Communications And Multimedia Commission Official website; *www.skmm.gov.my/what_we_do/Research/Industry%20studies/Analysis_Adex_Size08.pdf*

Internet#9 The Malaysian Communications And Multimedia Commission Official *website; http://www.skmm.gov.my/facts_figures/stats/index.asp*

Internet#10 MYNIC - Administrator Of The .my Domain Name; *http://www.mynic.net.my/statistics.php*

Internet#11 National Infrastructure Advisory Council (NIAC), *National Strategy to Secure Cyberspace report*; *http://www.whitehouse.gov/pcipb*

Internet#12 CSI Computer Security Institute; www.gocsi.com

Internet#13 www.gauntlettlaw.com/insurance.htm

Internet#14 DataQuest, *Cyber Media Publication*, Jan15, 2006