An Analysis of Internet Banking Security of Foreign Subsidiary Banks in Australia: A Customer Perspective

Panida Subsorn[1] and Sunsern Limwiriyakul[2]

[1] Department of Information Technology, Suan Dusit Rajabhat University
Bangkok, 10300, Thailand

[2] SECAU, Edith Cowan University
Joondalup, 6027, Western Australia

Abstract

Internet banking has been deployed more frequently over the past few decades to support and improve the operational and managerial performance within the banking industry. However, the security issues of confidentiality, integrity and privacy have become increasingly more serious concerns in Internet banking systems because of the potential negative impact on the banks and its customers. In a previous research paper, the security of the Internet banking systems of 16 selected Australian banks was examined. This paper further examines Internet banking security in nine foreign subsidiary banks in Australia for comparison with the results and findings of the previous research in order to produce a more practical and comprehensive guideline, as well as to include a weight rating of security related website information for the banking industry in Australia. The findings of both the previous research paper and this paper revealed that there was lack of related Internet banking security information in all the selected Australian owned and foreign owned banks' websites which have the potential to impact on the confidentiality of the banks and its customers as well as future potential customers.

Keywords: *Australia, customer perspective, foreign subsidiary banks, internet banking security.*

1. Introduction

Most industries have deployed internet technologies as an essential part of their business operations [1], [2], [3], [4]. The banking industry is one of the industries that has adopted internet technologies for their business operations and in their plans, policies and strategies to be more accessible, convenient, competitive and economical as an industry [3]-[8]. The aim of these strategies was to provide internet banking customers the facilities to access and manage their bank accounts easily and globally [2]-[4], [9].

Nevertheless, there are inherent information security threats and risks associated with the use of internet banking systems that can be variously classified as low, medium and high [3], [4], [10]. In particular the confidentiality, privacy and security of internet banking transactions and personal information are the major concerns for both the banking industry and internet banking customers [3], [4], [6], [11]. For instance, adware, keyloggers, malware, phishing, spyware, Trojans and viruses are currently the most common internet banking security threats and risks [3], [4], [12]-[14].

As a follow up to the previous investigation of 16 selected Australian banks, nine foreign subsidiary banks in Australia were scrutinized on the security of their internet banking systems. The prime objective of this paper was to assess their security weaknesses through a checklist based on the information provided on the banks' websites. The purpose of the checklist was to provide an idea of internet banking security background and information for the banks' internet banking customers and also for prospective new customers. The inclusion of a weight rating in each main category of the checklist for the nine foreign subsidiary banks was aimed at providing a more practical and comprehensive guideline.

In addition, this research also provided a comparative analysis between the nine foreign subsidiary banks and the previously investigated 16 Australian owned banks. The creation of the security weighting was also included for the 16 Australian owned banks for the purposes of the comparative analysis.

2. Methodology

This paper deployed a comparative analysis approach as a qualitative research method in two major parts. Firstly, the accessibility of internet banking security features of the foreign subsidiary banks was examined through a descriptive analysis. The results were then compared to the 16 selected Australian owned banks in order to evaluate the dissimilarity in the internet banking security features between the two entities.

2.1 Sample

Nine foreign subsidiary banks were selected to fulfill the aim of this paper of creating an internet banking security checklist as they provided a good basis for the comparative analysis. The list of the foreign subsidiary banks utilized in this analysis is presented in Table 1 [15, p. 1], [16, pp. 1-3].

Table 1: The list of foreign subsidiary banks used in the analysis

Count no.	Banks	Headquarters
1	Arab Bank Australia Limited	Sydney
2	Bank of China (Australia) Limited	Sydney
3	Bank of Cyprus Australia Limited	Melbourne
4	Beirut Hellenic Bank Limited	Sydney
5	Citigroup Pty Limited	Sydney
6	HSBC Bank Australia Limited	Sydney
7	ING Direct (the trading name of ING Bank (Australia) Limited)	Sydney
8	Investec Bank (Australia) Limited	Sydney
9	Rabobank Australia Limited	Sydney

2.2 Data collection

In order to examine the internet banking security features in each of the foreign subsidiary banks, this paper used a secondary data source that was publicly available via the selected banks' websites. Additionally, we applied and modified the internet banking security checklist from our previous research paper for assessing the security features of the selected foreign subsidiary banks.

2.3 The internet banking security checklist

The internet banking security checklist consists of six main security feature categories that these selected foreign subsidiary banks provided to their internet banking customers. Details of each category of the checklist are displayed in Table 2.

Table 2: The six main security feature categories deployed in the analysis

Numbers	Category names	Descriptions
1	General online security and privacy information to the internet banking customers	• account aggregation or privacy and confidentiality • losses compensation guarantee • online/internet banking security information • bank security mechanism system
2	Information Technology (IT) assistance, monitoring and support	• hotline/helpdesk service availability • internet banking transaction monitoring by the banks
3	Software and system requirements and settings information	• compatibility "best" with the popular internet browsers • internet banking user device system and browser setting requirement • free/paid security software/tool available to the internet banking customers
4	Bank site authentication technology	• employed encryption and digital certificate technologies
5	User site authentication technology	• two-factor authentication for logon and/or for transaction verification available • logon requirement, failure limitation and user input type • scramble an on-screen input keypad • password restriction/requirement • transaction verification
6	Internet banking application	• automatic timeout feature for inactivity

	security features	• limited default daily transfer amount to third party account/BPAY/international transactions • logging information • notifications and alerts • session management

2.4 The scoring technique

Each of the sub categories was assigned a maximum potential score of 10 points. The sub-points in each of the sub categories were assigned a value based on item's importance according to present knowledge.

3. Analysis

In order for the reader to evaluate the checklist, a system of coding was employed as a legend to the checklist. This legend coding and translations are presented in Table 3. Table 3 presents and summarizes the analysis and results findings with the discussions in the following sub sections.

	Represents		Represents		Represents
✓	Yes	*	Optional	NA	Not applicable
NI	No information	A	AES 256-bit encryption	D	3DES-EDE-CBC 168-bit encryption
R	RC4 128-bit encryption	V	VeriSign Authentication Services		

Table 3: A summary of the proposed internet banking security checklist

Internet banking information security checklist											
	Security feature categories	**Foreign-owned banks**									**Weight**
		Arab bank	**Bank of China**	**Bank of Cyprus**	**Beirut Hellenic**	**Citibank**	**HSBC**	**ING**	**Investec bank**	**Rabobank**	
1. General online security and privacy information to the internet banking customers											
1.1	**Account aggregation or privacy and confidentiality**										**10**
1.1.1	Complied with the National Privacy Principles and the Privacy Act	✓	NI	✓	✓	✓	✓	✓	✓	✓	10
1.2	**Losses compensation guarantee**										**10**
1.2.1	100%	✓	✓	✓	✓	✓	✓	✓	✓	✓	10
1.2.2	No any information										0
1.3	**Online/internet banking security information**										**10**
1.3.1	Threats: Hoax email, scam, phishing, spyware	✓				✓	✓	✓	✓		2
1.3.2	Virus and Trojan	✓				✓	✓	✓	✓		2
1.3.2	Keyloggers					✓	✓		✓		1
1.3.3	General online security guidelines	✓	✓	✓	✓	✓	✓	✓	✓	✓	2
1.3.4	Security alert/up-to-date issue	✓	✓			✓				✓	1
1.3.5	Provides password security tips	✓	✓		✓		✓				2
1.4	**Bank security mechanism system**										**10**
1.4.1	Antivirus protection						✓				2.5
1.4.2	Firewall(s)						✓			✓	2.5
1.4.3	IDS/alert system										2.5
1.4.4	Others (e.g. data encryption, password protected, physical security)			✓					✓	✓	2.5
1.4.5	No any information	✓	✓		✓	✓		✓			0

2. IT assistance, monitoring and support											
2.1	**Hotline/helpdesk service availability for internet banking customer**										**10**
2.1.1	24/7 customer contact centre by phone **OR**		✓			✓		✓			5
2.1.2	Not 24/7 customer contact centre by phone	✓		✓	✓		✓		✓	✓	3
2.1.3	Secured email	NI	NI			NI	✓	✓			2
2.1.4	Email	NI	NI			NI	NI	✓	✓		1
2.1.5	FAQ/online support form	✓	✓			✓	✓	✓	✓	✓	2
2.1.5	No any information										0
2.2	**Internet banking transaction monitoring by the banks**										**10**
2.2.1	Provides dedicated team and technology for monitoring all transactions					✓		✓			10
2.2.2	No any information	✓	✓	✓	✓		✓		✓	✓	0
3. Software and system requirements and settings information based on the bank website's information											
3.1	**Compatibility "best" with the popular internet browsers**										**10**
3.1.1	Google Chrome				✓	✓		✓			2
3.1.2	Firefox				✓	✓	✓	✓		✓	2
3.1.3	Internet Explorer		✓		✓	✓	✓	✓		✓	2
3.1.4	Netscape						✓				2
3.1.5	Opera				✓						1
3.1.6	Safari				✓	✓		✓			1
3.1.7	No any information	✓		✓					✓		0
3.2	**Internet banking user device system and browser setting requirement**										**10**
3.2.1	Operating system		✓		✓	✓	✓				2
3.2.2	Type of browser		✓		✓	✓	✓	✓			2
3.2.3	Browser setting (e.g. cookie, pop-up windows)									✓	2
3.2.4	Screen resolution		✓		✓		✓			✓	2
3.2.5	Browser automatic or manual test feature available										2
3.2.6	No any information	✓		✓					✓		0
3.3	**Free/paid security software/tool available to the internet banking customers**										**10**
3.3.1	Antivirus/anti-spyware										7
3.3.2	Internet security suite										10
3.3.3	Provides internet links/information to security software vendor(s)						✓		✓		5
3.3.4	No any information	✓	✓	✓	✓	✓		✓		✓	0
4. Bank site authentication technology											
4.1	**Employed encryption and digital certificate technologies**										**10**
4.1.1	SSL 128/168-bit encryption **OR**	R	R	R	R	R	R	R	D	R	5
4.1.2	SSL 256-bit encryption										6
4.1.3	Extended validation SSL certificates	✓	✓		✓	✓	✓	✓	✓	✓	2
4.1.4	Signing CA	V	V	V	V	V	V	V	V	V	2
5. User site authentication technology											
5.1	**Two-factor authentication for transaction verification available**										**10**
5.1.1	Token device (no. of digit pins) **OR**		6	✓	✓		✓	✓	✓	✓	10
5.1.2	SMS (no. of digit pins) **OR**	✓	✓		✓			✓	✓		10
5.1.2	Others (e.g. USB key digital certificate)		✓								10
5.1.3	Not in use					✓					0
5.2	**Logon requirement**										**10**
5.2.1	Bank/credit cards number or bank register/customer ID or email address	✓	✓	✓	✓	✓	✓	✓	✓	✓	2.5
5.2.2	Password/ personal code or security number	✓	✓	✓	✓	✓	✓	✓	✓	✓	2.5
5.2.3	Others (e.g. CAPTCHA, security question)		✓			✓					1
5.2.4	Two-factor authentication		✓		✓		✓		✓	✓	4
5.3	**Logon failure limitation**										**10**

5.3.1	Standard max. (3 times) **OR**	✓						✓			10
5.3.2	Max. more than 3 times **OR**		5								8
5.3.3	In use but does not specific maximum number of failure allowed						✓				5
5.3.4	No any information			✓	✓	✓			✓	✓	0
5.4	**Logon user input type**										**10**
5.4.1	Keyboard **AND/OR**	✓	✓	✓	✓	✓	✓	✓	✓	✓	8
5.4.2	Keypad	✓		✓		✓		✓			10
5.5	**Scramble an on-screen input keypad**										
5.5.1	Customer ID		NA		NA		NA		NA	NA	0
5.5.2	Password	✓	NA	✓	NA		NA	✓	NA	NA	0
5.6	**Password restriction/requirement**										**10**
5.6.1	Enforce good password practice		✓			✓	NI	NI	NI	NI	2
5.6.2	Password/pin length (minimum)		8-20			8-16	6	6	NI	4	1
5.6.3	Combination of numbers and letters		✓			✓	*	NI	✓		1
5.6.4	Combination of upper and lower cases		✓				NI	NI	✓		1
5.6.5	Special characters		NI			✓	NI	NI			1
5.6.6	Different passwords as compared to any of three previous used passwords		NI			3	NI	NI	NI		1
5.6.7	Cannot have three or more of the same characters in a row (e.g. aaa, 111)		✓			✓	NI	NI	NI	NI	1
5.6.8	Cannot have three or more consecutive characters (e.g. abc, 123)		✓			✓	NI	NI	NI		1
5.6.9	Automatically check password strength when creating or changing password		NI			NI	NI	NI	NI	NI	1
5.6.10	No any information	✓		✓	✓						0
5.7	**Transaction verification**										**10**
5.7.1	External transactions required token/SMS/extra password	✓	✓	✓	✓	✓	✓	✓	✓		10
5.7.2	Not required										0
5.7.3	No any information									✓	0
6. Internet banking application security features											
6.1	**Automatic timeout feature for inactivity**										**10**
6.1.1	Max. (mins) **OR**	8									10
6.1.2	In use but does not specify timeout length		✓		✓		✓				8
6.1.3	No any information			✓		✓		✓	✓	✓	0
6.2	**Limited default daily transfer amount to third party account/BPAY/international transactions**										**10**
6.2.1	Less or up to $5,000 AUD	NI			✓			NI			10
6.2.2	More than $5,000 AUD	NI	✓			✓	✓	NI			9
6.2.3	The default maximum daily limit transfer is vary depend on the type of the internet banking customer	✓	✓		✓	NI	NI	✓			0
6.2.4	The maximum daily limit transfer may be increased with the approval by the banks		✓		✓	✓	✓				0
6.2.5	No any information			✓					✓	✓	0
6.3	**Logging information and alert**										**10**
6.3.1	Last login	NI	NI		NI	✓		✓			4
6.3.2	Activity log	NI	NI		NI	NI		NI			4
6.3.3	Alert available via email and/or SMS	✓	✓		✓			✓			2
6.3.4	No any information			✓			✓		✓	✓	0
6.4	**Session management**										**10**
6.4.1	Use cookies technology **OR**					✓	✓		✓	✓	7
6.4.2	Use page tokens **OR**										10
6.4.3	Use session tokens										10

6.4.4	Use cookies for other purposes (e.g. marketing)					✓	✓				0
6.4.5	No any information	✓	✓	✓	✓			✓			0

3.1 Account aggregation or privacy and confidentiality

Only one (Bank of China) out of the nine foreign selected banks did not provide information regarding account aggregation or privacy and confidentiality. However, all of the nine selected banks did provide a total loss compensation guarantee to its customers in terms of any loss that occur related to any unauthorized internet banking transacted without the customer involved. See Sections 1.1 and 1.2 in Table 3 for more details.

3.2 Information on internet banking security and bank security mechanism system

In terms of internet banking security information, Bank of Cyprus, Beirut Hellenic and Rabobank have provided less information than the other remaining banks. In addition, five out of the nine selected banks have not provided any web information on the banking security mechanism being used in their system. The provision of online and internet security information will increase the level of security awareness to the bank's existing and potential customers. Moreover, by providing information of the bank security mechanism can increase bank's customers confidence in internet banking. See Table 3 in Sections 1.3 and 1.4 for more details.

3.3 Encryption and digital certificate

Eight out of the nine selected banks or 87.5 percent, deployed extended validation SSL certificates except bank of Cyprus. As stated by [17, p. 1] the use of the extended validation SSL certificate can provide clearer website identity as compared to the non-extended validation SSL certificate. Furthermore, eight out of the nine selected banks used 128 bit-encryption whereas the remaining one (Investec bank) used 168 bit-encryption. Changing to extended validation SSL certificate as well as increasing to the encryption to 256 bits can offer maximum security within the current technology for bank site authentication. This measure can also increase the confidence in internet security to both its existing and potential customers. Additionally, all of the nine selected banks used VeriSign Authentication Services for their certificate authentication (CA). See Section 4.1 in Table 3 for more details.

3.4 IT hotline/helpdesk support and monitoring

In terms of IT helpdesk provided through telephone support for internet banking system issues, only three out of the nine selected banks or 33 percent provided 24/7 support, whereas the remaining six selected banks provided normal or partly covered after hours telephony support. For example, the contactable times of HSBC Internet banking telephone support service were available from 8 a.m. to 8 p.m. on Monday to Friday. Consequently, providing 24/7 IT helpdesk can increase both the convenience and confidence to the banks' customers. Seven out of the nine selected banks or 78 percent did not provide any information in relation to the monitoring of internet banking transactions by the banks. More details in Sections 2.1 and Section 2.2 in Table 3.

3.5 Two-factor authentication and logon requirement

Only Citibank did not employ two-factor authentication for its internet banking customers. The other eight selected banks have supplied various two-factor authentication technologies such as token, SMS or USB key digital certificate to their customers. However, only five out of the eight selected banks have made the two-way authentication technique compulsory at logon to their internet banking facilities from the website. In addition, the Bank of China and Citibank required an extra input field to be entered at logon apart from username and password. For example, a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) and security/secret question. This method of the extra input field can provide an additional level of security at logon. See Table 3 in Sections 5.1 and 5.2 for more details.

3.6 Logon user input type

Four out of the nine selected banks used a combination of both keyboard and keypad for entering a user ID, a bank register ID, a bank card number or an email address. Three out of the four selected banks apart from Citibank, have utilized a scramble method on their keypad which is modified every time when the bank's webpage is opened. This additional technique provides a better security protection against keystroke attacks. See Sections 5.4 and 5.5 in Table 3 for more details.

3.7 Password requirements/restrictions

Three (Arab bank, Bank of Cyprus and Beirut Hellenic) out of the nine selected banks did not provide information regarding password requirements or restrictions. Rabobank and ING bank only required a password length of four and six characters respectively. Increasing the minimum password length to eight or more characters, can

considerably strengthen the passwords. Furthermore, only Citibank required its customers the use of special characters to be included into the customer password. Again, combining special characters into a password increases the password strength. In terms of a mechanism for automatically checking password strength, there was no information on all of the nine selected banks. The inclusion of a mechanism that indicates the strength of the password can assist the banks' customers to generate strong passwords. See Section 5.6 in Table 3 for more information.

3.8 Software and system requirements and available of protection software

In terms of software and system requirements including settings, three out of the nine selected banks did not provide any information on their website. Furthermore, seven out of the nine selected banks did not provide any access to free/paid virus or related protection software or alternatives through a web link.

3.9 Logging information, alert and session management

The Bank of Cyprus, HSBC, Investec bank and Rabobank did not provide any logging information such as last login, activity logs and alerts on their websites. With regard to session management, five of out of the nine selected banks have not provided any information on their websites. Citibank and HSBC have used cookie technology for their marketing purpose.

4. Comparison between the selected Australian domestic and the selected foreign-owned banks

The overall comparative analysis details on each of the six main categories as previously discussed in the analysis section were calculated and presented in Table 4 together with the summarized details of the 16 selected Australian local banks which were investigated in the previous research. In addition, the total marks and the percentages were calculated based on the results of the total combination of all checked marks from all sub categories including all sub sections in each sub category.

Table 4: A summary comparison information between the 16 selected Australian local and the 9 selected Australian foreign-owned banks

Bank	Category							
	1 40 marks	**2** 20 marks	**3** 30 marks	**4** 10 marks	**5** 60 marks	**6** 40 marks	**Total** 200	**%** 100
Local banks – four major banks								
ANZ	31.5	19	23	8	29	10	120.5	60.25
CBA	30.5	19	19	10	46	28	152.5	76.25
NAB	28.5	17	13	8	48	10	124.5	62.25
Westpac	30.5	17	17	10	40	9	123.5	61.75
Local banks – competitor banks								
Adelaide	26	7	14	7	25	0	79	39.5
AMP	31.5	17	16	9	20	20	113.5	56.75
Bank of Queensland	23	19	15	9	52	19	137	68.5
Bankwest	28.5	19	25	9	23	20	124.5	62.25
Bendigo	21.5	17	15	8	51	35	147.5	73.75
Macquarie bank	12	3	0	7	13	0	35	17.5
Members Equity	16	7	10	7	25	9	74	37
Rural	21.5	17	11	8	41	26	124.5	62.25
Suncorp-Metway	30.5	19	23	9	52	28	161.5	80.75
Local banks – sub banks								
Bank of South Australia	35	19	11	9	24	26	124	62
St. George	35	19	11	9	24	26	124	62
UBank	24.5	17	9	9	47	19	125.5	62.75
Foreign-owned banks								
Arab bank	29	5	0	9	45	12	100	50
Bank of China	15	7	8	9	53	21	113	56.5
Bank of Cyprus	24.5	3	0	7	35	0	69.5	34.75
Beirut Hellenic bank	24	3	14	9	37	20	107	53.5
Citibank	28	17	11	9	43	20	119	59.5

HSBC	34	7	14	9	49	24	137	68.5
ING	26	20	9	9	46	6	116	58
Investec bank	29.5	7	2	9	39	7	93.5	46.75
Rabobank	28	5	8	9	28	7	85	42.5

5. Conclusions and recommendations

All of the selected Australian owned and foreign-owned banks have scored high in Category 4 (employed encryption and digital certificate technologies). In terms of Category 5 (user site authentication technology), all of the foreign-owned banks except Rabobank have scored reasonably with 35 of out 60 marks. In addition, all of the selected foreign-owned banks should consider providing more information on their websites with regards to Category 6 (internet banking application security features). Furthermore, most of the selected foreign-owned banks have been deficient in providing internet banking security information related to free/paid security software/tool to their internet banking customers (Section 3.3). Providing such information will increase security awareness to both the current and future potential internet banking customers. In terms of multi-languages, only the Bank of China provided this feature which allows its internet banking customers to choose either English or Chinese language. As Australia becomes more multicultural, the multi-languages feature would enhance the internet banking website experience as it will provide language alternatives such as Arabic, Chinese and Japanese, to internet banking customers.

All the Australian owned and foreign-owned banks may utilize the checklist in order to standardize their internet banking websites particularly in terms of security as well as usability. This can increase internet banking security and usability as well as improve confidentiality to their existing and potential internet banking customers. Finally, the results and findings from the internet banking security checklist can provide a more applicable internet banking security checklist for foreign subsidiary banks. Moreover, other related organisations can benefit from this practical guideline as they can deploy the findings to enhance their own management on internet banking security systems as an external validity.

Acknowledgments

We would like to express our deep appreciation and sincere thanks to Associate Professor Ken Fowle and Mr. Yunous Vagh for providing us with all the necessary advices to contribute the idea and complete this paper.

References

[1] Gunasekaran, A., & Love, P. (1999). Current and future directions of multimedia technology in business. International Journal of Information Management, 19(2), 105-120.

[2] Karim, Z., et al. (2009). Towards secure information systems in online banking. Paper presented at the International Conference for Internet Technology and Secured Transactions, 2009 (ICITST 2009), London

[3] Subsorn, P. & S. Limwiriyakul. (2011a). A comparative analysis of the security of Internet banking in Australia: A customer perspective. Presented in 2nd International Cyber Resilience Conference (ICR2011). Perth, Australia: Edith Cowan University.

[4] Subsorn, P. & S. Limwiriyakul. (2011b). A comparative analysis of internet banking security in Thailand: A customer perspective. Presenting in 3rd International Social Science, Engineering and Energy Conference 2011 (I-SEEC2011). Nakhon Pathom, Thailand.

[5] Hamid, M. R. A., et al. (2007). A comparative analysis of Internet banking in Malaysia and Thailand. Journal of Internet Business(4), 1-19.

[6] Hutchinson, D., & Warren, M. (2003). Security for Internet banking: A framework. Logistics Information Management, 16(1), 64 -73.

[7] Steinfield, C. (2002). Understanding click and mortar e-commerce approaches: A conceptual framework and research agenda. Journal of Interactive Advertising, 2(2), 1-10.

[8] The National Office for the Information Economy (NOIE), et al. (1999). Banking on the Internet: A Guide to Personal Internet Banking Services. Retrieved April, 2011, from http://www.archive.dcita.gov.au/1999/08/banking

[9] Gurau, C. (2002). Online banking in transition economies: The implementation and development of online banking systems. International Journal of Bank Marketing, 20(6), 285-296.

[10] Usonlinebiz. (2008). Types of Internet banking and security threats Retrieved April, 2011, from http://www.usonlinebiz.com/article/Types-of-Internet-Banking-and-Security-Threats.php

[11] Hutchinson, D., & Warren, M. (2001). A framework of security authentication for internet banking. Paper presented at the International We-B Conference (2nd), Perth.

[12] BankMuscat. (2009). Internet banking security threats. Retrieved April, 2011, from http://www.bankmuscat.com/en-us/ConsumerBanking/bankingchannels/internetbanking/Pages/InternetBankingSecurityThreats.aspx

[13] Ekberg, P., et al. (2007). Online banking access system: Principles behind choices and further development, seen from a managerial perspective. Retrieved April, 2011, from http://www.essays.se/essay/6974685cb6/

[14] RSA. (2010). RSA 2010 global online consumer security survey. Retrieved April, 2011, from

www.rsa.com/.../consumer/.../10665_CSV_WP_1209_Global.pdf
[15] Australian Prudential Regulation Authority (APRA). (2011). List of authorised deposit-taking institutions: Foreign subsidiary banks. Retrieved October, 2011, from http://www.apra.gov.au/adi/pages/adilist.aspx
[16] The Australian Bankers Association (ABA). (2011). ABA members. Retrieved October, 2011, from http://www.bankers.asn.au/Members/default.aspx
[17] VeriSign Authentication Services. (n.d.). FAQ: Extended validation SSL. Retrieved April, 2011, from http://www.verisign.com.au/ssl/ssl-information-center/extended-validation-ssl-certificates/?

Panida Subsorn is a lecturer of the Department of Information Technology, Suan Dusit Rajabhat University, Thailand. She achieved her doctorate degree in Information Technology at Edith Cowan University, Western Australia. Her current research interest area is in information security.

Sunsern Limwiriyakul is currently undertaking his doctorate research at School of Computer and Security Science, Edith Cowan University, Perth, Western Australia in the field of network security. His research interests are in Internet and network security. He has over 14 years experience in the IT Industry in the areas of ICT and network security.