ITMSOC

Available online at http://itmsoc.org
Information Technology Management Society

ITMSOC Transactions on Innovation & Business Engineering 01 (2016) 7–13

ITMSOC–IBE
ITMSOC Transactions on Innovation and Business Engineering

http://www.itmsoc.org

Analysis of Global Mobile Devices in Thailand

Panyaphat Aekitsawatwikul*, Adisorn Leelasantitham, Supaporn Kiattisin, Smitti Darakorn Na Ayuthaya

Technology of Information System Management Division, Faculty of Engineering, Mahidol University, Puttamonthon, Nakorn Pathom, Thailand

Received 15 February 2016; Accepted 1 August 2016

Abstract

Nowadays the mobile device are becoming more attractive with business enterprise. So they are focus on welfare to realize the benefits of smart phones support to working productively. However, there are too many restrictions to control users' behavior and IT department is uncomfortable in the company. This paper proposes the guidelines have determining procedure to installing applications on organization's mobile devices a take into consideration the information as follows the scope of the policy; cost containment, data protection and application categories including risk analysis. This guideline is some tool for help choosing app download and selecting for installation on server organization. The research demonstrates that choose a decision to install an App has to consider more than just App information and look into its associated user behavior. The arrangement on guidelines for officially supported global mobile device policy as follows the security standards and guidelines. This is still important to ensure that these apps do not dangerous and impact to business systems. The proper handling of policy for recognize and continuous compliance that with any comprehensive information security. Furthermore, explore the satisfaction survey of employees in business standard policy.

Keywords: Mobile Security Policy Standard, Consideration Mobile Application, Application Behavior, Mobile Risk.

1. Introduction

THE part important of the mobile device is certainly undeniable today whether use in the personal or business organization. Mobile technologies are a growth engine for business, top 25% of adopter revenue growth of jobs creates [1]. Gartner predictions, employers are used to bring your own device for work purpose in 2017 [2]. BYOD stands for bring your own device, which is bring personally own mobile devices to the workplace for use and connectivity on the company system. BYOD getting to be better evaluated and security way to protect however are making security a concern for IT department. The idea is beginning by consider the concept of company mobile security. How to make the mobile security standard is not interrupt with employee expectations. Company mobile has been creating great ways to deal of interest among IT department. The companies sign a cell phone contract with mobile phone service providers to provide the smartphones cover package.

The situations that above becoming interest with design the corporation mobile standard policy and choose a decision to find out how to classify mobile apps install on company mobile. Include higher risk that the costs associated after download application installation. Monitoring the rate of adoption employee expectations after the policy announcement on company and involved interviews with the opinions among of employees.

Mobile Device of enterprises has more concerns about mobile device security [2]. The mobile devices create unreasonable costs. Particular care and attention should be paid to any service or download which is asking for access to contact data, pictures, Geo-tracking or similar, as this may lead to a data protection issue in certain jurisdictions or requires payment for connections, voice services or any downloads and transmission or whatever services

*Corresponding author.
Email address: panyaphat.aek@student.mahidol.ac.th (Panyaphat Aekitsawatwikul)

e-ISSN: 2539-5904

not covered by the respective telephone contract.

Adoption of the BYOD cannot enforce on security policies the company and opens up a multiplicity of potential security holes [3]. Due to there are many standards for mobile security policies, however cost containment and custody of the asset are with the employee who has to ensure safeguarding and proper usage in accordance with policy unconcerned.

According to Gartner [4], Enterprise employees are exposed to attacks and violations from download and used mobile application that can access business assets which applications have little or no security assurances. Mobile device of the costs associated after download application installation is higher risk. Any resulting fees, damages or other payment obligations resulting from non-business or injudicious and costs for the purchase of mobile applications.

This study focus on designing of global mobile device policy announced. The provisions of the acceptable use IT policy for corporate mobile telephone policy and local user guidelines. We propose information into consideration as follows the scope of the policy; cost containment, data protection and application categories. The study is not software development and this policy applies to all employees who use a mobile device provided by corporate business as part of their duties. Local user guidelines and policies may apply which contain more detailed measures on the use of the device either the account for potential local peculiarities or internet censorship by counties.

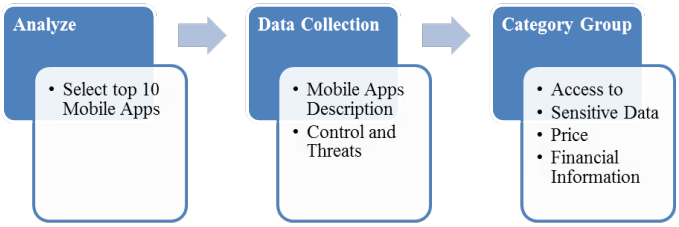

Fig. 1. Analyze information process.

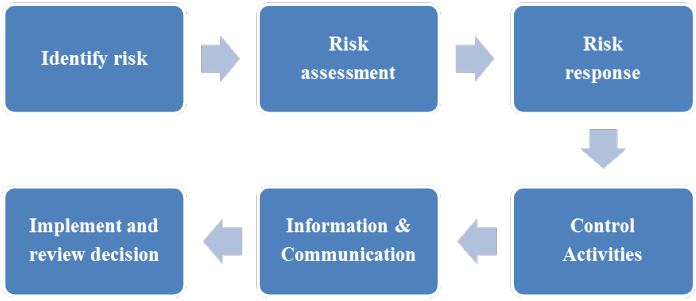

Fig. 2. Risk analysis process.

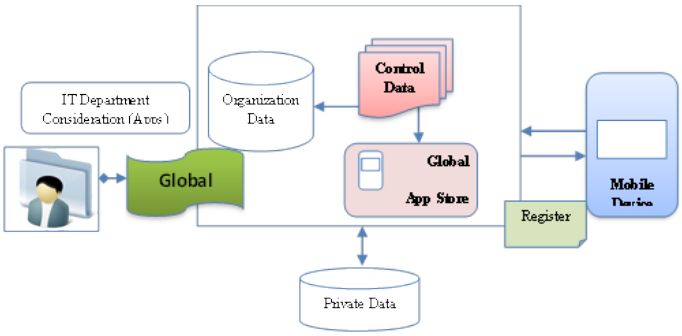

Fig. 3. Illustration of Mobile policy framework.

2. Related Works

Security mobile device has become very important. In particular, it was concerns relate to personal and security business the data stored on the device and preferred targets of attacks. Businesses organization used more mobile devices for communication also as planed and organized their data of work and private data. It is still impacting about IT Administrators. Users have accrued the use of data storage and access stored location for critical information. It has a higher risk to attack about control access to data, information either protect private data or intellectual property of a business. The mobile device has the focus of targeted attacks from threat, and then can useful weakness gap of device [5]. The security has standard different based on software development and application download of consumer behavior.

According to research mobile security, many research showed proposed focus on access to data, information and design framework that enforcement policy standard for users. For example, Jim Luo, Myong Kang (2011) the authors propose application lock box to protect threat environments and combines policy enforcement to support enterprise [6].

Sonia Meskini, Ali Bou Nassif, Luiz Fernando Capretz (2013), the authors explore Software Reliability Growth Models (SRGMs). SRGMs applied to check and evaluate for consideration reliability software [7]. However, the models presented only crash files except for sorting the application category.

Martin Kuehnhausen, Victor S. (2013) the authors propose about Trustworthiness of Smartphone Apps with assessments ranging of app rating [8]. In particular, they proposed several metrics that clearly result.

Yong Wang, Karthik Vangury and Jason Nikolai (2014) the authors present about MobileGuardian. The authors created policy.bin included determining isolation the security and mobile device resources. There were several limitations clarify results and focus only BYOD [9].

According to research the approaches in [6, 9] target create a program to risk management for application block. There was the security policies used to limit access another application to store.

Table 1. Vetting Application Description.

No.	App Name	Price	Paid	Description
1	Facebook Messenger	Free		For free. Messenger is just like texting, but you don't have to pay for every message (it works with your data plan). Message people in your phone book and just enter a phone number to add a new contact. Group chats, Photos and videos, Free calls, stickers. Preview your camera roll photos and videos without leaving the conversation. Turn on location to let people know when you're nearby.
2	Pandora	Free	Monthly Listening Extension 0.99 USD Pandora One 3.99 USD 4.99 USD	Create a free account to explore hundreds of music and comedy genre stations. Even easier. Just log in and enjoy the same free radio service. Your Pandora is the same across the web, on your TV and in your car. Your Pandora One subscription will automatically renew each month and your credit card will be charged through your iTunes account.

Table 2. Control and Threats Description.

Control and Threats	Description
Sensitive Data	The information that can identify you personally and the organization as a specific individual: Use weakest password for authorization and an unprotected device by virus protection.
Access to Financial Information	The Internet banking: Financial transaction through website on mobile devices without “https” channel detection and use credit cards register for shopping online.

Table 3. Mobile Application Description Category Group.

		Price and Financial Information				Access to and Sensitive Data					BL	
No	App Name	Free	Pay	Call	Game	Phone No.	Photo	VDO	GPS	Chat	Virus	SUM
1	Facebook Messenger	0	1	1	0	1	1	1	1	0	0	6
2	Facebook	0	0	0	1	0	1	1	1	1	0	5
3	YouTube	0	0	0	0	0	0	1	0	0	0	1
4	Instagram	0	0	0	0	0	1	1	0	0	0	2
5	Snapchat	0	0	0	0	0	1	1	0	1	0	3
6	Pandora	0	1	0	0	0	0	0	0	0	0	1
7	Google Maps	0	0	0	0	0	0	0	1	0	0	1
8	Dubsmash	0	0	0	0	0	1	1	0	0	0	2
9	iMovie	0	1	0	0	0	1	1	0	0	0	3
10	Find My iPhone	0	0	0	0	0	0	0	1	0	0	1

However, there focuses BYOD to use in business that IT department’s out of control and no expectations measurement with policy enforce from users. In [7, 8] approaches created a framework for checking reliability and trust software for consideration. This framework cannot be made apps category to classification apps level priority.

Security is paramount for the modern mobile business [10]. An organization should be development plan and employ software assurance processes. We were aware of potential security that impact to mitigate or accept the consequences. The software assurance process ensured that reliable software and based on standard and procedures [11]. The threats and vulnerabilities have an impact with the mobile devices [12].

Due to the Apps popularity of survey research that 85 percent of Americans have used the strongest social networking app and other smartphone owners have tended to be more entertaining social networking and games [13]. Nielsen and Pwc research suggest that for activities performed using smartphone consistently rank in the top 10 sites among mobile web users around the world was Facebook, Google, YouTube, Twitter, eBay [14, 15] also Canvas Survey results business Interested in File Storage [16].

The global survey confirms that the results from around the world with social media used Facebook as the primary social network on the majority. However, China was blocked access to Facebook while their preferred We Chat/Weixin social media as platforms. The use of social media varies significantly and considerably more distinctive by countries [17].

3. Methodology

We were beginning to create building a model case concept analysis. 4-Step Processes have been designed to transform and feel the forced thoughts in Fig. 4. We were designed to impose IT department by role management and classification the information of mobile application.

Table 4. Mobile Application Classify Standard.

Apps Category list	Example Apps Name
Class 2: Greylist Apps or services have potentially non-compliant with local data protection standards when installed without caution.	1. Facebook Messenger 2. Facebook 3. YouTube 4. Instagram 5. Snapchat 6. Pandora 7. Google Maps 8. Dubsmash 9. iMovie 10. FindMyiPhone

Step-1: Analyze information and classification mobile application

Step-2: Classify data mobile security standard

Step-3: Design mobile security guideline

Step-4: Test process

Step-5: Stakeholder expectations survey:

Fig. 4. 4-Step processes.

3.1. Analyze information and classification mobile application

Exploration of the top ten mobile apps, trends in the credibility survey. Data collection modes are distinguished by application description and classify by category group.

Vetting application description and grouping app at the same type see in Table 1, Apps have check information in control and threats description in Table Table:PP062:02 and risk analysis process in Fig. 2.

3.2. Classify data mobile security standard

3.2.1. Class 1: Blacklisted Apps

Example: Stealth Genie, Mobile Spy, Flexi spy, Other Game

Risks/reasons for blacklisting

- Products are capable of allowing a third party to remotely view emails, messenger chats, text messages, phone contacts, memos, call logs and calendar appointments, as well as pictures, videos and music files saved in the phone.
- Some allow subscribers to remotely listen in to voice conversations and view internet browsing history and saved bookmarks.
- A game which tracks usage can access to calendar, location, exhaustively the resources and increases the data bill.

3.2.2. Class 2: Greylist

Apps or services have potentially non-compliant with local data protection standards when installed without caution.

Example: Facebook, WhatsApp, LinkedIn, Xing, Flickr, Instagram, Dropbox, OneDrive, Google Drive.

Risks/reasons for blacklisting

- Access to address book
- Scanning of uploaded data
- Data exchange may cause unjustifiably higher cost

3.2.3. Class 3: Whitelisted

Risks/reasons for blacklisting

- App catalog available on the Global App Store

3.3. Design mobile security guidelines

3.3.1. Scope policy process

Scope definition exactly who use publication policies. Local country user guidelines and policies may apply which contain more detailed measurement on device and cost potential local peculiarities

3.3.2. Mobile devices provision

The employee has ensured protect the device asset and proper usage in accordance with the policy that company provided to perform their job responsibilities. This policy applied to the only company device except for any support for the private use of mobile device

3.3.3. Use of mobile devices

- Cost containment (includes optimization of total cost of communication and mobile data use)
- Private use (Backup, Data Protection)
- Wiping and other protective measures

3.3.4. Basic's first step

The user would need to create a user id first start of device based on company mail address on the device to be able to install the apps which is required to connect the mobile device with company resources (mail, calendar, Global App Store, etc.). This user ID will not be transferred upon termination of employment.

Other than common mobile phones, smartphones and tablets allow for a customized collection of Apps. For proper management and control, a company uses a Mobile Device Management (MDM) application which has to be installed by the user on each company mobile device, or configured in case of pre-installed.

The MDM application

- Enforces a 6 digit device password

- Operates provided Apps and data (e.g. E-mail) in secure containers which also separate business from private data
- Controls the integrity of the smartphone (e.g. to detect jailbreaks)
- Provides an App recommendation list
- Monitors installed Apps to ensure compliance against blacklisted Apps.

3.3.5. Apps Categories

Blacklist (Hazardous Apps - registered in Global App Store) Operation on mobile device prohibited

Greylist (Apps or services potentially non-compliant with local data protection standards when installed/operated without caution)

Whitelist (Registered in Global App Store) - Installation/Operation for business use

3.4. Test process

The first step process of testing process into the following: IT Department has used all reasonable trusted and famous in compiling the information. Example: App Annie, Google play store, App Store for consideration to installation on server sort by the App population. Server has control and security base on organization policy rule such as firewall and antivirus follow up IT system framework. After IT have upload app to Global App Store then user can download app to install on device. Step to download app. Mobile device'user must be sign Global mobile device policy in document agreement and approve authority. The ID registration can register to enterprise systems using business email. After Mobile have register to the system. Mobile device management has control all data by the system administrator. There have a separate data through the system, as the data being used. Enterprise system's file, customer contact number, and personal information of user, such as photo, video, data are generated by the device and save on device. Organizations can still wipe the device then look the risk of the threat. See in full diagram of system in Fig. 3.

3.5. Device Management Formulation

Assume $A = \{A_1, A_2, \ldots, A_n\}$ to represent the App's Description which includes apps classification C. First, we separate the n class into the following sets

$$\begin{aligned} c_1 &= \{A_1, A_2, \ldots, A_n\} \\ c_2 &= \{A_1, A_2, \ldots, A_n\} \\ c_3 &= \{A_1, A_2, \ldots, A_n\} \end{aligned}$$

We use Mobile Device as Assume $M = \{m_1, m_2, \ldots, m_n\}$ to be supported. We use $\Re = \{r_1, r_2, \ldots, r_n\}$ to relevant all the resources on the mobile device M_n use F to represent financial crises occurs after download app. For example, Mobile device m_1, we have

$$\begin{aligned} m_1 &= f(c_1, r_1, F) \\ m_2 &= f(c_2, r_2, F) \\ m_3 &= f(c_3, r_3, F) \end{aligned}$$

3.6. Stakeholder expectations survey

To design the user opinion on the level of service provided and complete result of brief survey. IT administered have global survey to understand and compare consumer usage behaviors and the policy contribute to under use of different feelings. The survey question will be selecting the population questions for analytic and considered suitable for improvements system. The associate of Global mobile device policy announcement was expectations of risk management that the desires for feel of employee by not putting pressure on them during work

4. Evaluation

It's separate app and classify category group see in Table 3.

In the classify category group above the table, calculate in the following formula. Assume:

$$x = a + b, x > 0 \tag{1}$$

a represent Price and Financial information, b represent Access and Sensitive data, and x to represent the Class 2: Greylist see in Table 4 by total must exceed 0.

This guidance document provides a detailed of the operating guidelines that consider and impact analysis as following as Operating Guideline.

1. Scope of Policy - This Policy applies to all employees.
2. Devices provision - Mobile devices are provided to staff to enable them to perform their job responsibilities.
3. Use of mobile devices - Any illegal or morally objectionable use is strictly prohibited. It is expected that employees use mobile devices judiciously. Cost containment shall be secured at any time. Job responsibilities and requirements, data security and protection shall not be harmed in any way.
4. Device basics - The user is required to create an Apple ID based on business mail address at the first start of device. IT has set the categories for the use of Apps.
5. Backup - No App backup that is not whitelisted or any content physically stored on a mobile device which is not processed with a whitelisted App. Private Apps or data stored on the device can be backed up on a private PC (e.g. by using Apple iTunes)
6. Data Protection - The setup separates strictly business and private data in individual device with this adequate data protection of privately used content is given backups by company.

7. Assignment - The relevant senior manager must approve the assignment of a mobile device.
8. Services providers - Corporate IT operations are determining the most effective mobile service provider.
9. Telephone administrator - A telephone administrator is responsible for contract, cost and device management include optimization of total cost of communication and mobile data use and execution of the principles of this policy.
10. Payment used - In some countries it may be a legal requirement to pay follow benefit in kind allowance.
11. Auditor - As the mobile device is company property and the invoices are paid by company, the invoices may be subject to internal audits.
12. Priority Order- The provisions of the acceptable use policy shall prevail over this mobile device policy and local user guidelines.

5. Conclusions

This research is concerned with the role of mobile security with the corporation. The global mobile device policy is expected that employees use mobile devices judiciously. Cost containment shall be secured at any time. Job responsibilities and requirements, data security and protection shall not be harmed in any way. Encourage to make employees aware of safety important and they are not feeling forced to use the policy.

References

1. Columbus L. Mobile Technologies Becoming A Growth Engine For Small and Medium Businesses; 2015. www.Forbes.com. Available from: http://goo.gl/bUuz7b.
2. Gartner, Inc . Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes; 2013. Available from: http://www.gartner.com/newsroom/id/2466615.
3. Miller KW, Voas J, Hurlburt GF. BYOD: Security and Privacy Considerations. IT Prof. 2012 Sep;14(5):53–55. Available from: http://dx.doi.org/10.1109/MITP.2012.93.
4. Gartner, Inc . Gartner Says More than 75 Percent of Mobile Applications will Fail Basic Security Tests Through 2015; 2014. Available from: http://www.gartner.com/newsroom/id/2846017.
5. Becher M, Freiling FC, Hoffmann J, Holz T, Uellenbeck S, Wolf C. Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. In: 2011 IEEE Symposium on Security and Privacy. Institute of Electrical & Electronics Engineers (IEEE); 2011. Available from: http://dx.doi.org/10.1109/SP.2011.29.
6. Luo J, Kang M. Application Lockbox for Mobile Device Security. In: 2011 Eighth International Conference on Information Technology: New Generations. Institute of Electrical & Electronics Engineers (IEEE); 2011. Available from: http://dx.doi.org/10.1109/ITNG.2011.66.
7. Meskini S, Nassif AB, Capretz LF. Reliability Models Applied to Mobile Applications. In: 2013 IEEE Seventh International Conference on Software Security and Reliability Companion. Institute of Electrical & Electronics Engineers (IEEE); 2013. Available from: http://dx.doi.org/10.1109/SERE-C.2013.30.
8. Kuehnhausen M, Frost VS. Trusting smartphone Apps? To install or not to install, that is the question. In: 2013 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA). Institute of Electrical & Electronics Engineers (IEEE); 2013. Available from: http://dx.doi.org/10.1109/CogSIMA.2013.6523820.
9. Wang Y, Vangury K, Nikolai J. MobileGuardian: A security policy enforcement framework for mobile devices. In: 2014 International Conference on Collaboration Technologies and Systems (CTS). Institute of Electrical & Electronics Engineers (IEEE); 2014. Available from: http://dx.doi.org/10.1109/CTS.2014.6867564.
10. Sawyer J. Mobile Security: All About the Data; 2014. Informationweek.com. Available from: http://reports.informationweek.com/abstract/104/12295/Government/Mobile-Security:-All-About-the-Data.html.
11. Quirolgico S, Voas J, Karygiannis T, Michael C, Scarfone K. Vetting the Security of Mobile Applications; 2015. Available from: http://dx.doi.org/10.6028/NIST.SP.800-163.
12. M S, G P. Mobile Device Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism. International Journal of Computer Applications. 2012 oct;56(14):24–29. Available from: http://dx.doi.org/10.5120/8960-3163.
13. The Nielsen Company. The Mobile Consumer: A Global Snapshot; 2013. Nielsen.com. Available from: http://www.nielsen.com/content/dam/corporate/uk/en/documents/Mobile-Consumer-Report-2013.pdf.
14. mobiThinking. Global mobile statistics 2013 Section E: Mobile apps, app stores, pricing and failure rates; 2013. mobiforge.com. Available from: https://goo.gl/i20sjB.
15. PricewaterhouseCoopers LLP. Total Retail 2015: Retailers and The Age of Disruption. PricewaterhouseCoopers LLP (PWC); 2015.
16. Peck J. How Businesses are Using Mobile Apps - 2015 Canvas Survey Results; 2015. gocanvas.com. Available from: https://www.gocanvas.com/content/blog/post/how-businesses-are-using-mobile-apps-2015-canvas-survey-results.
17. comScore, Inc . comScore Introduces Mobile Metrix©in the UK to Measure Total Mobile Audience Behaviour Across Smartphones and Tablets; 2015. Available from: http://goo.gl/XZFnfG.
18. Chavas JP. Risk Analysis in Theory and Practice (Academic Press Advanced Finance). Academic Press; 2004. Available from: http://www.sciencedirect.com/science/book/9780121706210.
19. OpenNet Initiative. Summarized global Internet filtering data spreadsheet and Country Profiles; 2012. Available from: http://opennet.net/research/data.
20. Walker RW. NIST Drafts Mobile App Security Guidelines; 2014. Informationweek.com. Available from: http://www.informationweek.com/government/mobile-and-wireless/nist-drafts-mobile-app-security-guidelines/d/d-id/1306815.
21. Kaur R, Mazzarella W, editors. Censorship in South Asia: Cultural Regulation from Sedition to Seduction. Indiana University Press; 2009. Available from: https://www.amazon.com/Censorship-South-Asia-Regulation-Seduction/dp/0253220939.

Biographies

Panyaphat Aekitsawatwikul received the B. Science. degree Business Information Technology from Silpakorn University (SU), Thailand, in 2007, M. Science in Information Technology Management from Mahidol University (MU), Thailand, in 2016.

She currently works at Siegwerk (Thailand) Ltd.

Her research interests include Development of Mobile Device Policy Using Expectation Survey and Risk Assessment.

Adisorn Leelasantitham received the B.Eng. degree in Electronics and Telecommunications and the M.Eng. degree in Electrical Engineering from King Mongkut's University of Technology Thonburi (KMUTT), Thailand, in 1997 and 1999, respectively.

He received his Ph.D. degree in Electrical Engineering from Sirindhorn International Institute of Technology (SIIT), Thammasat University, Thailand, in 2005.

He is currently the Associate Professor in Technology of Information System Management Program, Faculty of Engineering, Mahidol University, Thailand.

His research interests include forecasting, modeling, survey techniques, demand and supply chain managements, strategic planning, standard frameworks, healthcare IT, optimization and decision making, machine learning, fuzzy logic, neural network, image processing and medical imaging, chaotic encryptions, computer graphics, and virtual reality.

Supaporn Kiattisin received B.Eng. in Computer Engineering from Chiangmai University in 1995, M.Eng. in Electrical Engineering and Ph.D. in Electrical and Computer Engineering from King Mongkuts University of Technology Thonburi (KMUTT), Bangkok, Thailand.

She is currently the Assistant Professor in Technology of Information System Management Program, Faculty of Engineering, Mahidol University, Thailand.

Her research interests include enterprise architecture, information technology service standard, corporate governance, business process improvement, medical imaging, computer vision and modeling.

She is member of TESA, ThaiBME, IEICE and IEEE.

Smitti Darakorn Na Ayuthaya received the bachelor's degree in economics from University of the Thai Chamber of Commerce, Thailand, in 1981, and the master's degree in commerce and business administration from Colorado University, United States of America, in 1985.

He received his Ph.D. degree in Public Administration from University of Northern Philippines, Philippines, in 2010.

He is currently a lecturer in Technology of Information System Management Program, Faculty of Engineering, Mahidol University, Thailand.

His research interests include digital economy, macro/micro economic, e-logistic, economy value management, strategy management/planning, and human resource management.