International Conference on e-Business 2007 (INCEB 2007)
22 - 23 November 2007
P36

The Enterprise Architecture-Based Strategic ICT Security Planning Methodology

Panya Boonyapiwat
Pranakorn Rajabhat University
3 Jangwattana Rd, Bangkhen
Bangkok, 10220. Thailand
Email: boonyapiwat@yahoo.com

Rojarase Meksirivilai
Ministry of Information and Communication Technology
Jangwattana Rd, Laksi,
Bangkok, Thailand 10210
Email: rojarase@mictmail.com

Abstract

In designing the ICT security master plan for Thailand, It is critically importance to understand the security imperatives of Thai public and private sectors. Also, it is essential to adopt the international standards on security management as the guideline for ICT security, human resource training and education; including promoting the security professional certification. In this paper, the ICT security requirements for formulating the national ICT security master plan are addressed including the organizational aspects, the human resource development, computer networking, authorization and authentication, information security management, business continuity, security technology, security standards, ICT laws, ICT security research and development, security information management (SIM) and other related strategic plans at the national level. Then, enterprise architecture -based security methodology is proposed to formulate the desired ICT security master plan. This new methodology can guide the planning process that will result in a complete cyber security architectural plan.

Key Words: ICT Master Plan, Information Management,

1. The Issues of ICT Security

The increase utilization of ICT in developing Thailand's business, industry and society necessitates the formulation of national ICT security policy for the private and public sector agencies and Thai citizens to aware of the importance of ICT security. To implement this policy systematically, a National ICT Security Master Plan is needed as a roadmap to guide the implementation of ICT security measures to strengthen the critical information infrastructures, and provide the process guidelines in accordance with the international standards on information security management ISO 27000 series for the public and private enterprises, and the building of the ICT security capacity of Thailand.

The Ministry of Information and Communication Technology (MICT) which is responsible for the ICT policy and implementation of the National ICT Master Plan within the framework of IT2010 is therefore in charge of the execution of devising the National ICT Security Master Plan (NISMP) to complement the National ICT Master Plan for the year 2008-2012. This paper describes the fundamental issues that must be considered in designing the ICT security Master Plan.

The main goal of ICT Security management is to define the processes and procedures to ensure the security and privacy of data conforming to agency guidelines and laws. Certain procedures in ICT security would relate to the way security will be formulated to meet the ICT security requirements and the implementation priority. Hence the ICT security plan must ensure that the ICT security policy and laws are consistent with the control procedures in the implementation of the plan. The formulation of the National ICT Security Master Plan will take the following issues into considerations.

1. The structure for Managing ICT Security

The organizational and management structure has significant impact on the implementation of the ICT security measures that can be controlled and managed based on international standards, guidelines and practices. It is therefore important to define all the ICT processes and procedures clearly so that multi

agencies co-ordinate to counter the threats can be carried out efficiently.

2. ICT Security Personnel Development

Personnel in the ICT security operation is the weakest link. None of the ICT security policies, standards, guidelines, process, and practices will be executable if the personnel in charge or involved cannot execute and meet the security requirements. Consequently, it is of the utmost importance to address the issues of ICT security and personnel. ICT education, training and certification are therefore critical to the success of the implementation of any ICT security policy. Each person in the ICT security operation must be educated, trained as required by ICT security so that person is able to perform their particular function or job efficiently and effectively.

3. System Administration of Computer and Networks

Network security must be well-managed to ensure that it can withstand the attack from both inside and outside threats. All activities on the network should be monitored. The security management should consider both the level of quality of service balanced against the privacy and security which must be done dynamically and continuously. All the equipment used in the network must be certified to international standards to ensure the privacy and security of data that is stored, processed and transmitted. Moreover, it is also needed to define the method of data exchange between two processes or entities on the network. The exchange of data securely is importance in providing secured business transactions supporting e-business. Here, the ICT laws, secured network, ICT security-certified standard procedures and equipment would be imperative in creating a secured environment for e-business trading partners.

4. Authorization, Authentication and Access

The access to data must be based on the ICT security principles in which authorization and authentication process must be clearly specified and implemented. Both temporary and permanent, granting the right to access must be considered. It is essential to consider the ramification of each technology that can be used such as encryption, smartcard and biometrics, in implementing the access control based on the ICT security requirements.

For the authentication process, the Certificate of Authority (CA) must be implemented based on international accepted standards. For example, the CA products must be IFIP Level 2 certified to assure our trading partner that the system implemented is secured at our end.

5. Information Security Management

The ICT system consists of hardware, software, network, peopleware, processes and procedures. The system must be configured and managed in such a way that it can withstand threats from both inside and outside. The emergency response to an attack must be swift and counter measures can be deployed instantly. The weakness or system loop-holes must be identified and eliminated. Here it is essential for the ICT security master plan to encourage the security assessment of all the government agencies and implement the security policy, deploying the certified security products, and training the agencies and personnel to be ready to defend the system against any attack.

6. Business Continuity

After an ICT security emergency or other emergencies from natural disasters, attack by terrorists, or accidents, the recovery of critical data is the most important issue to ensure the survival of the organization's mission. Hence, the issue of ensuring business continuity in the presence of threats becomes an important issue in designing that National ICT Mater Plan. In case of a threat, the ensuring of the survival of national's critical infrastructures (CI) and critical information infrastructures (CII) is of paramount importance to ensure the well-being of our nation.

Moreover, it is imperative to investigate the risk and damage resulting from a threat or emergency situation and the lost of life, properties, services, and credentials due to the failure of ICT security management. The assessment should be done at the national level. Hence in the National ICT Security master Plan, the strategies must cover this important aspect of business continuity.

2. Strategic Goals and Objectives

The formulation of the National ICT Security master Plan must take into consideration the issues addressed in Section 1. In addition, the Plan must also address the issue of the international ICT security standards ISO 27000 to include in the human resource development plan and recommendation to base the organizational security management on these well-accepted security standards. In this section, the objectives and goals in designing the ICT Security Mater Plan are as follows.

Strategic Objectives

To define the policy framework, strategies and measures for information Security management at the national level.

To define the plan for developing ICT security technology for Thailand Conforming to the Self-sufficiency Economy paradigm.

Strategic Goals

Can operate e-business securely

Government agencies and the Thai society are secured by using ICT conforming with the ICT

security standards implemented as compliant to the national ICT Security Master Plan.

Equipment used in the network is certified and in conformance with the relevant ICT security standards, testing and certification procedures.

Have a national agency responsible for ICT security and is empowered to implement the National ICT Security master Plan.

The National ICT Security Master Plan is a Strategic Roadmap for the execution that will be met with stated goals and objectives. This Strategic Roadmap will assure that the nation's Critical Information Infrastructure (CII) will be defended from cyber attacks and the chance of threats that will physically damage the critical information infrastructure will be immobilized. The ICT security master plan will also take into consideration the National Emergency Master Plan in communications to ensure that cyber attacks during an emergency will be met aggressively by the national agency should an event occur.

The National Security Master Plan will operated within the context of Thai government, Thai society which values harmony, ethic and good governance, freedom of expression, privacy and protection for Thai citizens and it's political virtual or physical borders with aggression within and outside the Kingdom of Thailand.

3. ICT Security Policy and Operations

This section will briefly describe some of the key activates and issues as related to the development of the National ICT Master Plan. The policy stems from the IT 2010 framework will be outlined. This framework is important since the National ICT Master Plan 2001-2006 is based on this framework. The state of various ICT laws pending in Parliament. The passing of these laws are critical to the e-business as well as ICT security. Also, the emergency preparedness framework which is important providing a sound management to emergency will be considered. The issue of research and development in ICT security will be reviewed and various related issues will be examined.

3.1 Policy Framework from IT2010

The policy framework stemmed from IT 2010 as depicted in Figure 1 emphasizes the development of e – Industry, e – Commerce, e – Education, e – Government and e – Society. Founding on research and development of new knowledge, human resource development and build the ICT infrastructure with goals of creating knowledge economy. This policy framework therefore aims at utilizing ICT effective and efficiently. This framework neglects the ICT security and privacy aspect.

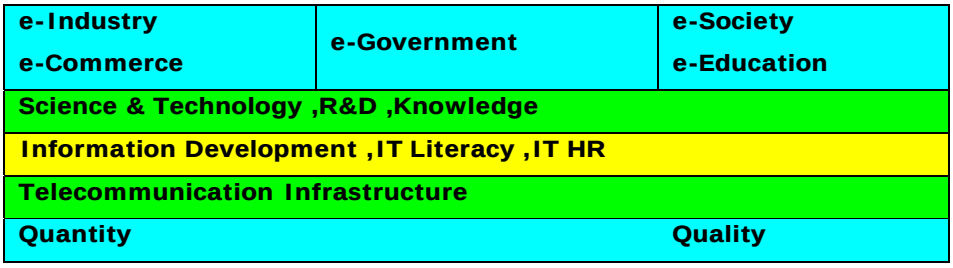

Figure 1. IT2010 (ICT Development Policy Frame

In conforming to the IT2010 framework, the National ICT Security Master Plan will complement the framework with the security and privacy aspects to provide a foundation for integrating ICT policy and implementation to the development of ICT in Thailand. At the highest level, all the ICT system targeted, e-Industry, e-Government, e-Commerce, e-Education and e-Society, will be monitored by the TISPAC (Thailand Info-Security Policy and Analysis Center) which must be established by the National Security Master Plan. The next layer, complementing the Science and Technology , R and D and knowledge in IT 2010 is the ICT security R and D , and the dissemination of international ICT security standards so that it can be understood, applied and operated by Thai workforce. Matching the next level is the ICT security system development in which most of the present ICT system must be verified, modified and re-designed due to system weakness and deficiencies making them vulnerable to attacks. Also in this layer is the capacity building so as to raise the ICT security awareness for the private and public sector workforce and technical competency of ICT personnel and creating ICT security professionals. Complementing the Telecommunication layer of IT2010 is the

telecommunication and network security to ensure that threats from network will be localized, mitigated, eliminated and countered effectively and efficiently.

The complementary framework to the IT 2010 is shown in Figure 2. As in IT 2010, the new complemented IT Security framework must have both quantity and quality in the implementation.

<table>
<tr><td colspan="3">e-Industry
e-Commerce</td><td>e-Government</td><td>e-Society
e-Education</td><td>Thailand Info-Security Policy and Analysis Center : TISPAC</td></tr>
<tr><td colspan="4">Science & Technology ,R&D ,Knowledge</td><td>ICT Security R&D, Standards</td></tr>
<tr><td colspan="4">Information Development , IT Literacy , IT HR</td><td>ICT Security System Development HRD, Capacity Building</td></tr>
<tr><td colspan="4">Telecommunication Infrastructure</td><td>Network Security</td></tr>
<tr><td colspan="4">Quantity Quality</td><td></td></tr>
</table>

Figure 2. Complementary of IT2010 Framework with ICT Security

3.2 The ICT Laws

The promulgating of various ICT laws is a slow meticulous process. The enactment of ICT laws is essential to development of not only the implementation of The National ICT Master Plan but also the realization of the National ICT Security Master plan. The laws will ensure more protection against cyber crimes and provide means to implement better ICT security mechanisms. The current state-of –of the ICT laws can be briefly summarized as follows.

Electronic Transactions Act
Electronic Signature Act
National Information infrastructure Act
Data Protection Act

- Awaiting approval from the cabinet

Computer Crime Act
Electronic fund Transfer Act

3.3 National Policy of Preparedness on Information System

The cabinet decision on 4 February 2535 approved the national Emergency Preparedness Plan 2535. The plan will be used to guide to prepare the response to emergency situations in 14 areas encompassing the normal situation, the crisis situations due to natural disaster, terrorists, invasion of force from outside the country, with the goal of being able to continue the operation of essential functions of government services so as to protect Thai citizens and the nation from the potential damages. The Emergency preparedness Plan must cover all the 14 areas shown in Table 1 and all plans must be integrated to ensure that Thailand can withstand and survive the national emergency situation and maintain her stability in economic and the well-being of Thai citizens.

For the preparedness on communications, the National Security Council has announced the Communication Preparedness Plan 1/2541 in 2541 in which a policy framework and procedure to strengthening the communication capability that will be able to response to both civil and military requirements in response to the threats from outside the country. The same plan can also be used for defending and responding to public and natural disasters in which the trend of occurring appears to be increasing and more virulent.

In December 2548, the Cabinet approved a new national emergency Preparedness Plan replacing the old national Emergency Preparedness 2535. The new plan provides a framework for defining strategies, measures, projects for responding effectively to handle national emergency and security concerns. The new national emergency preparedness plan calls for other involved agencies to devise plans that comply with the National Emergency preparedness Plan and must carry out drills and practices regularly in response to simulated events and circumstances.

The new Plan's directives call for the following:

1) **Prepare the resources**

It is required for all the agencies to prepare for disaster, militate against disasters; response to a community's needs after the disaster, and launch an effective recovery effort.

2) **Participation**

It is required that all government agencies, state enterprises, private sector companies and agencies, public enterprises, and all citizens to participate and support national emergency response plan and nation defense plan.

3) **Plan**

All government agencies must formulate an emergency preparedness plan in an integrated manner

4) **Management**

The government emergency management must be executed systematically, efficiently, in a timely manner in response to a crisis. The preparedness plan will be done in 11 areas: Disaster Alert, Search and Rescue, Water, Healthcare and Medical Services, Person Identification, Communications, Public Relation, Database and Information, Fuel and Energy, Agriculture, Transportation. Each of which is basically an emergency response support function. The National Preparedness Plan in Communications is the responsibility of the MICT. The National ICT Security Master Plan must take into consideration the National Preparedness Plan on Database and Information and the National Preparedness Plan on Communications to assure that the critical information infrastructure (CII) would not be compromised during a crisis or emergency situation. Measures must be designed to prepare the CII for disaster, to mitigate against disaster and to recovery effectively so that essential government service continuity can be assured.

3.4 ICT Support Policy

1) Research and Development

The research and development of ICT security in Thailand barely begins. The Thai Research Fund (TRF) supported only one research project in computer security in the last decade. The National Electronic and Computer Technology Center (NECTEC) also maintain no active research in ICT Security while the ThaiCert has spent substantial efforts in disseminating ISO 27000 security management standard for public.

The research at the graduate levels in many of the information technology, computer science, and engineering appear to have no research contributions in this area. In order to promote the ICT Security as a viable ICT industry segment that can bring substantial revenue to Thailand in the future. It is essential to start the research funding in this expanding and increasing important area. It is imperative that the National ICT Security master plan be provide a policy for strengthening research in ICT security so that Thai researchers would have chances in contributing to building a secured and safe Thai society that is advance and peaceful , adhering to the self-sufficiency principle.

2) Security Technical Reference Model

The technology of security is framed into a technical model which is a stack of technologies including Anti Virus, Anti Spam, URL Filtering, Firewall, VPN, Intrusion Detection, Identity Management, Strong Authentication, Early Warning and Security Monitoring. The aim of the deploying multiple ICT security technologies is to design a system which can withstand the attacks by deploying secured software and hardware with security functions that are integrated and can be handled by the operational staff. For the system the following technology must be considered: secured system architecture, encryption technology, authentication and authorization, network and system management , monitoring, checking and incident handling, backup and recovery technology, and physical security and access control technology

For the information security management to mitigate the threats and management the overall system security, the ISO 27000 must be deployed to ensure the security measures :

applying information security management process , applying best the practices in security management, developing human resources to be competent in ICT security management, instill in the organization the security awareness and the knowledge, skill, ability to manage the security aspects of the organization's operations.

3) Management

For a large organization, it is critically important to ensure the business continuity when a crisis or emergency occurs. The organization must have a disaster recovery procedure by deploying technology and staff at the organizational level to ensure the preparedness of the organization to handle the emergency or any attack from a threat.

In order to prepare for the ICT security threat, ISMS (Information Security Management System) based on ISO/IEC 27000 must be implemented. These include: ISO/IEC 27000 Fundamental and Vocabulary, ISO/IEC 27001 ISMS Requirement, ISO/IEC 27002 ISMS Code of practice, ISO/IEC 27003 ISMS Implementation Guideline, ISO/IEC 27004 ISMS Measurements, ISO/IEC 27005 ISMS Risk Management, ISO/IEC 27006 ISMS Accreditation Guideline. Consequently, human renounce development in the ISO 27000 security standards is needed to have sufficient number of qualified personnel among whom, a certain number must be certified. Deploying ISMS would reduce the risk of cyber attacks substantially and also promote the operation that is transparent, auditable and efficiency. The National ICT Security Master Plan would promote the policy that support the companies that provide ICT security training and certification and

support the educational institution to offer formal education and training in ICT security.

4) ICT Security Project management

ICT Security project must be managed based on the process as described in the ISO/IEC 27001 in which a Plan-Do-Check-Act (PDCA) loop is used as shown in Figure 4 Then a 10 step ISMS procedure can be applied to all agencies. All agencies must be required to execute the ISMS procedures.

4. Federated Model for ICT Security Planning

In designing the ICT Security Master Plan, a federated model is proposed since this model accommodates other component such as ICT security environment, investment and strategic planning, and national policy on e-business and ICT security. The model as shown in Figure 4 depicts that the Ministry of ICT provides the strategic initiatives to gather the strategic directions as outlined in Sections 2 and 3. The output from the first stage then drives the strategic planning processes. In addition to the traditional SWOT analysis to derive the strategic themes, this model uses the concept of Business Reference Model (BRM) from the Federal Enterprise Architecture Framework [3] . The corresponding Business Security Reference Model (BSRM) will define the security requirements of business functions independent of the agency that performs them. For the Security Technical Reference Model (STRM), it describes the standard specifications, and security technologies that support and enable the delivery of the agency's business services and capabilities securely. The result from the strategic analysis will guide the formulation of ICT security projects as well as other non-ICT projects and activities . In concretization of the ICT Security Master Plan implementation, it is proposed that the desired actual ICT environment must be considered at this stage of the planning process.

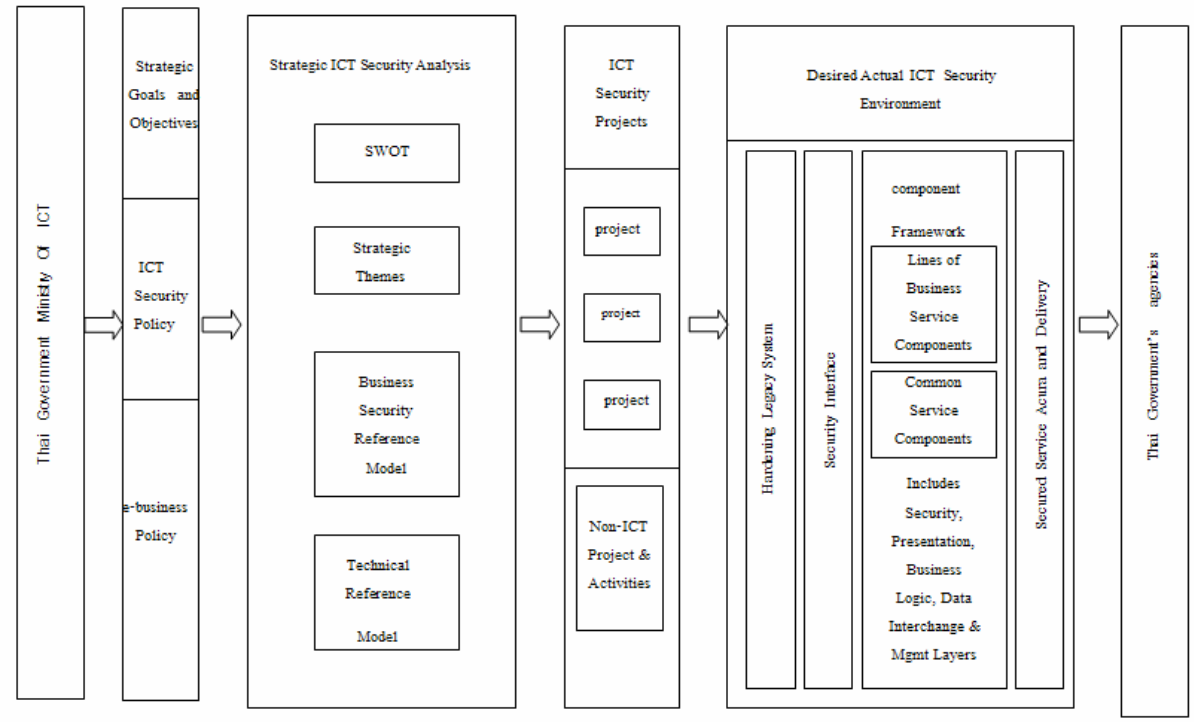

Figure 3. The Enterprise Architecture-Based Strategic Security Planning Methodology

5. Conclusion

In designing the ICT security master plan, many fundamental issues concerning ICT, technology development, human resource management, ICT laws, security standards and management issues must be addressed. The ICT Security Master Plan must also be aligned with the National ICT Master Plan and other plans related to national information infrastructure protection, national preparedness plans and business continuity plan. The National ICT Security Master Plan must guide the countries in implementing the measures and mechanics that ensure each agency can operate e-business securely.

Also, the National ICT Security Master Plan must set the policies encouraging government agencies and the Thai society that implement ICT systems to conform with the international ICT as recommended by the national ICT Security Master Plan. Finally, the equipment used in the network msut be certified and in conformance with the relevant ICT security standards, testing and certification procedures. The proposed enterprise-architecture based ICT security strategic planning methodology can provide the guidance of designing the ICT Secuirty master plan that includes all the critical factors that are essential to the success of implementing the master plan.

6. References

[1] The 1st National ICT Master Plan, NSTDA, Thailand

[2] Federal Enterprise Architecture, CIO Council, 1999.

[3] Australian Government Information Technology Security Manual (the Defense Signals Directorate, Department of Defenses) which are designed to enable government agencies to achieve an assured information technology security environment

[4] The Infosec-Registered Assessor Program (I-RAP) is a DSD initiative designed to register suitably qualified information security assessors to carry out specific types of ICT security assessments to Australian Government standards

[5] INTERNATIONAL STANDARD ISO/IEC 27001

[6] กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

[7] htt://thaicert.nectec.or.th ThaiCERT Nectec มาตรฐานการักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2) ประจำปี 2549