The Analysis and Evaluation of Security Readiness in ICT Infrastructure for Supporting e-Learning in Institute of Physical Education

Thanakorn Meehinkong¹  
Prasong Praneetpolgrang²  
Kittima Mekhabunchakij³  
Faculty of Informatics, Doctor of Philosophy Program in Information Technology  
Sripatum University, Bangkok, Thailand 10900.  
Email: ¹thanakorn_me@yahoo.com, ²prasong.pr@spu.ac.th, ³kittima.me@spu.ac.th

Abstract- Many educational organizations in Thailand have started to adapting e-Learning systems technique as a part of the learning program. However, there have been different levels of achievement due to many factors that affect the success of e-Learning program. One of the major factors that contribute to the ineffectiveness of e-Learning system is the readiness of security infrastructure of information and communication technology (ICT). This research aims to analyze and evaluate the readiness of ICT security infrastructure in order to determine the supporting of e-Learning systems against the international IT security standard. The methodologies used in this research are questionnaire, observation, and interview. After data collection and analysis, the result of research will show what factors are affected by infrastructure and will offer solutions to solve infrastructure security problems. This will lead to a successful implementation of e-Learning systems in the Institute of Physical Education.

Keywords- ICT Security Readiness, e-Learning, ICT Infrastructure.

I. INTRODUCTION

At present time, technology progress cause changing in all field, all society, all career. Institute of Physical Education is an organization do duty in education service and is one of developing education form organization. Institute of Physical Education’s model scheme year 2008-2012 has target to create readiness in ICT Infrastructure to be standard and continuity security, stress in providing legal computer system, develop together using network resource as infrastructure for computer and internet service.[1] The e-Learning project is one of a goal in Institute of Physical Education ICT strategy, for giving education service without limited of time and distance problem, then, information can exchange all time and place. The e-Learning is any type to pass on knowledge through electronics equipment as computer, internet, intranet, extranet or television signal, satellite. Information content is in form of Computer-Assisted Instruction, Web-Based Instruction, On-line Learning, Distance Learning via Satellite, Video On-Demand. When computer network and internet expands cover more areas, students or learners are more interested in and get in e-Learning system.

ICT Infrastructure is necessary for e-Learning management, preparing knowledge content, pass on knowledge, communicate between students and instructors or students and students. As if, ICT Infrastructure has no security readiness, education management may not successful. From this condition, should analysis study and evaluate security in ICT Infrastructure to
search for the way to protect and solve forbiddingness problem. Students might be get wrong information or distorted information which come from confidentiality, integrity and availability by non-permission person, cause to unsuccessful e-Learning in Institute of Physical Education.

II. THEORY

A. e-Learning

e-Learning means whatever type of learning that the information content pass through electronics equipment, computer, internet, extranet or television signal or satellite. The information content may be in form of Computer-Assisted Instruction, Web-Based Instruction, On-line Learning, Distance Learning via Satellite or not well-known media, such as Video On-Demand.[2] e-Learning is built up for Distance Learning, it is a learning form that learners do not necessary come to study in same place and same time. Learners have to study the content from e-Learning courseware that means studying or learning across the computer which efficient design and develop for display knowledge content in multi-media form, stress the content by non-linear, designed interaction activity, include exercises and tests for self understand confirmation. The content of e-Learning courseware is divided in modules, after self study, learners have to discuss and share their opinions and also ask question with their classmates through electronics. Although, e-Learning has established for long time, but it is not successful due to non-readiness ICT Infrastructure involve with e-Learning. Present, the price of this technology is cheaper than the past, many education institute or college give more priority in e-Learning. Government allocate budget for supporting ICT Infrastructure, such as computer, internet and network.

B. ICT Security

Protection ICT Security in organization refers to confidentiality, integrity and availability [3],[14] for ICT asset. ICT Infrastructure asset means people, equipment, software, information, network standard and transmission codes. As if these infrastructure has less or lose security condition it impact to the organization.

Many organizations adopt ICT Security international standard to be main principle to develop organization’s ICT Security for confidential and acceptance to public.

At present, many organization in Thailand and all over the world, emphasize in the word Best Practices or the direction standard that prepare organization’s ICT to IT Governance. The popular best practices are ISO/IEC 17799, CobiT and ITIL.

1) CobiT: CobiT comes from control objectives for information and related technology. Use for built up confident or trust in using ICT resource confrom with business objectives, cause to using efficiency resource, assist balancing between IT Risk and IT ROI. CobiT consist of main activities 34 items combine with minor activities 318 items, create framework in IT internal audit. CobiT process has 4 topics are

- PO : Planning and Organization has 10 objectives
- AI : Acquisition and Implementation has 7 objectives
- DS : Delivery and Support has 13 objectives
- M : Monitoring has 4 objectives

CobiT point to tell that what organization need but has no detail how to that state. CobiT proper with auditor to make Check Lists or Audit Program, but not proper with business executive and IT executive who use CobiT in their organization as practical implementation.[4]

2) ITIL: ITIL comes from IT Infrastructure Library, has objective to create Best Practices for IT Service Delivery and Support. But it is not a framework of widely controlling as CobiT. ITIL offers
practice procedure in only IT service management, however it gives more detail in working process for ICT system and service management. ITIL as a guidance about ICT Infrastructure, 8 items

- Software and Organization Asset Management
- Delivery and Service Standard
- After Delivery Quality
- Service Management Planning
- ICT Infrastructure Management
- Application Management
- Security Management
- Business Vision

Using ITIL in organization, Executives should have long distance vision which the benefit they have got worthy for invest in. However, ITIL best practice is well-known and used in many industrial, it does not mean that to directly work in organization, it must be know how to apply this knowledge proper with each organization.[5]

C.ISO/IEC 27001: ISO/IEC27001 is a regulation for making security management in organization, compose of

- Scope
- Terms and Definitions
- Structure of this standard
- Risk Assessment and Risk Management

ISO/IEC17799:2005 is a practice process lead to organization security management with acting under ISO/IEC27001. This standard gives detail how to decrease the risk in system weakness point, and give direction how to practice for increase appropriate and sufficient security state.

ISO/IEC17799:2005 has 11 domains

- Security Policy
- Organization Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communication and Operation Management
- Access Control
- Information Acquisition, Development and Maintenance System
- Information Security Incident Management
- Business Continuity Management
- Compliance

Nowadays, ISO/IEC27001 is extensive use, cause of it is a cycle, Plan-Do-Check-Act, and it uses risk assessment in consideration for find out method to risk defensive measure and organization IT asset protection.[6],[15]

D.Concept of Evaluation

Alkin defined the word “Evaluation” that it is a collecting information selection process and utility IT management, present to the person who has power in decision making or to specific activity or project.[7]

Shuffle beam and et.Al gave meaning of evaluation that it is a analysis process in order to get usefulness information for making decision the best choice.[8]

Robert. Stake said that evaluation paradigm is a basic idea which be the system and inclusive determine basic factor of standard practice and project value judgement, besides determine only objective product. Classify information to 2 parts, Description Matrix and Judgement Matrix. Robert Stake presented that before describe and judge the value of project, auditor should analyse the project principle and reason, it could get enough information for project value judgement.[9]

Briefly, Evaluation is an analysis standard information practices selection system, this information is utility for the best decision.
E. Related Research

1) The research “Security in Modern Business: Security Assessment Model for Information Security Practices”: by Daniel W K Tse from IT System, Hong Kong University. This research presents a model to evaluate IT security in modern business and refer to at present popular model, such as TCSEC, ITSEC, CIA, GASSP, BS7799, CobiT, ISO9000 and CMM.[10] Researcher selected BS7799, ISO9000 and CMM(Capability Maturity Model) for finding relationship and create a new model, to be more covering operation and stress in growth IT security system and follow CMM, specific growth level with BS7799 items.

2) The research “Information Security Management – A New Paradigm”: by Jan Eloff from Pretoria University and Mariki Eloff from University of South Africa, this research present a new form of information security management model, using ISMS model (Information Security Management) and refer information security standard ISO17799.[11] The research shows using model ISMS divided in ISMS process and ISMS product. In ISMS product, use ISO17799 items link up information system product type for evaluating the existent product, such as individual security in database product type, but not include network system and operation system.

F. Research Conceptual Framework

Analysis and Evaluation security readiness in ICT Infrastructure for supporting e-Learning, researcher determine factor of ICT Security using ISO/IEC 27001 for creating questionnaires. After explore the sample’s opinions and analysis data, this will know ICT Security level and main factors that impact to infrastructure.

Later, take these factors come to build up questionnaires and interview form to ask the sample how 4 factors impact to 5 ICT Infrastructure as shown in Fig 1.

III. RESEARCH METHODOLOGY

A. Population and Sampling Groups

Staff is in Institute of Physical Education with 17 campuses, 11 sports schools and central institutions of 29 agencies. The 767 samples of population that used in this research is random sample that classify by the Morgan and Krejcie [12]. The sample is divided into 4 groups as follows: 141 executives, 58 administrators, 288 instructors and 280 staff offices.

B. Research Tool

In this research, we use the questionnaires as research tool with sending 767 sets of questionnaires; we receive the return question papers with 513 sets that is only 66.88 percent.

C. Data Analysis

This research study, we have quantitative data from questionnaires, observation, interview and data analysis with statistical mean and standard deviation. We adopt t-test for hypothesis testing.
IV. RESEARCH RESULT

A. ICT Security Analysis Result

Researcher created questionnaires for collecting data which these questionnaires rely the standard ISO/IEC 27001, the ICT Security Standard. The questionnaires had used to enquire the security opinions from 4 groups of representative sample, these are executives, instructors, system administrators and office staff. The research result found that

1) Policy and Organization of Information Security: found that the office has specific written policy and broadcast, together with specific administration structure, responsible person assignment. All level of directors gave precedence to the ICT Security. Mean = 2.90 (Moderate)

2) Asset management: found that the office manipulate the asset list, disburse account, asset classification, secret category and important degree, rule, regulation, and using asset. Mean = 2.93 (Moderate)

3) Human Resources Security: found that the office has posed person and contractor selection process, educate the staff aware to ICT Security, specific employment condition, in case before resign they must be hand on and check over the asset and cancel that person to use the office ICT access. Mean = 2.94 (Moderate)

4) Physical and Environment Security: found that the office design in and out building control, taking computer accessory and network out of office control, appropriate safety equipment setup, fire and flooding prevention system, uninterruptible power system, air condition. Mean = 2.99 (Moderate)

5) Communication and Operations Management: found that the office has the plan for developing equipment and program to always be good quality, separate acting service system out of developing system, has detecting system for protection hacker who destroy ICT data, has good quality anti-virus software. Mean = 2.88 (Moderate)

6) Exchange of Information: found that the office create process control for receive and send e-mail, ICT data exchange and online business, has ICT data accuracy system. Mean = 2.69 (Moderate)

7) Back-up: found that the office has filing and store data system, testing data and information, destructive measure for disuse data, log file for user, defensive editing log file. Mean = 2.69 (Moderate)

8) Access control: found that the office has password account for control authority and information access, separate user, control arranging and editing operation system, control using utility program, time limit for importance information access, control using cell phone and notebook through network channel. Mean = 2.70 (Moderate)

9) Information Systems Acquisition, Development and Maintenance: found that the office improve acquisition system, development system, maintenance, verify, analysis and identify software characteristic, hardware and network equipment that appropriate with user requirement, error checking, information lost, program supplement old and new co-operation testing, control using secret testing system data. Mean = 2.75 (Moderate)

10) Information Security Incident Management: found that the office produce attack information preventing system, reporting the weakness and circumstance, compile evidences for process of legal reference, record the attack and aggression ICT Security, for making decision direction which immediately and accurately manage. Mean = 2.63 (Moderate)

11) Compliance: found that the office determine rule, regulation and principle for using the system. Add control, supervise and restrict user, has punishment process people and contractor who infringe or aggress for protecting intellectual property piracy. Mean = 2.72 (Moderate)

Result from an analysis of questionnaires a summary as shown in Table I
### TABLE I

Demonstrate the Level of ICT Security

<table>
<thead>
<tr>
<th>Dimension of Security</th>
<th>Mean</th>
<th>S.D.</th>
<th>Level of Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy and Organization of Information Security</td>
<td>2.90</td>
<td>0.88</td>
<td>Moderate</td>
</tr>
<tr>
<td>Asset Management</td>
<td>2.93</td>
<td>0.83</td>
<td>Moderate</td>
</tr>
<tr>
<td>Human Resources Security</td>
<td>2.94</td>
<td>0.84</td>
<td>Moderate</td>
</tr>
<tr>
<td>Physical and Environmental Security</td>
<td>3.00</td>
<td>0.78</td>
<td>Moderate</td>
</tr>
<tr>
<td>Communications and Operations Management</td>
<td>2.88</td>
<td>0.89</td>
<td>Moderate</td>
</tr>
<tr>
<td>Exchange of Information</td>
<td>2.69</td>
<td>0.92</td>
<td>Moderate</td>
</tr>
<tr>
<td>Back-up</td>
<td>2.69</td>
<td>0.90</td>
<td>Moderate</td>
</tr>
<tr>
<td>Access Control</td>
<td>2.71</td>
<td>0.92</td>
<td>Moderate</td>
</tr>
<tr>
<td>Information Systems Acquisition, Development and Maintenance</td>
<td>2.75</td>
<td>0.89</td>
<td>Moderate</td>
</tr>
<tr>
<td>Information Security Incident Management</td>
<td>2.63</td>
<td>0.93</td>
<td>Moderate</td>
</tr>
<tr>
<td>Compliance</td>
<td>2.72</td>
<td>0.95</td>
<td>Moderate</td>
</tr>
<tr>
<td>Average</td>
<td>2.80</td>
<td>0.88</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

#### B. Security Readiness in ICT Infrastructure Evaluation Result

The questionnaires that researcher created for collecting data to evaluate ICT Infrastructure Readiness, consideration from Institute of Physical Education’s ICT Security condition. Inquire 3 target groups, there are Executives, Instructors and system operators who directly involve with e-Learning. The considerate topics are Policy and Structure, People, Hardware and Accessory, Software, and Physical and Environmental. The research results are:

1) **Policy and Structure**: People in Institute of Physical Education ascribe that the office specific the policy, administration structure, appointing person in charge, for Security ICT Infrastructure in moderate level, mean = 2.83. Describe that Institute of Physical Education has ready in policy and security structure management but there has not thoroughly extensive operated. Supposing the control, follow up and examine the people act up seriously to the policy and assignment, and the office has punishment rule, it would have been more high quality.

2) **People**: Institute of Physical Education people give opinion moderately that the office of training and educate the staff aware to ICT Security has intellectual person and appropriate number with ICT assignment, has people selection system, has employment condition which supporting ICT Security. Mean = 2.87. It means that Institute of Physical Education has ready in people who can work but lacking in number and knowledge requirement.

3) **Physical and Environment**: Institute of Physical Education people express that the office provide suitable environment in moderate level with internet service, there has computer room, safely network control room, in-out control system both computer room and network control room, in-out office building control system, control moving hardware and network accessory, preventing fire and flooding control, uninterruptible power system, air condition. Mean = 2.93 It means that Institute of Physical Education has ready in physical and environmental but sufficient computer room, less quality security control. For increasing good quality security, should follow up people continuously operation. Computer room (place and environment) should have reasonable budget plan for affording the requirement.

4) **Hardware and Accessory**: People of Institute of Physical Education criticize that the office has number of computer, network accessory, network and internet system, development hardware and accessory planning, separate active service out of improving service, intrusion detection system for protection data from hacker, moderate level. Mean = 2.88 It refers that the Institute ready in hardware and accessory but not enough, it could not service all office. And intrusion detective system is less quality.

5) **Software**: Institute of Physical Education people comment that the office has Operating System Program, Application...
Software, Package Software which support office working, create multi-media, improve providing system, maintenance, check up, analysis, and specify user’s requirement software characteristic, error and data lost checking. All in moderate level, Mean = 2.73 It means that Institute of Physical Education has readiness in software but still has not enough, for example, Clint, Package Program for office administration, Graphic Program, Multi-Media Program.

Result from an analysis of questionnaires a summary as shown in Table II

<table>
<thead>
<tr>
<th>Infrastructure ICT</th>
<th>Mean</th>
<th>S.D.</th>
<th>Level of Security Readiness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy and Structure</td>
<td>2.83</td>
<td>0.93</td>
<td>Moderate</td>
</tr>
<tr>
<td>People</td>
<td>2.87</td>
<td>0.87</td>
<td>Moderate</td>
</tr>
<tr>
<td>Physical and Environmental</td>
<td>2.93</td>
<td>0.82</td>
<td>Moderate</td>
</tr>
<tr>
<td>Hardware</td>
<td>2.88</td>
<td>0.86</td>
<td>Moderate</td>
</tr>
<tr>
<td>Software</td>
<td>2.73</td>
<td>0.91</td>
<td>Moderate</td>
</tr>
<tr>
<td>Average</td>
<td>2.85</td>
<td>0.76</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

C. Security Readiness in ICT Infrastructure - Interview Evaluation Result

Analysis questions from groups of directors and instructors interview, there are

1) ICT Security Significance: Person or staff in Institute of Physical Education place importance in ICT Security. They give the reasons that for knowingly alternate current situation that communicate pass computer and internet network, it should be have security system to protect loosing data, editing data, break down control and to support the act or rule or bureaucracy.

2) ICT Security Actual Problem: The office has not using control system in computer and internet network, non-quality internet network, lack of knowhow technical person, these go to be destroy data by virus, loosing data, using other data which disallow, inactive computer because of inoperative program, slowly solving network problem.

3) ICT Infrastructure Budget Supporting: The 29 office in Institute of Physical Education all are operating settle ICT Infrastructure and testing the system and also develop the Application in e-Education, e-Library. Institute of Physical Education propose ICT model scheme year 2008-2012, the 5 strategies compose of 1) e-Learning education and sport management strategy - budget 47,820,000 baht 2) Arrange Readiness strategy for ICT Security Infrastructure in expectation standard and continuity – budget 305,025,000 baht 3) e-office Institute of Physical Education administration strategy – budget 59,650,000 baht 4) Improve people potentiality – budget 34,822,600 baht 5) Develop ICT Management and Service to public by e-Government – budget 16,000,000 baht. The whole budget 463,318,100 baht.[1]

D Infrastructure Effect Factors

Evaluation result of Security Readiness in ICT Infrastructure show that there have risky factors might be effect to unsuccessful e-Learning Program. The encounter problems are Executives do not administrate people working under the policy, less and discontinuous training about security knowledge and awareness.

The factors that effect to ICT infrastructure are executives, people, budget and plan.

1) Policy: The effects are Executives reinforce but do not govern their people to comply with the policy, People do not realize to act follow the policy, so security readiness is in moderate level.

2) People: The effects are Executives give supporting in selection and appointment people position but the people have got less knowledge training and discontinuous, and they do not realize the security. Security readiness is in moderate level.

3) Physical and Environment: The effects are Executives support Physical and Environment with proper budget but people...
have no awareness in office security. Moderate level in Security Readiness.

4) **Hardware**: Executives set up not enough budget for development plan in hardware and equipment, so Security Readiness in moderate level.

5) **Software**: Executives set up not enough budget for development plan in Software, people lack knowledge and skill. Security Readiness is in moderate level.

Evaluation result of Security Readiness in ICT Infrastructure Effect Factors as shown in Table III

<table>
<thead>
<tr>
<th>Factor</th>
<th>Infrastructure</th>
<th>Impact</th>
<th>Security Readiness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executives People Budget Plan</td>
<td>Policy</td>
<td>- Executives support - People are not awareness - Executives are not control for compliance</td>
<td>Moderate</td>
</tr>
<tr>
<td>People</td>
<td>- Executives support - People are not awareness - Peoples lack of knowledge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical and Environment</td>
<td>- Executives support - People are not awareness - Appropriate budget</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td>- Executives support - Plan update and development - People lack of knowledge - Budget is not enough</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>- Executives support - Plan update and development - People lack of knowledge - Budget is not enough</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**V. CONCLUSION**

The explore questionnaire result about ICT Security in Institute of Physical Education found that ICT Security degree totally 11 dimensions have mean 2.80, moderate level. Consider in each dimensions, explain that the highest mean 3.00 is Physical and Environment, the lowest mean 2.69 is Exchange of Information and Back up, another has mean between 2.71 – 2.94.

The Security Readiness in ICT Infrastructure in Institute of Physical Education, evaluate from the questionnaires, the result is all 5 dimensions have mean 2.85 moderate level. Physical and Environment has the highest mean 2.93 Software has the lowest mean, another has mean between 2.83 – 2.88.

Evaluation Security Readiness in ICT Infrastructure in Institute of Physical Education from document and interview the samples, can conclude that Executives and Instructors emphasize in ICT Security Infrastructure. The most security problems are about people security compliance control, non-quality network and internet system, people lack of knowledge and awareness in ICT Security, lack of good quality Anti-Virus Software. In part of ICT Infrastructure budget, Institute of Physical Education has model scheme year 2008-2012, divide suitable budget for ICT Infrastructure, budget amount 8,000,000 baht for e-Learning program and 305,025,500 baht for Hardware and equipment.

Entirely research result show that Institute of Physical Education has ICT Security in moderate degree and should be improve and develop some points. Recently, Institute of Physical Education is in the state of innovate computer and internet system, after this project complete it would ready for e-Learning program. From high budget for ICT Infrastructure, providing computer and all hardware, include software and network system cover every office, and now they are installing and testing service system, and developing need application for office, e-Office, e-Library, e-Government.
Therefore, the office in Institute of Physical Education is ready in ICT Infrastructure for service and support efficiency e-Learning in academic year 2010.

VI. SUGGESTION

From this research found that ICT Security in Institute of Physical Education has risky in information data damage. The office has to determine the risk control in acceptable rate. Main objective of this research is to study Security Readiness in ICT Infrastructure for giving support to e-Learning Program, research result found that Security Readiness in ICT Infrastructure condition which risky to be effected to e-Learning using, it might impact to unsuccessful as expected. Thus, it should seek procedure for acceptable risk control by applying revise point from this research result. As follows

1) Policy and Structure: Review the Policy and Management Structure in ICT Security to be coverage and clearance. Manage, follow up and examine people to work or act seriously comply with the policy and job assignment. Define punishment rules for out of control people. There will be more efficiency management.

2) People: Screen and assign ICT Security operators with the people who understand and realize in security. Provide constantly and continuously ICT Security training course to all staff level by duty and responsibility, for example, using computer training course, using Package Software, using Application Software. Inspire people aware in ICT Security.

3) Physical and Environment: Set up environment to support internet service and e-Learning. Specific computer service time schedule with user’s comfortable and sufficient. Control security guards to work with strict and ascetic action.

4) Hardware: Provide number of computer appropriate with number of students and staff. Expand network and internet to meet user’s requirement. Install the intrusion detection system, Log file system for more secure and to be in line with computer security law.


REFERENCES
