J Intell Manuf (2012) 23:965–975
DOI 10.1007/s10845-011-0503-y

Establish a secure and trustworthy ICT environment for educational systems: a case study

Yu-Hsiu Chuang · Chi-Yuan Chen · Tzong-Chen Wu · Han-Chieh Chao

Received: 10 May 2010 / Accepted: 9 January 2011 / Published online: 26 January 2011

Abstract Nowadays information and communication security has recently emerged as one of the most important tasks in the field of network management, operations and maintenance. The information security issue is of particular importance to the Taiwan Academic Network, a network which connects the networks of educational and research institutions in Taiwan. ICT environment in educational systems involves vast connected units and is featuring complexity, diversity and openness. In this paper, we investigate current situation of Taiwan Ministry of Education ICT security development and provide a case study. We also discussed challenges and solutions for improving ICT security environment in educational system.

Y.-H. Chuang
Graduate Institute of Management, National Taiwan University of Science and Technology, Taipei, Taiwan, ROC

Y.-H. Chuang · C.-Y. Chen · H.-C. Chao
Computer Center, Ministry of Education, Taipei, Taiwan, ROC

Y.-H. Chuang
e-mail: chuang@mail.moe.gov.tw

C.-Y. Chen
e-mail: justin@mail.moe.gov.tw

C.-Y. Chen · H.-C. Chao
Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan, ROC

T.-C. Wu
Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan, ROC
e-mail: tcwu@cs.ntust.edu.tw

H.-C. Chao (✉)
Department of Electronic Engineering and Institute of Computer Science & Information Engineering, National Ilan University, Ilan, Taiwan, ROC
e-mail: hcc@niu.edu.tw

Keywords Security policy · Educational system · Case study · ISMS · Cloud service · Security talent cultivation

Introduction

Information and communication security has recently emerged as one of the most important tasks in the field of network management, operations and maintenance (Sardana et al. 2008; Kang et al. 2009). It is of particular importance to the Taiwan Academic Network (TANet), a network which connects the networks of educational and research institutions in Taiwan, because it has a wide range of users. To create a secure and trustworthy academic Information and Communication Technologies (ICT) environment for TANet, the Taiwan Ministry of Education (MOE) undertakes a comprehensive planning in three areas of information security management policies, information security defense technologies, and information security awareness and manpower. The vision of Taiwan MOE for establishing a secure and trustworthy ICT environment is depicted in the Fig. 1.

In respect of information security management policies, MOE establishes its own certification scheme for educational institutions. It includes establishing an auditing system and educating Information Security Management System (ISMS) lead auditors for educational institutions. MOE also promote the ISMS concept with policies and activities. In addition, MOE also promote personal information protection and provide mechanisms for preventing information leakage.

In the past, due to the lack of an integrated information security defense and sharing mechanism, educational and research institutions were not able to establish their own information security teams, or only depended on a very small number of information security professionals to judge and

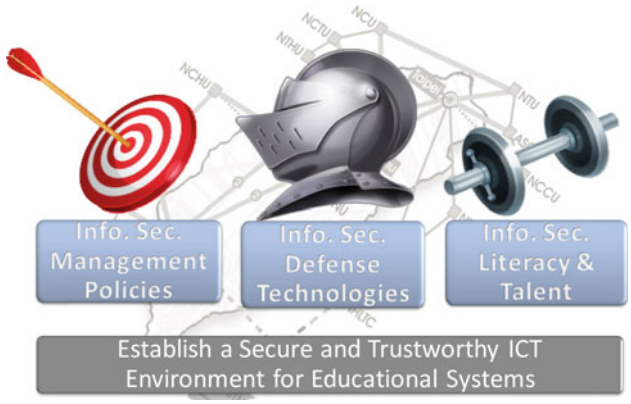

Fig. 1 Information security vision of Taiwan MOE

protect the security of TANet. In recent years, MOE has strived for a larger budget to expand TANet's hardware and software facilities. Since TANet provides service to such a large number of institutions across a vast area, a greater amount of funds is required to effectively strengthen the comprehensive defense system. The goal is implement a series of projects that will create a unified defense system for all regional, county and city network centers around Taiwan, and to achieve a multi-level longitudinal defense system for information security.

TANet has produced many academic and research professionals in this field. Through MOE's efforts, the information security education program offered by universities and colleges has become a significant channel for students to learn the theories and practices of information security. The MOE is also planning further promotions that will raise awareness of information security on campuses and to enhance students' information security literacy. MOE would also like to integrate the efforts of professionals and to lay an important foundation for the development of informational security in the educational system.

In this paper, we investigate Taiwan MOE ICT security development and provide a case study for improving ICT security environment in educational system. The remainder of the paper is organized as follows. In "Analysis of current situation", the current situation of Taiwan MOE ICT environment is analyzed. The Strategies and Action Plans of Taiwan MOE are studied in "Strategies and action plans". We also discussed these challenges and solutions in "Discussions" and made our conclusions finally.

Analysis of current situation

Every country has paid much attention to the cultivation of human talent. Advanced countries have embarked upon a path of education reform, with Taiwan recognizing education as the bedrock of national development. The Taiwan MOE (2010) is a cabinet-level governmental body of the Executive Yuan. It is responsible for formulating educational policies and managing public schools throughout Taiwan. The present Taiwan educational structure supports 22 years of formal study. Completion times are flexible, depending upon the needs of the students. On average, the entire process requires two years of preschool education, six years of primary school, three years of junior high school, three years of senior secondary school, 4–7 years of college or university, 1–4 years of a master's degree programme and 2–7 years of a doctoral degree programme.

In order to computerize administrative affairs, promote information education and web learning, and establish campus, inter-school, international networks, the Computer Center of MOE, MOECC (2010) was established in August 1982 on the approval of the Executive Yuan. It comprises six divisions—information education, digital infrastructure, information system, digital learning, digital resources, and information management. The MOECC has established an integrated information service system of comprehensive education administration and academic R&D environment.

Information security development of Taiwan MOE

The Taiwan Academic Network (TANet) is a national computer network for teaching research, jointly established by major national universities and the MOECC in July 1990. TANet's main purpose is to support teaching research activities in schools and research institutes throughout the nation by providing a medium for sharing resources and providing opportunities for cooperation. TANet has a backbone and a regional network structure as well as a research-related information infrastructure.

In July of 1999, a coordinated internal expansion began that promoted the use of ADSL in junior high and elementary schools to connect to TANet. The goal was for IT education to take root at lower levels and provide schools with network connections and a platform for IT education. In 2009, installation of fiber optic connections was begun at all levels, with the expectation that individual school network bandwidth could reach 100MB and have an IPv4/IPv6 dual stack network service environment.

Current TANet management is made up of a three-tier organizational structure that includes a TANet Management Committee, a Regional Network Center, and the City & County Network Center teams. It connects 4,108 schools and academic institutions, with over 4 million users. TANet's network structure is made up of 3 layers (as shown in Fig. 2):

(1) National Backbone Network
The MOE oversees Regional Network Centers, including domestic backbone and international circuits,

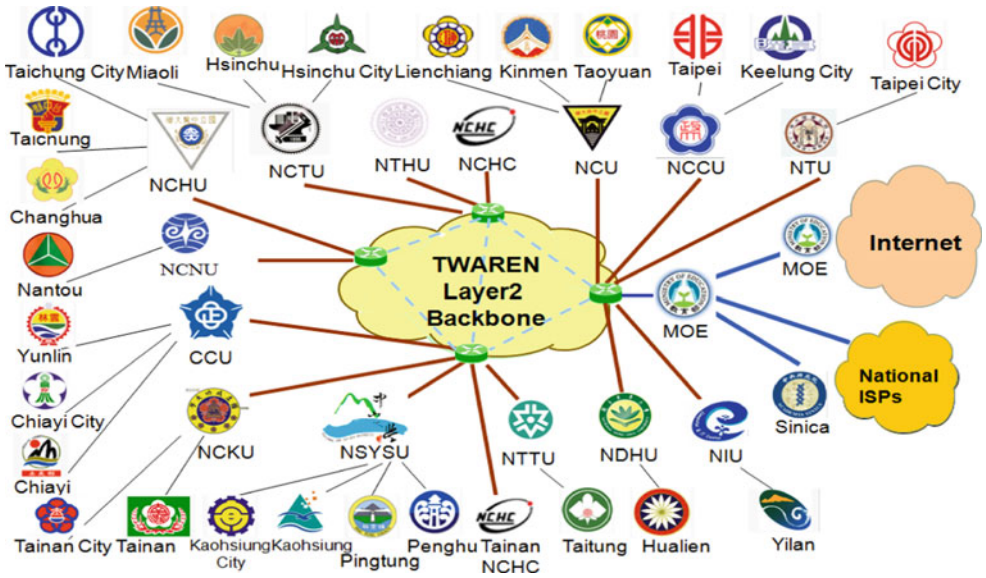

Fig. 2 Hierarchical structure of TANet

connections to each Regional Network Center, and the Internet along with other domestic network connections such as domestic ISPs, government networks and individual network exchange centers, etc.

(2) Area Networks
Area network backbone lines can be established via the Regional Network Centers and National Backbone Network connections. City & County Educational Network Centers connect city and county educational networks. In principle, each city and county should be able to provide an education and research related network. Responsibility for these networks lies with the Regional Network Centers and City & County Educational Network Centers.

(3) Campus Networks
Individual research unit, school, and campus area networks mined by the size and scope of an individual unit, network use requirements, actual experience and amount of funding available to establish a basic campus area network backbone-progressive expansion is possible. Responsibility for campus networks lies with individual school computing centers or related units.

On-campus information security is different from those in government agencies and private sectors because the former must consider factors like academic freedom. The most important issues include: the protection of student records and the personal information of both teachers and students; to ensure the security of networks but also keep the network traffic smoothly in computer classrooms and student dormitories; the flexible permission of network usage in research units and laboratories. Currently, senior high schools and below are generally encountering an environment beleaguered by insufficient security information, technical manpower shortages and budgets shortfalls. They are inadequate to enhance their networks against outside crackers and network viruses. Under such circumstances, promoting campus network security is a rather serious challenge. The Taiwan MOECC has plan a series of project for improving ICT security environment as shown in Fig. 3. These projects will be introduced in following sections with different aspects.

Information security and management policies

Information systems of cyberspace become attractive targets for hackers and crackers. Facing various threats from cyberspace, organizes must decrease attack impact and recover rapidly (Farn et al. 2008; Chu et al. 2009; Lai et al. 2003). Thus information classification is the primary work for Information Assurance (IA) (Frederick 2002). It is important to classify information according to its actual value and level of sensitivity in order to deploy the appropriate level of security (ISO/IEC 2005). In 2002, the National Information & Communication Security Taskforce, NICST (2010) of Executive Yuan in Taiwan specified Information Security Classification for government organization to continuously strengthen the implementation of information security operations. The Information Security Classification of NICST is shown in Table 1. It classifies all the organizations into four levels: Class A (Important Core), Class B (Core), Class C (Important), and Class D (General). These classes are based on "risk classification management" in BS 7799 Information Security Management System.

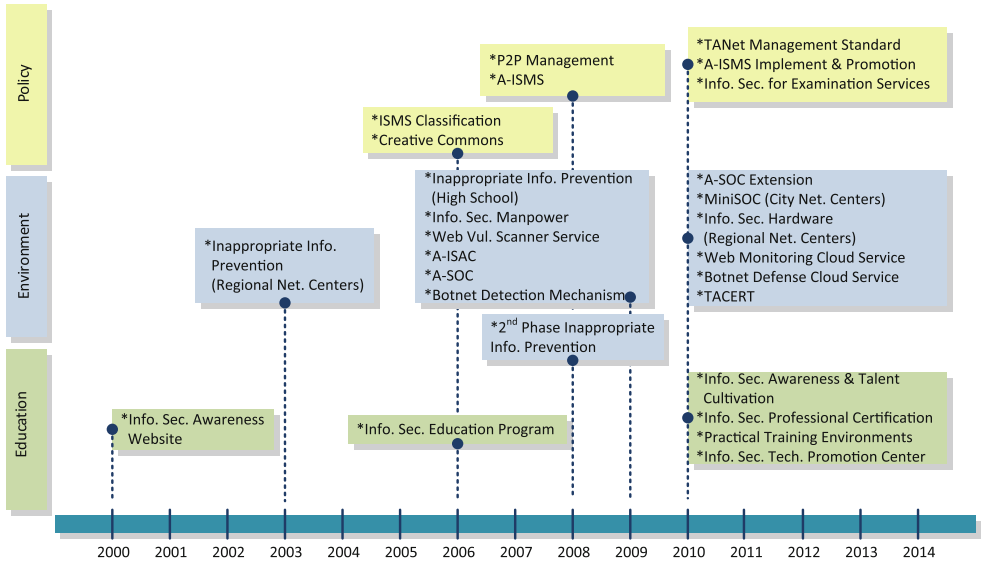

Fig. 3 Information security development Roadmap of Taiwan MOE

Table 1 Information security classification of NICST (2009)

Level	Defense in depth	ISMS approaches	Audit method	Information security training (officer, IT technicians, security technicians, user)	Professional certification	Detecting Website weakness
Class A	N-SOC/ SOC, IDS, Firewall, Anti-virus, SPAM	Passing third-party accreditation	At least 2 internal audit per year	At least 3,6,18,3 hrs/year	2 Copies of Info. Sec. certification	Twice/year
Class B	SOC (Opt.), IDS, Firewall, Anti-virus, SPAM	Passing third-party accreditation	At least 1 internal audit per year	At least 3,6,16,3 hrs/year	1 Copy of Info. Sec. certification	Twice/year
Class C	IDS, Firewall, Anti-virus, SPAM	Self-establishing ISMS working-group	Self-review	At least 2,6,12,3 hrs/year	Info. Sec. professional training	Once/ year
Class D	Firewall, Anti-virus, SPAM	Promoting ISMS concepts	Self-review	At least 1,4,8,2 hrs/year	Info. Sec. professional training	Once/year

Based on the classification of NICST, Taiwan MOE also classifies 4,080 educational institutions into four levels as shown in the Table 2.

Taking into consideration of factors of priority, emergency and available resources. Taiwan MOECC has designed the A-ISMS (Academic Information Security Management System) guidelines for educational institutions to help educational institutions procure ISMS certification. They also establish A-ISMS certification center for educational institutions and assist educational institutions to get A-ISMS certification. Taiwan MOECC mainly focus on the introduction of ISMS in B Level institutions (e.g. universities) and help 13 regional network centers and 25 county/city network centers to implement ISMS.

Information security and defense technology

Due to the imperative of establishing an integrated reporting and emergency response mechanism in TANet, the MOE established the Academic Information Sharing and Analysis Center (A-ISAC) platform and established an Academic Security Operation Center (A-SOC) in 2008. In the initiation phase, the MOE already deployed SOC monitor sites in 3 regional network systems to undertake the monitoring, control, and defense against malicious attack on the TANet. Through the A-ISAC platform, more than 4,000 connected educational and academic institutions can share their information and experience along with integrated reporting and emergency response mechanisms. In the future, the task will

Table 2 Information security classification of Taiwan MOE

Level	Institutions	
Class A important core	Educational authority (MOE)	3 Units
	2 Teaching hospitals	
	88 Universities	
	5 Permanent admission exam agencies	
Class B core	13 TANet regional network centers	132 Units
	25 County/city network centers	
	1 Teaching hospitals	
Class C Important	46 Colleges of technology and 17 junior colleges	87 Units
	24 MOE affiliated agencies	
Class D general	471 Senior high schools	3,858 Units
	3,387 Elementary and junior high schools	

be extended to cover all 13 regional networks, and create an integrated defense network.

In TANet, bot malicious software programs are quite a serious issue. The controllers may control thousands of bots to attack others, to send spam mails or to spread viruses. The hidden nature and incubation period of bot's as well as their ability to be gradually transformed from IRC to HTTP format has increased the difficulty of defense. The MOE planned a series of botnet detection and defense projects to effectively prevent the invasion of botnet malwares. Starting from 2008, the MOECC has established in regional networks a passive web application vulnerability scanning platform to prevent information leakage, focusing on SQL-injection and XSS (Cross-Site Scripting) problems, to help connected schools perform webpage vulnerability scans.

On the other hand, MOECC also paid attention to the network management issue. Network information is abundant, diversified and freely accessible. Contents may be muddled, and some may even be illegal, e.g. pornographic materials, illegal trade for firearms and drugs, suicide instructions, libel and cheating. Some, such as advocating pessimistic outlook on life, using rude and lewd words, and publicizing bloody or violent photos, are immoral and not appropriate for specific groups of people or under-age groups. Since all county/city network centers of TANet have established an inappropriate information filtering system, and reduced the ability of elementary and high school students to access inappropriate information through campus networks. They also established P2P bandwidth management system in regional network centers to protect the intellectual property rights. Furthermore, the MOECC worked together with private and non-profit organizations in enhancing the awareness and knowledge among parents.

Raise information security awareness and talent cultivation

The MOE actively concerns the promotion the information security awareness in order to enhance information security literacy for all people. From 2000, the Network Literacy and Awareness Platform called eTeacher is built under the support of MOECC. This platform not only provides newest information but also digital curriculum materials for teachers of elementary and high schools.

In the information security talent cultivation, the MOE promotes its "information security education program" in higher educational institutions to help students learn the theories and practical skills of information security and procure information security professional certificates. Since 2006, MOE has funded colleges and universities to promote the cross-department information security education program to cultivate information security talents through formal education systems. This project helps students obtain 256 certificates in total, including ISO27001LAC, ISO20000LAC, EC Council Security 5, and BS25999 LA. Among students who earned this information security program certificates in 2007 and 2008, about 73% continue their studies or go to military service, and about 12% enter the labor market. Sixty-one percent of the latter are working in industries relating to information security.

Strategies and action plans

In 2009, the Science and Technology Advisory Group of Taiwan Executive Yuan hosted a Strategy Review Board (SRB) on "Shaping a Culture of Security, Promoting ICT Security Industry." The MOE also proposed their vision and plans for 2010 to 2013. The whole picture of MOECC's goal is

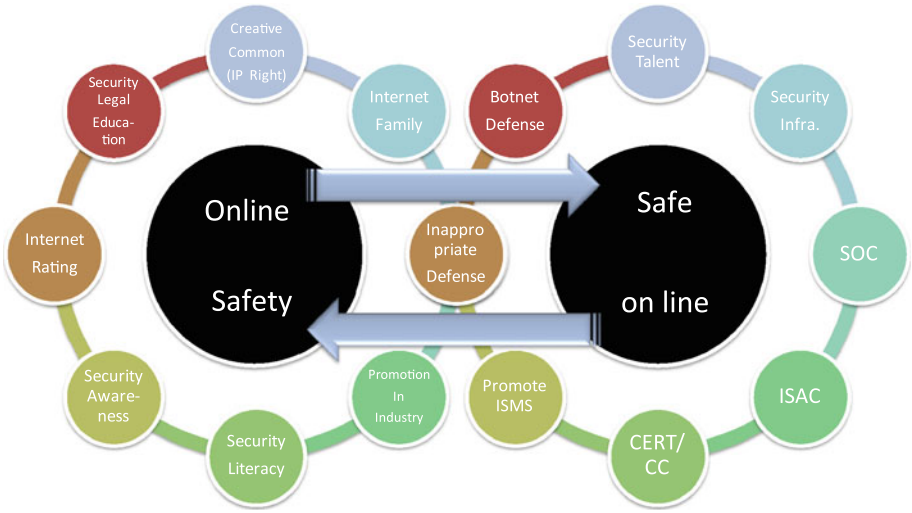

Fig. 4 Online safety and safe on line

shown in Fig. 4. In order to achieve "online safety" (cognitive education) and "safe on line" (safe environment), the MOE will implement strategies in different aspects to strengthen information security environment and enhance information security literacy in educational system. These strategies and corresponding action plans is depicted in Fig. 5 and summarized as follow.

Policy management aspect

The most information security incidents are resulted from the mistakes of management or operation inside organization. For this reason, to implement a suitable and cost-effective ISMS is a solution for the information security problem inside organization. Based on this approach, the MOECC has proposed these countermeasures.

Promote information security management system within educational systems

- Enact the guidelines concerning ISMS in educational system.

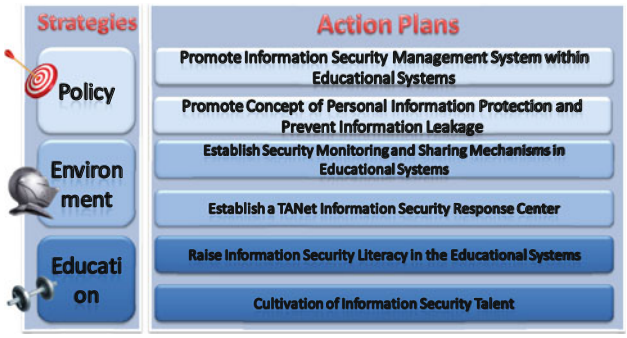

Fig. 5 Strategies and action plans

- Establish and maintain a Certification Center for Educational Institutions.
- Assist all level educational institutions in introducing ISMS and procuring certification.

Promote concept of personal information protection and prevent information leakage

- Incorporate personal information protection into information literacy promotion activities for public.
- Establish "Web Application Vulnerability Scanning Platforms for Educational Institutions" in all regional and country/city networks.
- Provide information security operation guidelines for all levels of admission examination systems.
- Provide security advising services for admission examination systems.

Environment and technical aspect

The most attack targets are information service systems. Moreover, in order to provide convenient electronic services and access services, the government of Taiwan has devoted to computerized various services. People can complete their business with public sector via Internet, such as the tax returns. In campus, school administration systems are also computerized, for example, web portal, registration system, and grading system. Hence the challenges of information security are increasing with the computerization degree of administration management and service business. Besides management policies, to provide defense technologies for protecting services and network is also important. Furthermore, automotive scanning and detection mechanisms are also under consideration for preventing intrusion and forecasting. Based on above-mentioned, the MOECC has proposed following mechanism.

Establish security monitoring and sharing mechanisms in the educational systems

- Extend Preliminary Academic Information Sharing and Analysis Center (A-ISAC) and Academic Security Operation Center (A-SOC).
- Support research teams of botnet detection and defense mechanisms.
- Strengthen the information security hardware facilities in regional network centers.
- Conduct research and development in information security message exchanges and automation mechanisms (miniSOC) for country/city network centers.

Establish a TANet information security response center

- Establish a TANet Computer Emergency Response Team (TACERT).
- Provide educational institutions with consultation and support in the field of information security technologies.
- Offer forecast and warnings for information security incidents

Education aspect

TANet is connected with domestic and international Internet Service Providers (ISPs). TANet users beside can utilize various information services inside campus but also access any service over Internet. Currently, many intrusion behaviors utilize common information service channels (such as E-mail and browsing phishing website) for enclosing malwares or backdoors to acquire valuable information. Raising user's awareness of judging the correctness information source or content is very important for strengthening information security protection capability. Based on this approach, the MOECC has planned these countermeasures.

Raise information security literacy in the educational systems

- Raise awareness of the importance of information security among students through various activities and competitions.
- Promote the information security literacy to all people.
- Conduct information security promotion programs in elementary and junior high schools.
- Integrate the subject of information security literacy into senior high school curricula.
- Integrate the subject of information security literacy into general education requirements at postsecondary educational institutions.

Cultivation of information security talent

- Provide practical information security training environment.
- Provide the manpower and enhance their skills in region and county network centers.
- Assist information security talent to obtain international security certifications.
- Cultivate ISMS lead auditors in educational institutions
- Hold information security seminars/study camps and organize voluntary information security defense team and communities in educational system.

Discussions

In the service scope of TANet, the users include students, teachers, staffs, parents and so on. The application fields include academic research, academic electronic journal, preliminary experiments of information technology, teaching, learning, administration, dormitory networks. In more detail, the application patterns include computerized school administration systems and various network application systems. These relationships are depicted in the Tables 3 and 4.

Based on the different educational structures (such as primary school, junior high school, senior high school, college or university), executive ownership (such as public, private, national, country or city), these institutes are featured with different resources including network environment, information resource, information services, and ICT security specialists. Hence the MOECC has classified these educational institutes into four security classes (A, B, C, and D). As we know, there is no such mechanism provides "absolute security". We just can implement suitable mechanisms for "relativity security". That is the reason why the MOECC adopt the PDCA (plan-do-check-act) (Deming 1986) of ISMS to evaluate and improve their planned projects iteratively. We will discuss these challenges and solutions with policy management aspect, environment and technical aspect, and education aspect in following sections.

Policy management aspect

In compliance with Executive Yuan's national information security policies, the MOECC will introduce a comprehensive information security management system in all educational institutions. In order to overcome the problem of insufficient funding, the MOECC also proposed A-ISMS (Academic Information Security Management System) guidelines for educational institutions in Taiwan. Furthermore, they also release the A-ISMS into complete version and simple version based on the difference of abovementioned information security classification. The MOECC

Table 3 The relationships of TANet users and application fields

	Students	Teachers	Staffs	Parents	Alumni	Trainees
Research	•	•				
Electronic journal	•	•				
Preliminary experiments		•	•			
Teaching and learning	•	•				
Administration	•	•	•		•	•
Dormitory networks	•	•				

Table 4 The relationships of TANet users and application patterns

	Students	Teachers	Staffs	Parents	Alumni	Trainees
School administration systems	•	•	•			
Web portal	•	•	•	•	•	•
E-mail Systems	•	•	•		•	•
E-learning systems	•	•				•
Wireless service systems	•	•	•			•
Bulletin board system (BBS)	•	•	•	•	•	•

claims educational institutes belong to class A and B would enforce complete A-ISMS and obtain certification, and educational institutes belong to class C and D would implement their ISMS refer to A-ISMS. In the promotion phase, the MOECC offers funding for educational institutions to apply A-ISMS certification. It can effectively to lower the threshold for implementing their ISMS. Moreover, through the spread of ISMS seed schools the MOECC can effectively promote their A-ISMS. The MOECC has established an A-ISMS Certification Center and proposed certification scheme as shown in Fig. 6. In the future, MOECC will implement the ISMS in all educational institutions and cultivate ISMS auditor. In order to fulfill the requirement of ISMS auditor, the MOECC also establish the A-ISMS auditor system. This system has completed evaluation process for cultivating Audit Observer, Auditor, and Lead Auditor.

MOECC also enact information security operation guidelines for all levels of admission examination systems, and provide advising services for information protection and defense. These admission examination systems include junior high school basic abilities examination, unified admission examination for technical and vocational colleges, and university admission examination. Furthermore, they will continue develop web application vulnerability scanning platforms to prevent information leakage.

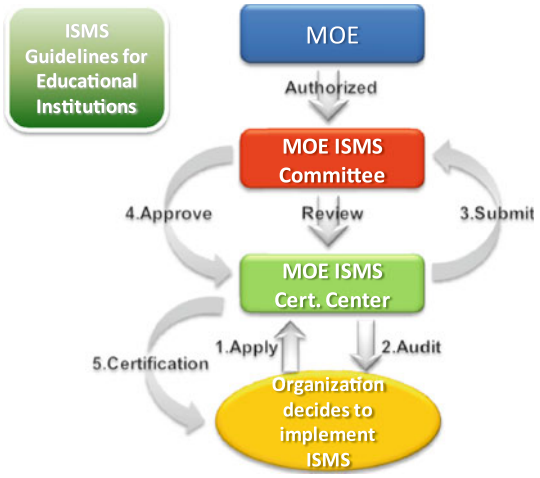

Fig. 6 A-ISMS certification scheme

Environment and technical aspect

Currently, there is insufficient manpower of ICT management in educational institutes. However, the related ICT management loading is increasing today. Especially, the information security specialists are not enough for industry and difficult to get recruited by educational institutes due to less salary. How to establish a cost-efficient information security framework and reduce the loading of specialists in educational institutes is a important issue. The MOECC has proposed following approaches to overcome these challenges.

The MOECC will take advantage of the A-ISAC (Academic Information Sharing and Analysis Center) as the platform to combine the capabilities of the regional and county network centers, to integrate the A-SOC (Academic Security Operation Center), web application vulnerability scanning systems, botnet defense mechanisms, inappropriate

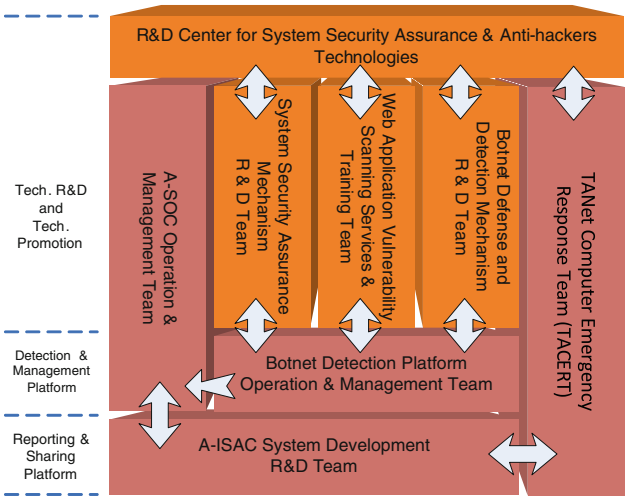

Fig. 7 The organization of Taiwan MOECC security projects

information prevention mechanism and others to achieve a multi-level defense. This A-ISAC is developed with SOA (Service-Oriented Architecture) and automatic workflow architecture to reduce the routine loading of information security specialists.

Furthermore, to overcome the issue of educational institutions' insufficient response ability to large scale attacks and school's individual incidents, the MOECC determine to establish TACERT (TANet Computer Emergency Response Team) system and establish the operation team. TACERT will provide incident response support, security information sharing, and collaboration with government, research, industry, and international partners (e.g. REN-ISAC, FIRST, CERT/CC). The relationship of above-mentioned security projects is depicted in the Fig. 7.

We may need different technologies and mechanisms to defend various threats. How to deploy different security services into all connected units is a big challenge in TANet. Cloud service may be a solution for educational systems. The MOECC based on the existing inappropriate information prevention service to extend their botnet defense mechanism. As shown in the Fig. 8, the botnet defense cloud is cooperated with inappropriate information prevention cloud by utilizing the same update system, report system, and filtering system. Furthermore, the MOECC also build a web monitoring cloud service for actively scanning and reporting. The monitoring is focused on the cross-site scripting (XSS) and compromised websites. In the Web Monitoring Cloud, monitoring agents collect target IP addresses which belong to MOE automatically and inspect the collected web pages like a normal user. Based on above-mentioned mechanisms, the MOECC can provide integrated security services in these three ways: (1) Monitor as a Service (MaaS); (2) Protection as a Service (PaaS); (3) Detection as a Service (DaaS).

Education aspect

Intrusion technologies emerge in endlessly. Thus our protection technologies and awareness need to be improved continually. The MOECC has classified the information security education into three levels including general users, managers, and specialists. The overall model of Information Security Talent Cultivation is depicted in the Fig. 9.

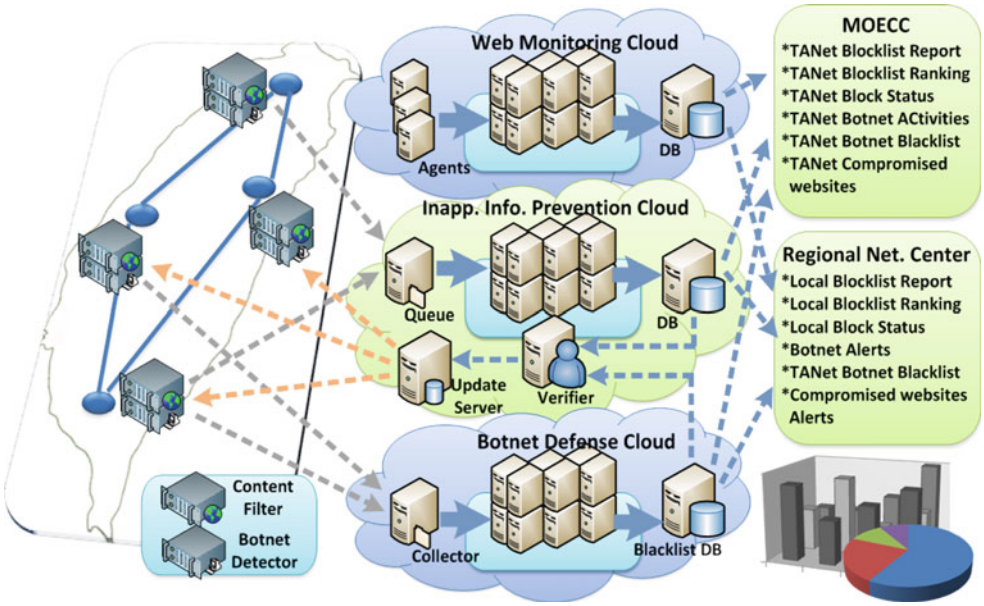

Fig. 8 Security cloud services in TANet

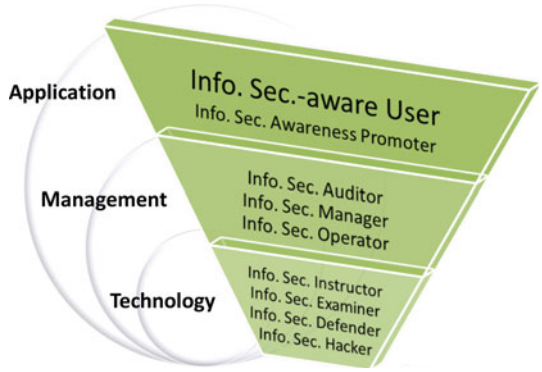

Fig. 9 Cultivation of information security talent

The MOE will promote public awareness and literacy on information security, through various channels, such as activities or competitions. Moreover, they intend to provide comprehensive information security education, including curriculum guidelines for elementary and junior high schools, general education curricula in senior high schools, and information security general education program in post-secondary institutions. These materials are developed with different purpose.

In cultivation of information security talent, they will continue to promote information security education programs in universities. On the other hand, the MOECC also provide training course for students and technician and help them to procure professional certificates (e.g. ISO 27001 Lead Auditor, CEH, CISSP). In the future, they will plan a practical training environment for students who complete the information security education program. The MOECC also funded a "TANet Information Security Promotion Center" for planning overall and systematic promotion activities. This center will hold information security camps and organize voluntary information security defense team and communities in educational system.

The MOECC adopt three security incident handling phases including prevention, response, and improvement to plan different countermeasures with policy management aspect, environment and technical aspect, and education aspect in educational systems. The overall information security countermeasures are depicted in the Table 5.

Conclusions

TANet is a service network which connected with each level campus networks in Taiwan. Based on the premise of campus network management is focused on academic freedom, the government of Taiwan has built up a campus information service network environment under openness principle. Hence establishing a secure, trustworthy, and free information service network environment is an important goal of Taiwan MOE.

In this paper, we investigate current situation of Taiwan MOE ICT security development and provide a case study. We discuss these challenges that educational systems would

Table 5 The overall countermeasure of Taiwan MOE

	Prevention	Response	Improvement
Policy management	1. Enact A-ISMS	1. Incident reporting and damage assessment	1. Review and discuss
	2. Periodic auditing	2. Incident response SOP	2. Revise A-ISMS
	3. INFOSEC supporting mechanism	3. Evaluation model	3. Track incident management
	4. INFOSEC incident drill	4. Reward mechanism	
Environment and technologies	1. IDS/IPS	1. TACERT	1. Fine tune security projects and mechanisms
	2. Vul. Scanning	2. Reporting platform	2. Provide technical consulting service
	3. Source code analysis	3. Malware and Botnet detection	3. Enact Redundancy and Recovery SOP
	4. A-SOC	4. Periodic patch	
	5. A-ISAC		
	6. Backup and redundancy mechanisms		
Education	1. Promotion of user awareness	1. INFOSEC talent cultivation	1. Provide newest technical training
	2. Education for managers		2. Provide digital curriculum materials

meet. Finally, we review their proposed solutions with policy management aspect, environment and technical aspect, and education aspect for improving ICT security environment in educational systems. It provides reference materials for establishing a secure and trustworthy ICT environment within educational systems.

References

Chu, H., Deng, D., Chao, H., & Huang, Y. (2009). Next generation of terrorism: Ubiquitous cyber terrorism with the accumulation of all intangible fears. *Journal of Universal Computer Science, 15*(12), 2373–2386.

Computer Center of MOE (MOECC). (2010). http://english.moe.gov.tw/ct.asp?xItem=579&ctNode=363. Accessed 25 April 2010.

Deming, W. E. (1986). *Out of the Crisis*. MIT Center for Advanced Engineering Study. ISBN 0-911379-01-0.

Farn, K., Lin, S., & Lo, C. (2008). A study on e-Taiwan information system security classification and implementation. *Computer Standards & Interfaces, 30*, 1–7.

Frederick, C. (2002). *Information Assurance Technical Framework*. Release 3.1. National Security Agency. https://www.iad.gov/library/iacf.cfm. Accessed 25 April 2010.

ISO/IEC. (2005). *Information technology—Code of practice for information security management*. ISO/IEC 17799:2005(E).

Kang, S., Park, J. H., Kahn, M. K., & Kwak, J. (2009). Study on the common criteria methodology for secure ubiquitous environment construction. *Journal of Intelligent Manufacturing*, doi:10.1007/s10845-009-0363-x.

Lai, S., Hsieh, M., & Kuo, W. (2003). Design and implementation of an intelligent defense system against network security incidents. *Journal of Internet Technology, 4*(2), 119–125.

Ministry of Education (MOE) of the R.O.C. (Taiwan). (2010). http://english.moe.gov.tw. Accessed 25 April 2010.

Sardana, A., Joshi, R. C., Kim, T., & Jang, S. (2008). Deciding optimal entropic thresholds to calibrate the detection mechanism for variable rate DDoS attacks in ISP domain: honeypot based approach. *Journal of Intelligent Manufacturing*, doi:10.1007/s10845-008-0204-3.

The Executive Yuan National Information Communication Security Taskforce (NICST) of Republic of China (R.O.C.). (2009). Information security dispatch document No. 0980100328, 2009-06-01.

The Executive Yuan National Information Communication Security Taskforce (NICST) of Republic of China (R.O.C.). (2010). http://www.nicst.nat.gov.tw. Accessed 25 April 2010.