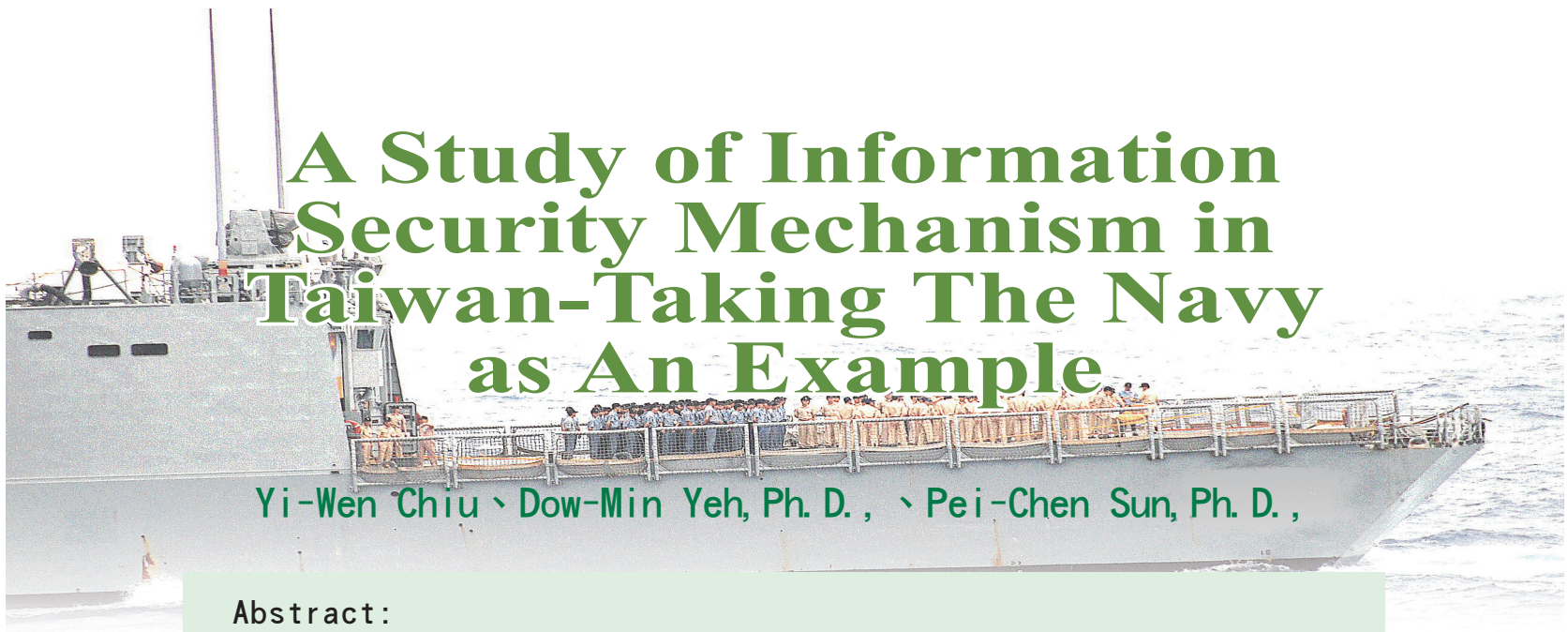




A Study of Information Security Mechanism in Taiwan-Taking The Navy as An Example

Yi-Wen Chiu、Dow-Min Yeh, Ph. D.,、Pei-Chen Sun, Ph. D.,

Abstract:

In recent years, computer intrusions occurring in government, military, and business have become common place. Even though only some of these were reported on newspapers and magazines, the overall loss is too great to estimate. Since Taiwan's military is on the frontline to protect the nation, robust security measures must be followed. This article provides information security examples and discusses regulations focused on info sec mechanisms in Taiwan's naval units. We provide analysis and recommendations for improvement that every unit can reference.

Keywords: Information Security (IS); Information Security Management System (ISMS); Information Security Incident (IS Incident)

1. Introduction

In 1990, the Computer Center in the Ministry of Education established the Taiwan Academic Net (TANet)¹, which is now universal throughout Taiwan. Utilizing this new technology to process information has become an in-

tegral part of daily life. According to the newest survey, FIND, conducted by Institute for Information Industry, the popularity of computers among families in 2009 reached 2.4 computers per family². By years end 2009, the number of broadband Internet users reached 4,960,000³, demonstrating

1.Li, Cheng-Chi, "The Promotion of Computerization in Universities", Unpublished Master's Thesis, National Sun Yat-sen University, Kaohsiung(2001)

2.Wu, Pei-Ling, <Foreseeing Innovative New Digiservices of Taiwan's Broadband Home Network in 2009-Network Indicator of Individual and Family>, <http://www.find.org.tw/find/home.aspx?page=many&id=249>.

3.Chen, Jyun-Fu, Li, Ya-Ping, "Taiwan Internet Users in 2009", <http://www.find.org.tw/find/home.aspx?page=many&id=251>.

that the internet has the advantage of breaking the limitations of time and space. As the result, it has become indispensable in the modern times.

The worldwide use of Internet applications has made IS incidents more prevalent. In addition, more powerful computer processing has also resulted in an increased threat, in both variety and occurrence. According to the statistics issued by the Directorate-General of Budget, Accounting, and Statistics in the Executive Yuan, organizations with more than 30 people using computers, 54.77% of them has experienced IS incidents. In these incidents, the most frequent ones were virus (53.20%), the second most frequent were backdoor (10.68%), and the third most frequent were distributed denial of service (DDOS) (2.96%)⁴. Moreover, CSI/FBI's investigation report about computer crimes and security states that the most frequent four major incidents in 2009^{5,6} were virus (64.3%), laptop theft/fraud

(42.2%), insider abuse (29.7%), and DDOS (29.2%).

There is a well known saying, "Prevention is better than cure." To ensure that information technology and network grow under safely secured environments in our nation, as well as to prevent IS incidents such as breach of confidentiality, destruction of important information systems and network crimes, the Executive Yuan enacted IS management guidelines for organizations in 1999⁷. The Executive Yuan also proclaimed several regulations subsequently to reinforce the overall protection of IS in the nation. Following national policies and laws, government bodies established their own IS mechanisms one after another. Moreover, complying with "The Concrete Solutions for Dealing with IS Incidents And Risk for Government Bodies by the Executive Yuan in 2004, government bodies are required to acquire IS certificates from third-party IS institutions (BSi7799-2/CNS17800),

4.The Data Management Processing Center of The Directorate-General of Budget, Accounting and Statistics of The Executive Yuan of the Republic of China, 〈A Report of Computer Applications in 2009〉, <http://www.stat.gov.tw/ct.asp?xItem=25562&CtNode=5210&mp=4>.

5.Robert Richardson," 2009 CSI Computer Crime and Security Survey Executive Summary" ,Computer Security Journal,December 2009.

6.Robert Richardson," 2008 CSI/FBI CSI Computer Crime and Security Survey" ,Computer Security Journal,2009.

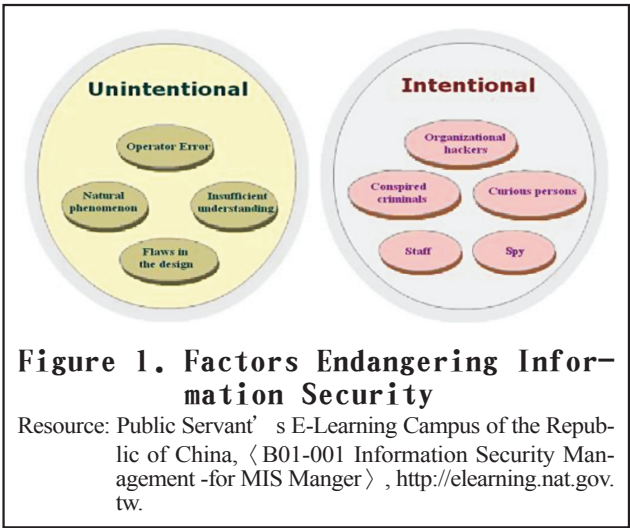
7.The Exective Yuan of the Republic of China, 〈IS Management Guidelines for Organizations of the Executive Yua〉, <http://cissnet.edu.tw/purpose02.aspx>.

making standardized IS management mechanisms directly by the Government.

The Taiwan Military, playing the role of protecting the country, has also faced rigorous challenges after information digitalization. Due diligence must be taken since a single careless accident may lead to leakage of military intelligence, and pose great damage to the country. To solve the difficult situation in IS, related departments in the Taiwan Military keep deliberating ways to improve IS in order to reduce the chances of incident occurrences. In this research, we take the Navy as an example, we discuss about the current situation of planning and deploying IS mechanisms, and perform a SWOT analysis on the current situation. We also provide recommendations for improvement against all kinds of information threats, hoping to prevent further risk.

2. About Information Security

2.1 The Definition of Information Security



The word “Information Security” has been used for more than 30 years. The Safety Criteria of FBI in the U.S. defined IS as “Protecting information from being intentionally or accidentally disclosed, transferred, altered, or destroyed”⁸. “Unintentionally” implies that information is leaked or damaged by nonhuman factors such as blackout, earthquake, and fire. In contrast, “Intentionally” means that the source of damage comes from human intents⁹.

The factors of “Unintentional” and “Intentional” are shown in Figure 1.

Therefore IS is to preserve information confidentiality, availability

8.Tnag, Yao-Jhong, “ A Study on Information Security from the Perspective of Warefare” , (Taipei:Chuan Hwa Book Corporation,2003).
9.Public Servant's E-Learning Campus of the Republic of China, 〈B01-001 Information Security Management -for MIS Manger〉 , <http://elearning.nat.gov.tw>.

Table 1. The IS weaknesses and threats of an organization

	Items	Contents
Weaknesses Inside An Organization	Informational Assets	Databases, data, and digital files.
	Documents	Contracts, guides, manuals, brochures, and paper documents.
	Software	Intellectual properties such as applications which support organization operations, self-developed software, and systems.
	Physical Assets	Operational equipment such as computers, servers, disks, tapes, power suppliers, and air conditioners.
	Personnel	Employees, customers, and contractors.
	Services	Applications and communication services.
	Image and Advertisements	Image of an organization and advertisements.
Threats Outside an Organization	Hacker Attacks	Networks or applications in a business attacked by hackers by any means.
	Information Theft	Organization documents or files thieved by employees.
	Spies	Other adversaries of an organization sending spies to penetrate and steal information.
	Virus or Trojan Horses	Important data sent or leaked automatically by computers infected by virus or Trojan Horses.
	Intentional or Unintentional Deletion	Data deleted or damaged by persons inside or outside the organization intentionally or unintentionally.
	Awareness	Applications or procedures being cracked without awareness.
	Power Outages	Power supplies for the operation of an organization being interrupted.

Resource: He, Ying-Jhou,” Information Security Risk Assessment of Regional Academic Network Organizations: Case Study on Yilan County Academic Network” , Unpublished Master’ s Thesis, Guang Universit(2007)¹¹

and integrity; other properties such as authenticity, accountability, non-repudiation and reliability can also be involved (CAN 17799)¹⁰. Effective safety measures must rely on the new ways of how new technologies make use of information, and prevent before things happen (Eugene C. Schneider

Gregory W. Therkalsen,1990) in order to ensure the perpetual existence of an organization.

2.2 The Risk in Information Security

“Safety” and “Risk” are highly related. The weaknesses and threats confronted by the organization forms

10.International Organization for Standardization,” ISO/IEC 27001 Information technology – Security techniques –Information security management systems – Requirements,first edition,ISO,2005.

11.He, Ying-Jhou,” Information Security Risk Assessment of Regional Academic Network Organizations: Case Study on Yilan County Academic Network” , Unpublished Master’ s Thesis, Guang Universit(2007)

the basis of risk¹⁰. Weaknesses are evaluated from the personnel, informational assets, and physical assets in an organization because the weaknesses inside can result in the threats outside. Threats mainly come from outside factors such as hacker attacks, industrial spies, virus, and Trojan Horses, because threats outside often result from the weaknesses inside.

The IS weaknesses and threats of an organization are shown in Table 1:

2.3 Information Security Incidents

An incident is how the source of a threat poses damages to an organization¹². An information security event is an identified occurrence of system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant. (ISO/IEC TR 18044:2004)

In the investigation report on computer crimes and security conducted by the CSI/FBI⁵, tracing back to the occurring rates of major types of IS incidents between 1990 and 2008 (as shown in Figure 2 and Table 2), 4 types with the highest occurring rates

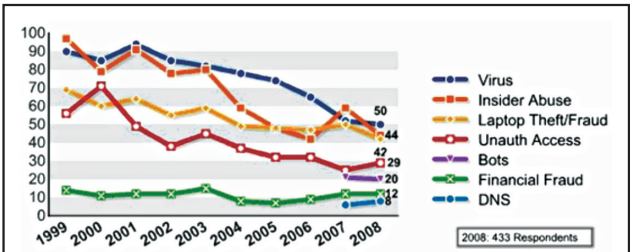


Figure 2. Occurring Rates of Major Types of IS Incidents

Resource:Robert Richardson," 2008 CSI/FBI CSI Computer Crime and Security Survey" ,Computer Security Journal,2009.

are “Virus”, “Insider Abuse”, “Laptop Theft/Fraud”, and “Unauthorized Access” respectively. The rate for “Insider Abuse” was even higher than “Virus” (which always had the highest rate) for a certain period in 2007. In addition, we can see that “unauthorized access” grew higher in 2008 than in 2007.

The Service Group for Planning on Elevating Campus Information Security Services in the Ministry of Education classified “Top 10 Threats on Network Security in 2008” announced by the organization SANS (responsible for security trainings, authentication, and study) into four major categories: “Website Threats”, “Act Threats”, “Insider Threats”, and “Social Engineering Threats”¹³. Here we refer to “Notes on Responding to Emergent In-

12.Eric Maiwald, Fundamentals of Network Security, (U.S.A.:McGraw-Hill Technology Education,2004).

13.Ministry of Education of the Republic of China, 〈 Network Security Analysis 〉 ,http://cissnet.edu.tw/knowledge_11.aspx.

Table 2. Occurring Rates of Major Types of IS Incidents

	2004	2005	2006	2007	2008
Denial of Service	39%	32%	25%	25%	21%
Laptop Theft	49%	48%	47%	50%	42%
Telecom Fraud	10%	10%	8%	5%	5%
Unauthorized Access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial Fraud	8%	7%	9%	12%	12%
Insider Abuse	59%	48%	42%	59%	44%
System Penetration	17%	14%	15%	13%	13%
Sabotage	5%	2%	3%	4%	2%
Theft/Loss of Proprietary Info	10%	9%	9%	8%	9%
-from Mobile Devices					4%
-from All Other Sources					5%
Abuse of Wireless Network	15%	16%	14%	17%	14%
Website Defacement	7%	5%	6%	10%	6%
Misuse of Web Application	10%	5%	6%	9%	11%
Bots				21	20
DNS Attacks				6%	8%
Instant Messaging Abuse				25%	21%
Password Sniffing				10%	9%
Theft/loss of customer data)				17%	17%
-from Mobile Devices					8%
-from All Other Sources					8%

Resource: Robert Richardson,” 2008 CSI/FBI CSI Computer Crime and Security Survey” ,Computer Security Journal,2009.

formation Security Incidents And Risk for Organizations”¹⁴⁾ enacted by the Executive Yuan and classify domestic and foreign IS incidents as follows:

1.Man-made disasters: can be classified as “Risk from Inside” and “Intrusion from Outside” according to

the sources. The “Internet Security” aspect includes sniffing, tampering, and DDOS; the “System Security” aspect includes virus, worms, backdoors, Trojan Horses, invasion, weakness threats; the “Management Security” aspect includes inappropriate access,

14.National Information and Communication Security Taskforce of the Republic of China, 〈Notes on Responding to Emergent Information Security Incidents And Risk for Organizations〉 , <http://www.tcfid.gov.tw/02mid/07trouble/96/96-02-01.doc>

Table 3.Responsibilities of Information Security Systems in Different Levels

Contents Level	Items	Defense Strength	Defense Depth	ISMS Promotion	Auditing Methods	IS Trainings (Commanders, Managers, Technicians, General Personnel)	Certificate
A		4	NSOC/SOC IDS Firewall Antivirus	Organizations certified by third-party in 2007	At least 2 self audit annually	(4, 6, 18, 4 hours)/year	2 certificates of IS proficiency in 2007
B		3	SOC(OP) IDS Firewall Antivirus	Organizations certified by third-party in 2008	At least 1 self audit annually	(4, 6, 18, 4 hours)/year	1 certificate of IS proficiency in 2008
C		2	IDS Firewall Antivirus	Organizations plan to set up their own promotion groups.	Self-examination	(2, 6, 12, 4 hours)/year	Trainings in IS proficiency
D		1	Firewall Antivirus	Promote ISMS concepts	Self-examination	(1, 4, 8, 2 hours)/year	Trainings in IS proficiency

Resource: National Information and Communication Security Taskforce of the Republic of China, 〈The Implementation Plan for Grading Government Organizations' Information Security Responsibility〉, <http://www.hjes.tpc.edu.tw/mediafile/445/fdownload/589/64/2009-9-14-23-19-55-64-nf1.pdf>

account embezzlement, unauthorized login, social engineering, theft, destruction of informational assets.

2.Natural disasters: such as hurricanes, floods, and earthquakes.

Unexpected incidents: unforeseen accidents such as conflagrations, explosions, nuclear incidents, severe building damages, hardware damages, power outages.

2.4 Information Management System

According to the 15th workgroup conference held by National Information And Communication Security Task-

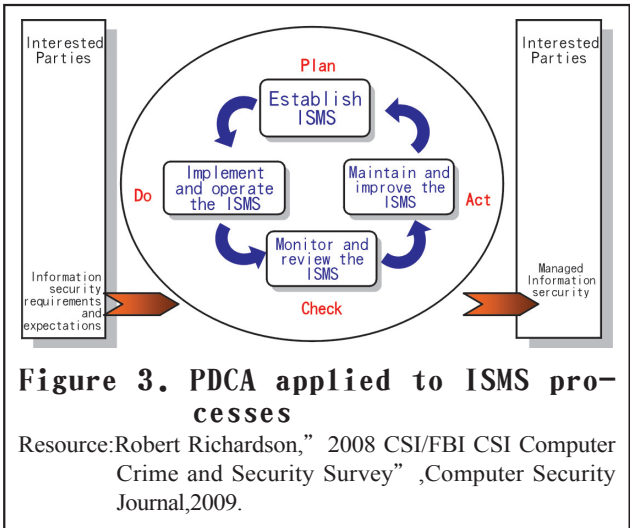
force (NICST) on July 7th, 2006, in order to define accurate procedures for IS responsibilities of government bodies, “The Execution Plan for Information Security Responsibility Classification for Government Bodies ” was enacted in the hope of preventing information from being destroyed by potential threats and elevating national IS protection level. By considering the subjective and objective situations from a management perspective, organizations were classified into 4 predefined IS levels: A (Impor-

tant Core), B (Core), C (Important), and D (General)¹⁵. Tasks that organizations in each level should execute are concluded in the following table 3:

The application of Information Security Management System (ISMS) is also included as part of the management tasks. ISMS is one of the largest management systems and also an important part in the overall management system. It is based on operational risk, using personnel, information, equipment, access, system security, and environment safety as the scope of IS and adopts a process approach for establishing, implementing, operating, monitoring, reviewing and improving an organization's ISMS (ISO/IEC 27001:2005).

ISIS applies Plan-Do-Check-Act (PDCA) model to correct the ISMS to ensure its efficacy. The model is shown in Figure 3. The following is the brief description for the model:

1. Plan (establish the ISMS): Establish ISMS policy, objectives, processes, and procedures relevant to managing risk and improving informa-



tion security to deliver results in accordance with an organization's overall policies and objectives.

2. Do (implement and operate the ISMS): Implement and operate the ISMS policy, controls, processes, and procedures.

3. Check (monitor and review the ISMS): Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.

4. Act (maintain and improve the ISMS): Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to

15. National Information and Communication Security Taskforce of the Republic of China, "The Implementation Plan for Grading Government Organizations' Information Security Responsibility", <http://www.hjes.tpc.edu.tw/mediafile/445/fdownload/589/64/2009-9-14-23-19-55-64-nfl.pdf>

achieve continual improvement of the ISMS^{10, 16, 17}.

Before the international standards for the ISMS are enacted, the Bureau of Standards, Metrology and Inspection, Ministry of Economic Affairs in Taiwan chose ISO/IEC 27001:2005 as the verification standard for the ISMS in our nation¹⁷. ISO27001 is an International Standard for the ISMS. It is a management system rather than a technique and includes 11 domain areas, 39 control objectives and 133 controls^{11, 17}.

11 domain areas are described briefly as follows:

1.Information Security Policy: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

2.Organization of Information Security: To set up a managing structure used to manage and control IS in an organization as well as executes existing IS regulations.

3.Asset Management: To ensure that all informational assets are efficiently protected in the organization.

4.Human Resources Security: To

define security responsibilities and roles of all personnel.

5.Physical and Environmental Security: To propose simple and precise safety requirements to all personnel in the work places.

6.Communications and Operations Management: To facilitate communication inside and outside the company as completely as possible in order to make ISMS function successfully.

7.Access Control: To control access to information.

8.Information Systems Acquisition, Development and Maintenance: To ensure IT projects and related supporting activities are safely controlled in the company, and controls and encrypts data when necessary.

9.Information Security Incident Management: To ensures IS incidents and weaknesses related to the ISMS are conveyed in some degree in order to take real time corrective actions and use persistent measures to manage IS incidents.

10.Business Continuity Management: To develop and maintain enterprise's continuous operation plans and protects key activities from the effects

16.Tang, Yu-Yu, 〈A Study of ISMS Policy〉, <http://sab.tycg.gov.tw/files/download/455d7741.ppt>.

17.Bureau of Standards, Metrology and Inspection, Ministry of Economic Affairs of the Republic of China, 〈ISO 27001:2005 Requirements Of Information Security Management System〉, <http://www.bsmi.gov.tw/wSite/public/Data/fl228114692438.ppt>.

of disasters or interruptions.

11.Compliance: To comply with IS regulations and requirements.

3.The Current Situation of Planning And Deploying Information Security Mechanisms in the Navy in Taiwan

As the era of digitization comes, learning how to prevent computer network crimes and crisis as well as maintaining information system security become the most important mission of the Government. Therefore, the Executive Yuan approved the first period “Establishing National Information And Communication Infrastructure Security Mechanisms Plan(2001-2004)” in January, 2001, and founded the National Information And Communication Security Taskforce (NICST). It was since then that the government started to systematically promote the establishment of information and communication security in our nation¹⁸.

Our nation experienced two periods of promotion of “Plan on Estab-

lishing Information And Communication Infrastructure Security Mechanisms in Taiwan (2001-2008)”^{19,20}, totaling up to 8 years. In the first period (2001-2004), national information and communication security organizations and emergency centers were established, and government bodies were encouraged to set up “Information And Communication Security Teams”, defining “Ensure a secured and reliable information and communication environment in our nation” as the goal of this period. In the second period (2005-2008), the Government planned four policy goals: “Shorten the timing of notification”, “Enhance the protection ability for information security”, “Reinforce understanding and education in information security”, and “Promote international cooperation”. The “Chief Information Security Officer (CISO)” responsibility system and the “Responsibility Level of Information Security” were approved, distinguished into four levels: A, B, C, and D, according to their importance. The Government also

18.National Information and Communication Security Taskforce of the Republic of China, 〈National Safety Communications Develop Plan(2009-2012)〉, http://www.hdais.gov.tw/13/0104726A00_ATTCH1.pdf.

19.National Information and Communication Security Taskforce of the Republic of China, 〈Establishing National Information And Communication Infrastructure Security Mechanisms Plan (2005-2008)〉, <http://www.libcc.nsysu.edu.tw/file.php/16/100210.pdf>,2007.

20.Lin, Chei-E, 〈Study of relation between Information Security Literacy and Law breaking recognition:A case of Military Personnel〉, Unpublished Master’s Thesis, Shu-Te University,(2006)

continuously worked on performing maneuver on the defense/attack/notification of information and communication security, spreading information and communication management systems, information and communication education, and services for audit, and actively constructed the infrastructure of information and communication security. Moreover, NICST was regrouped in July, 2004. After completing the missions in these two periods, following National Information and Communication Initiative Plans, the Government set its goal to construct quality Internet society.

In the organization structure of NICST, the Ministry of National Defense belongs to "The Standard Group", "The Audit Group", "The Regulation Group", and "The Response to Notification Group". It actively promoted each kind of IS protection constructions in order to establish the IS defense ability of "Alert early and respond to changes", and took the measure of "Detect and defend actively" to set up IS defense mechanisms. It proclaimed several IS control measures, deliberated reward and punishment regulations for IS, pushed identification mechanisms for IS, executed

physical segregation of networks, popularized IS education, required management by responsible people, and emphasized audit for IS in order to establish the defense systems that are protected by multilayered measures and immediate controllability, achieving the IS protection target: "Can't get in and out, not understandable, and can't be taken away".

3.1 The Defense Mechanisms for Information Security in The Navy

1. Computer Emergency Response: Complying with the IS policies proclaimed by the Ministry of National Defense, the Navy Command Headquarters approved "The Plan on Computer Emergency Response" which combines policy enactment, notification processing, development, consulting, and Computer Emergency Response Team (CERT) in every unit to set up the Navy Computer Emergency Response Team (NCERT), focusing on notification, early alert of information system and network incidents, effectively reducing the loss and recovering rapidly, ensuring the safety of the military networks to support combat missions.

2. The Navy Information Security Control Center: The Navy set up "The Navy Information Security Control Cen-

ters” in 2007, integrated all kinds of IS defense software, and set monitoring points inside the camps in coordination with the IS monitoring systems. They combined defense tools such as firewalls and intrusion protection systems to gather, report, respond to IS incidents with a single standard, enhancing the defense capability of the IS control system²¹.

3. Information Security Defense Structures: Regarding the IS management in an unit, the “Higher Authorities Instruct The Subordinates” mechanism was established to audit and supervise the IS situation of units in different levels²². Meetings between chief IS officers are held periodical-ly in order to eliminate IS incidents. The IS system is described as follows:

(1)The chief IS officer system: The vice leaders of all units of different levels play the role of the chief IS officers who are responsible for supervising the execution of IS related jobs.

(2)The IS manager system: The managers or vice managers of the IS departments take on the IS managers, in

charge of executing IS related jobs.

(3)The IS officer system: Every unit assigns IS officers to perform tasks including maintaining information systems, auditing and notifying IS incidents.

4. Information Security Defense Techniques: Facing current IS threats and following the development plans by the Ministry of National Defense, the Navy applied the single port mechanism to physically segregate targets, deploy AD access control, develop new electronic authentication system, use encryption software and USB disks, monitor the usage of wireless networks, and utilize the IS setting widget, informational assets and file security management systems. In the future, it will apply digital file protection mechanisms and enhance electronic authentication by combining other applications to satisfy the six needs in IS: “Physical Safety”, “Personnel Safety”, “System Security”, “Network Security”, “Computer Security”, and “Data Security”^{23, 24}.

3.2 Information Security Regula-

21. Youth Daily News, M.N.D. of the Republic of China, http://news.gpwb.gov.tw/newsgpwb_2009/news.php?css=3&nid=19199&rtype=2, 2007.

22. Ministry of National Defense of the Republic of China, <http://www.mnd.gov.tw/Publish.aspx?cnid=65&p=29363>, 2008.

23. Ministry of National Defense of the Republic of China, <http://www.mnd.gov.tw/publish.aspx?cnid=65&p=31639>, 2009.

24. General Political Warfare Bureau, M.N.D. of the Republic of China, http://gpwd.mnd.gov.tw/onweb.jsp?webno=3333333027&webitem_no=1053, 2007.

Table 4. Information Security Defense Related Regulations

Recent IS regulations and plans	
2001	The Regulation on Network Usage And Security
2001	The Regulation on Information Security for The Usage of Personal Computer
2004	The Notes on Physical Segregation and Control
2005	The Improvement Measures for The Control of Information Security
2005	The SOP of Information Networks
2005	The Regulation on PC I/O Devices
2006	The Disposition of Old/Broken Properties
2006	The Control of Informational Equipment And Storage Devices
2006	The Inspection And Learning of Physical Segregation of Networks and Storage Management of Informational Equipment
2006	The Management of Informational Equipment and Media
2006	The Management of URL
2006	The Management of Laptop
2007	The Policies on Information Security
2007	The Management of Websites
2007	The Control of CD/DVD Rom Usage
2007	The Control of Input/Output Devices And Portable Storage Media
2007	The Measures for The Improvement of Information Security Control Mechanisms
2007	The Wireless Network Monitoring System
2007	The Note on The Management of Information Security for Personnel Going Abroad on Business
2008	Lecturing for Personnel Violating Information Security Regulations
2008	The Supplement of Informational Equipment
2008	The Usage And Management of Encrypting USB Disks
2008	The Evaluation And Instruction of New Generation Personal Computer Systems
2008	The Regulation on The Rewards/Punishments for Information Security
2008	The Regulation on The Control of Portable Media And Management of Software
2009	The Revision of The Regulation on The Auditing Process of Military Data on The Internet
2009	The SOP of The Information Security Control Center
2009	The Revision of the SOP on The Assignment of Informational Equipment
2009	The Promotion of Education on Information and Communication Security
2009	The Plan of Computer Emergency Response
2009	The Execution of Connecting to The Internet through Single Port for All Units
2010	The Control of Informational Assets
2010	The Education And Trainings in Information
2010	The Certification of Information Security Proficiency
2010	The Revision of The Concrete Measures for Controlling And Auditing “Higher Authorities Instruct The Subordinates”
2010	The Deployment of PKI

Resource: Lin, Chei-E, 〈Study of relation between Information Security Literacy and Law breaking recognition:A case of Military Personnel〉,Unpublished Master’ s Thesis, Shu-Te University,(2006)

tions

The Navy Command Headquarters complied with the regulations and plans by the Ministry of National Defense and required that all units should prohibit doing business at home without exceptions. Moreover, in the efforts to completely cover all aspects related to IS and make officers and soldiers work within a standard, IS regulations and plans were proclaimed. Recent IS regulations are summarized in Table 4.

3.3 Education and Promotion Activities for Information Security Awareness

To reinforce officers and soldiers' belief in the idea that IS defense should be treated like wars, and enable them to understand more about the severe results of breaches of confidentiality, IS classes are included into the fundamental and advanced education in the Navy. Officers and soldiers are trained and imbued with IS knowledge as well as confidentiality keeping and related laws. Small cards Educational material and CDs that describe the control of IS are created, and personnel are educated and tested on the issues of IS when entering a new department in order to reinforce

IS concepts.

General trainings on IS are held periodically through itinerant lectures, certificate of IS proficiency for IS officers, lecturing for personnel violating IS regulations, and lectures on IS for personnel going abroad on business. E-learning platforms on IS are also created so that officers and officers and soldiers can learn by themselves through Internet at any time.

IS proficiency trainings are held by the Navy itself or non-governmental organizations. The scope of the former includes trainings on the systems the military uses, project trainings, and seminars. Trainings held by non-governmental organizations are funded by units at different levels. Representatives of these units are sent to the trainings, and are responsible for training others in the units afterward. The proficiency in IS is elevated by doing so.

To promote IS education even more, all kinds of military or academic magazines (such as the Naval Academia Bimonthly, Naval Officer School Quarterly, and the Army Forum) publish IS-related articles and even provide special columns as the interaction

platforms between soldiers and IS experts. They discuss about the points on IS affairs and key experiences on the defense measures, imbuing officers and soldiers with the concept that everyone is responsible for IS.

3.4 Information Security Supervision And Examination

The Taiwan Military faces current IS threats and identified “Information of national defense does not leak” and “Information processing does not stop” as the major needs for IS. To testify all kinds of defense measures, in addition to the attack/defense in the annual maneuvers, the Navy receives annual and nonscheduled IS audit from the Ministry of National Defense. Moreover, the Navy also carries through the plan on “Higher Authorities Instruct The Subordinates”, supervising the subordinates and discussing about the advantages and disadvantages in IS meetings. Personnel performing well or violating regulations are rewarded or punished according to regulations, expecting that officers and soldiers can follow the requirements on IS and fulfill IS defense rules.

Beside the audit by the Ministry

of National Defense, the Navy Command Headquarters even promoted ISO27001, which is about the certificate of IS management. Under the PDCA model of ISMS, the Navy continuously supervised IS management of all units and got the certification in October, 2008. In addition to conforming to the international standards, the Navy also expects to reduce organizational IS risk and impacts on officers and soldiers’ work, and makes officers and soldiers acquire the ability to defend themselves in the long run, proceeding to create a quality IS environment²⁵.

4. SWOT Analysis

Recently, based on the strategy of the Ministry of National Defense, the Navy put emphasis of information war on protecting network security. This can be achieved through effective countermeasures and the construction of monitoring systems, while considering the IS situations of the troops. Although IS policies have been implemented for several years, there is still room for improvement, such as transforming passive defense into active detection and control, and developing digital recognition abilities

25.Navy Command Headquarters,M.N.D. of the Republic of China,<http://navy.mnd.gov.tw/Publish.aspx?cnid=846&p=30579&Level=1>.

Table 5. The SWOT of IS defense in the Navy

	Strengths ; S	Weaknesses ; W	Opportunities ; O	Threats ; T
Information And Communication Awareness And Environment	1. Has higher IS awareness and alertness. 2. Executes every punishment without exceptions. 3. IS policies greatly supported by higher managers. 4. Has higher personnel reliability. 5. Well propagated IS knowledge	1. Lower will to participate and common consensus. 2. Does not separate responsibilities from rights; Only few informational operators execute IS missions. 3. Personnel put their faith in luck.	1. Higher authorities require more rigorous disciplines. 2. Encourage participation in IS trainings and seminars; IS knowledge is more comprehensive.	1. More incidents on social engineering and malware infection are found due to violation of portable media and Internet related regulations. 2. IS efficacies are hard to be evaluated; potential effects are often unseen, resulting in insufficient investments and difficulties in practicing.
Overall Defense Ability in Information And Communication	1. Periodically promote IS policies and audit, making IS control more complete 2. Comprehensive infrastructure of IS defense	1. There are too many security settings in the systems and networks; versions vary too fast, but there are too few professionals that can handle. 2. IS attacking methods change every day, and weaknesses are too many to defend. 3. Current systems and networks cannot be upgraded due to insufficient budget.	1. The Government and Military promote all kinds of IS defense resources with great efforts. 2. Loss due to IS incidents stimulates the development and applications of IS defense skills.	1. The Military becomes undesirables' favorite attacking target. 2. Trojan Horses and virus flow everywhere on the Internet. 3. Intentional damage made by people who are discontent with the unit.

Emergency Response Function	1. Establish definite responding plans and organizations, effectively elevating IS notification and response ability 2. Possess complete duty system and can receive incident reports and deal with them immediately.	1. Does not include the possibility that IS incidents may be concealed without being reported. 2. Personnel receiving incident notifications are not familiar with the responding procedures.	1. Retrospection after IS incidents to elevate the appreciation of the responding process. 2. The spread of IS incidents and the restrictions by laws draw more attention to IS incidents.	1. People intentionally publish fake incident reports unspotted by the people on duty. 2. Cannot recover immediately when severe incidents occur.
-----------------------------	--	--	---	--

Resource:

¹⁸. Here we perform an SWOT analysis of IS defense in the Navy as shown in the following table 5 so that we know how to make use of the strengths and opportunities as well as reduce weaknesses and prevent threats ^{26, 27}).

5. Conclusion

The Navy reinforces protection measures for IS based on the establishment of troops for information wars, and actively constructs tight IS protection mechanisms and capability. Besides enhancing multilayered and comprehensive IS mechanisms for

troops at different levels, the Navy should further enhance professional IS skills, transform IS from passive defense into active detection and control, and continuously maintain its strength in the battlefield of information between China and Taiwan. Five suggestions for improvement are provided as follows²¹:

- 1.Enhance information management, absolutely follow IS regulations, and strengthen cross examination to prevent breaches of confidentiality.
- 2.Reinforce IS disciplines, carry out security supervision, and estab-

26.Jiang Tung-Ru, Guo Jhen-Siang, Jhang Ruei-Yi, Syu Kai-Ping, 〈A Study on The Establishment of The ISMS Maturity Model in Educational Organizations〉,Taiwan Academic Network Conference 2008,http://ccnet.km.nccu.edu.tw/xms/index.php?view=content_show&id=977.
27.Tsai, Chung-Han, ” A Study on Information Security in Government Organization” , Unpublished Master’ Thesis, National Chengchi University, Taipei(2003).

lish IS management systems with complete confidentiality.

3. Increase training in information technology and communication, cultivate information and communication talents, and develop professional skills in information technology to maintain the strengths.

4. Accelerate the combination of the resources in the military and complete the transformation process of information technology and communication human resources.

5. Continuously enhance information and communication systems and defensive combat techniques by interacting with the industry and

academy, and gathering information about the deeds in information war of other countries. 

Yi-Wen Chiu
B. B. A., Dept. of Information Management, NDMC (ROC)
Military Training Officer in National Magong High School

Dow-Min Yeh, Ph. D.,
Ph. D., Dept. of Computer Science, UTAH (USA)
Dept. of Software-Engineering Professor, NKNU (ROC)

Pei-Chen Sun, Ph. D.,
Ph. D., Dept. of Information Management, NSYSU (ROC)
Professor and Director of Information and Computer Education Institute, NKNU (ROC) and Computer Center Director

老軍艦的故事

永靖軍艦 MMC-70

永靖軍艦為掃佈雷艦，第二次世界大戰後，盟國決定徹底解除日本武裝力量，將其海軍艦艇大部份拆毀，剩下艦艇在拆除武裝後，由中、美、英、蘇等四國以抽籤方式均分，該艦則由我國第4批抽籤獲得。該艦係由Sasebo Dockyard建造，公元1941年建造完成，在日服役時命名為「saishu」，民國36年10月4日在青島，由第二基地司令董沐曾代表接收，並命名為「永靖」軍艦，編號為MMC-70，隸屬於海防第一艦隊，民國39年再改隸第三艦隊(民國44年1月改為掃佈雷艦隊)，擔任海岸巡防等任務，該艦可裝水雷120顆，以便佈放。



該艦成軍服役後曾參加過多次戰役，其中較重要戰役計有遼西會戰及淞滬保衛戰。
該艦除參加戰役外，亦曾參加多次中美聯合操演，以精進戰力，民國49年5月1日，該艦由於艦體老舊，機件多損壞且無法修復，而奉命除役。(取材自老軍艦的故事)

老軍艦的故事

沱江(嘉陵)軍艦 PC-104

沱江(嘉陵)軍艦係由美國 Nashville Bridge 造船廠所建造之巡邏艦，1943年8月7日下水成軍，在美服役時，編號PC-1247，曾於第二次世界大戰中參加過多次戰役。

二次世界大戰結束後，美軍即停止使用該艦，並靠泊於菲律賓蘇比克灣，民國37年6月15日美國根據「五一二號法案」，於蘇比克灣將該艦移交我國，我海軍於接收該艦後命名為「嘉陵」軍艦，編號PGM-104，由於當時該艦已破損不堪，無法行駛，乃由拖船將其拖帶返國，進廠實施大修工程，於民國38年中修復，開始成軍服勤，隸屬海防第二艦隊，擔任海峽巡弋及護航等任務，曾先後參加過民國39年7月12日披山戰役、民國41年10月的南鎮、羊嶼、雞冠、白馬及寨頭等多次突擊支援任務及民國43年3月30日北箕山海戰等戰役。

民國43年4月1日，由於我海軍將所有接收自美海軍之巡邏艦均以「江」字號命名，故該艦自此日起更名為「沱江」軍艦，編號PC-104。該艦更名後仍繼續服勤，且參加了更多次的戰役，如4月28日與太平等友艦4艘在三門灣菜花岐海域巡弋時遭遇中共巨型艦4艘，經激戰後，中共軍艦2艘受創，該艦則安全返航。5月16日該艦與永定等三友艦巡弋於一江山西南與中共軍艦遭遇，發生激烈砲戰，中共軍艦中彈受創逃逸。

民國47年8月24日，金門砲戰正激烈之時，我中海等艦運補金門，正在泊地搶灘下卸物資之際，突遭中共岸砲猛烈射擊，撤離時又遭其魚雷艇八艘及YP艇9艘圍攻情況甚為危急，此時在附近巡弋之沱江等艦立即趕往支援，加入戰鬥，先後共擊沉中共快艇8艘傷5艘，此役由於各艦官兵士氣旺盛，英勇奮戰的優異表現，故戰後各艦艦長暨官兵均獲頒勳獎。

同年9月2日沱江與維源、柳江三艦奉令護航美堅艦金門運補，在料羅灣執行掩護及卸運任務時，遭中共海軍大批艦艇圍攻，該艦為確保運補任務達成，不顧本身安全，衝入敵陣，與敵艦群浴血奮戰達兩個多小時，創造了單艦擊沉敵艦艇5艘重傷2艘之輝煌戰績。但該艦也中彈累累，機



艙進水，動力全失，且有下沉之慮，後經維源及柳江二艦合力拖救及其它趕來支援友艦協助下，始脫離戰場，返抵澎湖。此役告捷當日參謀總長王叔銘上將即致電祝捷，並親頒有功官兵勳獎，該艦亦獲頒團體褒狀一軸。

沱江軍艦在「九二」海戰中受創極為嚴重，拖返澎湖第二造船廠後經多次勘驗，均認為已無法再修復，乃於民國47年11月1日奉國防部核定除役。(取材自老軍艦的故事)