我國資訊安全發展與海軍官校資安現況之SWOT分析

著者/邱意雯

國防大學管理學院資訊管理系正期92年班
現任海軍官校資圖中心上尉資訊官

指導老師/國立高雄師範大學副教授葉道明 國立高雄師範大學副教授孫培真

壹、前言

在網際網路及資訊科技蓬勃發展的趨勢下，政府及企業紛紛推行資訊電腦化作業，以追求增加作業效率(efficiency)及管理效能(effectiveness)，各級學校也不例外地積極建置校園資訊及網路基礎建設，以提供各類資訊服務來增加效率，不論在學術研究、教育學習、生活環境及校務行政等方面，莫不以資訊化為努力的方向，雖然如此帶來了許多的便利及交流，但也同時隱藏不少資訊安全的威脅，例如病毒癱瘓電腦、駭客竊取資料、攻擊系統等，使得資訊安全成為不得不面對的嚴肅課題，本文將以資訊安全認知、規範及管理系統進行探討，最後依文獻探討對軍事訓練及學術教育特殊身份的單位—海軍官校，就資訊安全現況進行SWOT分析，以了解在建立在「優勢」之上、利用「機會」、對抗「威脅」、克服「劣勢」，並對於海軍官校推動資訊安全提出建議與結論。

貳、研究背景與動機

一、研究背景

自1960 年美國國防部設置先進研究計畫署(ARPA)為防禦通訊系統遭癱瘓進而建造軍事設施間相互連結的電子通訊網：ARPANet，隨後，在加州大學洛杉機分校及各大學也相繼設置網路轉接點，透過連結使得數個大學與研究機構可以相互傳遞資料；80年代中期更由美國國家科學基金會研發出NSFNet取代成為全球網路的骨幹，使得網路拓展到其他非軍事用途。

台灣最早從1962年交通大學引進全國第1部電子計算機IBM650進入校園，其他各校也相繼引進，使得電腦化的工作便在校園持續的發展，1990年教育部電算中心成立台灣學術網路(TANet)，為促進國內大專院校及學術單位間交換學術資訊及共享資訊[1]。在資訊網路的大力推展下，校園對於e 化的系統及服務更是如雨後春筍般快速發展，如校務系統(教務、學務、總務、公文、圖書管理等系統)、遠距教學、e-learning、e-mail信箱帳號、個人網頁空間、電腦維修、線上服務等，都使得全校的教師、職員、學生可以不受空間、時間的限制，隨時方便存取及使用，達成資源的整合與共享。

二、研究動機

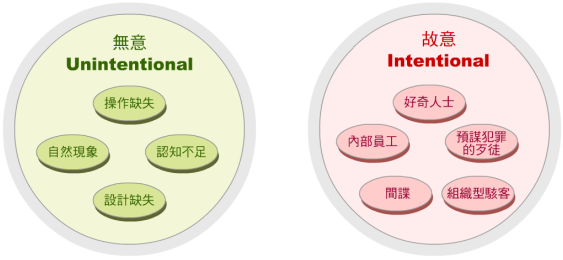
在大學校園e化發達的情形下，使得原本傳統的紙本作業以數位化的方式被處理及傳遞，雖然帶來了便利，但也同時隱含著許多風險，例如含有機敏性及個人隱私的資料在公開的網路上遭竊取、或偽冒身份從事不當行為、癱瘓系統網路導致造成損失等，種種的資安事件已頻傳在政府、企業等單位，甚至在單純校園裡也難以倖免，雖然學校是以「學術研究」及「培育人才」為目的，對於入侵者來說不如政府機關擁有國家機密、企業有著商業機密來得有誘因，但也不可掉以輕心，因為在資訊應用普及下，學校的行政流程以及學生的教學互動等作業大量倚賴電腦系統的運作，同時伴隨網路上種種越權存取(unauthenticated access)、入侵(cracking)、電腦犯罪(computer crime)的新挑戰[2]，因此希望在本研究中，能針對面臨資訊安全進行探討，了解資訊安全的事件、政策推行、及標準規範，並以兼具軍事及學術的海軍官校進行SWOT分析，最後提供建議與結論。

參、研究目的與範圍

本研究目的在於探討資訊安全的相關文獻後，分析海軍官校在資訊安全上之SWOT，以更深入瞭解海軍官校的資訊安全現況及所面臨的問題，並建議未來對於資訊安全的推行精進的方向。

由於不同的單位有不同的任務及特性，所面對資訊安全的風險及環境各自有異。因限於研究時程，僅就資訊安全之事件風險、政府組織、政策推行、資安管理系統等進行說明，且因牽涉範圍廣泛，只能由文獻呈現概觀，而無法詳盡陳述比較。研究分析則就海軍官校進行個案探討，雖海軍官校兼具教育與軍事單位的身份，但其結論並無法與各教育單位或軍事單位的資訊安全需求完全相符。

圖1 危害資訊安全的因素
資料來源：電子化政府網路文官學院，B01-001資安管理-資訊主管篇[4]



肆、文獻探討

一、資訊安全的定義

資訊安全一詞，已有30餘年的歷史。美國聯邦政府的安全準則，將資訊安全定義為「保護資料，使之免於遭受故意或無意的洩露、移轉、變更、破壞」，所謂無意的，是指如因停電、地震、失火等非人為的因素，使得資訊外洩或損害；所謂故意的，是指破壞的源頭是源於人為的設計[3]。其「無意」及「故意」的因素如下圖1：

所以資訊安全就是要達到資訊的機密性(Confidentiality)、可用性(Availability)與完整性(Integrity)；另外也包含如鑑別性、可歸責性、不可否認性及可靠性等特性(CAN 17799)[5]，而有效的安全措施必須賴於新科技對於運用資訊的新方法，並且要未雨綢繆事先預防(Eugene C.Schneider Gregory W. Therkalsen，1990)。

二、資訊安全的風險

(一)資訊安全風險

「安全」和「風險」是息息相關的，一個組織面臨的弱點與威脅構成了風險的基礎[6]。弱點主要是針對內部組織本身的人員、資訊資產、實體資產等項目進行評估，因為內部的弱點會造成外在的威脅；威脅的項目主要是組織外部駭客攻擊、工業間諜、病毒或木馬等項目，因為外在的威脅通常都是由內部的弱點所引起。組織資訊安全的弱點與威脅整理如下表1：

表1 組織資訊安全的弱點與威脅；資料來源：何瀛州122222(2007)[7]

	項目	說明
組織內部弱點項目	資訊資產	組織內部資料庫、資料檔等相關文件或電子檔。
	文件	對於組織內部合約文件、指導文件、使用手冊、操作手冊、公司資料等書面文件。
	軟體資產	內部業務運作用之應用軟體、自行設計軟體、系統軟體等與智慧財產權有關之項目。
	實體資產	內部業務運作所需之電腦、伺服器、磁片、磁帶、電源供應器、空調等硬體設備資產。
	人員	組織內部人員、外部顧客及協力合約商等人員。
	服務	企業服務之應用系統、通訊服務等服務性質之項目。
	形象及宣傳	組織本身的形象及有心人士的宣傳等。
外在威脅項目	駭客攻擊	企業內部網路或應用系統，被駭客透過各種方式進行攻擊。
	資訊竊取	組織文件或資料備內部員工竊取。
	間諜	外在敵對單位派任間諜進行組織滲透竊取資訊。
	病毒或木馬	因中毒或木馬感染，導致企業內部電腦自動傳送或外洩重要電子資料。
	故意或非故意刪除	組織內部人員或外部人員以故意或非故意方式，刪除、毀損組織資料。
	察覺	對於各項應用系統或作業流程遭受破解而不自知。
	電力中斷	組織運作所需之能源供應中斷。

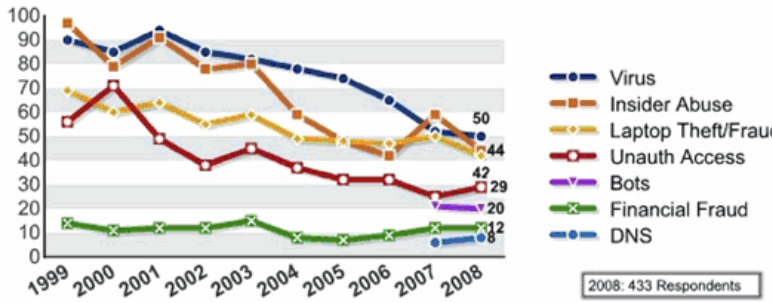


圖2　肇生資安事件主要種類的百分比
資料來源：Robert Richardson(2009)，CSI 2008[8]

(二)資訊安全事件

事件是一個威脅起源對於一個組織造成傷害的方法[6]。資訊安全事件是指系統、服務或網路發生一個已識別的狀態，其指示可能的資訊安全政策違例或保護措施失效，或是可能與安全相關先前未知的狀況等(ISO/IEC TR 18044：2004)。

美國電腦安全局及聯邦調查局CSI/FBI 對於電腦犯罪及安全所做的調查統計報告中[8]，在追溯到1990 年至2008 年肇生資安事件主要種類的百分比(如圖2及表2 所示)，可以發現風險最高發生率的前4類分別為「病毒」、「內部不當網路存取」、「移動式電腦的失竊及欺騙」、「未授權存取」，在2007年「內部不當網路存取」一度高於位於首位的「病毒」，另外可以發現在「未授權資訊存取」的部分在2008 年較2007年成長。

在教育部提升校園資訊安全服務計畫服務團將安全訓練、認證與研究機構SANS公佈的「2008十大網路安全威脅」報告歸納之後分為「網站威脅」、「行動威脅」、「病毒威脅」、「內部威脅」、「社交工程威脅」[9]，本研究依其分類方式及相關文獻分別將其資安事件的風險整理說明如下：

1. 網站威脅：

一 利用瀏覽器安全漏洞的攻擊，使合法網站成為最主要的攻擊目標，尤其是針對Flash 和Quick time 等未更新外掛程式的漏洞，致使駭客入侵，而瀏覽者因經其感染的網站而遭受入侵。

肇生資安事件主要種類	2004	2005	2006	2007	2008
阻斷服務(Denial of service)	39%	32%	25%	25%	21%
移動式電腦失竊(Laptop theft)	49%	48%	47%	50%	42%
電信詐騙(Telecom fraud)	10%	10%	8%	5%	5%
未授權存取(Unauthorized access)	37%	32%	32%	25%	29%
病毒(Virus)	78%	74%	65%	52%	50%
財務詐騙(Financial fraud)	8%	7%	9%	12%	12%
內部不當網路存取(Insider abuse)	59%	48%	42%	59%	44%
系統入侵/滲透(System penetration)	17%	14%	15%	13%	13%
蓄意破壞(Sabotage)	5%	2%	3%	4%	2%
竊取或遺失隱私資料 (Theft/loss of proprietary info)	10%	9%	9%	8%	9%
-來自行動裝置(from mobile devices)					4%
-來自所有其他來源(from all other sources)					5%
濫用無線網路資源 (Abuse of wireless network)	15%	16%	14%	17%	14%
網站的損壞(Web site defacement)	7%	5%	6%	10%	6%
隨意瀏覽網站 (Misuse of Web application)	10%	5%	6%	9%	11%
機器人程式(Bots)				21	20
DNS攻擊(DNS attacks)				6%	8%
濫用即時傳訊(Instant messaging abuse)				25%	21%
密碼偵測(Password sniffing)				10%	9%
竊取或遺失顧客資 (Theft/loss of customer data)				17%	17%
-來自行動裝置(from mobile devices)					8%
-來自所有其他的來源(from all other sources)					8%

表2　肇生資安事件主要種類的百分比；資料來源：Robert Richardson(2009)，CSI 2008[8]

一 由於程式開發過程上的疏失，網站存在著許多安全漏洞，如SQL Injection和XSS的問題，因此隨著Web廣泛的應用，針對網站應用程式漏洞的攻擊更為普遍，導致重要資料遭竊取、修改及毀損等未授權的存取。

一 利用電子郵件來誘騙使用者到詐欺型的仿冒網站，以騙取重要資料，也稱網路釣魚(Phishing)。

一 利用系統或軟體的漏洞進行癱瘓攻擊(如DOS)、網頁置換、系統資料破壞等。

2. 行動威脅

一 可移動式的筆記型電腦或多功手機等，由於可攜便利，因而失竊案件頻傳，另行動手機內建開放的作業平台，使駭客透過各種行動套件與VOIP的攻擊工具發動攻擊。

一 許多行動裝置，像是隨身碟、數位相機、GPS等消費性電子產品，都具備了USB介面以及儲存媒體的功能，只要一連接電腦，很容易就可入侵成功，並且容易散佈。

3. 病毒威脅：

一 如木馬程式、後門程式、蠕蟲病毒、間碟程式等，利用漏洞、email或下載程式感染惡意程式，被用來作為跳板主機、側錄及竊取、損毀資料、遠端遙控等。

一 如BontNet，俗稱「殭屍網路」（Zombie Network ），也稱「機器人網路」（Robot Network ），隨著 e-mail、即時通訊軟體或電腦系統漏洞侵入電腦，其會植入電腦，並攻擊其他電腦，具有「蟲」的特性具有自我複製並主動散播的能力，攻擊方法如下令被控制眾多殭屍電腦向郵件伺服器發送垃圾郵件等，除外，也會和木馬程式結合，進行資料竊取。

4. 內部威脅：

一 單位內部員工、顧問和委外廠商，因為這些人員具有一定的合法權限，所以藉由他們所獲取的資料，都是具有相當價值的資訊，可能發生蓄意或無意的資料外洩、遺失、毀壞等。

5. 社交工程威脅：

一 來自國與國之間的間諜活動，透過鎖定目標的魚叉式釣魚攻擊，目的在於竊取有價值的情報資訊，攻擊者會利用郵件夾藏木馬，並且透過系統漏洞來取得目標電腦的控制權。

一 結合特定事件和VOIP語音電話方式的混合式社交工程手法，已形成一項社會問題，駭客偽裝成政府單位或金融單位，配合email和語音系統的詐騙手法，使一般人很容易就會掉入釣魚陷阱。

三、我國資訊安全發展

(一)資訊安全組織

隨著現代資訊化的來臨，面對如何防範電腦網路犯罪與危機，並維護資通系統安全成為政府施政最迫切的課題，因此行政院於民國90年1月第2718次院會核定通過第1期「建立我國通資訊基礎建設安全機制計畫」(民國90至93年)，並於行政院下成立「國家資通安全會報」(National Informaiton & Communication Security Taskforce，簡稱NICI)積極推動我國資通安全基礎建設工作，從此開啟政府有計畫的推動我國資通安全建設之路。另於93年7月完成「國家資通安全會報」組織調整，自94年1月正式實施，將原有7個工作組變更為6個。復經95年9月修正部分設置要點，現行架構包含綜合規劃、通報應變、標準規範、稽核服

務、資訊服務及法規偵防等組，組織架構如下圖3[10]。

就教育單位而言，並無獨立資訊安全組織，教育部故委託中央研究院資訊科學研究所、台灣科技大學及台灣大學三個單位合作，於94年4月設立台灣資訊安全中心(Taiwan Information Security Center，簡稱TWISC)的組織。藉由此一研究與教學中心的成立，預期達成以下目標：(1)提昇我國資安科技學術與工程能量(2)提昇我國資安產業工程應用與管理能量(3)促進資安國際合作交流(4)培育資安種子，推廣資安新知與認知。同時也寄望促成「資安學程」能先在國內大學部推動，繼而往下紮根，融入國民基礎教育並與全民社區教育，終身學習接軌[11]。

(二)資訊安全政策

我國先後經過兩期總計8年推動「建立我國通資訊基礎建設安全機制計畫」(90年至97年)，在第一期(90年至93年)進行設立國家資通安全組織、國家資通安全應變中心、推動政府機關設立「資通安全處理小組」，並依組織重要性區分A、B、C及D級機構之資通安全分級及辦理資通安全攻防演練、通報演練、及推廣資通安全管理制度、資通安全教育宣導、稽核服務等，積極建設資通安全基礎建設工作；第二期(94年至97年)主要推行政府機關資訊安全長(Chief Information Security Officer；CISO)責任制度、資通安全責任等級分級作業與機密資訊分階段實體隔離等(行政院國家資通安全會報，2007、行政院科技顧問組，2008)，以強化政機關之資通安全能力。在完成 年的計畫執行，業已建立我國「通資訊基礎建設安全機制」，並達成「建立整體資安防護體系、健全資安防護能力」之階段目標。

於98年起將前揭計畫之賡續發展計畫定名為「國家資通訊安全發展方案(98年至101年)」，並考量資安政策延續性，以達成「安全信賴的智慧台灣，安心優質的數位生活」的願景，其方案之發展藍圖(如圖4)，在執行上，從「需求端」、「供應端」及「環境」三個面向加以考量，在「需求端」與「供應端」規劃符合政府、關鍵基礎建設及企業需要的5項資安措施(20 個行動方案)；在「環境」面建立利於形塑資安文化的4項措施(10個行動方案)，如表3，預期可達成「強化整

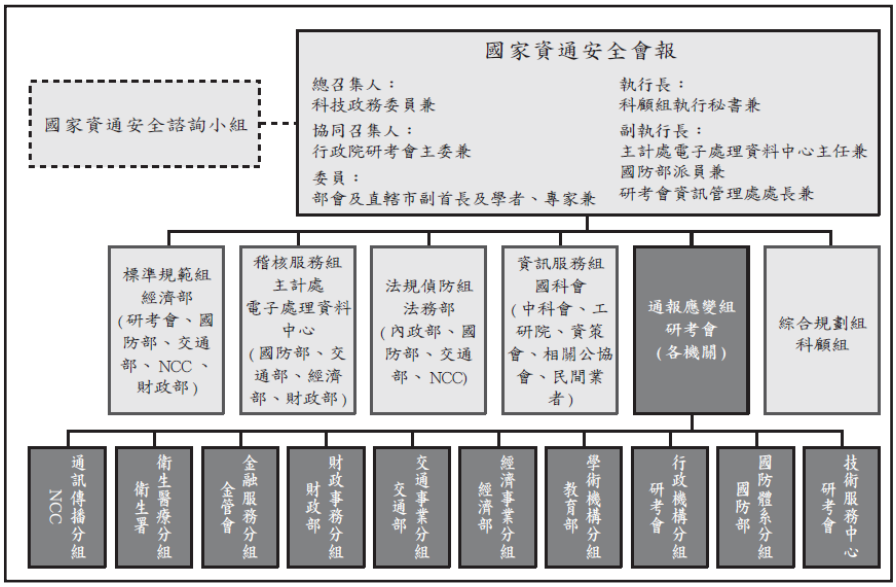


圖3 行政院國家資通安全會報組織架構。資料來源：行政院國家資通安全會報(2007)[10]

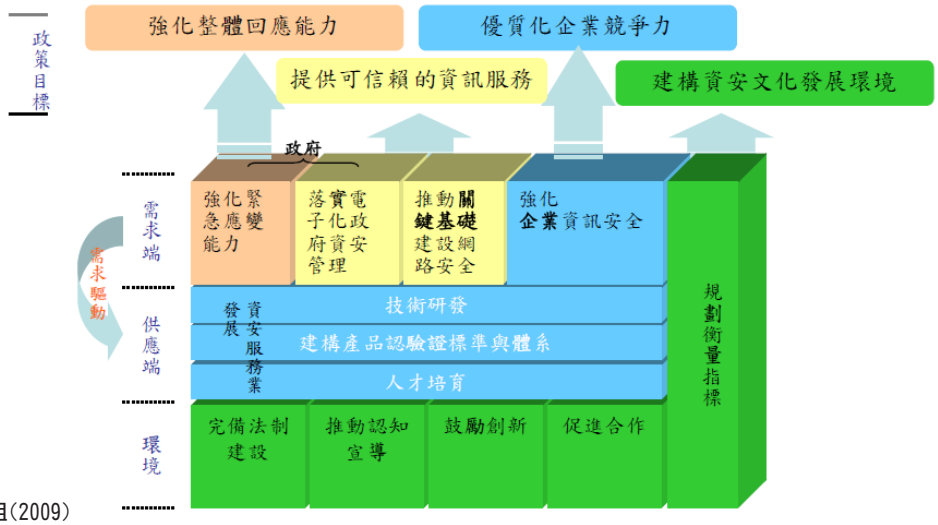


圖4 發展藍圖[13]
資料來源：行政院科技顧問組(2009)

目標	重要措施		行推動方案
強化整體回應能力	提升通報應變及復原能力力	1	提升通報時效
		2	建立資安事件管理與回應程序
		3	持續發展緊急應變及復原能力
		4	訓練資安事件回應人力
提供可信賴的資訊服務	落實電子化政府資安管理	5	發展與維護政府機關資安作業規範與參考指引
		6	推動資安治理
		7	推動資訊與資訊系統分類分級
		8	強化電子化政府資通安全，落實公務資料保護
		9	推動政府機關(構)採購符合安全驗證之資通訊設備
		10	充實資安人力
		11	提升資安防護技術與服務品質
		12	強化資安素養與能力培訓
		13	加強資安稽核與推動資訊安全管理系統驗證
	推動關鍵基礎建設網路安全	14	發展關鍵資訊基礎建設保護策略
優質化企業競爭力	強化企業資訊安全	15	強化電子商務信賴安全
		16	依法規授權，促進事業機構運用第三方評鑑
		17	促使業者發揮自律精神，善盡資安社會責任
	發展資安服務業	18	發展資通安全產品及管理系統認驗證標準及體系
		19	強化國家資安研究能量
		20	建構資安人才培育體系
建構資安文化發展環境	完備法制建設	21	檢討修訂國家資通安全相關法規
		22	持續發展數位鑑識能量
	推動認知宣導	23	推動教育體系資通安全計畫
		24	提供全方位資安資訊服務
		25	整合資安資源之訊息，分眾加強宣導
	鼓勵創新合作	26	規劃依資安策略需要而運作的新型組織
		27	鼓勵讓資源發揮最佳效益的創新作法

表3 發展藍圖[12]。資料來源：行政院科技顧問組(2008)

體回應能力」、「提供可信賴的資訊服務」、「優質化企業競爭力」及「建構資安文化發展環境」的目標[12][13]。

(三)資訊安全的推行現況

將我國資安關鍵指標共分為3大類：「資安認知與環境」、「整體資安防護能力」及「緊急應變功能」，在透過量化資訊、定性分析，可概略瞭解資安政策發展狀況、實施成效及趨勢，下表4為我國95～97年資安關鍵指標的總表現[12]。

(四)資訊管理系統

依據95年7月20日國家資通安全會報第十五次工作小組會議，為明確各政府機關(構)資訊安全責任等級分級作業流程，特訂定「各政府機關(構)資訊安全責任等級分級作業研訂施行計畫」，透過有效的資訊安全管理，來防止資訊受到潛在威脅的破壞，進而全面提升國家資通安全防護水準，以管理手段考量主客觀之形勢，明確律定資安等級之規範[14]，因此對於資訊安全管理系統(Information Security Management System，簡稱ISMS)的推動列入管理的工作事項，將單

大類	小類	指標名稱（單位）	數據			資源
			95	96	97	
資通安全認知與環境	資安資源投入程度	組織資安經費占資訊經費比例（%）	5.08	4.56	5.4	政院主計處
		組織具有資安教育訓練之比例（%）	-	38.0	39.9	台經院
		組織設置資安專責主管之比例（%）	-	16.2	9.6	台經院
	資通安全法規整備度	資通安全法規建立之整備度（%）	72.7	72.7	72.7	台經院
	民眾資安素養	民眾具資安素養之比例（%）	*75.3	*65.5	*70.8	NII
整體資通安全防護能	資安防護裝置完備	防毒產品使用普及率（%）	86.4	90.7	86.7	政院主計處
		防火牆普及率（%）	67.5	76.9	76.4	政院主計處
		入侵偵測系統（IDS）普及率（%）	17.6	21.9	28.4	政院主計處
		漏洞修補程式管理普及率（%）	-	38.8	46.0	台經院
	資安認驗證情形	政府及上市櫃企業通過資安驗證之比例（%）	-	5.3	6.7	台經院彙整
		人員取得資安專業證照數（張/每百萬人）	-	196	248	台經院彙整
	安全網路伺服器普及率	擁有安全網路伺服器（SSL 伺服器）數（台/每百萬住民）	*169	*298	*312	台經院
	資安事件發生	組織遭受資安事件侵害之比例（%）	40.5	51.8	52.4	政院主計處
		資料遭竊或被破壞之比例（%）	0.65	0.8	1.5	政院主計處
		組織遭遇病毒侵害之比例（%）	38.8	49.9	49.5	政院主計處
		組織遭遇傀儡程式感染之比例（%）	5.0	7.1	9.3	政院主計處
緊急應變功能	資通安全演練	組織舉辦資安演練之比例（%）	-	33.8	42.7	台經院
	資安事件損害	資安事件危害與復原時間（小時）	-	11.35	12.34	台經院

表4 95~97 年我國資安關鍵指標表現總表。資料來源：行政院科技顧問組(2008)[12]

(說明：標示*數據表示當年度調查結果，其餘數據表示調查前一年狀況；部分指標項目於95年未進行調查，故無數據。)

作業 / 內容 / 等級	防禦機制強度	防護縱深	ISMS推動作業	稽核方式	資安教育訓練（主官, 主管, 技術, 一般）	專業證照
A級	強度等級4	NSOC/SOC、IDS、防火牆 防毒	96年通過第三者認証	每年至少執行2次內稽	(4, 6, 18, 4小時)/每年	96年資安專業鑑定證照2張
B級	強度等級3	SOC(OP) IDS、防火牆 防毒	97年通過第三者認証	每年至少執行1次內稽	(4, 6, 18, 4小時)/每年	96年資安專業鑑定證照1張
C級	強度等級2	IDS 防火牆 防毒	各單位自行成立推動小組規劃作業	自我檢視	(2, 6, 12, 4小時)/每年	資安專業訓練
D級	強度等級1	防火牆 防毒	推動ISMS觀念宣導	自我檢視	(1, 4, 8, 2小時)/每年	資安專業訓練

表5 各類資安系統等級應執行之工作事項。資料來源：行政院國家資通安全會報(2005)[14]

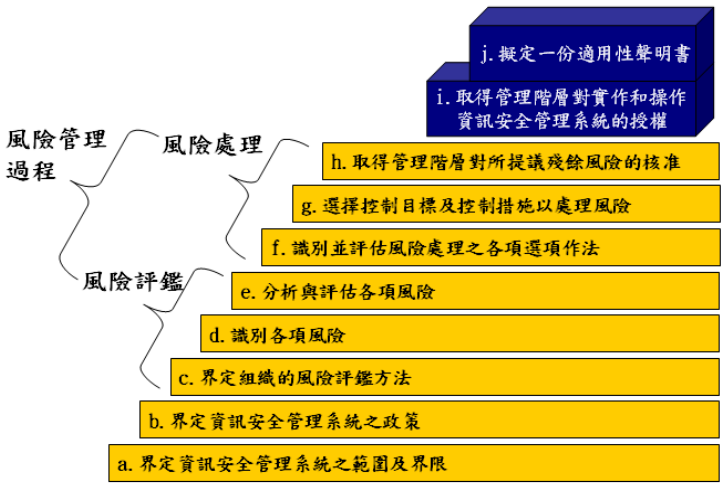


圖5 建立ISMS的步驟。資料來源：本研究自繪，參考ISO/IEC 27001:2005 [5]

位依資安等級區分為A級(重要核心)、B級(核心)、C 級(重要)、D級(一般)，並規範各類資安系統等級應執行之工作事項如表5：

1. ISMS

為國際現行五大管理系統之一，乃整體管理系統的一部份，以營運風險方案為基礎，以人員、資料、設備、存取、系統安全、環境安全作為資訊安全的範圍，用以建立、實施、操作、監督、審查、維持及改進組織的資訊安全(ISO/IEC 27001:2005)。在ISMS國際標準未制定前，目前我國經濟部標準檢驗局業依ISO/IEC 27001:2005 作為我國受理ISMS 驗證之標準[15]。

建立ISMS的步驟如左圖5。

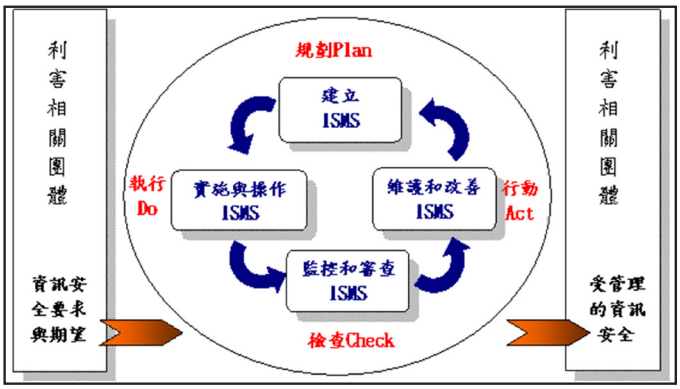


圖6 PDCA模式應用到ISMS過程
資料來源：經濟部標準檢驗局(2008)[15]

ISMS依「規劃-執行-檢查-行動」(Plan-DO-Check-Act，簡稱PDCA)過程模式來進行ISMS的矯正，以確保ISMS之有效性，其模式如圖6，模式簡要說明：

(1)規劃(建立ISMS)：

建立安全政策、目標、標的、過程及相關程序以管理風險及改進資訊安全，使結果與組織整體政策與目標相一致。

(2)執行(實施與操作ISMS)：

實施與操作ISMS 政策、控制措施、過程與程序。

(3)檢查(監視及審查ISMS)：

依據ISMS政策、目標與實際經驗，評鑑及在適用時測量過程績效，並將結果回報給管理階層審查。

(4)行動(維持和改善ISMS)：

依據ISMS內部稽核與管理階層審查結果或其他相關資訊採取矯正與預防措施，以達成ISMS的持續改進[5] [16] [17]。

2. ISO27001認證標準

ISO27001是國際資訊安全管理系統標準，它不是一種技術，而是一種管理制度，係為提供用以建立、實作、運作、監視、審查、維持及改進ISMS之模型，包含了11個管理領域、39個控制目標、133個控制要點，架構圖如下圖7[15]。11個管理領域簡要說明如下：

(1)安全政策：表達對資訊安全管理系統的支持和承諾。

(2)資訊安全組織：建立一個管理架構，用於單位內部資訊安全的管理和控制，以及執行現有的資訊安全規定。

(3)資產管理：確保對組織各項資產的安全進行有效保護。

(4)人力資源安全：明訂所有人員在安全方面的職責和角色。

(5)實體和環境安全：對單位作業場所及人員提出簡單明確的安全要求。

(6)通訊與作業管理：盡可能完善公司內外的溝通聯繫，以利於資訊安全管理系統的順利運行。

(7)存取控制：管理對資訊的存取行為。

(8)資訊系統取得、開發和維護：確保公司IT專案和相關的支援活動已實施安全控制，必要時進行資料管制和加密。

(9)資訊安全事故管理：確保在某種程度上傳達與資訊系統有關的資訊安全事件與弱點，始能採取即時的矯正行動。確保實施一致與有效的方法管理資訊安全事故。

(10)營運持續管理：發展和維護企業營運持續計劃，保護關鍵的業務活動免受重大災難或中斷的影響。

(11)遵循性：符合資訊安全法令或規定的相關要求。

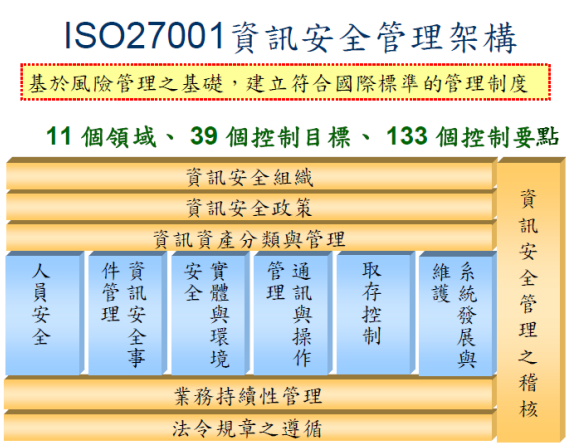


圖7 ISO27001資訊安全架構圖
資料來源：經濟部標準檢驗局(2008)[15]

肆、海軍官校之資訊安全SWOT探討

一、海軍官校簡介

海軍官校為隸屬國防部，得委任國防部海軍司令部辦理，並依相關教育法令之規定，兼受教育部指導。其宗旨為培養海軍軍官人才，並辦理基礎教育，設置校長一人，綜理校務；教育長、政戰主任各一人，襄助校長處理校務，行政單位包含教務處、總務處、學員生事務處、資訊圖書中心、主計室、學生總隊、軍史館、勤務隊；教學單位包含一般學科部、軍事學科部、通識中心[18]。在學生部分計有正期班(畢業賦予學士學位)及士官二專班(畢業賦予副學士學位)，約700餘員。

二、SWOT分析

由於網際網路的發達使得作業環境不再侷限於封閉的空間，而是建置在跨越國界與時空的平台，對於可能產生的危安因素也相對地增加，另一方面由於數位化資訊的易於複製、流傳及修改等特性，也致使資訊外洩的風險大大提升。就海軍官校的資訊安全現況而言，因兼具軍事與教育單位的特殊身份，在資訊安全推行上亦配合國防部政策已行之有年，但仍有待改善之處，在此對於所面對資訊安全的環境之SWOT進行分析，以更清楚了解如何善用優勢及機會，並補強弱點及預防威脅，就海軍官校資安現況之優勢、弱點、機會和威脅說明如下[19 20 21]：

(一)優勢(Strengths；S)

1. 係屬國軍體系，人員對於資訊安全的認知與警覺性較高，資安應變及回報能力較確實
2. 人力進用均經基本考核，人員可信賴度較高。
3. 係屬國軍體系，對於違規嚴懲不怠，資安工作較能確實實踐。
4. 國軍每年定期推行各項資安政策及稽核，使單位資安管控更加落實。
5. 高階主管對於資安政策大力支持，有利於單位資安政策推動。
6. 係屬教育單位，人員資安知識汲取及推廣較能普遍，如教師藉由資訊課程進行資安教育等。

(二) 弱點(Weaknesses；W)

1. 因係屬教育性質，在強調資訊服務需求及學術自的環境下，因「便利性」與「安全性」難以兩全，並偏重資訊「可用性」，致使資安參與意願與共識度低。
2. 學校專屬資安人力少，均以兼任職務方式辦理，且雖設定資安體系，但多由低階人員擔任，從事全單位資安執行及稽核作業，無法達到責權區分及全面落實現有繁鎖之資安管控。
3. 資安規管多且繁鎖，變化快速，專精人數不多。
4. 資設設備繁多，人力不足，專業資安技術及操作不熟悉、管理不易。
5. 因係屬國防體系，對於資安獎勵與懲處僅適用於國軍人員，對於教師及學生無實質激勵作為，行為面常未落實資訊安全。
6. 雖各方面資安機制均堪稱完備，但資安攻擊之手法日新月異，系統、網路弱點防不勝防。
7. 對於已知系統或網路脆弱性、未知的攻擊之預警及防護策略，資訊繁多分散及分享不易。
8. 委外系統、網路廠商資安專業水準良莠不齊，致使資安弱點層出不窮。
9. 人員心存僥倖，對於資安防護並未加以注意，提高資安事件肇生機率。
10. 對於未列入資安監控之設備，若發生資安事件，會有隱匿不報之情事。

	優勢 (Strengths；S)	弱點 (Weaknesses；W)	機會 (Opportunities；O)	威脅 (Threats；T)
資通安全認知與環境	1.資安認知與警覺性較高。 2.對於國軍人員違規嚴懲不怠。 3.高階主管對於資安政策大力支持。 4.人員可信賴度較高。 5.資安知識汲取及推廣較普遍。	1.資安參與意願與共識度低。 2.資安人力少，未落實責權區分。 3.教師及學生無實質激勵作為。 4.人員心存僥倖。	1.上級要求與規範較嚴謹 2.參加各界資安教育訓練或研究會，資安認知較全面性。	1.因資料蒐集或未依規定使用儲存媒體而提高誤入釣魚網站、或感染惡意程式等之機率。 2.資安績效評量不易，潛在效益也經常無法彰顯，致使經費投資不足，及造成一般業務及教學單位推動上的瓶頸。
整體資通安全防護能力	1.定期推行各項資安政策及稽核，使單位資安管控更加落實。 2.資安裝備完整。	1.資安規管多且繁鎖，變化快速，專精人數不多。 2.資安攻擊之手法日新月異，系統、網路弱點防不勝防。 3.委外系統、網路廠商資安專業水準良莠不齊。	1.政府及國軍大力推行各項資安防護資源。 2.資安事件損失刺激資安防護技術發展及應用之增長。	1.外界對軍校為攻擊目標的興趣濃厚。 2.網路上充斥著各式的木馬、病毒等威脅。 3.對於單位心存不滿之人士恐蓄意破壞。
緊急應變功能	資安應變及回報能力較確實。	未列入資安監控之設備發生資安事件，會有隱匿不報之情事。	各級資安應變中心架構完整，反應即時。	

表6 海軍官校資訊安全SWOT分析。資料來源：經濟部標準檢驗局(2008)

三、機會(Opportunities；O)

1. 係屬國軍體系，上層單位對於資訊安全的要求與規範較其他一般大學嚴謹。
2. 政府及國軍大力推行各項資安防護資源，如憑證卡等，可強化單位資訊之安全程度
3. 由於資安事件損失(如個人隱私外洩、單位資料遺失或遭竊等)造成對於資安防護的重視，不論在資安市場需求的增加及單位對資安投資動機提升，致使資安防護技術的發展及應用持續增長。
4. 對於國防部或教育部之資安教育訓練或研討會，均可參與及對照學習，使得資安認知較全面性。
5. 各級資安應變中心架構完整，通報及處理之反應即時，降低資安事件的肇生及擴散。

四、威脅(Threats；T)

1. 係屬國軍體系，外界對學校作為攻擊目標的興趣濃厚。
2. 伴隨著資訊網路的發達，網路上充斥著各式的木馬、病毒等威脅。
3. 學生及老師因資料蒐集或未依規定使用儲存媒體而提高誤入釣魚網站或感染惡意程式等之機率。
4. 係屬國軍體系，講求嚴謹紀律及服從，對於單位心存不滿之有心人士恐有蓄意破壞及釀成資安事件之威脅。
5. 資訊安全績效評量不易，潛在效益也經常無法彰顯，致使教育經費投資不足，及造成一般業務及教學單位推動上的瓶頸。

綜整以上優劣勢與機會、威脅，依據行政院科技顧問組之資安關鍵指標項目作為分析面向項目，進行綜合(多面向)之分析如表6。

伍、結論

透過SWOT分析所反映的情形，提出以下對策因應的建議：

一、落實執行資安政策並持續檢討改進，並依ISO 27001完成資訊安全管理。

二、加強資安防護措施及專業技術，以因應千變萬化的病毒及駭客手法。

三、強化資安認知與警覺性，以降低資安威脅。

四、提供資安防護資源平台及人性化之防護機制，以獲得共識及支持。

學校資訊安全可說是建構於環環相扣的保護機制下，攻擊者只要找出其中最脆弱的一環，就可以完全瓦解整個保護機制，因此我們應秉持著「資訊安全，人人有責」的心態，以更謹慎的態度面對資訊安全的防護，而不是認為沒有處理機密資料就忽略資訊安全，造成資安漏洞或成為駭客的跳板。在面對千變萬化的病毒及駭客等威脅，惟有主動積極做好資訊安全防護，如此才能享受安心優質的e化環境。

參考文獻

1 李呈奇(2002)。大學推動校園e化之探討。國立中山大學人力資源管理研究所未出版之碩士論文。
2 臺灣電腦網路危機處理中心(2001)。校園網路安全性之評估。本文公告於臺灣電腦網路危機處理暨協調中心之TWCERT/CC 文件。取自http://www.cert.org.tw/document/docfile/campus.pdf。政研究所未出版之碩士論文。
3 湯耀中(2003)。從戰爭的觀點論資訊安全。台北市：全華。
4 電子化政府網路文官學。B01-001 資安管理-資訊主管篇。本文張貼電子化政府網路文官學院之資訊安全教學課程簡報。取自http://elearning.nat.gov.tw。
5 ISO (2005)。ISO/IEC 27001 Information technology - Security techniques -Information security management systems - Requirements, first edition. ISO.
6 Eric Maiwald 著，尤培麟、謝侑純、王子敬譯(2002)。網路安全入門手冊。台北市：麥格羅希爾。
7 何瀛州(2007)。區域級學術網路組織之資訊安全風險評估－以宜蘭縣學術網路為例。佛光大學資訊學系碩士在職專班未出版之碩士論文。
8 Robert Richardson(2009). 2008 CSI Computer Crime & Security Survey. CSI/FBI, 取自http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf。
9 教育部提升校園資訊安全服務計畫服務團(2008)。網路安全威脅分析。本文張貼於教育部校園資訊安全服務網之資安新知。取自http://cissnet.edu.tw/knowledge_11.aspx。
10 行政院國家資通安全會報(2007)。建立我國通資訊基礎建設安全機制計畫(94 年至97 年)。本計畫於中華民國96 年2 月15 日行政院核定修正。取自http://www.pthg.gov.tw/CmsFile%5C200742694854234.pdf。
11 國家資通安全會報。本文張貼於國家資通安全會報之資通安全相關組織介紹。取自http://www.nicst.nat.gov.tw/content/application/nicst/weblink/guest-cnt-browse.php?cnt_id=116。
12 行政院科技顧問組(2008)。2008 資通安全政策白皮書。行政院。
13 行政院科技顧問組(2009)。國家資通訊安全發展方案(98 年至101年)。行政院國家資通安全會報中華民國98 年1 月製。取自http://www.penghu.gov.tw/chinese/03news/01view.asp?bull_id=21202。
14 行政院國家資通安全會報(2005)。政府機關(構)資訊安全責任等級分級作業實施計畫。行政院國家資通安全會報94 年7 月22 日資安發字第0940100615 號函頒。
15 [經濟部標準檢驗局(2008)。ISO 27001：2005 資訊安全管理系統要求。本文張貼於經濟部標準檢驗局之最新消息。取自http://www.bsmi.gov.tw/wSite/public/Data/f1228114692438.ppt。
16 唐雨漁(2006)。ISMS 政策探討。本文張貼於行政院人事行政局之資訊機密維護專精研習班課程簡報。取自http://www.tycg.gov.tw/files/download/455d7741.ppt#259,4,三、何謂ISMS(Information Security Management System)。
17 謝惠玲(2007)。資訊安全機制規劃及建置之現況調查與分析--以國內大學校園系統為例。靜宜大學資訊管理學系未出版之碩士論文。
18 海軍軍官學校(2007)。海軍軍官學校組織規章。本文張貼於全國法規資料庫。取自http://law.moj.gov.tw/Scripts/Query4A.asp?FullDoc=all&Fcode=F0000054。
19 江通儒、郭真祥、張瑞益、許凱平(2008)。學術機關資訊安全管理建置成熟度模型。本論文發表於教育部舉辦之「2008 臺灣網際網路研討會(TANET)」，取自http://ccnet.km.nccu.edu.tw/xms/index.php?view=content_show&id=977。
20 汪耀華(2004)。國立大學資訊安全管理之研究。國立臺灣師範大學教育學系在職進修班未出版之碩士論文。
21 蔡忠翰(2003)。政府部門資訊安全管理之研究。國立政治大學公共行政研究所未出版之碩士論文。