推廣不離開工作崗位亦可達到資安職能之養成教育，期能學以致用協助單位內資安防護績效。

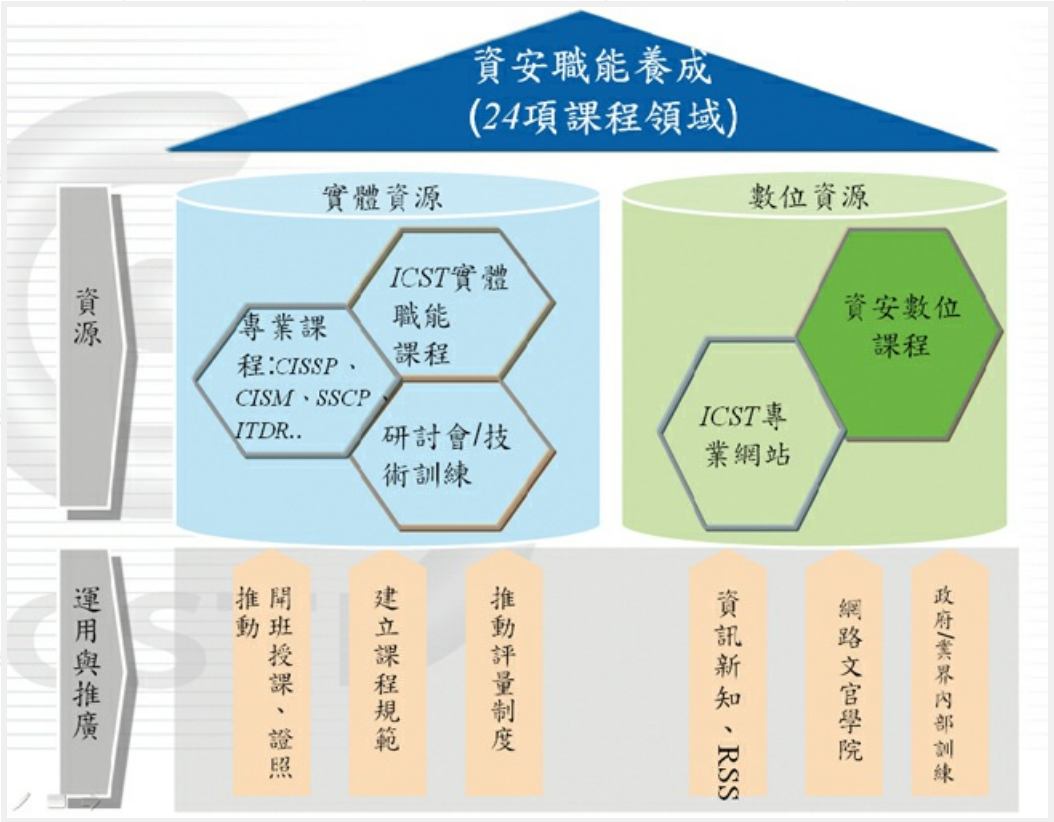
資安數位學習發展與推廣

◎紀佳妮

一、數位學習的趨勢

數位學習具備隨時隨地高取得資訊的特性，尤其符合現代社會快速變遷的模式，能克服傳統學習空間、時間的限制，透過學習網站、學習社群、虛擬教室等方法，營造一個自主的、個人的學習空間，有效率地學習各種知識與技能，因此數位學習深受政府機關與一般企業的喜愛，且已被納入單位內教育訓練之重要方式之一。

多年來國家資通安全會報技術服務中心（以下簡稱技服中心）戮力於資安認知推廣與職能培訓。考量公務人員散布全省且人數眾多，資安教育範疇廣大，單是以實體課程資源誠不足以顧及所需，因此在僧多粥少的情況下，資安數位學習不受時間、地域、人數限制的特性與網路的方便性，著實成為訓練推廣的好幫手。



資料來源：國家資通安全會報技術服務中心

圖1　資安推廣與訓練資源

二、資安數位課程發展

技服中心推動公務人員資安職能規劃，進行整體訓練研擬與資源分配，運用多元的學習管道與訓練方式，包括實體資源與數位資源（圖1）。實體資源涵蓋職能課程、專業課程、證照課程、巡迴研討會及資安推廣活動－資安週與競賽活動等；而數位資源則包括資安數位課程與網站服務，對於資安推廣與訓練具有實質的成效。

技服中心規劃資安數位學習的課程，主要為提供遍及全省的五千多個政府單位，接受資安教育的另一項選擇，尤其是鮮少有機會參加資安實體課程的一般人員、C和D級之資安（訊）人員，以及時間常常無法配合而只能抽空學習之主管人員。技服中心考量這些族群的需求，早在多年前即著手發展資安數位學習課程。另一方面，行政院國家資通安全會報頒布之「國家資通訊安全發展方案（98－101）」與「政府機關資訊安全責任等級分級作業施行計畫」，對各級機關之人員類別，分別規範出資安訓練學習時數，逐步建立公務人員的資安能力。各機關亦可自行規劃資安訓練課程，如資安研討會、資安專業技術講習及資安數位學習等方式，以取得授課時數。由此可見資安訓練之重要性與需求量之大，發展資安數位課程確實提供公務人員自我成長的另一種訓練選擇。

目前有關資安數位學習的資源，以行政院研考會所屬電子化政府網路文官學院（http://elearning.nat.gov.tw）提供的資訊安全類訓練課程為大宗，此類

課程為技服中心所規劃發展。其他如國家文官培訓所設置的文官e學苑、臺北市政府公務人員訓練處、臺北e大數位學習網、高雄市政府資訊處設置的港都e學苑、行政院主計處電子處理資料中心設置的公務員資訊學習網，也有開辦與資安相關的資訊科技或資訊管理課程。

由技服中心發展的資安數位課程配合資安職能規劃，考量課程內容數位化之適宜性進行規劃與開發；數位化的課程包含通識入門、資安技術、資安管理、資安法令法規的介紹等。自94年至98年共開發71小時61門數位課程，每門課程均設定學習目標，期望藉由數位學習達到職能養成之目的。

在數位課程的學習建議方面，參考資安職能之人員類別後，將一般主管、一般人員、資訊人員及資安人員，可以修習的數位課程分為必修與選修兩類，如表１。

表1　數位課程學習建議

註：*必修　・選修

課程類別	職能領域	數位課程名稱	一般主管	一般人員	資訊人員	資安人員
資安入門(通識)	資通安全概論	資安管理－個人篇	*	*	*	*
		資訊安全概論	*	*	*	*
		資安管理－資訊主管篇	*		・	・
		資安管理－主管篇	*			
	電腦作業安全概念	Email社交工程及防護	*	*	*	*
		個人電腦基本安全防護	*	*	*	*
		存取控制概觀	*	*	*	*
		可攜式儲存媒體安全管理	*	*	*	*
		Windows 安全防護應用	*	*	*	*
	機關資安管理規定	涉外人員資通安全作業實務		*		
	資通安全相關法律	資訊相關法律簡介	*	*	*	*
		政府資訊公開法制對政府機關處理資訊之因應作為	*	*	*	*
	個人資料保護	個人資料保護	*	*	*	*
資安管理	資通安全管理制度	資訊安全管理制度(ISMS)簡介	*	*	*	*
		資訊安全稽核使用之標準CNS(ISO)27001(上)(下)				*
		資訊安全政策制定與資訊安全組織建立	*			*
		資訊資產管理				*
		軟體智財權管理				*
	資訊系統風險評鑑	資安風險管理概觀				*
		資安風險評鑑實務				*
	業務持續運作管理	營運持續管理(BCM)概觀	・		・	*
		營運持續計畫之災害復原實務	・		・	*
	資通安全稽核	資訊安全稽核介紹與實務1~4				*
	資安事件應變作業	資訊安全事件通報機制簡介	・		*	*
資安技術	通訊網路安全原理與應用	網路安全概論			・	
		VPN虛擬私有網路技術概說			・	
		網路封包、流量解析與監控			・	
		網路攻擊技術分析			・	
		VOIP安全威脅與防護			・	
		網站設定、搜尋引擎弱點防護			・	
	入侵偵測／預防系統理論與	入侵偵測與預防系統簡介與應用			・	
		駭客入侵之DDNS手法及因				

資安技術	應用	應措施			•	
	防火牆理論與應用	防火牆原理、架構和種類介紹			•	
		防火牆建構及設定			•	
		防火牆理論與應用			•	
	網路弱點評估實務	電腦病毒原理及防治			•	
		作業系統漏洞修補			•	
		弱點掃瞄技術			•	
		網路弱點認知			•	
	密碼學原理與應用	密碼學原理與技術			•	
	無線網路安全理論與應用	無線區域網路安全防護			•	
	Linux系統安全管理	Linux安全防護基礎			•	
	備援技術理論與應用	備援技術與應用			•	
	Web應用程式安全	應用服務安全實作－Web應用程式之威脅與防護1~2			*	•
		安全的系統發展生命週期(SSDLC)介紹			*	•
其他	新興科技資安議題	web 2.0安全防護	•		•	•

三、資安數位課程開發

資安數位課程之學習對象以公務人員為主，因此課程規劃以本國政府機關之作業需求為主要內容；考量公務人員之實務環境、操作練習、實務研習、案例情境、設備環境等因素進行課程規劃。課程規劃內容大致包含課程大綱架構、課程總目標（知識與技能）、章節目標、課程摘要、適學對象、課程時數、先備知識及內容專家資歷等，並符合我國數位教材品質認證v3.0之規範，包含教材內容、教學設計、教學媒體、導引與追蹤，及創意等五大檢核要求，確保所設計之教材有助於學習者達成預定的學習目標。

資料來源：國家資通安全會報技術服務中心

圖2　網路文官學院

資料來源：國家資通安全會報技術服務中心

圖3　資安數位課程教學光碟1-4輯

四、資安數位學習推廣

技服中心所開發的數位課程分為兩種，一種以講師影像搭配簡報進行教學；另一種則以flash多媒體呈現，搭配教學設計腳本與配音而成。至目前為止，以flash方式製作的課程約占四分之三，未來將視需要陸續調整教學與呈現方式，以達到更好的學習效果。另外在傳播方面，資安數位課程傳播方式分成兩種管道，一是提供線上學習，統一放置於行政院研考會e化政府網路文官學院網站http://elearning.nat.gov.tw（圖2），使用者需加入該網站成為會員，學習紀錄則可列為公務人員的終身學習時數。

考量地方政府與偏遠機關的網路連線品質和學習需求，技服中心將資安數位課程壓製成「資通安全數位課程教學」光碟（如圖3），提供單位內部自行舉辦資安訓練；此類的服務亦開放給一般企業申請。

五、結論

數位學習課程發展以協助公務人員在不離開工作崗位亦可達到資安職能養成為目標，期能學以致用協助單位內資安防護績效。目前技服中心之資安數位課程開發已日趨成熟，未來將持續以滾輪式檢討，調整課程之正確性與適宜性，並配合年度推廣計畫開發新課程，以實體、數位雙軌資源，持續推廣資安職能之知識與技能。

（作者現任財團法人資訊工業策進會與行政院國家資通安全會報技術服務中心工程師）

▲Top

清流月刊中華民國九十九年八月號

主管身負資安推動工作重要職責，應具備基本的資安認知與技能，以及資安管理決策能力。

資安數位課程—資安管理主管篇

◎紀佳妮

一、前言

組織內凡是與人相關的議題，都必須由管理者協助推動始能順利。同樣的，資安的推動需要組織內每個人員的投入與配合，推動期間面對的種種異聲，主管的態度與支持有如神助般地有效又有力。在面臨駭客手法日新月異、人心不古、外在環境干擾等不可控制因素，身為一個組織的主管，應該具備哪些資安認知與技能，才能讓組織在充滿資安的危機中仍能屹立不搖且持續運作呢？

技服中心深知主管在資安推動工作中身負重要職責，因此，主管的職務能力應具備基本的資安認知與技能，及資安管理的決策能力。主管如何具備這些能力呢？基本上可透過訓練來加強。技服中心針對主管職能需求，已開發數門課程協助其能力的培養；然而考量主管公務繁忙，可配合實體課程的時間有限，因此特規劃主管的資安數位課程，以便主管自由學習。

二、數位課程開發程序

資安數位課程，結合內容專家、教學設計師及多媒體設計師共同開發。為確保課程之品質，採以ADDIE系統化教學模式，即：規劃分析（Analysis）、需求設計（Design）、內容產出（Development）、建置（Implement）、評鑑（Evaluation），循序漸進地掌控各階段的品質，進行課程開發，同時在重要階段進行審查，包括：課程大綱、教材、教學設計、腳本及成品的審查會議，以確保符合課程的需求。

有關ADDIE系統化教學模式分述如下：

（一）規劃分析：針對學習者之需求進行分析，了解學習者學習環境與目標需求；透過使用者、教學設計師及講師三方的溝通方式，產出第一階段之課程名稱與課程大綱。

（二）需求設計：進行課程內容討論與課程呈現設計，透過編審團隊審核課程大綱之合理性，由內容專家與教學設計師共同設計課程架構與內容案例。

（三）內容產出：由專案小組依據內容專家與教學設計師討論之結果，完成腳本產出，並依照作業流程進行課程編撰及提供審查；為確保課程內容符合需求，需於課程製作階段即安排審查。

（四）課程上線與建置：課程完成最後審核階段，由工程人員系統化為平台規格，安裝至指定之平台上，測試課程的完整性及正確性。

（五）評鑑：數位課程上線服務後，學員使用意見的回饋與持續改善，並且定期檢視內容的適切性。

三、「資安管理主管篇」課程設計理念

數位課程「資安管理主管篇」之課程核心發展方向，是從主管的角度切入，對於主管而言資安管理之意義為何？哪些是主管必須了解的資安認知？主管的職責是什麼？切身相關又是為何？資安防護應如何決策？從這些角度作為本課程之核心，釐清主管在資安威脅當中需要了解的事項，再進而讓主管能夠具備資安管理決策的基本概念。

「資安管理主管篇」數位課程之教學設計，應用多元手法，以輕鬆不失內涵的授課方式，為獨自學習的主管們增添學習的興致。這門課程我們模擬專業談話性節目，設計由主持人引言，搭配與資安相關領域專家互動談論，以專業認知及資安案例探討，再加上圖像化的視覺設計，和專業的配音效果，凸顯課程的可看性。

四、「資安管理主管篇」課程簡介

第一章：資安威脅

1-1資安之重要性

近年來政府單位資安事件頻傳，造成單位聲譽嚴重受損，諸如網站遭作停擺、遭駭客入侵、民眾個資曝光等等，導致個人資料、機密公文、筆錄資料、醫療紀錄，甚至連總統的手機號碼在網路上也查得到；資安事件讓組織單位遭受各種有形、無形的衝擊。
資訊系統內的重要資料外洩，可能導致社會事件，例如資料被詐騙集團使用，造成金錢、生命的威脅，人民恐慌，社會不穩定，所以資安事件已不是單純的電腦出問題或中毒這麼簡單了，而是涉及社會安全、經濟安全及國家安全等不可輕視的重要議題。資安事件一旦發生，主管難脫責任，資安對於機關首長來說，更是關鍵的風險管理課題！

1-2資安威脅趨勢

根據美國CSI（Computer Security Institute）針對重要的政府組織、教育機構、醫療機構及企業人員，所作的2009年資安調查報告，其中資安攻擊事件的研

究顯示，惡意軟體感染事件、筆記型電腦失竊、內部人員舞弊分占前三名，可能伴隨著機密資料的外洩問題，值得注意；CSI另一項研究顯示資安占IT預算的比例，雖然2008年遭遇全球不景氣，2009在資安預算上仍有微幅的成長，反映出組織對於資安重視的程度提高，越來越多單位願意投注資源在資安上，由於舊系統可能無法抵擋新型態且多樣化的資安事件，所以在可允許的範圍內漸漸提高資安的預算比例。

第二章：資安管理

2-1組織應保護的資產

資訊資產保護是資訊安全管理的基礎，如何對資訊資產進行適當的控管，是組織主管必須認知的重要課題。主管應了解組織裡應保護的資產範疇，了解到底哪些資產對組織是重要的，及其可能面臨的風險，並且盡到資訊資產保護的監督責任。資訊安全的資產依ISO 27002大致分為資訊、軟體資產、實體資產、服務、人員、無形資產等六類，保護的原則主要確保資產的機密性、完整性、可用性。政府機關主要職責即為保護機密敏感資料的妥善使用，資訊系統、網站及網路等資訊設備的正常運作，以及政府的聲譽。

2-2資產的威脅與防範

本章節藉由資安案例說明資產可能面臨的威脅並提出防範建議，提供給主管們了解資安的重要性與未來資安事件因應的參考，案例包括：資訊系統安全控管、民眾個資的保護、作業流程與人員控管、資訊系統備份與備援機制建立等討論。課程中詳細說明事件的原因與問題，並且提出防護之建議，可做為機關內安全防護的借鏡。

第三章：風險管理

3-1資安風險管理概念

主管應認知資訊安全風險之意義及風險管理包含之要素與之間的關聯，並且了解資安風險管理程序，善盡資安管理之職責。在風險管理程序中主管應扮演的角色，包括決定保護的範圍與需要保護的資產，並且決定風險評鑑的方法，以及組織可以接受的風險等級，從而決定組織的關鍵業務與相關風險管理所需要的資源；主管之考量依據可從成本、工作效率、組織所真正關心的議題角度來思考。

管控好資安風險三要素：人、流程、技術。「人」意指人員的管理，定期給予職能的教育訓練、提升資安知識與能力，並對人員權責分工進行管理；「流程」泛指訂定各種資訊安全政策、規範、流程、手冊、管理方案，作為可依循的準則；「技術」層面則運用資安技術，針對實體安全、系統存取、身分驗證技術、備援機制等達到安全的要求。

3-2資安管理職責

所有主管在面對資安議題時應先具備幾項觀念，第一、資安事件無孔不入，資安威脅無所不在，因此人人應有資安意識，隨時做好資安防護之全面考量。第二、覆巢之下無完卵，重大資安事件可能會對組織造成難以想像的衝擊，因此組織內所有人員不應有事不關己或存有僥倖的心理。第三、沒有百分百的安全，基於病毒、惡意攻擊、駭客手法等日新月異、防不勝防的情況下，組織必須建立資安管理的防護機制；在有限的資源內透過安全控制將風險降低到可接受的程度，並定期做好資安管理的審視作業。因此，主管對於資安管理的職責，包括推動建立資安管理制度、明訂資訊安全政策，並提出支持與承諾所需人力與預算等。

第四章：資安關鍵成功因素

主管應認知組織內推動資訊安全的成功因素，並且適時給予指導與資源，若能多了解資安防護的重點，將有助於資源的分配。一般而言資安首重３步驟：事前預防、事中發現、事後應變；主管應注意組織在此３步驟間的防護能量。事前的預防即是考量現有防護措施是否足以預防可預期的資安風險；至於事件發生時的察覺時間長短則關係著事件影響的層面，因此完善的監控機制是必要的；而在事件發生後，組織是否有足夠的應變資源，在最短時間內減低傷害以回復持續組織的營運，這些都是主管們應當關切的重點。總之，主管在資安推動上扮演非常重要的角色，對於資安除基本認知外，了解資安的成功關鍵因素，更有助於推動資安的成效。成功因素簡述如下：

第一、主管明確的支持與承諾，沒有高階主管的支持，人力、經費及資源都會面臨短缺的問題，資安難以成為由上而下通達的理念。

第二、組織必須制訂能夠反映營運目標的安全政策，具體的執行方法必須能符合組織營運目標的安全政策。

第三、辦理適當的教育訓練，對管理階層有效地宣導資訊安全概念。此外，就是要建立管理者與員工正確的安全認知，能夠了解什麼是安全需求、風險評鑑的目的，及風險管理的意義。

第四、要建立一套全面且均衡的資通安全稽核機制，並針對如何改善的意見，適當回覆並提出解決的方案。

五、結論

資通安全事件的發生，往往都是由管理者承擔相關責任，因此主管的職責顯得格外重要。本文除強調主管應具備之資安職務能力，包括基本資安認知、技能及資安管理的決策能力外，並精簡地說明資安的基本認知、主管應盡之職責，以及必要知識與技能內涵。此外，技服中心亦開發其他與資安相關的基本認知課程，包含資通安全概論、電腦作業安全概念、資安管理制度、資通安全相關法律及個人資料保護等課程，俾協助主管們培養及累積資安職能，進而領導單位推動資安，以提升單位的資安防護能力。

（作者現任財團法人資訊工業策進會與行政院國家資通安全會報技術服務中心工程師）

▲Top