APT 攻擊對企業資安政策之影響初探
Preliminary Study on the Impacts of Advanced Persistent Threat (APT) on Corporate Information Security Policy

季祥*
中國文化大學資訊管理學系
研究生
xiang0224@yahoo.com.tw

郭建良
中國文化大學推廣教育部
助理教授
clkuo@sce.pccu.edu.tw

摘　要

駭客攻擊係為企業因應網路時代的重要課題；尤其，當資訊安全威脅轉向鎖定特定標的之進階持續性滲透攻擊(Advanced Persistent Threat, APT)模式時，現有企業的資安政策與防禦策略是否仍可有效因應，則成為值得探究的議題。

為協助政府、金融業與大型企業因應此一挑戰，本研究透過文獻分析與內容分析法的方式，針對理論文獻與實務報告，藉由企業資安策略、資安產品架構及解決方案選擇要素、資安服務提供商與資安解決方案業者之觀點及其對 APT 威脅防禦建議，及資安標準議題等面向之比對，找出 APT 對現有資安關鍵要素影響，提出五構面、29 項的企業因應 APT 的資安策略與議題，據此探究對企業實際資安政策改變之關聯，並提出企業資安策略，期為企業與資安顧問業者帶來實務上參考與啟發。

關鍵字：進階持續性滲透攻擊(APT)、資安政策、關鍵要素

一、研究背景

駭客攻擊在這個與網路密不可分的年代已是一個重大議題，駭客僅透過網路即能夠竊取所有企業運作所需的資訊，其中包含商業機密與個人資料。近年來駭客組織已轉換其攻擊型態與策略，也就是從過去專精於駭客技術展示的意圖，轉變為利益取得－無論是取得實質金錢取得或是無形的資訊機密，於是形塑了讓駭客源源不絕發動攻擊的強力誘因。其中，最具威脅的就是 APT 進階持續性滲透攻擊(Advanced Persistent Threats, APTs)；Mandiant 在 2010 年的 M-Tremd 報告首次對 APT 有了詳細的描述，當時指出可能有龐大的組織認可這樣的攻擊活動，直至 2013 年 Mandiant APT1-Exposing One of China's Cyber Espionage Units 報告中說明在進行了數百件的調查後，發現這些主要的 APT 活動發起地都是來自中國，所竊取的重要資訊絕對超過 Mandiant 報告中所觀察到的，因此 APT 可被視為資安威脅型態的典範性轉移(Paradigm shift)，它常來自跨國駭客的攻擊(且主要來自中國)，APT 威脅主要鎖定政府單位，意圖藉此取得特定的國家機密資訊，但從 2011 年開始則發現跨國駭客組織將目標轉向大型企業，許多企業資安防護在 APT 下失守，包括知名的蘋果與臉書等，企業除了造成財務損失，更因個人資料外洩而支付大筆的賠償金。

因此，不容諱言，資安環境已然越來越險惡，連近日美國總統歐巴馬也提到類似論調[1]；所以，企業要有效面對這些威脅也更加的困難；尤其，在 APT 將漸成未來幾年資訊安全環境所面臨的挑戰的情況下，企業組織是否具備足夠的資安防禦策略面對這樣的先進資安威脅？類似的情況在台灣尤為明顯，根據 2012 ISACA Advanced Persistent Threat Awareness 研究報告指出，截至 2012 年為止，國內企業面對 APT 攻擊仍沒有明確的防護策略，縱使資訊安全服務廠商提供了各式因應新型態的資訊安全威脅所設計的防禦方案，但是否能夠真正補足企業的缺失或是仍無法明確的給予企業一個安全的資訊環境則需要做更多的研究與探討(趨勢科技，民 101)。

二、研究目的與方法

承前所述，APT 反應了未來的資安威脅將有顯著的改變，也讓 APT 議題在近幾年引起台灣政府與企業組織的高度關注，因為，企業所面臨的資訊安全威脅已不再是大規模的病毒爆發造成損害，而是要面對精密設計的針對性攻擊，這是一個資訊安全攻擊模式典範性的移轉，是由一個具有大量攻擊資源的特定組織，長期鎖定目標所發起的多方位資安攻擊。

易言之，基於下述三項主要差異，本研究認為資安威脅的轉變對於既有的資安策略會有顯著的影響：(1)攻擊者有充足的資源；(2)攻擊循環周期長；以及(3)攻擊手段全面。所以，若是資安人員繼續使用舊有的資安概念與防護投資比重在面臨 APT 威脅時可能會有更多的挑戰。

因此，本研究希望透過文獻分析與內容分析法的方式，針對理論文獻與實務報告，藉由企業資安策略、資安產品架構及解決方案選擇要素、資安服務提供商與資安解決方案業者之觀點及其對 APT 威脅防禦建議，及資安標準議題等面向之比對，找出 APT 對現有資安關鍵要素影響，提出

[1] 美國總統歐巴馬也在公開演說中提到：「現在我們的敵人也企圖(以網軍)攻擊癱瘓我們的供電網路、金融機構和飛航管制系統。」

因應 APT 資安策略與議題，據此探究對企業實際資安政策改變之關聯，並提出企業資安策略。

三、重要文獻回顧

承前所述，本研究從對抗 APT 威脅的角度探討近年企業資安策略的轉變，包括從主要的資訊安全標準中篩選出對 APT 威脅有直接關係的領域，結合台灣資訊安全發展藍圖重點項目、資訊安全產品、資訊安全服務與資訊安全方案提供商對防禦 APT 威脅的防禦建議進行彙整，歸納出對應 APT 攻擊企業所應採取的資安政策調整範圍。以下，本研究針對 APT 威脅，資訊安全標準，台灣資訊安全發展藍圖，資訊安全解決方案，資訊安全服務，資訊安全威脅，APT 議題與台灣資訊安全環境逐一做探討。

(一) APT 威脅

在攻擊者發起 APT 攻擊前會對其鎖定的目標蒐集情資及分析弱點整理，接著開始對目標展開進攻，會用的攻擊手法包含下載病毒程式，社交工程攻擊，零時差漏洞攻擊等，而攻擊成功以後會持續在企業組織中橫向擴散，以取得更多的控制範圍與持續提升系統權限，本研究也彙整於 2012 年有提出 APT 相關調查報告的六家資訊安全廠商與 Gartner APT 報告中所探討的 APT 攻擊流程彙整於表 1。

因此，企業應對於既有的資安政策做正確的調整，以因應 APT，並投入更多資安防護資源持續監控重要資訊系統與資訊資產的安全。

表 1:APT 攻擊流程

Symantec	Websense	TrendMicro	CA	Fireeye	Mandiant	Gartner
偵查弱點	偵查掃描與感染	偵查情資	偵查	入侵系統	偵查	滲透
發現、研究、分析		建立網路後門	入侵		網路入侵	
長期潛伏與控制	控制與潛伏	控制與潛伏	權限提升與控制範圍擴散	下載惡意程式長期控制	建立後門	潛伏
				與 C&C 主機連線	安裝工具	佔領重要目標
					權限提升	
資料滲出與分析	取出情資與攻擊	橫向權限提升與資料滲出	持續挖掘	資料外洩	資料外洩	資料外洩
					持續維護潛伏狀態	

資料來源:本研究整理

(二) 資訊安全政策

行政院研考會於九十四年度國家資通安全技術服務與防護管理計畫中，曾提出資安規範整體發展藍圖，規劃發展一系列的資安規範與參考指引提供組織基本的安全要求水準。現今的政府單位皆是根據我國「國家資通安全會報」應變作業綱要提及資通安全需依照此綱要進行建置整理如表 2。

表 2: 資安規範整體發展藍圖項目

資安規範整體發展藍圖	
規劃	資安管理要點
	資安管理規範
	實務導入指引
	資安產品選擇
	資訊系統風險評鑑
執行	資訊作業委外安全
	電子資料庫保護
	電子郵件安全
	網頁程式安全
	控制措施建議
	檢查表發展指引
檢查	作業系統
	入侵偵測
	網頁伺服器
	防火牆
	無線網路
	可攜式媒體
	營運持續管理
	資安事故通備應變作業
	資安事故通報應變規範
維持與改進	指引審查
	教育訓練機構認證作業
	資安人員驗證機構認證作業
	資安人員驗證作業
	第三方驗證機構認證作業
	第三方驗證稽核驗證作業

資料來源:行政院研考會與本研究整理

大體而言，此藍圖雖然完整涵蓋資訊安全的

規範，但該藍圖發展至今已近八年，因此，如將之與 APT 威脅分析進行比對，不難發現政府資安規範仍有需加強關注的項目宜進行加入的動作，例如對於事件調查、事件回應與第三方技術性稽核等。

(三) 資訊安全產品

Siponen & Kukkonen (2007)認為，資訊安全產品在資訊安全的四大構面為：對於資訊系統的存取控制、確保網路傳輸之過程安全、資訊安全之管理策略，及開發安全的資訊系統。

吳東城(2011)依據 Gartner(2009)列名的前三名資安軟體廠商及國內 MIC(2009)認為的前十大國內資安廠商信賴品牌，解析國內外資安產品供應商之產品架構及解決方案分析，彙整出 24 個可作為資訊安全產品四大構面的衡量問項。

整體而言，吳東城(2011)所列舉的項目對應到 APT 皆有其重要性，以 APT 的攻擊流程對照資安產品，需要在早期發現威脅的角度以及威脅阻攔的產品有更好的建置與管理，例如對於資訊系統的存取控制面向中的入侵偵測防護、弱點掃描、防火牆，確保網路傳輸過程之安全構面的郵件安全，內容過濾防護、訊息傳遞安全。

(四) 資訊安全服務

資訊安全服務業（Information Security Service Industry）成為近年來新崛起的產業之一，而隨著企業急於應用資訊科技以提升其整體競爭力的同時，資訊安全服務業的重要性與日俱增。本研究為了能夠將資安關鍵議題涵蓋的面向更加完整，依據公司業務屬性較專注於提供資安服務的公司共計六家進行服務項目彙整 23 項不同服務項目。

整體而言，資訊服務公司各自有專注的項目，其中以防護外部攻擊如弱點掃描、滲透測試服務等技術型服務，以及輔導導入 ISO27001 與提供資安教育訓練等顧問服務為主要共通點。根據趨勢科技 2013 年所發表之台灣進階持續性攻擊 APT 白皮書中所提到的 APT 威脅發現，其中高科技製造業的平均入侵時間最久 346 天，接下來是金融業的 275 天，第三名則是政府機關的 264 天。而經過整理後也發現資訊服務公司對於事件調查、事件回應、數位鑑識等事件發生後的處理服務比較少，因此資安服務無法提早發現 APT 的威脅進入企業。

表 4: 資安服務項目

	A	B	C	D	E	F
資訊安全管理規劃服務					○	○
資安架構設計與建置服務					○	○
網路安全評估與檢測服務		○	○			○
弱點掃描與漏洞修補諮詢	○			○	○	○
滲透測試服務	○			○		○
數位鑑識服務	○					○
管理策略與政策制定					○	○
遠端集中資安即時整體監控	○			○		
電腦稽核管理服務						○
資訊安全技術教育訓練	○	○				○
資訊安全委外管理服務						○
資訊安全事件緊急應變處理	○					○
資訊安全管理系統導入	○		○		○	
資訊安全法令遵循服務	○		○			
資料保護服務	○		○			
電子商務/數位交易安全	○	○				
網路與基礎架構安全保護	○				○	
系統安全維運與解決方案諮詢	○				○	
電子郵件警覺性測試		○		○		
主機安全稽核		○	○			
主機代管				○		
原始碼掃描				○		
網站異動監控				○		

資料來源：本研究整理

註: 服務廠商分別為 A:勤業眾信、B:數聯資安、C:資拓宏宇、D:關貿網路、E:敦陽科技、F:定威科技。

(五) APT 的防禦策略分析

雖然各家資訊安全廠商都對 APT 提出了相對應的防護策略，但由於每一個資訊安全廠商對於其在資訊安全領域的解決方案各有優缺點，所顧及的資安威脅面向也會有所差異，就本研究將針對主要防禦 APT 攻擊的資訊安全廠商所提及的防禦面相與 Gartner 的 APT 最佳實務原則建議進行整理，發現各廠商在探討解決方案時有 75%會強調事件回應與數位資產控管，代表對抗 APT 攻擊時需要

有足夠的事件回應能力以及控管避免情資外洩，75%會關注於數位資產控管，此數據顯示企業必須了解自己的數位資產分布以及散布路徑，避免因為遭受APT攻擊而損失重要的數位資產，另外有63%會強調惡意內容過濾與漏洞修補，這表示惡意檔案的偵測效能須能維持，並且將系統的弱點以及被攻擊面降到最低，完整的APT防護建議彙整如表5。

整體而言，各廠商的建議皆無法涵蓋所有APT防護，因此在需搭配不同廠商的建議，評估資安預算後盡可能地進行防護。

表5: APT防護建議

	A	B	C	D	E	F	G	H
掌握攻擊情資	○	○						○
加強教育訓練	○						○	○
提升邊界安全	○		○	○				○
惡意內容過濾	○	○	○	○				○
端點控管	○		○			○		○
關聯分析	○					○	○	○
事件回應	○			○	○	○	○	○
漏洞修補	○	○		○	○	○		
系統權限控管					○	○		○
存取控管					○	○	○	
即時威脅監控	○			○	○		○	
數位資產控管		○	○	○	○	○	○	
伺服器安全強化					○			
安全政策一致性					○			○
虛擬化安全策略					○			
網路事件監控			○			○	○	○
高層資安感知							○	
IT架構重建							○	
安全的資訊傳遞			○			○	○	
異動管理						○		
行動安全			○					

資料來源:本研究整理

註: A:TrendMicro, B:Symantec, C:Sophos, D:Websense, E:CA, F:Fire Eye, G:RSA, H:Gartner

(六) 資訊安全標準

面對層出不窮的資訊安全事件，解決資訊安全問題不能單由技術面著手，應有完整管理系統來有效解決資訊安全問題。其中，ISO27001為資訊安全的領域裡有著一個長年發展的國際資安標準，該標準由英國在1995年制定了資訊安全管理實務準則經過十年的修訂，最後將ISO/IEC 17799改為ISO/IEC 27001，使資訊安全標準成為ISO 27000系列，更可見其代表性

大體而言，ISO27001為現今國際間公認最完整之資安管理標準，它並非一種技術，而是一種管理制度，是資訊安全管理系統要求的標準。其規範之安全內容包含：建立、實施、操作、監督、維持與改善ISMS資訊安全管理系統及風險評估，ISO27001所發行的標準共11個管理領域、39個控制目標、133個控制要點。根據政府資通會報規定：政府部會中A、B級單位需在民國97年以前通過ISO27001認證。由此可見，資訊標準內容的適用性與重要性。

因此本研究參考ISO27001架構為基礎與國際同質性之資安標準或規範進行權重分析比對，發現了四個面向是所有標準與規範都十分重視，分別為存取控制、通訊、事件管理、IT維運。

表6: 資安標準與規範整理

	A	B	C	D	E	F	G	H	I
存取控制	○	○	○	○	○	○	○	○	○
應用程式開發	○	○			○	○	○		○
資產管理	○	○		○	○				○
業務運作	○	○		○	○	○	○	○	
通訊	○	○	○	○	○	○	○	○	○
法規符合	○	○	○	○	○	○			
企業治理	○				○	○			
客戶	○	○	○	○	○	○		○	○
事件管理	○	○	○	○	○	○	○	○	○
IT 維運	○	○	○	○	○	○	○	○	○
委外	○	○		○	○	○	○	○	○
實體環境	○	○					○		○
政策與流程	○	○		○	○	○	○	○	○
隱私	○	○	○	○	○			○	
安全	○	○		○	○	○	○		○

資料來源: www.itservicestrategy.com

註: A: ISO 17799/ISO27002；B: SAS70 Type II；C: GLBA；D: PCI DSS；E: EU Privacy；F: Cobit；G: Common Criteria；H: Generally Accepted Privacy Principles；I: Generally Accepted Systems Security Principles

四、彙整方式與研究發現

(一)彙整方式

本研究關注於APT對於資安政策的影響，而資安政策制定時皆會參考國際資安標準，因此經比對後，本研究以ISO27001為項目收斂的基準，以從構面而形塑項目(Top-down)的方法在資安產品、資安服務、國家資安發展藍圖、APT防護建議策略等四個資安議題進行彙整，項目中若有同質性的項目再做第二步的內涵分析，若是內涵相似則歸類到ISO27001的關聯控制項；反之，若是不易與ISO27001進行關聯的項目，則將之歸入「其他」這個構面。

(一)研究發現

本研究彙整國際資安標準 ISO27002 共計 25 項要點、國家資訊安全發展藍圖中共有 26 項、Siponen & Kukkonen (2007)所提出的資訊安全四大構面中共計有 24 個子項目、資訊安全服務構面共有六個服務提供商取聯集，共計 23 個服務項目、APT 防護策略面向中有七個解決方案提供商與 Gartner 共八個資料來源，取聯集共有 21 項，將所有構面中與 APT 間接影響控制範圍之要項扣除，發現已 IOS27001 為基礎架構的四個構面並將未包含在 ISO27001 中的項目另外分類為其他構面，如此便包含了至今為止的資安政策項目，最後提出涵蓋五構面、29 項的因應 APT 的資安策略與議題，如表 7 所示。

其中，五個構面分別為通訊與作業管理(10 項)、存取控制(7 項)、資訊系統取得、開發及維護(6 項)、資安事故管理(2 項)，及其他(4 項)。

整體而言，藉由此彙整過程發現，即使 APT 威脅是近年資安防護較新的議題，資安廠商也提出許多新的看法，但很大比例的防護建議與方案都已包含在過去企業所依循的資安標準中。易言之，本研究認為，雖然在因應新 APT 典範的資安議題上，企業應注意的涵蓋面向與議題，和因應傳統資安與資訊治理的表面差異無幾，但在重心與思維上，則似有顯著差異。

(三)實務建議

過去企業制定的資安政策之有效性其實不易驗證，因為在建立政策或是透過外部稽核來驗證資安政策皆是以檢查表的方式作評核，只要該項目有規劃或是有建置則該項控制措施則為成立，每一個項目並未使用技術等級進行評估。並且在過去大部分的企業不會把 APT 威脅當作風險評估的一個項目，因此建議企業應該重新檢視目前的資安政策，並且要以技術面的標準進行完整評估，找出企業資安政策較弱的環節予以強化，並且在事件管理的構面進行更詳細的防護規劃，當遭受 APT 攻擊時才能在較短的時間內完成事件調查與事件回應，並立即修正被攻擊的弱點。

表 7:APT 防護關鍵項目彙整

構面	項次	關鍵項目
通訊與作業管理	1	作業程序與責任(異動管理)
	2	第三方服務交付管理(委外管理)
	3	系統規劃與驗收
	4	防範惡意碼與行動碼(端點安全)
	5	備份(資料儲存)
	6	網路的安全管理(防火牆、入侵偵測)
	7	媒體處置(外接儲存)
	8	資訊交換(電子郵件)
	9	電子商務服務(網頁伺服器)
	10	監視(威脅日誌監控)
存取控制	11	存取控制的營運要求(權限控管)
	12	使用者存取管理(身分認證)
	13	使用者責任(教育訓練)
	14	網路存取控制(網路隔離)
	15	作業系統存取控制(登入與密碼)
	16	應用與資訊存取控制(資料庫安全)
	17	行動計算與遠距工作(行動安全與 VPN)
資訊系統取得/開發及維護	18	資訊系統的安全要求(安全的系統規劃)
	19	應用系統的正確處理(正確資料輸入)
	20	密碼控制措施(資訊加密與控管)
	21	系統檔案的安全(應用程式控管)
	22	開發與支援過程的安全(原始碼掃描與資料外洩)
	23	技術脆弱性管理(弱點掃描與修補漏洞)
資安事故管理	24	通報資訊安全事件與弱點(掌握情資)
	25	資訊安全事故與改善的管理(數位鑑識與事件回應)
其他	26	營運持續管理(將資安管理納入營運管理)
	27	資訊系統風險評鑑(風險管理)
	28	ISO/IEC 27001 系統導入顧問
	29	資安認證(資安人員驗證)

資料來源:本研究整理

參考文獻

[1] Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook Section I: Introduction & overview.

[2] Andy Greenberg, Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits，Forbes.com, 2012.

[3] Mikko T. Siponen, Harri Oinas-Kukkonen, A review of information security issues and respective research contributions, 2007.

[4] Protecting Against Advanced Malware and Target APT Attacks, FireEye, 2012.

[5] Gartner，民 101，對付進階持續性滲透攻擊(APT) 的最佳實務原則。

[6] 王志斌，民 98，結合層級分析法與德非法發展資訊安全認知評量表之研究，世新大學資訊管理學研究所碩士論文。

[7] 吳東城，民 100，探討資安產品之顧客需求與滿意度，國立高雄應用科技大學資訊管理碩士班碩士論文。

[8] 吳啟文，民 101，政府資通安全威脅趨勢及防護，行政院研究發展考核委員會。

[9] 邱博顯，民 100，民臺灣大專校院資訊部門

調查及關鍵資訊議題之研究，中國文化大學資訊管理研究所碩士論文。
[10] 洪國興、季延平與趙榮耀，民 95，影響資訊安全關鍵因素之研究，資訊管理研究，第六期。
[11] 孫淑景，民 92，內控處理準則電腦資訊循環之個案研究-以 BS779 資訊安全及 COBIT 控制目標為例，中原大學會計學系碩士論文。
[12] 徐廣寅，民 93，資訊安全管理導論，金禾資訊股份有限公司。
[13] 陳彥駿，民 99，植基於資安治理建構數位證據鑑識機制之研究，國防大學資訊管理學系碩士論文。
[14] 陳炳炫，民 101，建構以風險管理為導向的資安政策，國防大學戰略研究所，頁 281-310。
[15] 陳瓊瑤，民 97，資訊安全風險評鑑模式建構之研究， 2008 知識社群與系統發展研討會。
[16] 詹燦芳，民 97，國內 ISMS 導入效益、成功要素與遭遇困難之研究，國立台灣科技大學資訊管理系，碩士論文。
[17] 資安人編輯部，民 101，動靜之間 讓 APT 無所遁形，資安人科技網。(http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7202#ixzz2KsrQqygT)
[18] 資訊安全課程講義，行政院主計處電子處理資料中心。
[19] 廖釗頡，民 99，網路釣魚被害類型及其成因，國立臺北大學犯罪學研究所碩士論文。
[20] 劉興浚，民 99，建構以風險管理為導向的資安政策，國防大學國防管理教育訓練中心，頁 1-40。
[21] 樊國楨，民 93，美國聯邦政府資訊安全管理系統稽核作業與相關標準初探，資訊管理研究期刊，第 4 期，頁 35-58。
[22] 謝岳庭，民 95，組織中各種不同角色之資安指導綱要，中國文化大學資訊管理研究所碩士倫文。
[23] 趨勢科技，民 101，APT 攻擊策略指導方針。
[24] 瞿鴻斌，民 94，資訊安全風險評估驗證系統，世新大學資訊管理學研究所碩士論文。
[25] 趨勢科技，民 102，2013 年台灣進階持續性威脅 APT 白皮書。
[26] Mandiant，民 102，APT1-Exposing One of China’s Cyber Espionage Units。