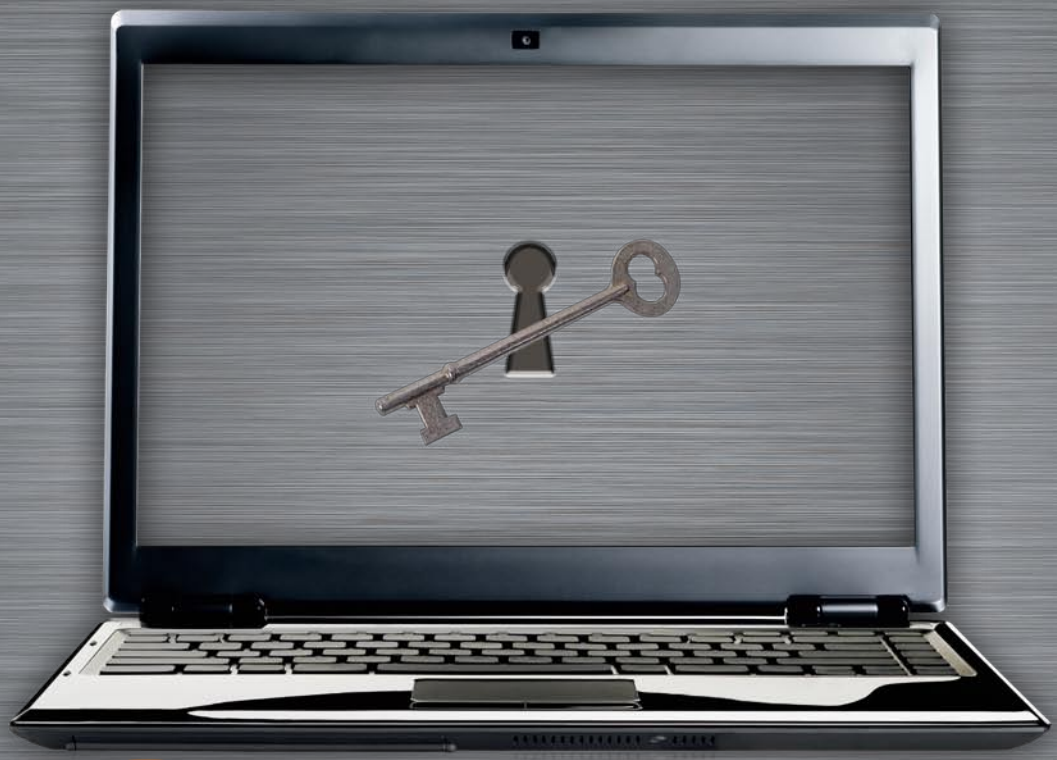
Microsoft®

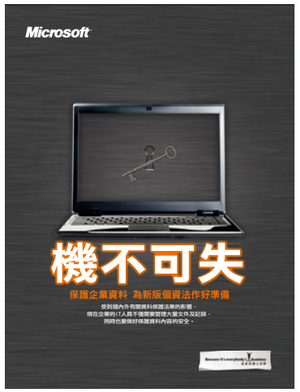


機不可失

保護企業資料 為新版個資法作好準備

受到國內外有關資料保護法案的影響，
現在企業的IT人員不僅需要管理大量文件及記錄，
同時也要做好保護資料內容的安全。

Because it's everybody's business
這是每個人的事



企業資安現況與新版個人資料保護法

新版《電腦處理個人資料保護法》即將獲立法院通過，與之前的版本相比有何差異？因應這樣的變化，台灣的企業在保護消費者資料方面又做好準備了嗎？

台灣雖然早在約15年前就已經通過《電腦處理個人資料保護法》，但該法案保護範圍與適用對象極其有限，對於近年來因駭客攻擊、設備遺失/毀損、內部員工監守自盜等事件，導致企業大量客戶與交易資料流失，造成消費者權益嚴重損害的問題，無法進行有效規範。

由於現在網路上各項應用服務早已深入到一般人們的日常生活中，舉凡小從最基本的e-mail、MSN、Skype、視訊交談等通訊應用，Foxy、Emule、KKBox等P2P檔案分享服務，大到直接與金錢交易相關的線上購物、繳費、轉帳、遊戲娛樂服務等項目，無一不涉及到網路活動。但在人們享受這些服務所帶來便利的同時，在個人資訊安全方面也受到嚴重的威脅。

合法使用者為企業機密資料的主要外洩管道

根據美國CSI的調查數據顯示，公司機密資料外洩的狀況有70%是由內部合法使用者所造成。而ICM的研究報告亦指出，有39%的員工曾將客戶資料寄出，52%曾在離職時帶走工作資料，86%坦承習慣性將郵件轉寄他人，因此「合法使用者」才是真正危害公司安全的最大因素。

為此新版個資法已進行了相關修正，將以往僅限於政府機構與8種特定行業的適用範圍，擴大到所有會搜集消費者個人資料的企業，往後業者將不能再以「自己也是受害者」為由來規避責任，而有必須保護消費者資料隱密性，做好公司資訊安全的義務，以防止駭客入侵與資料外洩等問題發生。

個資犯罪行為日益嚴重

以美國為例，因為使用了不安全的Wi-Fi系統，使得TJX等零售業者有高達4,570萬筆的信用卡與現金卡的卡號被竊；EDS承包Medicaid理賠處專員在2009年2月，承認犯下盜賣客戶社會安全號碼與生日資料，以冒領退稅金；而猶他州大學醫院的快遞人員更因駕駛自用車輛，而非公司配發的保全車，使得其在運送資料的過程中遺失了2,200萬名病患的帳單資料。

至於在台灣方面，個資外洩的嚴重程度與美國相比也不遑多讓。由於一般台灣的企業及政府單位，普遍都有搜集個人資料的習慣，其所建立的龐大客戶資料庫，若沒有採取適當的保護措施，極容易成為歹徒下手的目標。根據聯合報在97年8月28日的報導，就有駭客曾經成功入侵健保局、教育部及各大電信公司的資料庫，取得高達5,000萬筆的個人資料記錄，就連政府高官及大企業老闆都不能倖免於難。有心人士甚至能因此鎖定特定族群為下手目標，以進行後續更精密的詐騙計劃與行動。

有專家指出，歹徒在取得個人隱私資料後，除可冒用他人身分，從事簽約、買賣，甚至是詐騙等犯罪行為之外，更可利用所偷取到的密碼與登入帳號，直接進行銀行轉帳交易作業，從而獲取帳戶持有人的所有資產。且個人隱私資料還能賣到黑市，供不法份子利用製造假證件，以掩護其進行走私、黑市勞工，甚至是人口買賣、毒品交易等犯罪活動。因此資料外洩不僅造成企業損失，對消費者個人的權益也會產生很大的影響。

新版個資法通過後，企業需加強對於個資保護的重視

依據國外的經驗顯示，如金融、保險、製造等產業，因為有了相關法規的要求，對資料外洩防制的問題更加重視。

企業機密資料的主要外洩管道

儘管有不少政府單位及公司行號已經添購百萬級的網路設備，安裝資安防護軟體，用DRM技術保護文件，甚至於導入ISO 27001的規範，但卻仍會出現敏感性資料(包括客戶個人的資料文件)外洩的狀況。根據美國CSI的調查數據顯示，公司機密資料外洩的狀況有70%是由內部合法使用者所造成。而ICM的研究報告亦指出，有39%的員工曾將客戶資料寄出，52%曾在離職時帶走工作資料，86%坦承習慣性將郵件轉寄他人，因此「合法使用者」才是真正危害公司安全的最大因素。不過目前多數企業仍是將大部份的防護資源，放在處理來自外部的威脅項目上，顯見對因內部人員所造成的資料外洩問題，企業IT人員依然缺乏足夠的認知及防堵措施。

根據ITRC(Identity Theft Resource Center)的研究報告，企業資訊外洩的管道，大致可分為意外、員工疏忽、IT服務供應商服務品質不佳…的「人為疏失」；未經授權的存取、病毒/蠕蟲等惡意軟體攻擊、盜版/侵犯著作權等方面的「蓄意行為」；設備失效、程式錯誤、系統未知漏洞等項目的「技術問題」，以及因採用老舊或過時技術而造成的「管理漏洞」等幾種類型。但是由於過去台灣個資法規並對沒有對企業進行嚴格的要求，對於洩露資料的廠商亦無立即性懲罰機制，這都使得台灣部份企業針對上述管道進行「個人資料外洩防堵」工作，普遍缺乏一種迫切性的心理需求，並造成此議題長期之來受到相當程度的漠視。

雖然1995年台灣就已經實施「電腦處理個人資料保護法」，但不可諱言的，由於網路與企業IT應用環境變化相當快速，該法已然出現規範不足的問題。不僅受到保護的個人資料種類過於狹隘，也由於缺乏外部的監督控管機制，導致消費者的權益因而受到損害，這不僅妨礙了個人資料保護觀念的形成與推廣，而且也造成台灣在國際上的資訊應用程度表現雖然優異，但政府機關、公司行號，甚至是消費者本身，對於個人資料安全的重視程度卻嚴重不足的詭異現象。

新版個資法將強化企業對於個資保護的重視

依據國外的經驗顯示，如金融、保險、製造等產業，都是因為有了相關法規的要求，才開始重視起有關資料外洩防制的問題。如美國的「醫療資料相關健康保險可攜性與責任草案(HIPAA)」、財務資料相關的「沙賓法案(Sarbanes-Oxley)」，與信用卡資料相關的「支付卡產業標準(Payment Card Industry Standard」…等，因其訂定的鉅額罰款，使得企業負責人必須更重視資安的強化。

舉例來說，美國Xanga.com公司(美國著名的blog託管服務網站，擁有4,000萬名使用客戶)因「未經父母同意，搜集、使用、揭露未滿13歲孩童的個人資料」；Nations Title Agency(曾為美國第八大產權保險公司，後遭FNTIC併購)因「沒有評估儲存重要資料的風險機制」、「對於重要資料沒有進行未授權存取的

偵測」、「沒有有效監督合作廠商重要敏感資料」…等因素，被美國聯邦交易署(FTC)列入資安黑名單中，要求其限期改善；而ChoicePoint(美國最大的資料經銷商，2007年營業額為10億美金)更曾因為「沒有建立適當程序過濾可能購買者」、「沒有拒絕將重要的個人隱私資料賣給不肖商人」，遭受到FTC 1,500萬美金的重罰；近期又因為「將安全檢測功能關閉，導致13,750名用戶資料外洩」事件，罰款27.5萬美元。

有鑑於此，針對台灣法令在個人資料保護不足，缺乏有效罰則的部份，法務部亦自2001年起，即開始積極推動修法工作，其內容重點包括：擴大保護客體、普遍適用主體、增修行為規範、強化行動監督、促進民眾參與、適度調整罰責等項目。由於本修正法案預計有可能在近期經立法院審議並獲三讀通過，一旦施行之後，不僅消費者的個人資料將可得到更大的保障，企業也必須對其使用者資料的保護負起更多責任。

台灣新舊版個資法差異的比較

舊版個資法最大的問題在於，除公部門外，一般民間企業僅限於徵信、醫院、學校、電信、金融業、證券、保險及大眾傳播…等8大行業適用，不及於其他一般企業與個人；而受保護的範圍，亦只有經電腦所處理的個人資料，紙本資料則不在此範圍內。新版法案則刪去「電腦處理」的字樣，更名為「個人資料保護法」，除適用主體擴大到自然人、法人、公務與非公務機關外，紙本資料也納入受保護的範圍，另外並增加了基因、醫療、性生活、健康檢查與犯罪前科等5項「敏感性資料」的蒐集、處理及利用規範。事業主管機關的管理查核權限變得比以往更大，企業所需負擔的安全維護責任也更被加重。

舉例來說，國內以往有許多知名企業都會出現過大規模的個人資料外洩事件，但受害者往往卻因不知情，而導致其權益受損卻無法主張。因此新版法案特別規定，當企業或政府單位所蒐集的個人資料遭到竊取、洩漏、竄改…等狀況時，有義務即時以適當方式(像是電話、信函、公告等)通知當事人。如有違反規定，主管機關可令其限期改正，並可按次處以2~20萬元的罰款。

此外，現行的個資法只有原則性的規定，個人資料的搜集單位應指定專人依相關法令辦理安全維護事項，以防止資料遭到竊取、洩漏、竄改等狀況。但所謂的安全維護事項為何？該如何執行？應執行到何種程度？現行的個資法均未予以明確規範，這使得各單位在進行資訊安全維護時，缺乏統一的標準。新版法案對此進行了相關修正，要求指定機關（如銀行、保險、電信）應依中央目的事業主管機關的要求，明訂個人資料檔案的各項安全維護的計劃及處理辦法，並得接受政府機關的檢查，以確認其是否真有依照所提出的辦法執行，做為日後若有法律糾紛時的判決依據。

而為遏阻犯罪，督促企業善盡資訊安全維護的責任，新版法案也提高了企業賠償上限，由原來的2,000萬增加到二億元。當非公務單位依新版法案受到行政罰緩的處罰時，企業代表人、管理人或其他代表人，除非能證明已盡防止義務者外，否則都應接受相同的罰款處罰。財團法人或公益社團法人亦可代表被害人提出團體訴訟主張權利，參與團體訴訟的當事人裁判費減免的規定，讓未盡保護責任的企業，較以往更易遭到受害人的訴訟，可能付出的賠償金額也更大。這些相關法令的施行，企業不僅必須提高對於資訊安全風險的意識，同時也必須強化對於個人資料安全的保護。

不只防護系統 更要防護資訊

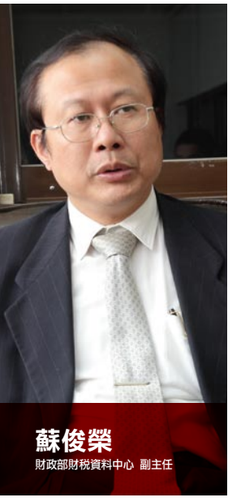
加強個人資料保護已是新版法案明確的立法方向。為了避免客戶喪失對公司的信任，以及考量到未盡個人資料保護所要負起的法律責任，有不少企業已經考慮增加預算添購資安產品，或是引進外部顧問協助提升資訊安全的管控能力。根據國外的經驗顯示，現在有65%的企業在汰換舊電腦時，會清除硬碟中的資料及應用程式；有63%採用入侵偵測軟體；67%針對個別應用安裝防火牆；而為資料庫、筆記型電腦、備份磁帶進行資料加密的比例，也分別有55%、50%及47%的水準。

而在台灣方面，由於新版個資法的立法思維改變，擴大了對於個人資料保護的範圍，並且加重了企業管理的責任，因此台灣企業資安重點投資的項目也跟著產生異動，由原來內部網路及系統安全，轉移到資料安全的防護。根據CIO雜誌於2008年底的調查結果，在台灣，有高達50%的企業計劃在今年導入「資料外洩防範(Data Loss Prevention，DLP)」方案。異地備援/災難復原、入侵檢測/弱點評估、資訊安全總體管理…等項目則分別佔46.20%、45.57%及39.87%的比例，與前年同期調查的結果相比，有相當大的變化。而除了技術之外，灌輸員工資料防護與完整責任觀念，也是確保企業免於資訊外洩威脅的要點。想要單純依靠技術來保護企業不受資安風險，那是不可能的事情。」Brandeis的CSO Dennis Devlin表示：「我們必須把這思維傳達給每位員工。」另一方面，良好的資訊安全也能當做是一種吸引客戶的手段，如果企業能夠比競爭者更能保護客戶資料，資安也可以成為公司有力的競爭優勢。

新舊個資法內容比較

	舊法	新法草案
適用行業	政府機構、徵信、醫院、學校、電信、金融業、證券、保險及大眾傳播。	全體適用。
保護對象	電腦處理的個人資料檔案。	所有個人資料(不限電腦處理)。
行為規範	蒐集、電腦處理、利用的行為(含國際傳遞)。	▪ 除符合法定要件外，原則上不得蒐集、處理或利用關於個人的醫療、基因、性生活、健康檢查及犯罪前科…等5項資料。 ▪ 應明確告知當事人蒐集者名稱、目的、資料類別、利用方式…等相關事項。 ▪ 如需以超出原目的之方式使用個人資料，應另外單獨徵求當事人書面同意，不得以概括方式處理。 ▪ 公務機關可主動或依當事人請求，停止資料相關處理單位的違反行為。 ▪ 該資料若用於產品行銷，應於首次使用時免費提供客戶表示拒絕的方式。 ▪ 若發生個資外洩事件，應主動即時告知當事人。
行政監督		▪ 相關主管機關若認為有必要，或發現非公務機關違反事項時，得派員依法檢查，並採取必要處分。
民眾參與		▪ 財團法人或公益社團法人若符合規定者，得代受害當事人提起團體訴訟。 ▪ 二十人以上之團體訴訟，且其訴訟標的價額超過新臺幣60萬元者，超過部分免徵裁判費。
罰責	▪ 同一事實上限新臺幣2,000萬。 ▪ 2年以下有期徒刑及新臺幣20萬元以下罰金之刑事責任。	▪ 同一事實上限新臺幣二億，若不法獲利超過該上限者，以不法獲利金額為限。 ▪ 加重「意圖營利」者的處罰。刑責提高為5年以下有期徒刑及新臺幣100萬元以下罰金。 ▪ 非公務機關之代表人、管理人或其他有代表權人，除能證明已盡防止義務，應並受同一罰緩處罰。

個資法的重要性與預期衝擊



蘇俊榮
財政部財稅資料中心 副主任

朱瑞陽
國巨律師事務所 律師

為了改善原「電腦處理個人資料保護法」無法保障民眾應有權益的問題，新修訂的「個資法」不僅擴大了原適用範圍，對於企業與個人在蒐集民眾個資時，所應採用的程序與所應盡義務亦做了詳細的規範。這對於經常會接觸與蒐集個資而目前尚不適用的行業來說，預期將會產生相當的衝擊與影響。至於像健保局、主計處、財稅中心、戶政事務所…等政府資訊處理相關單位，原本即已適用「電腦處理個人資料保護法」，對於新個資法的施行與調整幅度多大，更應保持密切注意。

台灣個人資料外洩問題亟需被高度的關切。早在97年8月刑事局就曾破獲過某大型個資外洩案—有駭客集團大舉入侵政府單位與電信公司主機，竊走高達5,000萬筆民眾個人資料，而在其他網站商城、電視購物頻道…等方面，個資外洩事件更是時有所聞，往往都造成民眾龐大的財產損失。雖然在現行民法中對於隱私權早已訂有保障，「電腦處理個人資料保護法」中也有相關的條文，但卻因其適用對象與範圍極其有限，又缺乏執行的手段，使得法律執行力道有限。對於如何保障消費者個人資料隱私的問題，有些企業做到了，但仍有很多的企業在這部分仍有改進提升的空間。

但這一切在新版個資法未來修法通過後即將改觀。國巨律師事務所律師朱瑞陽表示說，相較於前一版本的法案，新版個資法不僅將適用主體擴大至所有行業機關及個人非家庭社交活動外，保護客體除原有的「電腦處理資料」外，「人工處理資料」也包括在內，並新增對於醫療、基因、性生活、健康檢查、犯罪前科…等敏感性資料原則不得蒐集、處理或利用的限制，以及蒐集前應盡的告知義務、特定目的外使用應另行告知、資料保存階段應善盡保護…等義務。朱瑞陽表示：「這也就是說，這項法案會要求企業盡更強的保護責任，以確保個人資料不會被濫用或外洩。」

儲有民眾大量個資的企業與政府單位將首當其衝

由於新版法案在企業資料蒐集、保存、利用與銷毀…等步驟與階段上，都進行了嚴格的要求與限制，違者會有嚴重的處罰，台灣微軟伺服器平台事業部產品行銷經理簡志偉建議，公司或組織應該先從評估企業個資外洩的風險開始做起，以進行全面性的檢討與改善。

以隸屬於政府財政部的財稅中心為例，因其擁有全國所有民眾的納稅與所得資料記錄，機密性與敏感程度比一般企業所蒐集的個人資料更高，因此其在整體管控作業與程序上，不僅相對於其他政府單位而言更為嚴謹，也更關心個資法草案的各階段修正狀況與在立法院的審理進度。

財稅資料中心副主任蘇俊榮表示：「只要草案內容有修正，我們就立刻跟著將作業流程進行調整。」此外，他還強調：「我們會經常不斷找機會重新檢視各項內外部作業流程，看看哪裡有地方需要加以改進。」

對於新進人員來說，只要能遵循其規範好的作業步驟，即可以最短時間達到一定的品質要求水準。」另一方面，該單位還會組成外部專家團體，藉由定期的「ISO 27001換照」與3個月一次的資安檢視，重新檢視是否有可能違反個資法的相關規定，並立即尋求改善措施。「雖然無法做到100%，但希望經由這種反復修正的方式，做到在內部管理面、技術面滴水不漏的地步。」

可能會降低政府各單位之間的資料交換頻率

不過他也表示，除了「內部管理不當/作業疏失」、「外部駭客入侵/竊取」這兩大因素外，「單位與單位間的資料交換」也常是造成資料外洩的主要原因。「財稅中心經常與政府其他單位，如監察院、經濟部、主計處、內政部、立法院、健保局、警察單位…等進行資料交換。」蘇俊榮說：「文件項目可高達300多種。」而此部份在新版「個人資料保護法」實施後，即可能受到衝擊。「大家會害怕資料外流到不適當的人手中，不願意從事彼此的資料交換，反而造成各機關之間資訊流通的障礙，失去電子化政府的美意。」

「在此方面，我們的資安小組單位會重新全面性的檢討交換資料欄位的必要性、合理性與比例原則。」蘇俊榮表示：「財稅中心日後，將更審慎提供接收單位的必要欄位」此外，利用「浮水印」的技術，財稅中心也可藉此追蹤與掌握每份交換至其他單位資料的流向，以避免其落入不適當人的手中。

將稽核範圍擴大到其他資料接收單位

但除上述的做法外，蘇俊榮認為，更重要的是，其他單位人員的資安觀念與資安制度落實程度。為了達成此目的，蘇俊榮說：「我們的資安教育訓練除了內部單位同仁外，還會開放幾個名額開放給部內其他單位的學員參加，以培養其資安種子成員。」而在稽核方面，除了財稅中心本身外，「其他資料接收單位也在我們的稽核範圍內。」

此外，「我們也非常積極鼓勵內部同仁取得資安、網管相關證照。」蘇俊榮認為：「雖然現在有許多IT工作都可以外包給民間單位執行，但機關本身的IT單位還是要保有一定的技術能力做為基礎，才能為單位的資安問題及其解決方案進行把關動作。」他強調：「許多專案最後出狀況，往往也就是甲方技術方面的層次跟不上乙方。」目前有關此部份的資訊，除許多坊間業者都提供有大量線上資料可供參考外，台灣微軟資訊安全小組亦提供「資訊外洩風險評估暨個資外洩衝擊度鑑識」的網路服務，可協助企業客戶先了解自身IT環境的弱點與風險所在，及早做好補強措施，以強化IT基礎架構並提升客戶服務品質。

「資訊外洩風險評估暨個資外洩衝擊度鑑識」網址：http://www.microsoft.com/taiwan/security/privacy/services.htm

包化富
國巨管理顧問(股)公司 執行董事

林宏嘉
微軟亞太區全球技術支援中心 專案經理

企業應如何保護個資與衡量洩漏風險？

新版個人資料保護法雖然仍在立法院審議中，但預料很快就會通過施行。由於此項法律在施行後，不僅適用的範圍與對象擴大，對企業也課以更多在個人資料保護方面的責任與義務。面對此項衝擊與變化，台灣企業應該要由何處著手進行評估，以避免因管理、流程與技術…等問題而引發個資外洩風險，進而造成公司在金錢與商譽上的重大損失？

與舊版個資法相較，新版適用對象已擴及到所有的自然人、法人、公務與非公務機關；受保護的資料亦由原來所限定的電腦處理資料，擴大到紙本資料也納入其範圍內；未來企業不僅需要對手中所擁有的個人資料，明訂出各項安全維護計劃及處理辦法之外，並有接受政府機關檢查，以確認其是否真有依照所提出辦法執行的義務；這對於在營運作業上一向有搜集、保存與利用客戶資料習慣的台灣企業而言，無論是在管理、流程與技術…等層面，都帶來相當大的影響及衝擊。

由評估對營運流程的風險衝擊著手

由於個資外洩本身所造成的商譽損失，除了可能會導致大量客戶從此對於公司營運模式產生不信任，進而危害到企業生存之外，新版法案也加重了對於違反業者的相關罰則，不僅將賠償上限提高到二億，企業代表人、管理人或其他代表人也需連帶負起相同的責任。面對此風險提高的威脅下，國巨管理顧問公司執行董事包化富認為：「這表示企業現在設計與執行各項有關客戶個人資料的處理流程時，應該要比以往更加小心謹慎，並以更為積極主動的態度，確保這些資料的安全性。」

舉例來說，客服與業務人員經常會詢問與記錄一些有關於客戶的基本資料、使用行為、消費需求…等問題；行銷人員會利用客戶問卷、交易記錄進行市場分析；財務人員在處理帳務作業時，也常有機會接觸及使用到客戶的資料，並將其資料交換到銀行或其他週邊協力廠商的手中。包化富強調：「這些商業行為模式由於都牽涉到個人隱私資料，所以其搜集、保存、處理與利用方式，都會受到新版個資法所規範。」

因此企業現在就應該要開始針對各項營運流程的風險衝擊進行評估，特別是所有會經手「客戶個人隱私資料」的流程，都應分別就其作業型式、程序、處理應用範圍、作業人員身分/權限…等項目，一一重新加以檢視，以確認其是否有違反新版個資法規定的疑慮，及其所可能引發的風險高低程度。「評估的結果最後可做為企業在風險決策上的依據。」包化富說：「相關人員可就其在個資保護不足之處，選擇合乎其成本效益與風險承受能力的解決方案，在管理、技術，甚至是員工教育等方面加以控制與改善，或是乾脆重新設計出新的營運模式與作業流程。」

藉由檢視系統行為找出個資問題所在

另一方面，在此風險評估與決策過程中，CIO可站在系統技術層面的立場，就其所展現的行為模式進行問題分析。「由上而下的風險評估與分析方式，往往有其盲點。」微軟亞太區全球技術支援中心專案經理林宏嘉說：「常常看到有企業人員表示：『所有能做管理與技術的防護我都做了！』」可是還是不斷會有個資外洩的問題發生。「這是因為傳統的稽核機制只能檢查企業有沒有執行某一項目，但無法就其落實的程度，動態地予以檢視。」而這也使得風險評估人員的認知，與企業在實際執行時的表現，產生相當大的落差。

林宏嘉表示：「由於現在企業營運流程已經高度仰賴電腦進行運作，因此我們可以透過直接觀察系統異常行為的方式，從中找出其潛在的問題。」舉例來說，林宏嘉就曾遇到有某公司出現「系統每15分鐘出現一次『拒絕存取』」及「夜晚無人上班的時間，網路流量達到最高峰」的狀況。「問題往往是潛藏在人們無法查覺的檯面下。」林宏嘉說：「而透過針對各種犯罪行為模式的分析，稽查人員就能從這些蛛絲馬跡其中找尋出真正的問題所在。」

此外，由於新版個資法亦規定，「企業必須證明已善盡個資保護義務，才能在問題發生後免除其責任」，因此有關於各種個資防護措施的證據記錄與保存相當重要。「許多企業明明已經採取了許多必要的防護動作，但因為不知道要如何提出證明來進行自我保護，而在發生訴訟時遭到敗訴。」林宏嘉表示：「CIO在平日就有責任善盡證據搜集的義務，以減少企業在個資外洩事件發生時所可能的損失。」

個資法施行後衝擊的範圍是企業整體

由於IT單位保存了企業最大量的資料，因此新版個資法實施後對於IT的衝擊與影響層面最大，但這並不表示「保護個資僅是IT部門的責任」。事實上，包化富表示：「若不幸真的有意外發生時，受傷害的會是公司整體。」除了法務人員必須出面因應司法程序，公關部門要設法面對群眾，將問題停損到最低點之外，相關的業務單位也需要針對出狀況的流程重新進行檢討。對此包化富建議：「面對新版個資法，企業應該要拉高層級，從公司的整體角度思考才是。」

林宜隆
中央警察大學資訊管理學系 教授

新版個資法施行 將有助於警方查緝網路犯罪

根據國外專門蒐集「資料外洩事件」的分析網站—DataLossDB.org所公告的資料顯示，2000年~2004年全球資料外洩事件仍屬罕見，每年均不會超過30次；但至2005年之後，這情況遽然改觀，不僅較前一年爆增4倍以上，之後更呈現幾近倍數的成長。

中央警察大學資訊管理學系教授林宜隆認為，「B2C商業營運模式」興起正是促成此現象的主要原因，「由於網路環境的成熟與便利性，有越來越多消費者開始能接受透過網路、電視購物的方式，購買各項日常生活中所需的必需品。」但此種交易方式必然會在網路與企業資料庫中留下各項消費者的個人記錄，也因而相對地提高個資外洩的機會。

資料設備遺失是個資外洩的主要原因

歸納各種導致個資外洩的原因，以「資料設備遺失」高居第一，其次是駭客入侵、網站入侵、詐騙集團…等因素。以2007年英國政府所爆發的個資遺失案件為例，就是由於兩張存有全國請領兒童福利補助民眾資料的光碟在郵寄過程中遺失，造成有高達2,500萬人的姓名、地址、生日、國家保險號碼與銀行帳戶…等個人敏感性資料因而外洩。「即便是將資訊儲存設備經由正常程序，交給外部廠商維修，如果沒有做好相關防護措施，也會提高個資外洩發生機率。」陳冠希艷照事件即是其中著名的代表。

而除了上述因素之外，企業單位本身在處理民眾資料的過程不夠謹慎，也是導致發生資料外洩的主要原因之一。以政府單位為例，「基於政府資訊公開的原則，政府各機關需要對社會大眾發佈許多訊息。」林宜隆教授表示：「這其中常會摻雜不少關於民眾本身個人的敏感性資料，稍有不慎即會造成其權益受損。」而即便是選擇性揭露部份訊息，「有心人士還是能從不同機關所發佈的各項資料條目中，拼湊出關於目標對象的完整資訊。」因此在新版個資法實施之後，如何使其與「政府資訊公開法」兩者達成平衡，避免民眾資訊過度曝光，會是日後相關單位極需研究的課題與提出各項相關配套措施。

民間企業單位配合調查的意願不高

有鑑於因個資外洩情事日益嚴重，後續所引發的各項網路犯罪、詐騙事件所造成民眾在財產方面的重大損失，警政機關現在除成立科技犯罪防治中心，特別針對網路、電信…等高科技犯罪行為加以因應外，並另設立「165反詐騙電話」與相關網站，以提供社會一般民眾各項預防詐騙問題的諮詢服務管道，避免個資外洩問題所造成的不良影響持續擴大。

不過如果想要完全杜絕民眾個資被外洩的狀況，唯有從發生問題的企業下手根治才是正本清源之道，但這需要業者的配合才可能達成。「有不少企業基於維護本身商譽的考量，即便受到損害，亦不會主動對外通報或告知受影響的客戶，甚至是在事件對外曝光後，對於警方各項查緝行為仍會採取消極的不配合態度。」林宜隆教授認為，正是因為業者普遍有這樣的想法與作為，在提高了警方查緝時的困難度之餘，也助長近年來網路犯罪行為、個資外洩發生次數的不斷上升。

徒法不足自行 政府應提出各項機制以確保企業遵守

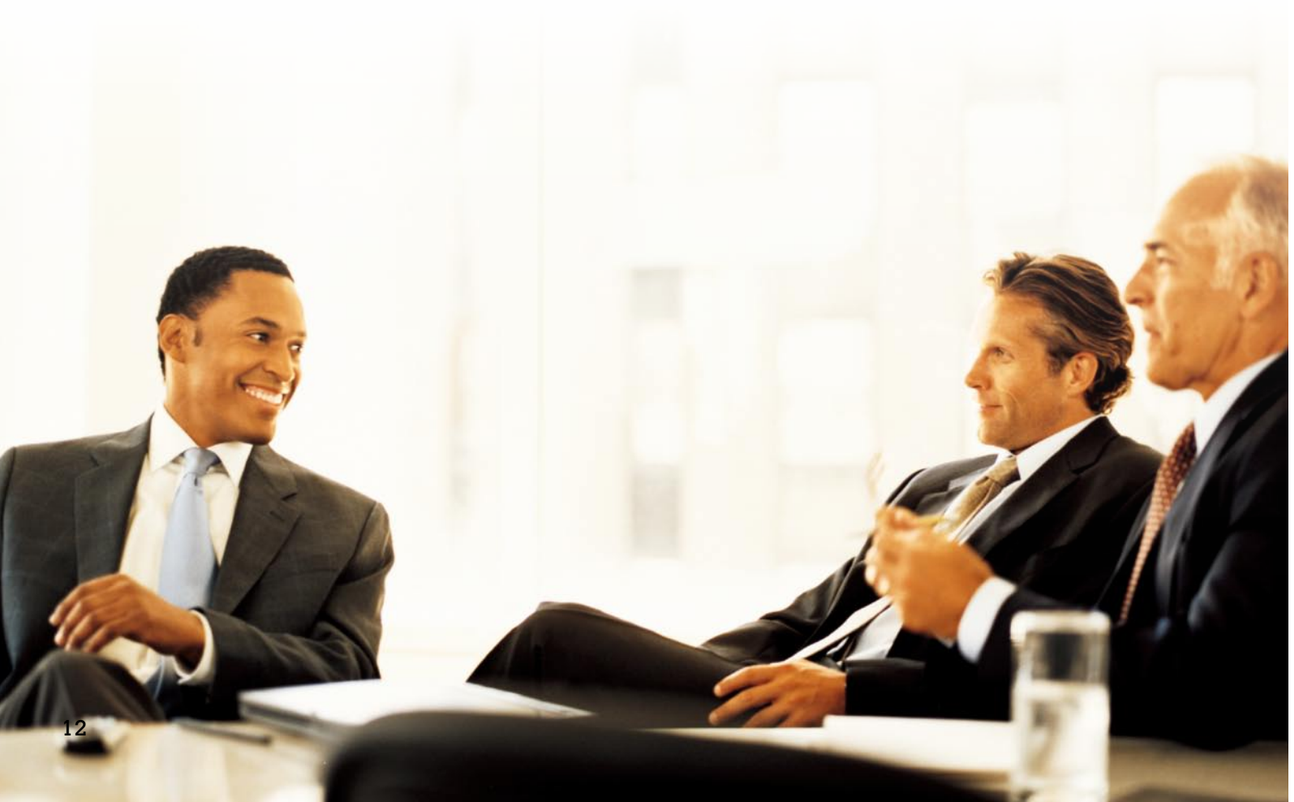
為了改善上述問題，新版個資法不僅賦予企業應保護其客戶個人資料的責任，同時在受侵害時亦應盡主動告知的義務，違者將會受到嚴厲的重罰。林宜隆教授說：「這會使得警方在偵辦網路犯罪事件時更加容易。」而在行政院資通安全會報中，也開始將「資安治理」機制納入電信業、金融業與醫療業的發展重點項目。「事實上，有許多個資外洩事件是在網購業者(含網際網路、購物頻道…等的電子商務網站中發生。」林宜隆教授不僅強調「網購業」亦應納入「資安治理」的範圍，還主張政府應儘速草擬類似於「網路購物交易法(電子交易法)」…等類型的法案，以維護網路業整體的市場交易秩序，避免個資外洩事件的一再發生。

不過光是有法條規定，也無法保證業者會確實遵守。這除了冀望於民眾本身的守法素質，以及此觀念是否能被快速推廣並普遍接受外，由於現階段政府仍未成立專責的主管機構來進行監督，而是交由各相關部會單位自行處理，受到其人力與資源有限的情況下，很難期望可達成法令預期的效果。林宜隆教授提議：「或許財政、金融單位在日後企業年度的財務報告上，應增列有關『個資防護政策與措施』的項目要求。」亦或是申請上市上櫃時所提供的財務報表內，增設有關資安與個人資料防護相關措施的建置、施行報告。「這種監督機制應可確保企業確實有依照個資法令的規定要求施行。」

B2C商業營運模式（Business Model）的興起固然刺激了Internet網路交易，但同時卻也造成消費者與員工個資外洩機率提升，不過受害企業基於所需防護成本與本身商譽的考量，不僅在主動建置資安措施方面並不積極，甚至對於警方各項查緝行為亦多半採取不配合的消極態度。但這種情況預料在新版個資法通過施行後即會獲得改善。

如何扮演好
新版個資法下的IT人員

受到國內外有關資料保護法案的影響，現在企業的IT人員不僅需要管理大量文件及記錄，同時也要做好保護資料內容的安全。雖然現今有不少企業已經投入大量預算與人力在資安工作上，但就目前整體的表現來看，IT人員仍有許多空間尚待努力。



因應法規遵循的需求，企業需重新進行「資訊安全風險評估」，將手上有限的資源，投資在最重要的關鍵點上。

以美國大陸航空為例子，該公司將所有的資料檔案依照所有人、商業價值及風險層次3個變項來進行分類，而各分類都有其不同的安全技術與程序標準。唯有企業在採用某一防護方式所能得到的效益，大於其可接受的損失程度時，企業的IT人員才會引進該套技術與工具。

研究發現，目前全球資料量正以每年36%的速度在成長，而其中有70%的比例未曾受到任何管理，這使得企業機密資料或所搜集的客戶個人敏感性資料，極容易在此情況下被人誤用或外流。另一方面，受到新版個人資料保護法即將實施的影響，沒有做好資料安全控管的企業，除了會受到巨額罰款之外，企業主也可能會因此吃上官司。面對這樣內外的雙重的壓力，現在有不少IT人員已經開始將資安工作的重點，由傳統的網路基礎架構防護，轉移到資料的安全控管上。

資安技術不是萬靈丹

一般而言，保護「企業資料」安全的主要經費來源多半來自IT部門，因此「IT技術」常被視為是解決此項問題的不二法門。而隨著資安技術的不斷演進，IT人員所採購的資安工具也跟著越來越多—從惡意程式碼偵測工具、應用層防火牆、入侵偵測/防禦工具、資料庫/筆記型電腦/備份磁帶的資料加解密與無線手持設備安全…等項目，所欲防護的項目範圍越來越廣。但這是否表示，IT人員在投入如此多的努力與金錢後，企業的資安真能就此高枕無憂？

很明顯，這答案是否定的。有研究機構的調查資料顯示，雖然大型企業一般在「資訊安全」方面，會比中小型企業投入更多的資金，建置更多的防護技術，但由於大型企業受到的資安攻擊更多，使得其表現出的防護水準往往和中小企業相同，有時甚至更差(有42%的大型企業表示不知道自己的網路曾出現哪些問題—這比例在中小企業只有16%)。另一方面，一旦企業的資安真的出現問題時，大型企業的損失，往往也較中小型企業更為慘重。由此可證明，並非盲目採用越多的資安防護技術，企業的資訊安全程度就會越高。

根據企業個資安全需求進行投資

特別是受到全球經濟不景氣的影響，現在企業對於IT的總體投資亦跟著下滑，在這種情況之下，IT人員對於IT預算的分配更是要小心謹慎，因此在選擇資安解決方案之時，除了要評估資安工具與技術的功能、產品、服務與成本…等基本項目外，還應重新檢視企業在資安上所面對的各項問題，包括在法規實施後，對於企業的「資訊安全風險評估」，再將手上有限的資源，投資在最重要的關鍵點上。

以美國大陸航空為例子，該公司將所有的資料檔案依照所有人、商業價值及風險層次3個變項來進行分類，而各分類都有其不同的安全技術與程序標準。唯有企業在採用某一防護方式所能得到的效益，大於其可接受的

損失程度時，企業的IT人員才會引進該套技術與工具。該公司的CISO Stanley表示：「沒有必要為了保護僅值5元的資料，而導入需要10元成本的解決方案。」

此外，「如果新導入的解決方案，需要動用到大量資源才能完成，即使公司願意不惜血本，最後的成效也會很難看。」因此有專家認為，企業應儘量以既有的工具平台為基礎來導入資安解決方案，才能有效地降低成本，並從而減輕IT人員的負擔。

再透過IT人員額外的協助。由於這樣的管控方式使用起來相當簡便，一般員工在短時間內都能很快上手，因此不僅可以大量降低人們對於IT部門的依賴，並可將相關管理責任分散到企業全體員工身上。

只要能做到「集中管理，分散授權」，IT人員就不用疲於奔命於應付各個使用單位的需求。由於這種做法會讓使用者對資料文件擁有更大的自主權限，也可以減少許多用戶端對於IT人員導

使用者接受度是企業資料保護方案導入成功與否的重要關鍵

過去許多企業導入資安方案失敗的原因，絕大部份都是因為「改變其現狀」會讓使用者在作業時感到不甚方便，因而拒絕採用並設法加以規避。

集中管理、分散授權

以目前辦公室常見的Office工具來說，當某個部門的員工想要將某份檔案內容分享給其他同事，並控管其相關讀取、修改、列印、刪除…等權限時，只要利用「另存新檔」的方式，儲存在公司既有伺服器上的特定檔案夾內，該檔案夾自動就會賦予該檔案預先設定好的分享權限，無需

入系統管理工具的反彈。「如果可由非IT人員自行管理，不但能節省IT人員寶貴的工作時間，同時也能增加使用者對資安管理工具的信心。」且一旦企業部門知道不用再麻煩IT人員幫忙時，他們也會更樂意進行嘗試，並自我摸索出更好的資料安全管理辦法。

法令是死的辦法是活的

另一方面，無論企業選擇那一種方案，「使用者的接受度」也都是非常重要的關鍵。成功的資安控管機制應要能配合公司使用者日常的工作程序，而不是反過來要求使用者配合改變。過去許多企業導入資安方案失敗的原因，絕大部份都是因為「改變其現狀」會讓使用者在作業時感到不甚方便，因而拒絕採用並設法加以規避。

舉例來說，根據美國醫療保險流程及責任法案(Health Insurance Portability and Account Act, HIPAA)的規定，不同科別的醫生是不能跨單位進行病患資料的查詢。但根據CIO雜誌的報導，美國曾發生有醫院的某位由腫瘤科轉調婦產科的醫生，基於持續追蹤病患，以提供其精神支持及相關醫療建議的需求，要求繼續保留其查閱既有腫瘤病患資料的權力。

為了平衡資安法令與醫療作業需求兩方面的矛盾，該醫院的CIO Glen Damiani採行讓這位醫師到腫瘤部門時，仍擁有存取病患資料權利的做法。而PWC顧問服務部處長Stergio Pedro針對此案更進一步建議，院方可採用自動加密的IT技術，讓所有流出醫院主

機的資料，都自動進行加密的程序，以確保醫院的機密或敏感資料只能在醫院網路範圍內讀取，而不會產生外洩的問題。

「IT人員需要設法平衡兩者矛盾的需求。」Damiani認為：「站在醫療原則的觀點，院方也必須保障醫生在診療時的方便性。」不過他也強調，不管如何，任何有關開放資料存取權限的決策過程，一定要有詳加的明文記錄，並強調其開放的理由。Damiani說：「若不幸真的發生意外狀況，被檢調單位人員找上門來時，你才會有一個足夠堅實的理由來支持你的做法，並幫助你說服他們，相信你的確有考慮過相關風險，也想過要如何緩和問題之間的衝突，以及展現你自己對於法律規範重視的程度。」

從法律模糊空間中找出定位

不過也由於CIO與CSO本身日常的工作就相當忙碌，絕大部份的時間都花費在不斷創新、維持專案正常運行、充當救火隊以隨時支援解決問題等項目上，因此很難有時間來研究這些會影響他們的法律條文，更不要說會為了符合法規要求，而投入相關時間進行系統與流程修正。因此有不少國家的企業，在資安法規的遵循狀況方面，其表現都不甚理想。

這主要原因是出於心存僥倖，許多CIO都認為會被抓到違規的風險很低，而且也因為法令適用的情境與要求並不明確，導致人們乾脆某部份就偷懶不做。以美國加州安全破壞通報法規為例，其規定如果公司的資料有進行加密，當發生客戶的資料安全遭到破壞時即無需通報。然而該法規卻沒有規定公司資料一定要加密。

因為心存僥倖，不少國家企業在資安法規遵循上，其表現都不甚理想

以美國加州安全破壞通報法規為例，其規定如果公司的資料有進行加密，當發生客戶的資料安全遭到破壞時即無需通報，然而該法規卻沒有規定公司資料一定要加密。

Sony的CSO Jason Spaltro表示：「由於有這種模糊空間的存在，使得公司在思考如何保護個人資料方面，往往成為一種風險考量的商業決策行為。」而他建議CIO與企業資安執行者應該要與外部法規稽核人員一起坐下來談，公司的法務人員與人力資源部門主管也要主動多了解這些資安法規真正的意涵，以及其對企業產生的特殊意義與影響力。

以Sarbanes-Oxley法規為例，對銀行的要求程度就會比娛樂公司更高。「因為他們直接管的是客戶的金錢。」Spaltro說：「這表示像Sony這樣的公司在面對法規時，稽核人員稽查的頻率與要求可能會少一些，讓公司因此不必像銀行那樣花大錢來投資。」但是他也相信，這並不代表企業無需主動思考遵循法規的方法，Spaltro說：「如果要等稽核人員來告訴企業：哪些方式行得通，哪些行不通時，對公司而言那可就太慢了。」

Spaltro強調：「IT人員要非常清楚知道自己在做什麼，並確定自己應做的功課在事先都有做完才行。」

因應個資法實施 微軟的解決之道

對於以往較不重視消費者個人資料安全防護機制的台灣企業而言，新版個資法的實施將對其造成嚴重衝擊。面對此一變局，微軟建議，企業可從自身的個資外洩風險評估開始著手，再針對制度、管理、技術…等層面，逐步建立符合需求的個人資料保護系統，以減少個資外洩機會與企業面臨的風險危機。

由於目前台灣政府、民間各單位與企業的資訊應用環境，不論從作業系統、應用程式開發工具、伺服器軟體與相關解決方案…等，微軟均有極高的市佔率，而且市面上大部份的應用程式與系統，如ERP、e-mail、辦公室作業軟體、應用伺服器…等，也都是在微軟的系統環境或平台中執行，因此微軟因應個資法所提出的解決之道，也就格外受到企業關注。

先由自我的個資外洩風險評估做起

台灣微軟伺服器平台事業部產品行銷經理簡志偉認為：「一般企業發生個資外洩的管道，不外乎可分為『外部入侵』、『內部人員洩漏』、『內部程序疏失』與『委外廠商洩漏』…等4大類型。」而且無論是在資料的傳輸、使用與儲存過程中，都可能存在有外洩的風險。

舉例來說，在使用資訊時，內部員工就可能因寄發機密郵件時，沒有加密e-mail本身與附件、委外廠商取得未經加密的郵件或附件檔案，加以任意開啟與轉寄、外部駭客利用SQL Injection入侵企業網站，或是寄發垃圾郵件到企業內部郵件伺服器，以及未強制貫徹郵件與檔案加密的保護政策…等狀況，造成企業個資嚴重外洩的問題。而同樣的，企業所蒐集到的資訊，其在傳輸與儲存的過程中，也會有類似的情境重覆上演。

簡志偉建議企業，「因應個資法的第一步，應先從評估企業個資外洩的風險開始做起，以了解企業內個人資料可能洩露至外部的各項管道。」特別是新版個資法實施之後，對於企業內的消費者個人資料，從其蒐集、保存、利用與銷毀…等階段，都有各項明確且嚴格的規定需要遵守。他表示：「這表示企業在制度、管理、技術、員工、委外、標準作業程序…等層面，都必須因應評估的結果加以詳盡規畫，以建立符合企業需求的個人資料保護系統。」

連結客戶資安需求與個資法規範的微軟商務安全就緒解決方案

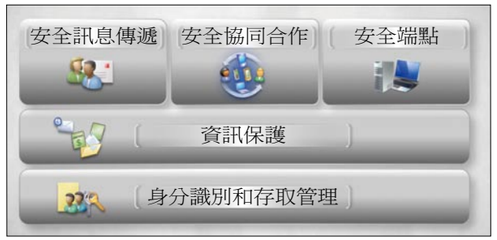
為了協助企業進行個資外洩風險的評估，目前台灣微軟資訊安全小組與其合作夥伴，會分別由「技術」與「管理」兩方面出發，協助客戶進行與個資法相關的檢驗，並提出後續的風險評估與報告。這除了可讓企業能更加了解自身在個人資料防護上安全的弱點所在外，並可據此分析結果，進一步與「微軟商務安全就緒解決方案」進行連結與導入，協助客戶以最經濟實惠且有效的方式，提升其安全防護的等級。

簡志偉強調，目前市面上雖然已有大量關於資安防護的產品可供選擇，但由於其彼此之間缺乏整合性，整體建置與維運成本也太高，隨著法務遵循的壓力增加，IT作業環境的複雜程度日益提升，及金融風暴後公司高層對於IT預算投資越趨謹慎等因素的影響，這些產品已經難以滿足此波商務需求與新商機的安全性。

「重點是要建立『具有高度安全性且可互通的平台』。」簡志偉認為，為了達到便利存取，跨越網路、主機、應用程式等實體/虛擬/雲端環境的多重層級防護，在企業中進行安全性整合和延伸，以及簡化安全使用經驗並管理法規遵循的目的，企業會越來越需要以更完整的資安方案來保護其整體資料安全。「而這正是『微軟具備縱深防禦架構的商務安全就緒解決方案』所要做的。」簡志偉表示。

管理風險及賦予人員權限

簡志偉說：「微軟商務安全就緒方案大致可區分為『安全傳訊』、『安全共同作業』、『安全端點』，以及『資訊保護』、『身分識別與存取管理』5大區塊類型。」其中「安全傳訊」、「安全共同作業」、「安全端點」主要是針對用戶在進行通訊、協同作業與一般終端作業使用環境的安全性所設計；而「資訊保護」與「身分識別與存取管理」則是以滿足企業IT基礎架構與多功應用的安全需求為其應用範圍。



微軟具備縱深防禦架構的商務安全就緒解決方案

「『微軟商務安全就緒解決方案』會以其現有產品為基礎，後再針對企業需求進行改善與強化。」簡志偉表示，以「安全傳訊」區塊為例，其目的便在於「確保任意裝置之間的商業通訊安全，防止機密資訊在未獲授權的情況下遭到竊取與外洩」的問題。而該區塊微軟所提供的解決方案，主要便是由Forefront Protection 2010 for Exhange Server、Forefront online Protection for Exchange、Forefront Unified Access Gateway、Exchange Server、應用程式伺服器…等產品項目所組合而成。

另一方面，除了提供上述具體的產品與資安防護功能之外，微軟還會對於有需求的客戶，為其進行全公司系統健康檢查、資料庫管理監控及Windows安全機制…等相關資安服務。簡志偉表示：「這對大幅減少企業個資外洩風險，改善公司整體服務品質的競爭力，亦有極大的幫助與影響力。」

關於台灣微軟資訊安全小組提供之「資訊外洩風險評估暨個資外洩衝擊度鑑識」服務，請洽網址：http://www.microsoft.com/taiwan/security/privacy/services.htm