愈早偵測出資訊環境或資訊系統中變化之資訊，愈能增加採取適當風險處理機制降低風險的機會。

資訊系統風險評鑑介紹（下）

◎林子群

我國資訊系統的風險架構，乃是根據ISO/IEC27005標準之風險管理架構發展而成，其作法可分為「高階風險評鑑作法」、「詳細風險評鑑作法」及「既有風險評鑑作法」等３種。在資訊系統風險評鑑介紹（上）說明了「高階風險評鑑作法」與「既有風險評鑑」，賡續將介紹「詳細風險評鑑作法」。

壹、詳細風險評鑑作法

詳細風險評鑑作法，即藉由系統化的方式，找出資訊系統中應該優先處理的資訊資產所對應的風險，而施予適切的防護安控措施，以維持組織能夠持續運作。

「詳細風險評鑑作法」有兩項主要工作，分別為「風險分析」與「風險評估」；其中「風險分析」可再細分為「風險識別」與「風險估計」兩項步驟，最後針對該資訊系統的資訊資產，分別產生相對的風險評鑑風險等級－「普、中、高」。

機關應針對「資訊系統」的所有資產，進行「弱點、威脅及可能性分析」，並參考建立全景階段所訂定的「風險評估準則」與「衝擊準則」執行風險分析，得到所有資訊資產的風險值；接著執行風險評估，以訂定風險等級，再依據「風險接受準則」，決定「接受風險等級」。詳細的風險評鑑作法之細部活動程序包含「資產識別」、「威脅與脆弱性識別」、「現有控制措施識別」、「後果識別」、「鑑別資訊資產價值」、「評鑑事故可能性」、「估計風險等級」、「訂定風險等級」及「決定可接受風險等級」等９項作業步驟。

一、風險識別

「風險識別」是針對資訊系統鑑別出每個資訊資產、該資訊資產脆弱性被威脅利用的難易度、相關威脅發生的可能性、威脅與脆弱性結合發生事故時對組織衝擊的嚴重性及其資訊資產現有控制措施等；完成前述之識別後，為便於找出各個威脅與脆弱性組合之風險的優先順序，對威脅發生之可能性、脆弱性被利用的難易度及衝擊之嚴重性各給予一個數值，再計算各個威脅與脆弱性組合之風險值。

(一)資產識別（Identification of Assets）

機關可藉由此資訊系統所提供的業務流程活動，識別該資訊系統之資訊資產。

(二)威脅與脆弱性識別（Identification of Threats and Vulnerabilities）

針對各項現有控制措施識別（Identification of Existing Controls），資訊資產分別鑑別其在使用或處理過程中，各項可能的威脅，運用該資訊資產脆弱性對「機密性（C）」、「完整性（I）」及「可用性（A）」造成之衝擊。

(三)現有控制措施識別（Identification of Existing Controls）

了解現有控制措施之施行成效與已規劃的控制措施，再參考「安全控制措施參考指引」，確切描述安控措施，以避免重複的資源浪費。

(四)後果識別（Identification of Consequences）

識別資訊資產發生事故之後，對組織造成的後果。

二、風險估計

資訊資產相關的風險識別完成後，需要估算每一個資訊資產的相對風險大小，故需藉由量化資訊資產的價值、後果對機關衝擊的嚴重性，及事故發生的可能性，以估算風險值。

(一)鑑別資訊資產價值（Identification of Assets Value）

以資訊資產在事故發生時，破壞「機密性」、「完整性」及「可用性」造成的後果，對組織衝擊的嚴重性，鑑別資訊資產的價值，並將識別的後果（普、中、高）分別給予一個值，將每一資產的「機密性」、「完整性」及「可用性」代表值相加，即可得到資訊資產的價值。資訊資產價值的計算方式，如下列公式所示：

資訊資產價值＝機密性鑑價 ＋ 完整性鑑價 ＋ 可用性鑑價

(二)評鑑事故可能性（Assessment of Incident Likelihood）

事故可能性是由分析威脅發生的可能性與脆弱性被運用的難易度組合而成，給予威脅發生的可能性與脆弱性被運用的難易度（普、中、高）各一個值，分別代表「威脅等級」與「脆弱性等級」。

在評鑑事故可能性時，請在現有控制措施識別完成之後，考量在現有控制措施實施之下，仍會發生事故的可能性來作評鑑。

威脅等級評估方式，詳見表1所示：

表1威脅等級評等表

等級	等級值	說明	發生頻率
普	1	防制脆弱性被利用的安全對策有效 威脅來源缺乏動機或能力不足 發生頻率低	• 事件或威脅雖然沒發生過，但有可能發生 • 平均每年發生不到1次 • 平均每月人為阻止事件或威脅發生不到1次
中	2	威脅來源有動機也有能力 防制脆弱性被利用的安全對策有效 有可能發生	• 平均每年可能發生1次以上，低於6次 • 平均每月人為阻止事件或威脅發生1至3次
高	3	威脅來源有強烈的動機與足夠的能力 防制脆弱性被利用的安全對策無效 時常發生	• 平均每年可能發生6次（含）以上 • 平均每月人為阻止事件或威脅發生超過4次（含）以上

資料來源：資訊系統風險評鑑參考指引

脆弱性等級評估方式，詳見表2所示：

脆弱性等級評估方式，詳見表2所示：

表2脆弱性等級評等表

等級	等級值	說明	發生頻率
普	1	脆弱性很難被利用	• 僅限深入了解脆弱性技術，並於特定條件或環境下方能利用脆弱性 • 不會損害資訊資產，或是受到損害後能立即回復 • 必須運用特殊的方法才能利用脆弱性進行攻擊 • 威脅來源必須花費長時間（可能需一個月以上）的資料蒐集，突破各層防護，才能接觸到關鍵資訊 • 攻擊成功：可能要1至數個月以上 • 可能之原因： - 管理防護機制完備並落實實施（例如流程控管、存取權限、通行碼政策、變更管理、稽核及應用系統經過完整測試等皆落實進行）
普	1	脆弱性很難被利用	• 僅限深入了解脆弱性技術，並於特定條件或環境下方能利用脆弱性 • 不會損害資訊資產，或是受到損害後能立即回復 • 必須運用特殊的方法才能利用脆弱性進行攻擊 • 威脅來源必須花費長時間（可能需一個月以上）的資料蒐集，突破各層防護，才能接觸到關鍵資訊 • 攻擊成功：可能要1至數個月以上 • 可能之原因： - 管理防護機制完備並落實實施（例如流程控管、存取權限、通行碼政策、變更管理、稽核及應用系統經過完整測試等皆落實進行） - 資訊或處理設備的使用手冊完整或說明清晰 - 使用者或管理者受過完整教育訓練，對資訊處理設備操作熟練 - 使用者或管理者對資訊處理程序熟悉 - 技術性防護機制完備（例如資訊採用加密保護、網路區隔並採用安全設備監控系統效能、容量及安全事件；有效管理入侵／病毒／木馬、備援線路） - 可被利用的方法的技術層次高或技術不容易取得實體環境的特性（例如劃分安全區域並實施監控與出入管控、環境溫濕度控管、建築物或防護設施材質等）讓威脅源被杜絕
中	2	脆弱性被利用的難易度適中	• 具備了解脆弱性技術知識，方能利用脆弱性 • 資訊資產受到損害，且無法立即回復 • 不需用特殊的方法就能利用脆弱性進行攻擊 • 已實施保護的機制，威脅來源必須花費一段時間（可能是數天）進行資料蒐集，始能接觸到關鍵資訊 • 攻擊成功：可能是數天以上 • 可能之原因： - 已建立管理防護機制但未落實（例如：流程控管、存取權限、通行碼政策、變更管理、稽核及應用系統測試等） - 資訊或處理設備的使用手冊過於簡單或說明不詳細 - 使用者或管理者雖受過教育訓練，但對資訊處理設備操作不熟練 - 使用者或管理者對資訊處理程序不熟悉 - 雖實施技術性防護機制（例如：資訊採用加密保護、網路區隔並採用安全設備、監控系統效能、容量及安全事件；有效管理入侵／病毒／木馬、備援線路），但是設定或防護能力不足 - 可被利用的方法的技術層次高，但技術容易取得 - 實體環境的特性（例如：未劃分安全區域出入管控、環境溫濕度控管不足及建築物或防護設施材質等）讓威脅源存在
高	3	脆弱性很容易被利用	• 任何人不需具備任何能力，均能有意或無意地利用脆弱性 • 資訊資產受到嚴重損害，影響或中斷資產相關業務運作，或導致資訊資產消失無法復原 • 運用簡易的方法就能利用脆弱性進行攻擊 • 未實施保護或保護機制無效，威脅來源於短期內即可攻擊成功 • 攻擊成功：可能是一天內到數天 • 可能之原因： - 管理防護機制缺乏（例如：流程控管、存取權限、通行碼政策、變更管理、稽核及應用系統測試等） - 缺乏資訊或處理設備的操作手冊或手冊錯誤 - 使用者或管理者未受過教育訓練，或對資訊處理設備操作不熟練 - 使用者或管理者對資訊處理程序不了解 - 缺乏技術性防護機制（例如：資訊採用加密保護、網路區隔並採用安全設備、監控系統效能、容量及安全事件；有效管理入侵／病毒／木馬、備援線路） - 可被利用的方法其技術層次低且容易取得 - 實體環境的特性（例如：未劃分安全區域出入管控、環境溫濕度控管不足及建築物或防護設施材質等）讓威脅源持續存在

資料來源：資訊系統風險評鑑參考指引

(三)估計風險等級（Level of Risk Estimation）

估計風險等級乃是將量化的資訊資產價值、後果對組織衝擊的嚴重性，及事故發生的可能性結合，計算每一個資訊資產的價值與風險值。資訊資產風險值計算方式，如下列公式所示：資訊資產風險值＝資訊資產價值 x 威脅發生可能性 x 脆弱性利用難易度

三、風險評估

(一)訂定風險等級

將所有資訊資產相關風險值，在其最大值與最小值區間等分為「普、中、高」3 個等級。初次風險評鑑，可先依據理論值計算公式，風險值將落在 3 至81分之間，區分為 3 個等級之後，詳見表 3 所示。

表 3 風險等級區分表

風險等級	起始間隔	結束間隔
高	55	81
中	29	54
普	3	28

資料來源：資訊系統風險評鑑參考指引

上述風險值區間乃是依照理論值方式進行說明，惟機關可本著持續改善的精神，選擇採用實際的風險的最大值與最小值，區分為 3 個等級，在有效地管控原屬於高風險等級的風險之後，於人力與預算許可之下，逐年改善機關所可能遭遇的風險，以提升機關的資安防護等級。

(二)決定「可接受風險等級」

依據「建立全景階段」所訂「風險接受準則」，再檢視資訊資產風險清單，訂定組織可以承受的風險等級，以決定風險處理的範疇。此階段政府機關亦可再依其所負責任務的類別與性質、服務對象、內部資源及經費預算等因素，修正風險的接受準則。

四、根據「風險接受準則（普、中、高）」，針對「未能接受」之風險，判斷風險處理的「資產」對象。即依「高風險」、「中風險」、「普風險」之資產，建議從「安全控制措施參考指引」中，對照選擇「適合」該資產類型之相對風險的「高防護等級」、「中防護等級」、「普防護等級」的控制措施。

五、根據「風險評估準則」，針對「未能接受」之風險，判斷風險處理的優先順序。

貳、結論

行政院研考會於「99年資通安全技術服務與防護管理計畫」中，責成「行政院國家資通安全會報技術服務中心」，修訂資通安全有關作業規範與參考指引，其中「資訊系統風險評鑑參考指引」旨在說明「行政院及所屬各機關資訊安全管理要點」之「各機關應依有關法令，考量施政目標，進行資訊安全風險評估，確定各項資訊作業安全需求水準，採行適當及充足之資訊安全措施，確保各機關資訊蒐集、處理、傳送、儲存及流通之安全」的內容。

資訊系統風險評鑑之高階風險評鑑作法為應用鑑別機制，可快速掌握資訊系統之衝擊影響，並得以將資源投入於最需要的系統；詳細風險評鑑作法透過風險分析與風險評估，較能有效掌握機關資訊系統中各項資訊資產之風險。

（作者現為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專案諮詢）

▲Top

網路「臉書」很可能侵犯使用者的隱私權並造成洩密，所以在按下任何按鈕之前，必須小心謹慎。

在您按「讚」之前

◎林俊安

隨著社群網站的興起，人們得以結合即時通訊、部落格、相簿等多種功能，掌握親朋好友的最新訊息；而自己也可透過網路，將個人的訊息即時地和全世界互動分享。以目前最熱門的社群網站」（facebook）為例，成立6年多來，參與人數就突破6億！當你有了臉書的帳號，看到好友的新訊息，會不會很想按下一個「讚」呢？

但當你按「讚」的同時，也有許許多多人看到你按下這個「讚」！根據統計，一筆公開的個資，約有近三百多家的廠商會感興趣！而臉書的授權網頁上寫著：當使用者將圖文上傳時，等同授權這些資料的使用權利。「臉書」會不會將資料賣給廠商，讓您成為廠商傾銷的對象呢？去（99）年，臉書在未通知使用者的情形下，推出Social Graph API語意網，使網路上的每一個網頁，都能代表些具體的意義，而後可以透過分析，掌握使用者的行為模式，甚至一切紀錄！而根據美國波士頓東北大學的研究發現，透過演算法分析某一個人的行為模式，可精確預測其行蹤的機率高達93.6%！有關臉書疑似侵犯隱私權問題，也使得美國聯邦貿易委員會展開調查，要求提供獨立的隱私設定及盡事先告知之義務。惟某些社群網站上的小遊戲卻依舊包藏禍心，如來路不明的「德州撲克」等，它會夾帶木馬程式，偷偷竊取你電腦中的資料並回報。

有些新開發的功能，例如能顯示地理位置的小程式，就提供有心者一個方便的管道，就像網站「www.pleaserobme.com（請搶我）」用搜尋連結警告網友們：透過社群網站的搜尋引擎，可以發現有哪些人正在分享所在位置，同時標記自己目前是否在竊賊要下手的目的地。諸如：「某人剛離開家，前往某地，預計幾天回來」、「某人剛剛離開辦公室」等等，這也難怪當iPHONE傳出有可能紀錄使用者的路徑時，蘋果的總裁賈伯斯隨即在第一時間出庭否認；美國甚至因而傳出保險公司為此傳播途徑導致風險增加，而要調漲住宅保險費用的消息。

當隱私無存、個資外洩，又會是如何？想想您的個人資料、住所、信用卡、各種通聯記錄、密碼等資料人人皆知時，就會令人不寒而慄！而這就是日本電子大廠索尼（sony）目前頭痛之處－索尼在今（100）年5月初傳出有史以來最嚴重的個資外洩事件，總計近億名的個資外流。其風靡世界的線上遊戲系統「PlayStation Networks 」(PSN)以及「Quriocity」共7,700萬名用戶的個資與信用卡資料全數外流，後來又發現美國分公司的PC線上遊戲亦有2,460萬名用戶的個資外流。這些還可視為是駭客的網路攻擊事件，但是另一個美國分公司則流出二千五百多名的會員個資，使得任何人都可以任意於網路查閱，這就是公司控管的問題了。索尼的資訊長長谷島承認「我們無法意識到，所有系統竟是那麼脆弱！」脆弱嗎？大半是由於公司的不用心，日本眾多輿論皆認為索尼接二連三的個資外流，是因其公司自持強項為硬體，而忽略了對軟體的控管－索尼的部分系統存在著普遍已知的弱點，其網路控管程度甚至不如量販店的等級！加拿大的用戶堅持提出告訴，求償約十億元加幣；其代表聲稱：「企業既然手握個資，就應產生管理義務，畢竟顧客是因為相信你，才將資訊提供給你。」

在網路的世界裡，使用者的所做所為幾乎無所遁形；但我們可以盡量不使用未加密的網路、盡量勿下載來路不明的軟體、盡量安裝各種防毒軟體、盡量瀏覽固定或經過加密（SSL、https連結）的網站，以避免惡意軟體的侵入。

時時小心、處處謹慎，不要當您在按下「讚」的同時，讓另一群有心人士同時間在黑暗處按下更多的「讚」、「讚」、「讚」！

▲Top