狀況掌握與危機處理

所謂「魔鬼藏於細節中」，事情的發生必有徵兆，若能提高警覺、防微杜漸，便是最經濟的危機處理。

◎洪子晴

電影中的意外狀況總有劇本設計好的英雄前來解救，然而真實生活一旦發生意外，是無法一廂情願地期待英雄的救援。所以災禍發生時該如何自處，便成爲各機關、部隊，乃至個人學習的重要課題。

「意外」並非總是「意料之外」，往往是人員未確實遵守安全規定或作業程序所致；如去年延燒全臺的塑化劑事件，就是不肖商人擅自更改配方牟取暴利所引發的風暴。災難可區分爲「天災」及「人禍」，其中人禍可以靠制度加以控制並降低其發生率；天災雖無從阻止，但仍可藉經驗法則預判其災損，事先訂立處理機制並實施預防演練，以求降低損害。因此，上級的職責除建立制度外，還包括預想一切可能的狀況並訂定處理流程，即「危機處理」。

九一一事件及卡翠娜風災後，美國國土安全部研擬出 15 種「想定」，內容包括核爆、化學攻擊、自然災害、食物汙染及網路攻擊等，做爲事先預判災損、事後應變處置的準則。同樣面對天災，我國軍也依「超前部署、預置兵力、隨時防救」的原則行動，並在全軍推行「風險管理」觀念，亦即事前評估可能發生的危安因素，預先提出對策、建立應變機制及教育部屬等，都與美國國土安全部的「想定」原則不謀而合。可見先進國家面臨詭譎的世界局勢及極端的氣候變遷時，已經越來越能以積極正面的態度回應，而非消極地逃避，顯示此一觀念受重視的程度。

近來人們常說：「魔鬼藏於細節中」，事情的發生必有徵兆，只是人們常不以爲意；所謂「千里之堤，潰於蟻穴」，若能提高警覺、防微杜漸，便是最經濟的危機處理。我政府雖已建立許多應變機制，然而若國人缺乏危機處理的觀念，也難以發揮作用。唯有從上到下建立正確觀念、建構嚴密的網絡，方可消弭危安因素，確保國家安全、社會安定、民眾安寧。

（本篇轉載自法務部調查局清流月刊 102 年 4 月號）

在家加班真的安全嗎？

小華家裡電腦安裝了 P2P 軟體，又將企劃案帶回家裡工作，結果，讓公司新產品的消息提早在網路上曝了光…

◎魯晏汝

小華是一位剛從名校畢業的大學生，成績優異的他在畢業後，很快就找到了現在這份喜歡的工作；爲了不辜負主管對他的期望，小華每天都很努力地加班到三更半夜。某天，小華正猶豫著晚上是否要去參加同學會，還是留在公司加班把企劃書做完。小華的同學見他猶豫不決，就出主意說：「這還不簡單，你先參加同學會和大家吃個飯，再把企劃書帶回家繼續做就好啦！」小華心想說的也是，同學們畢業後就沒再見過面了，難得趁此機會和大家聯繫一下感情。於是把東西收一收趕去聚餐，工作的事就等晚上回家再挑燈夜戰。

隔天一早，小華果然不負主管的期望，準時交出一份漂亮的企劃書，而且這份企劃書在公司會議時更獲得一致的好評，認爲這個 idea 一定可以打敗對手，取得市場競爭的優勢，於是在會議上就拍板定案，並指定小華擔任此企劃案的專案負責人。初生之犢的小華接到這重責大任，自然是喜不自勝；爲了感謝大家給他的機會，接下來他每天都加班到很晚，做不完的工作也會帶回家再繼續做。

然而，就在產品上市的當天，網路上突然開始大量流傳小華公司預備推出的新產品資訊，從產品規格、測試報告、行銷計畫到價格策略，網路上都可以找到很詳細的資料。消費者透過網路知道了測試報告和行銷價格策略，對於小華公司推出的新產品就失去了原先預期的搶購熱忱，於是新產品推出後乏人問津。

小華的主管知道這件事情後，很生氣地把小華叫進辦公室裡了解原因，質疑小華私自將公司未上市的產品計畫洩漏出去。小華一聽急忙否認，馬上向主管解釋自己平時的作業流程，而且爲了表達自己敬業的程度，還跟主管提到爲了能確實掌握進度，自己都會利用假日在家準備企劃案的作業。小華的主管一聽到這裡，馬上就猜想到這次企劃案外流的可能原因了。主管於是問小華：「小華，你家裡的電腦裡是不是有安裝 P2P 軟體呢？」小華聽了很納悶地說：「有呀！但這跟企劃案提前曝光有什麼關係呢？」主管見小華還是個剛畢業的新鮮人，對資訊安全的危機意識還不夠，決定趁此機會給小華機會教育一下，免得日後又發生一樣的問題。

P2P（Peer – To – Peer）是一種點對點的網路傳輸型態，可以讓兩台以上的電腦彼此分享對方電腦裡的資源；最早出現的背景是因爲傳統的網路傳輸型態必須將資源放在伺服器（Server）後，才能提供給別人下載；但如果同時下載的人數過多，會造成伺服器不小的負擔，所以出現了 P2P 這種傳輸型態。P2P 的優點在於每個用戶端（Client）都可以當做伺服器分享資源，不需要再像傳統傳輸模式一樣先將資源放在伺服器後再供人下載，而且，在同一時間分享的人越多，下載速度會越快；但也因爲 P2P 軟體可以將自己的電腦變成用戶端，提供給別人下載資源，所以

小華家裡的電腦安裝了 P2P 軟體後，又將公司的企劃案帶回家裡工作，才會讓新產品的消息提早在網路上曝光。

小華聽完主管的解說這才恍然大悟，原來是自己在電腦裡裝了 P2P 軟體惹的禍。主管這時又補充解釋說：「在企業裡爲提高資訊的安全性，一般我們在公司的電腦裡都會設置有防火牆（Firewall），防火牆可說是將電腦和網路中間隔起一道安全的牆，是一種確保資訊安全的裝置，它會檢查網路上的資訊，並依據使用者設定的規則允許或封鎖資訊的傳輸，確保資訊的安全性。

除此之外，基於安全性的考量，大部分企業都是使用封閉式的網路架構，以避免駭客入侵，或是將未經授權的用戶阻隔於企業網路之外，以保障企業網路的安全。所以如果非不得已必須在公司以外的地方工作，也要透過虛擬私人網路（Virtual Private Network, VPN）連回公司，虛擬私人網路架構中有各項的安全機制，例如通道、加密、認證、防火牆及入侵偵防系統，藉由通道點對點的傳輸方式，將加密的資料傳送出去，更透過使用者認證（User Authentication）的機制，來確保非授權的使用者無法讀取到他們的機密文件；即使資料被竊取了，透過加密技術編碼及計算後傳送的資料，也只有發送者和接收者能夠解讀，提升了資料傳輸的安全性。而在此架構下，入侵偵防系統更是不可或缺的角色，這個機制可以將入侵的駭客或是非授權的使用者阻隔在企業網路之外，保障企業的資訊安全。

所以，爲了避免資料外洩，提高資訊的安全性，盡量不要在電腦裡安裝 P2P 軟體，以免電腦裡的檔案資料被分享出去，而且還要正確地使用防火牆，阻隔外界的入侵機會。如要在公司以外的地方使用公司的資源或加班，也一定要透過虛擬私人網路的方式，以免像這次一樣，因爲產品資訊提早曝光而讓這段時間的努力白費，還造成公司的損失。」

小華聽完馬上點頭稱是，心想主管真是替他上了寶貴的一課。當學生時只知道使用 P2P 軟體可以下載檔案，經過這件事之後，他決定回家立刻把這類的軟體從電腦裡移除，免得同樣的慘劇再度發生。

（作者服務於特力股份有限公司人力資源部）

（本篇轉載自法務部調查局清流月刊 102 年 4 月號）

從分層授權談資訊系統的權限管理

分層授權不僅是作業面上的口號而已，更應落實在資訊系統的權限管理。

◎魯晏汝

「小威呀，偷偷跟你說，我前幾天在公司的系統裡面看到我們經理的薪資耶！」小威一聽到馬上露出不可思議的表情說：「怎麼可能？薪資資料在公司屬於機密文件，非相關作業人員或主管是無法查看的，你既不負責教育訓練，又不是薪資作業人員，爲什麼你能看得到呢？」小文神秘兮兮地說：「雖然我不是薪資作業人員，但我們使用同一個應用系統執行日常作業，所以我們可以看到一樣的資料啦！」

聽完上述的對話，您是否有發現不合理的地方呢？一般來說，公司企業會依據業務特性分別使用不同的系統，例如業務單位使用客戶（會員）管理系統、物料管理單位使用進銷存管理系統、人事單位使用人力資源管理系統。即便使用同一系統，也會因職務權責而開放不同的權限，例如財務部門使用的是財務和會計的模組，人資部門使用的是人力資源的模組，不同部門間，是無法看到彼此的資料；而主管和其所屬員工使用的權限，當然也不同。所以在系統權限的設置上，大致可以分成下面幾種：

一、使用者權限： 使用者爲使用系統的人員，每位使用者都有一組屬於自己的帳號密碼，在使用前必須先透過帳號密碼加以認證，通過認證後，系統會賦予該使用者應有的操作權限，限制哪些爲可以使用的功能，哪些爲無法使用的功能，這個過程稱之爲「授權」。

二、使用者群組權限： 使用者群組爲同性質使用者所組成的集合，使用者可以同時屬於多個群組，例如業務人員都會加入「業務群組」，這個群組的人員透過自己的使用者帳號登入後，僅能使用業務群組所授權使用的功能；而業務部門的主管除加入業務群組外，同時也會被加入管理職人員所組成的主管群組，使用主管群組擁有的權限。

三、權限等級： 權限等級爲系統的操作功能。首先系統管理員可以使用權限等級的定義，來區分每個角色可執行哪些操作，例如「MIS」的權限可以使用 A、B、C 三個模組的功能，「Sales」權限可以使用 D、E 的功能，「管理職」可以使用 F 的權限，這些定義可視爲一個基本的授權單位，權限等級即是由這些基本單位所組成。而一個使用者群組也可以擁有多個功能權限，例如先前提到的業務部門主管，可能擁有「Sales」加「管理職」的權限，當他使用自己的使用者帳號登入系統時，既能使用 Sales 可使用的模組功能，也能使用主管所屬的管理職模組功能；而其他非管理職的業務部門同仁使用自己的帳號登入後，僅只能使用 Sales 的功能。這種對應關係可以稱爲「權限指派」，每位使用者只能依據其權限所定義的操作權限操作系統。

四、讀寫的權限： 資訊系統中最重要的是儲存資料的資料庫，資料庫內容的良窳，將影響資訊系統的正確性。因此，資料庫讀寫權限也是很重要的議題。例如會計系統的第一線使用者，他的

工作就是輸入各種原始憑證、傳票的資料，並且要對其正確性負責；因此，系統管理者就會賦予他寫入的權限，而且寫入的權限即同時包含讀取的權限。但是，各階主管的權限等級，只能擁有讀取資料的權限，而沒有寫入資料的權限。這樣的設計最主要的考量就是權責分明。試想，如果第一線承辦人員所輸入的資料，其長官都可以任意修改，當出現問題時，責任應歸屬誰？因此，資訊安全必須透過讀寫權限來加以確保。

以前述故事來說，小文雖然和薪資人員使用同一套日常作業系統，但以系統權限的設定與管理原則言之，應將權限細分爲「薪資權限」及「訓練權限」，如此一來，「薪資權限」只能使用和薪資相關的模組設定，而「訓練權限」登入後，也只能看到員工的基本資料及相關受訓紀錄等資料。所以小文的使用者權限應該被設置爲訓練的權限，當她使用自己的帳號登入系統後，只能使用系統裡定義的訓練權限所使用的模組，並不能看到其他人的薪資資料。

總之，分層授權不僅是作業面上的口號而已，更應落實在資訊系統的權限管理，其最高指導原則爲：「不讓與業務無關的人，看到與其業務無關的資訊。」如此方得以確保資訊系統的安全。

（作者現服務於特力股份有限公司）

（本篇轉載自法務部調查局清流月刊 102 年 5 月號）

透過文件審查避免機密資訊外洩

研發成果發表的報告內容必須經過審查，一方面確認資料內容無誤，另一方面決定資訊公開的程度，以確保公司的重要資訊不會外洩。

◎魯明德

小潘的公司多年來致力於資訊安全領域的研發，產品市場占有率很高，在業界亦頗負盛名，因此在今年的國際資訊安全研討會中，受邀擔任協辦單位，並在會中發表論文。公司把這個重責大任交給研發部，於是主管小強就交待小潘負責撰文，並指示他：「發表內容必須依程序核定之後，才能寄給主辦單位發表。」小潘聽完後一頭霧水，回想當初在學校唸書的時候，老師也曾交待他去投稿期刊跟研討會，從來也沒有審查程序，現在爲什麼要這麼麻煩？何況我們公司還是協辦單位。當然，小潘所想的問題，是一向唯命是從的經理小強無法回答的。因此，小潘在悶了幾天之後，決定趁著下午茶約會的時間請教司馬特老師。

好不容易盼到了下午茶時間，小潘一見到司馬特老師，就迫不及待地把這個月碰到的問題及心中的疑惑，一股腦兒地講給司馬特老師聽。老師聽完了問題，喝了口咖啡，說道：「貴公司會不會想知道競爭對手正在研發什麼產品？進度如何？對我們的威脅程度有多大？」小潘想都不想就回答：「當然想知道啊！小強經理平時就經常叮嚀我們，要隨時蒐集對手的各項情資，定期回報給他。」

老師接著笑說：「那就對啦，你會每天盯著你的對手看，他們當然也是每天盯著你看啊！商場如戰場，商機稍縱即逝，大家都在處心積慮地蒐集對手的情資，若一不小心就會把自己的機密洩露給對手；因此，任何可能洩密的管道，都要隨時加以防堵。」

小潘聽了司馬特老師這番話，心中更加迷惑了：「不過就是在研討會上報告一篇文章，難道競爭對手能從投影片上蒐集到什麼情資嗎？」司馬特老師一眼即看穿了小潘的心思，喝口咖啡繼續問道：「你覺得競爭對手最想要知道你的什麼事？」

小潘心中竊笑，老師怎麼會問這麼簡單的問題，便立即答道：「當然是我們公司新產品開發的方向與進度，以及我們目前所用的新技術囉！」老師緊接著又追問：「平常這些資訊，你們的競爭對手有沒有辦法拿到？」小潘喝口咖啡得意地說：「我們公司門禁管制森嚴，任何閒雜人等都不能隨意進出；而且內部也有嚴格的資訊安全規定，足以確保機密資訊不會外流，競爭對手當然拿不到我們的研發資料。」

「那麼，你在研討會上準備報告什麼內容？」司馬特老師接著問。

小潘又得意地告訴老師，報告內容是公司即將推出的資安產品，這個新產品，可將聲音檔加密，且不太占頻寬，也不需要太長的加解密時間，用在電話上兼具保密性及便利性。老師點點頭

頗爲讚許小潘公司的研發能力，喝了口咖啡再問他：「如果你的競爭對手坐在臺下，他最想知道的訊息會是什麼？」小潘回答說：「當然是想知道我們是用什麼技術做到的，但我不會告訴他。」老師又問：「你怎麼知道你所報告的內容符合公司現階段的政策？也許公司並不想那麼早讓產品曝光，被你這麼一公開，競爭對手就可以提早因應了，那不就造成公司未來在市場上的損失嗎？」小潘一聽，當場語塞。「所以，這次的研發成果發表，公司之所以要求審查報告內容，其目的就是希望透過審查，能在技術面上確認資料內容無誤，並從策略面上決定資訊公開的程度，以確保公司的重要資訊不外洩，這樣才能維持產品未來在市場上的競爭力。」

小潘聽完司馬特老師的說明這才恍然大悟，原來研討會的報告還涉及公司的策略層面以及資訊保密的考量。但他馬上又聯想到另一個問題：既然成功的經驗需要保密，那失敗的經驗是不是也要保密呢？

司馬特老師十分讚許小潘舉一反三的機靈反應，繼續說道：「研發失敗的經驗也是公司投入資源的結果，包括：人力、財力、時間…等，這些也算是研發成本的投入。如果讓競爭對手輕易得知，那就等於幫對手節省研發的時間及經費，降低了他的研發成本，相對於本身在市場上的競爭力是有害的。所以，失敗的經驗當然也要保密啦！」

小潘聽完司馬特老師的這番說明，發現資訊安全並非以前想的這麼單純，原來資訊安全也是企業策略的一部分，當資訊安全跟企業策略結合後，考量的因素就變多了。所以，爲了要提高企業的競爭力，對於研發成果的發表，一定要非常小心。

師徒的這場下午茶約會，就在華燈初上時進入了尾聲。小潘又是帶著滿滿的收穫而歸，期待著下次的相聚。

（作者服務於新心科技有限公司及科技大學資訊管理系）

（本篇轉載自法務部調查局清流月刊 101 年 6 月號）

帳號密碼的安全

選用複雜度較高的密碼，且務必經常更換；在輸入密碼時勿偷懶勾選「記住密碼」，可降低遭駭客入侵風險。

◎魯明德

當資訊變成數位型式後，雖然傳遞的速度變快，有助於社會的進步，但是機密資料外洩的機率也相對增加；爲了保護數位資料的安全，大多數的系統都是採用帳號、密碼的方式，做爲把關篩選的工具。

據報載，美國佛羅里達州的坦帕大學（University of Tampa）的學生，在某堂電腦課程練習搜尋技術時，赫然發現可從 Google 上找到 6,818 筆該校的學生資料，包括學生證號碼、社會安全碼、姓名與生日等，這些資料外洩的時間從 2011 年的７月 12 日至 2012 年的３月 12 日，期間長達８個月之久，受影響的學生總計達三萬餘人。

幾乎在同一時間點的３月 15 日，世界著名的資訊安全大廠推出一種新的網路安全產品，號稱可以將會員的個人帳號、密碼，由客戶端（Client）的電腦主機移到該公司的伺服端（Server）保管儲存，要登入時可自動回填資料，如此一來，就可以減少客戶端的電腦被駭客入侵時，導致個人帳號密碼被竊的可能性。

小潘在看到這兩則新聞後，基於工作上的敏感性，很快就聯想到：我們在生活中經常要靠帳號密碼登入系統，如上班時開電腦要用帳號密碼，領錢的時候使用自動提款機也要密碼，上網寫 blog、登入 Facebook，都要帳號密碼，那麼多的帳號密碼存在不同的系統中，如果系統被駭客入侵，豈不是「全都露」了嗎？

趁著與司馬特老師下午茶的聚會，小潘提出他的疑問：資訊系統的安全大多靠帳號密碼來驗證使用者的身分，很多系統在使用者輸入帳號密碼後，下一次再登入時，會自行帶出來，方便使用者不用重新輸入，系統爲什麼會這麼聰明？

對於小潘的問題，司馬特老師喝著焦糖瑪琪朵說：當我們使用網頁瀏覽器登入系統需要輸入帳號密碼時，常因偷懶而勾選「記住密碼」，這些資料就會被系統記錄在 cookie 檔中；當使用者再次登入時，系統會自動到 cookie 檔中找到帳號密碼，以減少使用者重新輸入的麻煩。

聽到這裏，機警的小潘又提出疑問：一旦系統遭到入侵，駭客把 cookie 偷走，找到使用者的帳號、密碼，駭客豈不是可以光明正大地登堂入室、爲所欲爲？司馬特老師在喝口咖啡後，一邊稱讚小潘能舉一反三，一邊繼續說明：爲了要避免駭客入侵把個人的帳號密碼竊走，在設定密碼時，一定要選用複雜度較高的密碼，而且還要經常性更換，如此電腦較不易被駭客入侵；另外，在輸入帳號密碼時也要注意，盡量不要勾選「記住密碼」，以免增加遭駭客入侵的風險。

小潘聽後又提出新的問題：微軟的作業系統常常不受控制，自動會記錄一些 cookie，一般人又不知道它記了些什麼，要怎麼防範？

司馬特老師回答說：沒錯，微軟的作業系統會自動記錄使用者無法預期的資料，爲了避免被記錄機敏資料，危害個人資訊安全，使用者應養成定期清理 cookie 的習慣，不要讓電腦中存在著可能的危安因子。

小潘接著又想到在報上看到的網路安全產品，繼續問道：帳號密碼存在自己電腦的 cookie 中會被偷，如果放到雲端呢？因爲像有專人看守著，是不是比較安全呢？司馬特老師喝了口咖啡笑著說，cookie 中的資料是以明碼的型式存放，安全性很低；而伺服端的資料若經加密，即使是管理者，如果沒有金鑰，也無法解密，安全性相對較高。但是，資訊並不是放在伺服端就百分之百的安全，因爲解密技術的進步，駭客只需花較長的時間，雲端資料庫也有被入侵的可能性。

小潘聽完之後，頓時覺得很洩氣，感到資訊安全似乎十分脆弱。不過，司馬特老師最後提出他的看法：資訊戰其實是一場矛與盾的戰爭，不管防禦方築的牆有多高，攻擊方總會不斷地精進武器攻破城牆；既然無法阻擋敵人竊取、破解我們的密碼，最好的方式就是要經常地更換新密碼，也就是說一個密碼不能使用太久，因爲破解密碼需要花相當長的時間，即使舊密碼被破解，只要密碼一經更換，駭客就無法再登入系統竊取資料。因此經常性地更換密碼，是保護電腦不被入侵非常重要的一個觀念。

（作者服務於新心科技有限公司及科技大學資訊管理系）

（本篇轉載自法務部調查局清流月刊 102 年 5 月號）