

論述	大陸現況	法今天地	全民國防	資通安全	科技新知	健康生活	生態保育	文與藝	美麗台灣·文化領航	其他
----	------	------	------	------	------	------	------	-----	-----------	----

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。

透過文件審查避免機密資訊外洩

◎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，現在為什麼要這麼麻煩？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。老師點點頭頗為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，為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)

論述	大陸現況	法今天地	全民國防	資通安全	科技新知	健康生活	生態保育	文與藝	美麗台灣·文化領航	其他
----	------	------	------	------	------	------	------	-----	-----------	----

非法授權軟體可能內含電腦病毒、間諜軟體等惡意程式，一旦下載並經安裝，等於將這些惡意程式安裝在電腦裡。

從盜版軟體談軟體使用的安全性

◎魯晏汝

某堂課的下課休息時間，一群學生和老師正聚在一起聊天。小文突然問起小華：「上次跟你借電腦寫報告，發現你的電腦裡裝了好多不錯的軟體，應該花了不少錢吧！」小華一臉自豪地說：「當然沒有啦，現在網路資訊這麼發達，想要什麼軟體上網找就有了，而且還應有盡有，根本不用付費。」小文驚訝地說：「不用付費！這怎麼可能？安裝軟體不是都應該購買使用版權嗎？」小華看了看四周，小聲地說：「網路上有很多地方都有提供破解版的軟體，可以直接下載、安裝，完全不需要花半毛錢喔！」此時一直在旁邊聽著兩人對話的老師，終於出聲說：「小華，你知道這樣的行為涉及侵權嗎？而且非法盜版的軟體往往隱藏著很多的風險喔！」

老師趁著這次難得的機會，順便給大家一個機會教育，教導同學如何正確地使用軟體。首先，將常見的軟體使用方法分成幾大類：

一、合法授權軟體：使用者向軟體開發廠商購買產品使用權限後，開發廠商會提供產品使用序號，使用者在安裝軟體時輸入產品金鑰（Key）並通過驗證後，可以得到完整的原廠技術支援，並且定期進行軟體更新或升級。

二、共享軟體：共享軟體是一種電腦軟體的銷售模式，它提供使用者在一定的期限內免費試用，藉以評估適用與否，繼而決定是否要購買。一般來說，共享軟體一旦過了試用期限如不付費購買，即自動停止授權使用；有些軟體仍提供試用，但有較多的限制。

三、綠色軟體：也稱為可攜式軟體，多數為免費軟體，其優點是檔案小，無需安裝便可使用，可直接存放於可移除式儲存裝置（例如隨身碟）中隨身攜帶；這類軟體只占少量系統資源，使用後不需刪除或解除安裝，也不會留存登錄檔紀錄在電腦裡。

四、免費軟體：可自由免費使用，不需支付任何費用給程式開發者，使用上也不會有期間的限制。一般都是開發者出於興趣或分享的性質而提供使用，有些則是替現存軟體開發新程式或是其優化程式。

五、自由軟體：根據自由軟體基金會（Free Software Foundation, FSF）的定義，自由軟體是一種可以不受限制地自由使用、複製、研究、修改和散布的軟體。「不受限制」正是自由軟體最重要的本質，其軟體的原始碼全部開放。使用者可以自由地以不付費或是支付合理散布費用的方式，在任何時間、地點，再散布該軟體的原版或改寫版給任何人使用。

而所謂「盜版軟體」通常有幾種型態，最常見的是將正版軟體複製給未經授權的使用者使用，也有將正版軟體複製在網路上散布或是透過網路非法使用的情形；還有一些使用者雖已購買軟體版權，但超過授權數使用，例如只購買了5位使用者的授權，但實際上卻安裝在10部電腦使用，這類情形也屬於非法使用軟體。

使用非合法授權的軟體，其實隱藏著很多風險，尤其是網路上來路不明的軟體，可能內含電腦病毒、間諜軟體等惡意程式，一旦下載並經安裝，等於將這些惡意程式安裝在電腦裡。這些惡意程式可自動或被動地竊取電腦裡的資料，傳送到另一端，造成資料外洩；也能用來監控該部遭入侵的電腦，掌握使用者的一舉一動；亦可盜取使用者輸入的帳號密碼，用於其他非法用途。此外，使用盜版軟體的缺點，當然也包含不能獲得產品升級及技術的相關支援，也就是說，當軟體廠商推出產品的修補程式或更新程式時，安裝盜版軟體的使用者是不能做更新的。

以國內的企業來說，許多公司常基於營業成本的考量，在購買軟體時未足額購買授權，例如公司有30位員工，卻只購買了15個授權，並將15個授權安裝在30部電腦裡，或直接使用破解的盜版軟體。這樣的做法，除了會產生資訊安全防護上的漏洞外，更涉及軟體的侵權行為，嚴重者甚至會影響公司企業整體的營運，因此，經營者都應引以為戒。

那麼，企業主該如何杜絕使用盜版軟體的問題發生呢？首先，應設置專門人員或部門，統一負責資訊的安全管理，並訂出稽核機制來做控管。其次，應清查內部資產及軟體數量，加以造冊列管；接著再依據資產清單，定期檢核是否有未列管的資產及軟體。如有必要購買新軟體時，不宜交由各部門自行購買，應由資訊部門統一申購，此舉除方便控管外，更可選擇較適合公司的方案，為企業省下不必要的支出。至於員工部分，應於新任人員到職簽訂僱用合約時即一併簽署聲明，日後在公司任職期間，不得下載或使用任何非法盜版軟體；再則，公司亦須定期舉辦員工教育訓練，提升員工的資訊安全觀念。藉由稽核制度、資安宣導及人員訓練，方能有效地降低企業資安漏洞的風險。

聽完老師的說明，同學們個個恍然大悟地猛點頭，原來使用盜版軟體有這麼多的缺點，不僅對個人及企業的資安造成危害，更涉及侵權的問題。所以大家心裡一致決定，回家後馬上將電腦裡的盜版軟體移除，千萬別因貪圖小利而因小失大！

（作者服務於特力股份有限公司人力資源部）

論述	大陸現況	法令天地	全民國防	資通安全	科技新知	健康生活	生態保育	文與藝	美麗台灣·文化領航	其他
----	------	------	------	------	------	------	------	-----	-----------	----

一旦執法人員有了正確的工具和足夠的訓練，自然會提升破案的能力，進而使後續的調查更深入而廣泛。

行動裝置與科技偵查

◎陳銘宏

根據國家通訊傳播委員會（NCC）的統計，近五年來，第三代行動通信（3G）的用戶數逐年攀升，以今年（101）年1月份與96年同期相比，成長了5.7倍。由於3G的上網頻寬較2G為佳，加上智慧型手機的普及，行動上網已成為多數民眾日常生活的一部分。

行動網路的便利性，不僅成為民眾新寵，亦成為有心人士的犯罪新天堂。因此，行動網路儼然成為一把雙面刃，運用得宜將飽嚙科技碩果，若被惡意使用，也恐孕育為犯罪溫床，且越是普及的行動裝置，就越容易吸引不肖者藉由行動裝置的漏洞遂行其犯罪目的。

對於行動網路所衍生的犯罪，執法作為就要採取更為周延的科技取證方式，才能完整且維持原樣地得到相關的佐證內容。美國加州首府Sacramento執法當局曾在2010年做過一個小型研究，結果發現，罪犯在被警方逮捕後的60天內，其持用之手機的通訊錄名單，仍有82%的電話號碼是有效的；但若將時間拉長至180天後，則有效號碼的比率即降為40%。上述結果意味著，若執法機關能夠有效地掌握各種關鍵線索，應當很容易由某些「線頭」開始抽絲剝繭，進而勾勒出整個犯罪網絡與成員互動情形。Sacramento的研究還發現兩項有趣的現象：一、若遭逮捕的罪犯有組織犯罪背景或加入幫派，則其手機通訊錄內的電話號碼，在60天後只有57%有效，而在180天後，更只剩下16%有效。二、所有遭逮捕的罪犯，於拘留期間，至少都會與其手機通訊錄裡的25%以上人員聯繫。

對當今的執法人員而言，傳統的偵辦方式在面對新興犯罪時，已經有其侷限性，因此，一些科技偵查的手法乃應運而生。以科技辦案的觀點來看，當犯罪者逍遙法外時，行動裝置的相關證據就顯得相當重要，尤其在他們受到監禁、緩刑或是假釋時，這些證據的重要性更是不容忽視。

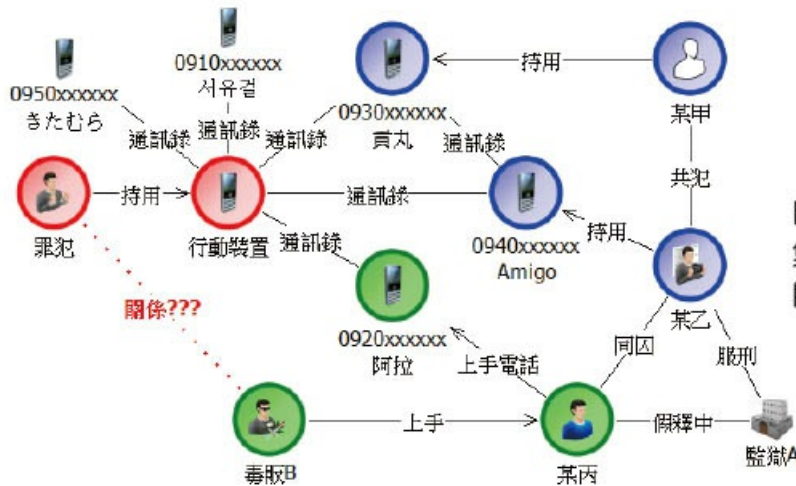


圖 1 將片段資訊匯集後勾勒出完整的關係網路

事實上，除了手機本身所能「透露」的訊息外，犯罪者也與常人無異，喜歡將手機當作社會認同（Social Proof）的工具，利用MySpace、Facebook、Twitter、YouTube等社群網站，記錄本身或屬於幫派的「成就」，進而達到招募新成員、誇耀占領的地盤、恐嚇其他幫派的成員，以及尋找新的下手目標等目的。

再者，現今的智慧型手機除了可以保存通訊錄外，還能儲存聲音、影像、SMS等內容；加上手機本身的撥打紀錄，也能協助執法人員從中找出販賣毒品、持有槍枝、不明現金等犯罪跡證，或將調查對象之虛擬世界中的「朋友」加以匯聚分析，以描繪出幫派分子的個人社交網路，並更深入了解幫派的組織架構。

換言之，行動電話的功能已不再侷限於語音及文字簡訊的傳遞，而是開創一個全新的行動社交網絡領域。由公關公司Ruder Finn的調查顯示，在行動裝置上網的使用者中，有91%會以行動裝置進行網路社交活動；他們最常進行的前五名為：使用即時通訊軟體（62%）、轉寄Email（58%）或圖片（38%）、張貼訊息至社群網站（45%）、在社群網站上與他人連絡（43%）等。此外，有62%以行動裝置上網的使用者，會透過行動網路進行相關的財務管理行為，前三名為：登入使用網路銀行（46%）、確認帳單金額或信用卡的狀態（40%）、閱讀財經相關的網路文章（33%）。

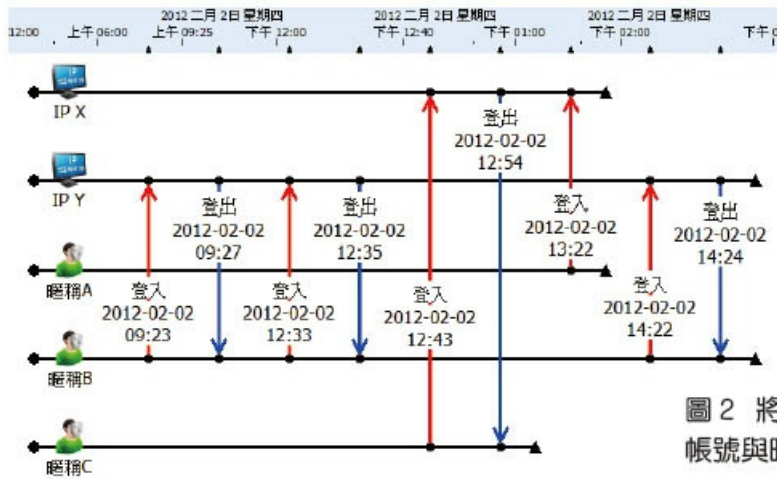


圖 2 將 IP 申裝位置、遊戲帳號與時間序列進行分析

此外，犯罪者亦會使用GPS裝置來協助犯罪網絡的運作。舉例來說，人口販子能夠定位招募者的行程和位置，並進行人口走私的活動，最後將受害者安置到工作地點。所謂「道高一尺，魔高一丈」，不僅是執法人員已經意識到行動裝置內所藏之資訊對案件調查的重要性，犯罪者也具有相同的認知。舉例來說，犯罪者開始使用由第三方所申辦的SIM卡或預付卡來隱匿他們的通訊活動。這意味單一的犯罪者能同時使用多張SIM卡來從事犯罪活動，如此將使得通話紀錄、簡訊，以及追蹤IP位置的行動更加困難。為了因應上述這些問題，調查人員需要更強而有力的工具來分析這些資料，並針對大量SIM卡中的內容進行關聯性的分析。

但不論犯罪或犯罪者的本質為何，執法人員可資依循的一項很單純的原則即是「社交是人的本性」，畢竟人與人之間的聯繫遠超乎行動裝置本身。而在社交網站中亦包含了大量關於個人的資訊、行動裝置，以及用來進行彼此聯繫和社交活動的線上網站等。因此，執法人員需要的法寶，不僅是能夠輸入並協助連結所有線索的工具，亦需要能夠支援鑑識分析的工具，例如時間序列圖和關聯圖表之建構。一旦執法人員有了正確的工具和足夠的訓練，自然會有跳脫工具本身而實際去尋找答案的意願，進而使後續的調查能夠更加深入而廣泛。

(作者為卓越動力資訊股份有限公司顧問)