在家加班真的安全嗎？

◎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；為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，認為這個 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；為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，而且為了表達自己敬業的程度，還跟主管提到為了能確實掌握進度，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為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；但也因為 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：「在企業裡為提高資訊的安全性，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，為了避免資料外洩，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，因為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）