掌握低成本高效率防禦訣竅，讓資安成為營運助力而不是阻力

商業間諜，是早期電視劇常見的角色，他們通常選擇在午夜時分悄悄溜進總經理辦公司，拿著手電筒翻找辦公桌抽屜，再拿走自己所需要的文件。不過隨著IT與網路的普及，現在竊取商業機密不必再這麼辛苦，透過惡意軟體或木馬程式，駭客不必親臨辦公室現場，就能在企業不知情狀況下竊走機密資料，台灣某知名工程顧問公司便是因此而導致公司獲利受影響。

競爭同業掌握內部資料　利潤大受影響

事情的起因源自於，該工程顧問公司在最近幾次與同業競爭客戶專案時發現，競爭同業對內部數據、報價等資料瞭若指掌，導致業務人員爭取案件不順利，在思考各種狀況後，該工程顧問公司主管最終懷疑資訊系統或個人電腦被入侵，導致存放其中的資料被盜，是最有可能的原因。

於是，該工程顧問公司開始清查各個資料外洩的可能管道，由於該工程顧問公司在各地都有小型據點或臨時據點，員工經常在外辦公，透過筆電連上公司ERP系統來取得業務所需資訊，因此最有可能的外洩管道就是ERP系統，或是員工所使用的個人筆電。

在釐清可能的管道後，下一步就是尋求外部資安檢測廠商的協助，希望找出潛藏在其中的資安風險，經過審慎評估後，決定委由中華電信進行全面檢測，而測試結果也顯示，ERP系統的權限管控機制並不完善，駭客或有心人士只要修改Cookie或調整某些頁面的參數，就可以突破權限控管，取得高階主管才能存取的機密檔案，同時不會留下任何紀錄。

三步驟強化資安防禦　以租代買更具CP值

經此一役，該工程顧問公司決心強化資安防禦能力，要求ERP系統開發商修補程式，以補強既有漏洞為第一優先。接著導入中華電信資安艦隊防火牆解決方案，透過網路端防護設備與既有防毒軟體的相互搭配強化員工上網安全。第三則是加強員工的資安意識，要求員工不要透過工作用筆電瀏覽奇怪或來路不明的網站，降低中毒、資料被竊甚至是感染勒索軟體的機會。

該工程顧問公司透露，在導入網路端防護設備時，其實有個小插曲，原本計劃直接採購硬體設備，但價格與公司預算不符，經過多方評比後，最後選擇了中華電信資安艦隊，應用機房端服務以租代買的商業模式，每月分期支付防火牆設備費用，不必一次投入大筆採購費用，而且合約期滿後，還能擁有防火牆的所有權。此外，中華電信還提供安裝設定服務，不只派工程師協助安裝與設定，還提供一套完整的使用手冊，省去IT人員自行學習的時間與成本。

低成本也能落實資安防禦

其實，該工程顧問公司就像台灣眾多中小企業的縮影，這些中小企業受限於預算、普遍不重視資安，加上早期資安風險並不像現在這麼高，導致很多中小企業主將資安視為花錢又不見成效的投資，在採購IT設備時以價格為主要考量，IT設備只要「可以運作」就好，並不會特別去思考背後的資安防禦能力是強或弱，也因此一旦遇到資安攻擊，往往毫無招架之力，最著名的例子就是2017年WannCry勒索軟體盛行時，台灣許多中小企業可說是災情慘重，除了日常營運因此中斷數小時到數天之久，有些甚至不得不支付贖金給駭客，以求取回檔案。

為了協助中小企業強化資安防禦能力、降低資安攻擊所造成的影響，中華電信特別推出資安艦隊解決方案，彙集目前市面上各大資安廠商的解決方案，經過品質、效能與穩定度的測試後，再整合成機房端服務，企業無需一次花大筆預算採購投入，只要每個月固定付出一筆費用（整合至電信帳單中），就能享有完善的資安防禦，降低駭客入侵或資料被竊的風險。

除了提供以租代買的商業模式外，中華電信資安艦隊在後續服務上也提供完整支援，包含專業工程師協助企業完成設備安裝、設定與調校作業，還有7天X24小時客服團隊隨時待命，協助企業解決使用上的疑難雜症。

此外，考量到資安攻擊手法不斷更新，中華電信定期研究最新資安攻擊趨勢與漏洞，除了資安檢測能幫企業找出關鍵弱點外，也據此適時調整防禦內容，讓中小企業能夠享有最新最即時的防禦。舉例來說，前幾年APT攻擊盛行的時候，中華電信便將APT防護解決方案納入資安艦隊服務範圍裡，去(2017)年勒索病毒肆虐時，中華電信資安艦隊亦推出檔案安心存服務，讓企業可以把資料存在經過加密的硬碟裡，降低被駭客用來勒索取財的風險。

隨著社會型態轉變，資安攻擊已經不再只是竊取資料，更多的是讓企業無法運作，像前述提及的勒索軟體，或是DDoS攻擊癱瘓企業用來服務客戶的網站（例如：線上購物網站），所以企業必須正視資安防禦的必要性，避免日常營運受到影響，而中華電信資安艦隊是專為中小企業而設計，透過彈性、專業且多元的資安服務，協助企業用低成本落實資安防禦，讓資安不再是企業的負擔，而是為品牌商譽與企業經營加分的利器。