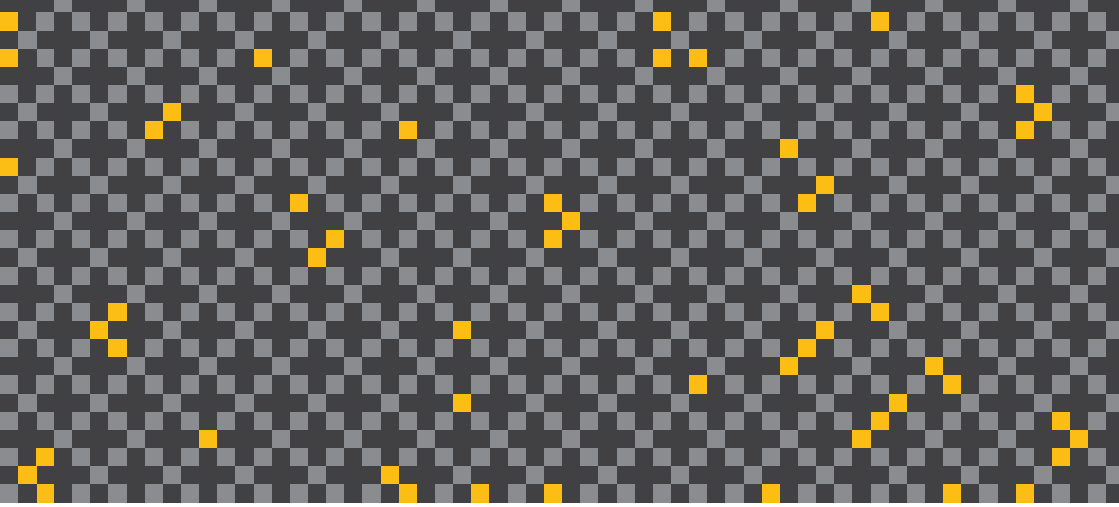
www.pwc.tw

數位轉型下的資安與數位鑑識

pwc



序言

創新科技對企業帶來不同程度的衝擊，過去壁壘分明的產業疆界已經開始逐漸模糊，面對如此快速變化的科技創新，許多企業也加速進行數位轉型，期能接軌國際。依據瑞士世界經濟論壇(WEF)「2018 年全球競爭力報告」，臺灣排名全球第 13，其中更在「創新能力」排名第 4，主要係在專利權數量、研發支出占GDP之比重、產業群聚完善發展的普遍程度等項目表現優異。

有鑑於此，面對數位化時代來臨，企業要在劇烈產業競爭中維持主導及優勢地位，提升資訊安全危機意識及強化核心資訊保護，是數位轉型下企業的必經之路。

資訊保護有三層境界：先知先覺、後知後覺、不知不覺。當企業因數位轉型而對資訊科技仰賴日深時，面對無所不在的駭客攻擊及經濟犯罪威脅，企業如何在侵害尚未開始前就先進行防禦甚至反制，應從改變資訊保護思維開始。合理的資安管理思考、重視威脅情資及從數位鑑識角度出發重構資安策略等方式，是企業減少事後的衝擊影響及防止損害擴大的要素。

本手冊以資訊保護為核心，提供數位轉型下的資安新思維，從資訊安全、數位鑑識、營業秘密及個人資料保護視角切入分析，期勉企業在攻防成本不對等的情況下，將有限的資源投注在最關鍵的地方，成為數位轉型浪潮下的真正贏家。

目錄

前言

科技改寫了人類的生活樣貌，也為全球企業競爭帶來了變數。當臺灣企業競相投入數位轉型浪潮時，每一個想在這個數位時代抓住成長契機的企業，莫不期待從數位科技帶來的新商業模式及服務中，建構數位創新的藍海商機。

智慧製造、大數據分析、區塊鏈、Fintech、物聯網及人工智慧等數位科技全面改寫既有產業競爭規則，企業投入數位轉型的緊迫感正在上升，同時也讓另一批新創企業藉由這些顛覆性的科技進入市場。這些沒有過去成長包袱的新創者得以用更有效的科技技術、更廣泛的資源及更低的成本，突破競爭壁壘進入原本無法企及的領域，使得既有企業遭受極大的衝擊。當企業無法再安享產業優勢帶來的超額利潤時，變革成了許多企業的必經之路。

資訊科技整合運用是數位轉型關鍵，但不僅止於將資訊科技融入企業各營運層面，更重要的是運用策略性的思維將其轉型為智慧型企業，即時掌握數據以利決策制定，讓企業能更靈活且精確地適應全球市場變化，洞悉新商機。

數位轉型是一條沒有回頭路的單行道，一旦變革開始，企業營運對資訊科技的仰賴會逐漸加深。當企業發現資訊科技能讓他們有更多機會接觸新客戶、開發新產品或服務，並且提升資源和資本的分配最佳化時，企業會開始樂於享受資訊科技帶來的優勢，且願意進行更多投資。

從數位轉型浪潮中，可以看出幾個隱憂：

第一、面對新興技術，企業不一定有自身能力可掌握

外包在數位轉型需求下非常普遍，實務上企業將開發過程外包，安全規格和要求卻很少寫清楚，主要是功能正確，迅速完成就好，且招標過程很難對顧問於資安的投入進行衡量，於是招標結果往往是價低者得，再加上市場上有資訊委外服務人員計價得以參考，在節省成本考量下，資安就像被秤斤論兩的商品，與硬體一體適用評選流程。這樣的心態與作法，如何能期待資安能落實於整個數位轉型過程中？

第二、全球對經濟犯罪威脅的擔憂提升

即使資訊科技將世界更緊密連結，如區塊鏈及人工智慧連結了過去不曾想像過的應用，這些顛覆性的創新雖然改變了競爭格局，但也加深企業對資訊科技整合運用的隱憂。

2018 年世界經濟論壇之全球風險報告指出，可能性最高的十大風險中，「網路攻擊」及「數據詐騙或數據盜竊」分別排名第三及第四，僅次於極端氣候及自然災害。值得注意的例子包括肆虐全球的勒索病毒如WannaCry和NotPetya，導致一些受影響企業每季度虧損 3 億美元。在臺灣，PwC「2018 年全球經濟犯罪調查」結果顯示，惡意軟體攻擊(46%)成為臺灣企業最常遇見之威脅，遠高於全球(36%)及亞太區(33%)之統計結果。而網路釣魚攻擊穩居第二，其對企業的威脅不容小覷。

第三、儘管有資安危機意識，許多企業仍未做好準備

企業要維持競爭優勢，防範各種來自內外部的威脅則是成功轉型不可或缺的先決要件。然而，PwC「2018 全球資訊安全調查報告」指出，全球有 44%企業沒有完整資安策略、48%缺乏員工資安意識訓練計畫，及 54%缺乏事故反應流程。雖然網路攻擊非常嚴重，但PwC「2018 年全球經濟犯罪調查」結果指出，36%的臺灣企業不認為它們會成為網路攻擊的目標，或不知道是否成為網路攻擊的目標，顯示臺灣企業資安危機意識的提升，還有很大的進步空間。

數位轉型下的資安思維

可以確定的是，資安威脅會隨著數位轉型的深化持續對企業帶來紛擾。在現實社會中，瞬息萬變的政經局勢牽引著市場變化，例如企業在劇烈產業競爭中維持主導和優勢地位的關鍵要素–營業秘密，成了企業領袖感到焦慮不安的因素。尤其，近年來臺灣相繼發生許多知名的營業秘密外洩事件，讓許多企業膽顫心驚，擔心自己會成為下一個受害者。面對數位化時代來臨，企業如何從紛擾的局勢中找到方向？資安思維又該如何調整呢？

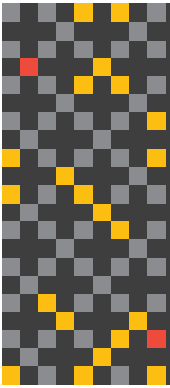
資安是數位轉型先決要件

企業的研發模式及人才策略隨著數位時代來臨將為之改變。根據PwC在 2017 年 10 月公布的「2017 全球創新一千大企業調查」，全球創新一千大企業的研發費用高達 7,016 億美元，創下歷史新高。臺灣 2017 年共有 31 家企業入榜，總研發經費達 3,987 億新台幣，較 2016 年增加 59 億新台幣。

研發是企業累積競爭優勢的重要基礎，與國際市場互動緊密的臺灣企業，自然深刻感受到來自競爭對手的威脅與日俱增，研發成果及智慧財產的覬覦也導致各種資安議題如惡意挖角、內鬼、洩密、駭客入侵等威脅層出不窮，成了許多臺灣企業揮之不去的夢魘。因此資安成為企業數位轉型中必然面對的議題。

合理的資安管理思考

在臺灣，隨著資安威脅益發精微複雜，企業逐年提高資安預算比重，自然也希望資安資源規劃與配置能發揮最大效益。合理的資安管理就是解決「企業想的」與「威脅者想的」之間的差異：沒有釐清兩者差異，將造成許多資源與時間的浪費，這也是近年來資安事件頻傳的原因之一。

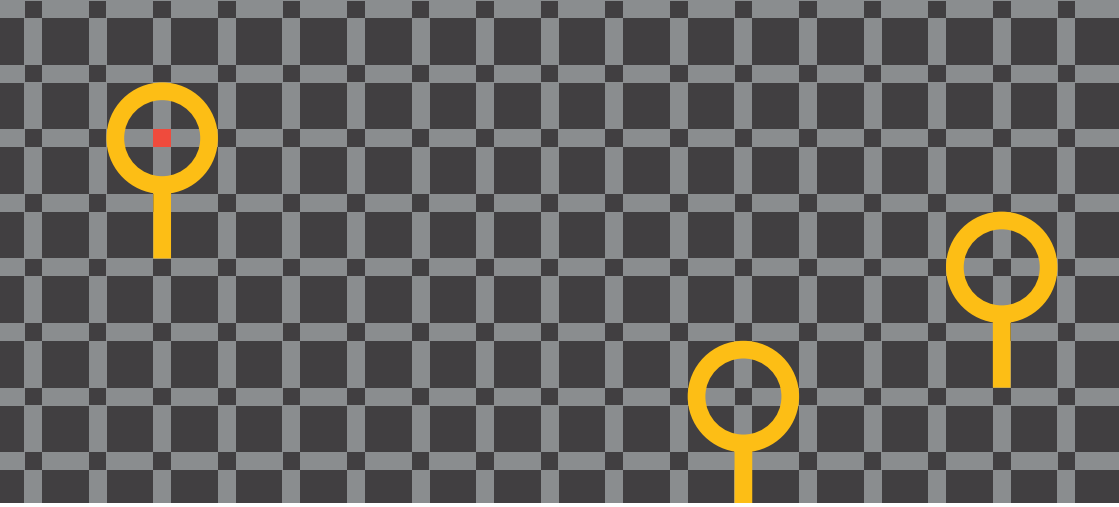


從威脅者角度思考，了解其想法及作法十分重要，企業愈能掌握狀況，就愈能把資安資源做合適投入。企業的資安管理可參考以下三大重點：

1. 對維持競爭力的關鍵是什麼？
2. 對威脅者來說什麼是重要的？
3. 可能之入侵路徑有哪些？其傳遞/擴散情形如何，及其保有者與接觸者情形如何？

威脅者重視什麼，就保護什麼，威脅者不重視的，就表示資安資源可以轉向。在與競爭對手較量過程中，市場占有率、客戶滿意度、獲利能力和發展水平等通常是競爭力的參照項目。企業必然知道維持其競爭力的關鍵是什麼，而支撐這些關鍵競爭力的綜合優勢，如客戶資料、配方、人才、研發成果等，通常也是威脅者最感興趣的標的。盤點維持競爭力的相關資產，計算其財務損害價值、信譽損害價值及負面監管衝擊，評估其發生頻率及與現有控制成熟度之差異，並對其進行分級及分類，是合理資安管理的第一步。惟有找出「皇冠上的寶石」，企業才知道資安資源應該投入的方向。

在資產分級分類過程中，「知識外顯化」是資安管理重要觀念。如果知識(如營業秘密)只藏在知悉者腦袋中，必然會隨著知悉者的異動而對企業營運產生巨大風險。知識沒有外顯化，例如沒有透過資料檔案、電腦程式或任何其它形式分類記錄儲存，資安必然無法使力，一旦遭到竊取或主張不法取得，會有不易察知及界定的風險，再加上客觀的侵害事實鏈無法彰顯，必會讓企業陷入苦戰。



維持競爭力一直是企業努力目標，也是臺灣得以躋身國際產業主流位置的關鍵。然而，資訊科技獲取不法利益的便利性及危害性，隨著企業加速數位轉型的步伐而大增。威脅者因同業競爭、地緣政治等因素，必然想方設法透過利誘、脅迫、入侵等方法取得企業的關鍵資產－皇冠上的寶石。這些「寶石」若無法集中監管，其目前所在處必然要進行妥善保護。企業要思考的是，威脅者究竟會透過哪些路徑獲得寶石？

資安有三境界：

不知不覺 >>> 後知後覺 >>> 先知先覺

先知先覺者，站在威脅者角度思考並窮盡辦法找出攻擊路徑，在入侵尚未開始前就先進行防禦甚至反制；後知後覺者待資安事件發生後才亡羊補牢；而不知不覺者是資安事件發生了還不知曉，仍以為企業資安系統運作安然無恙。

「沒有攻不下的城牆」，尤其是近年來一向給人資安防護森嚴印象的國內外金融銀行機構及晶圓代工龍頭相繼淪陷後，資安無法做到 100 分的觀念，更被廣泛理解。

通往寶石的路徑有哪些？有哪些路徑過去不通，現在被發掘出來了？所需的技術為何？是否對既有資訊系統造成影響？數位時代來臨，資安再也無法閉門造車，企業一定要走出去，看看外面的世界發生了什麼事，有哪些新的資安漏洞被駭客使用，企業既有系統是否存在相同漏洞而造成隱患。駭客技術變革的速度，是企業應該關心重視的。

威脅情資帶來資安觀點改變與衝擊

資安是一場永不完結的攻防戰役。《孫子．謀攻篇》說：「知彼知己，百戰不殆；不知彼而知己，一勝一負；不知彼，不知己，每戰必殆。」企業透過社交工程演練、定期執行弱點掃描、滲透測試及內稽內控等措施花了很多時間了解自己，也因此用了很多資源強化資安防護，但很多企業卻不了解敵人，不知道敵人在哪，也不了解敵人的攻擊手法。一些企業在強化資安的當下，如同在黑暗中摸索前往，不知道威脅者現況而一昧築高城牆以求心安。但前景絕非一片悲觀，不少企業也從中看到了曙光–資安威脅情資所帶來的防禦觀點改變。

威脅情資之使用可分為兩大類：第一類是透過情資資訊的轉換提升被動防禦的效果；第二類是企業因應數位轉型所產生的資訊架構改變及關鍵資產的保護所需，而積極消化威脅情資背後的資訊，找出真正的敵人及其戰略目的。

對許多企業而言，威脅情資不外乎是資安廠商持續收集整理各種威脅情報，並將這些情報轉換為一系列可以被資安設備使用的資料，如IP及網域黑名單、檔案雜湊值等，再派送到資安設備進行攻擊攔阻，這些做法對企業而言，是再熟悉不過的。但是僅僅依賴以開發與銷售產品為主的資安廠商提供制式情資，很難兼顧資安品質。這也是為什麼相關的情資已持續部署到資安設備，資安事件如駭客入侵及惡意軟體攻擊依然層出不窮的原因。化被動防禦為主動回應，才是資安威脅情資最可貴之處。

駭客攻擊改寫了資安防禦的面貌，由駭客的思維、目標及手法所構成的攻擊策略中，歸納整理找出真正攻擊者，進而了解其背後的動機，用以評估未來企業本身是否將成為被攻擊的目標，是威脅情資最有價值之所在。例如從 2013 年迄今，多家銀行因SWIFT系統被駭客入侵而造成損失的事件就可以了解發生在他國的資安事件，很可能在轉瞬間就對企業造成傷害。世界因資訊科技而變得更平坦，企業的資安觀點可透過威脅情資而改變，醞釀中的資安弱點也因威脅情資而得以提前被識別及防範。

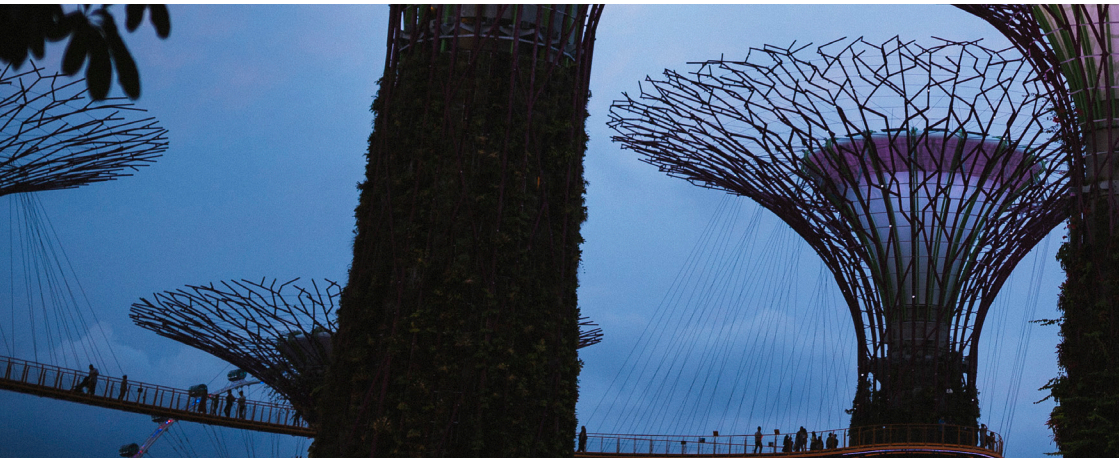
簡而言之，資安風險就是外在威脅利用內部弱點對資訊資產造成損害的可能性。而駭客所共用的一個策略，就是找出企業的弱點並加以利用，企圖竊取企業皇冠上的寶石。對企業而言，解析並「消化」外部威脅情資背後所帶來的資訊，並將之與企業內部可能發生的威脅狀況進行分析比對，主動發掘潛在之入侵路徑，積極監控、回應、學習並應用相關知識對抗威脅者，才是確保進化到先知先覺的關鍵。當找到通往寶石的路徑後，資安管理就可以做出不一樣的思考：如何將入侵路徑所蒐集到的侵害跡證轉變成訴訟可使用的證據。

不可或缺的數位鑑識

覬覦企業關鍵資產的威脅者除了駭客外，還包括內部不肖員工。現實世界中，對企業關鍵資產感興趣的除了駭客外，競爭同業及企業內部的不肖員工也是威脅企業資安的重要來源。因激烈競爭而惡意挖角對手員工攜帶重要資料跳槽事件，或員工因為意識到機會、壓力及自我合理化藉口而產生的舞弊事件，已成了企業的日常。

企業經營首重誠信，從事商業行為過程中，做出違反誠信、不法或違背受託義務等行為將嚴重傷害企業形象甚至其獲利能力。因為個人利益而涉及經濟犯罪案件的員工數量，近年來有逐漸上升的趨勢。PwC「2018 全球經濟犯罪調查報告」指出，有 52% 的經濟犯罪案件來自於內部員工，較 2017 年的統計數據上升了 6 個百分點；而來自於中高管理階層的經濟犯罪案件，更從 2017 年的 16%，一舉躍升至 2018 年的 24%。相較於來自外部的威脅如駭客入侵等，這些內部威脅對企業造成的破壞更為嚴重。調查結果顯示，臺灣問卷回覆者所經歷最具破壞性的經濟犯罪中，有 68% 係由內部人士犯下，且該內部人士中有 79%為中高階的管理階層。內部不肖員工因為熟悉資訊環境，故可能透過一些更隱密的途徑侵害企業關鍵資產。企業在分析入侵路徑時，除了駭客考量外，資訊如何在其內部傳遞、擴散，以及其保有者與接觸者情形如何，也是必需納入考量的重點。

這個最壞的時代，或許就是最好的時代。在數位轉型過程中，有不少企業開始注重經濟犯罪的偵防，例如加強在電子郵件監控及入侵事件通知規則強化等投資。然而，被動式防禦無法在案件發生時帶來震懾力量，結合數位鑑識，做好證據保全，在必要時可透過司法維護自身權益，資安投資才能發揮最大效益。



證據保全

科技犯罪隨著數位轉型深刻影響企業的營運及發展。相較於傳統犯罪，科技犯罪的成本及門檻較低、具跨區域性、隱匿性及有偵查不易等特點。資訊科技雖然帶給企業極大的便利性，同樣地也提供了許多合適的場域給威脅者。因科技犯罪本質上較不易遭察覺，故證據保全成了事後追究責任的關鍵。

所謂「凡走過必留下痕跡」，客觀的侵害事實鏈，就是入侵路徑上所留存的跡證，用以支持或排除犯罪假設。企業能否在事故發生前就確認關鍵資產所在處，以及通往這些關鍵資產的可能路徑所留下的數位跡證是否被妥善保全，是鑑識分析重要的憑據。因處理不當而導致唯一的證據遭受破壞和污染的案例層出不窮，企業必須高度關注此一風險。

建立有效的數位證據保全作業是往後鑑識分析重要的基礎。當資安事件發生後，企業首要維持現場的完整，確認關鍵資產遭到侵害的項目名稱及其存放處。所謂的證據保全標的物，係指通往關鍵資產的路徑上所留下的數位跡證(如系統日誌)，以及往外的傳遞與擴散路徑上的跡證。透過分析這些數位跡證，將有助於釐清嫌疑人、其犯罪手法與時間。如果嫌疑人為內部員工，必要時會對該員工持有的個人電腦、外接式儲存裝置等資訊設備進行證據保全，分析釐清關鍵資產從該員工往外的傳遞及擴散情形，以及與該員工接觸的其它涉案人員等。鑑定遭損害途徑是進入司法程序前的重要目標。為了避免證據遭蓄意湮滅，保持低調進行事前蒐證並做好證據保全，是提升鑑定結果效力的關鍵。

必需提防的證據湮滅行為

如同毒品嫌疑人看到警察臨檢時選擇逃跑、倒車迴轉、丟棄證物等一樣，偽造、變造、湮滅或隱匿犯罪證據，是科技犯罪者試圖規避法律責任的常見行為。以震驚國內的首宗國際駭客集團盜領案為例，駭客犯案後刪除工具程式及相關資料已是慣例；同樣地，內部威脅者一旦發現其不法行為已引起警覺，人性使然必會開始滅證或向同伙通風報信，增加鑑識分析的難度。

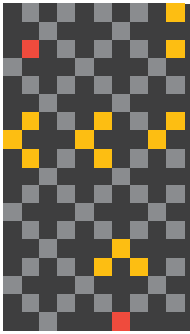
PwC「2018 年經濟犯罪與舞弊調查」指出，臺灣的舞弊/經濟犯罪案件有 55% 透過既有之公司內控機制發現，30%經由執法機關通知、新聞報導等外部管道發現，僅有 15%係透過舉發或吹哨而揭露。然而，一般內控措施(如：例行及非例行性之內部稽核、可疑活動監控、實體資產、商業資訊系統保全/防護措施等)無法持續、有效地預防及偵測舞弊行為，主要原因包含：

1. 多數舞弊涉及裡應外合的共犯架構以隱藏犯罪行為並躲避偵測；
2. 多數的舞弊源自掌握機密內幕並擁有可規避相關控制措施決策權之內部人士。

是否有共犯及高階管理層涉案，是舞弊案調查必須謹慎處理的事。企業應在初期採取暗地調查求證的方式，並妥善保全相關的數位證據；一旦確認涉案，主動提告進入司法程序後，所保留的資料將可成為有力的證據。

以下四大注意事項可降低證據遭到湮滅的機率：

1. 在掌握充份證據前，調查應保持低調，避免打草驚蛇；
2. 對重要資料如日誌等做好安全備份及管控；
3. 從威脅者角度思考會如何滅證，並做好反制措施；
4. 必要時越級舉發，以維護公司權益。



除了思考證據保全及證據遭湮滅的議題外，企業還需要關注以下幾個問題：

1. 是否有證據被忽略了？
2. 這些證據能證明什麼？為何不能證明什麼？
3. 為什麼會發生上述這些情況？

儘管企業對資安問題的關注度提高，但上述這些問題顯然被擺到事情發生了才會引起關心的階段，而很多時候，這已經太遲了。要解決上述問題，企業必須一開始就從「事後」數位鑑識追究責任的角度，思考全盤的資安布局是否經得起資安事件發生後的考驗。如果投資的資安防護措施無法在事後至少提供追究責任的能力，從「資安事件終將發生」的面向來看，這些資安投資終究是浪費了企業的人力、物力、成本，意即，威脅者一定進得來，而企業卻無法在事後有反擊能力，例如取得足夠的證據追究法律責任。

當企業邁向數位轉型以建立新競爭優勢時，資安觀念也必須隨之轉型。從嚴謹的事後數位鑑識角度來看待事中及事前的資安問題，企業將可重新思考其資訊安全策略，是否能在「資安事故終將發生」的現實中，提前做好最妥善的準備。

資安觀念的改變
從數位鑑識角度重構資安策略

從許多實例來看，資訊安全有其限制，安全防護結果絕不會如此單純往企業所想像地發展。在談及企業所經歷的資安挑戰時，有 46% 的臺灣企業認為惡意軟體攻擊是最常遇見之外部威脅，遠高於全球及亞太區的統計結果。在問及所經歷最具破壞性的經濟犯罪中，有 68% 係由內部人士犯下，且該內部人士中有 79% 為中高階的管理階層。調查結果顯示受訪之企業領袖對於內外夾擊的資安壓力感到極為沉重。而在每個資安事件的背後，都代表著企業誠正經營的文化已被追求私利的威脅者所扭曲。

現實世界中，「資安事故終將發生」已成為普遍認知，訴訟成為企業終將面對的事實。整合資安與數位鑑識，讓證據可以說話，從而彙集改善各層面資安防護弱點，是企業因應新局重構資安策略的發展方向。而這一切，應從「讓證據可以說話」開始。

以下三個問題是資安事件發生後，企業首先會關注的問題：

1. 事情怎麼發生的？　2. 損失有多少？　3. 誰該負責任？

尤其，當企業必須依事故的嚴重性及複雜度組成緊急應變小組進行損害控制時，這三道難題能否快速獲得解答十分關鍵。這些都需要「證據」，如果沒有在資安事故發生前做好妥善準備，這顯然是個難解的題目。「資安事故緊急應變演練」可協助企業檢視既有資安防護成果能否解決這些問題。

事後—資安事故緊急應變演練

再強大的防護，威脅者總可以找到漏洞。當發生資安事故後，企業的緊急應變應注重「點、線、面、體」的遞次推進，即首先在「點」上找到事故本體，進而由「點」及「線」找出相關連串可能遭受影響的系統，由「線」到「面」分析系統間的互動是否隱藏未被發掘的問題，最後由「面」到「體」分析組織管理、物件及人員的風險處置方法。

要從「點」找到事故本體，企業首先要知道企業的關鍵資產－皇冠上的寶石位在何處，然後由「點」及「線」知道通往寶石的路徑，即可找出相關連串可能遭受影響的系統。這些相關連串系統上的跡證，如日誌等，即是事故緊急應變演練要驗證的標的物：即所留存的跡證，是否能重建犯罪經過？告知企業所造成的損失？及得知誰該負責任？

如果所留存的證據無法提供足夠的情報，讓企業研判情勢，找出正確的戰略及戰術決策以進行損害控制，將危機化險為夷，這樣的資安策略需要從根本上檢討問題何在，包含：是否所留存的證據廣度及深度不足，還是「線」到「面」存在其它隱藏未被發掘的問題，如尚未被發現的弱點或入侵路徑等。這些都是企業可以在真實資安事件發生前解決的議題。在事故回應的時效壓力下，應變過程之風險處置是否妥當十分關鍵。降低風險及減少事後的衝擊，組織管理、物件及人員的風險處置方法，是從「面」到「體」所關注的目標。資安防護無法一廂情願，從事後的證據有效性出發，企業才能知道一旦發生事故後，平時所依賴的資安措施是否可以成為舉證的利器。

緊急應變計畫成功實施關鍵主要有三項：

1. 企業經營者必須非常重視事故發生的「點、線、面、體」之間的密切關係，方能從單一事件一窺事件全貌，從根本解決問題；
2. 緊急應變小組所有成員對事故背景及內容有深刻認知，並對事故應變程序有正確的理解；
3. 事故緊急應變是企業治理的一環，需要因地制宜方能取得最大效果。

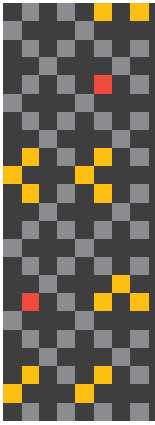
隨著資安威脅提升，企業在事故發生後所付出的代價將越來越高，若能在事件發生的當下就及早警覺並處理，將可降低損失。

事中—事故偵測

相較於其它國家，台灣企業使用監控技術來偵測網路攻擊或弱點的比例最高，但是大部份僅止於防範來自於外部的威脅。因員工忽略而開啟惡意郵件或惡意連結導致的入侵事件層出不窮。

過去許多企業一直通過在其網路的邊界建立防禦措施來試圖保護網路安全，這種傳統的策略是盡可能強化邊防，同時假設他人無法穿透防火牆。但是這種「外在」的方法是基於企業可以明確地控制網路進入點。然而，企業內部網路通常由非安全感知的設備組成(如交換機、路由器、橋接器等)，其網路是非常平坦和開放的。因此一旦駭客突破防火牆進入內部網路，那麼駭客就可以任意訪問整個企業網路，包括所有有價值的資產，且不容易被發現。

居心叵測的內部員工，因熟悉內部資安防護措施與作業流程，其對企業的傷害更甚於外部威脅者。這些員工的可疑網路行為能否提前被發現而做好隱密監控，是企業避免重要資產如營業秘密遭外洩的關鍵。



隨著組織規模日漸複雜，企業無法得知惡意郵件或連結何時被點擊開啟，也難以知道哪些員工圖謀不軌，因此企業應轉而評估目前整體防禦能力的現況，包括：

1. 既有的資安防護偵測架構，是否能有效阻擋威脅者？
2. 被入侵後能否阻擋機敏資料外洩？
3. 現有資安設備偵測機制是否符合要求？
4. 資安事件通報處理機制是否有啟動？

雖然臺灣企業持續投入網路攻擊的監控，但對於威脅者在內部網路的行為偵測，尚有待努力加強，例如：

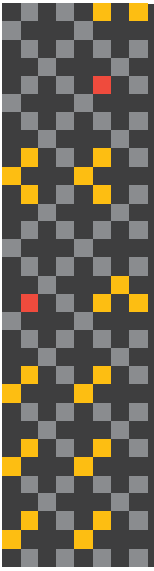
1. 當惡意程式或連結被開啟時，既有的偵測及反制能力如何；
2. 當惡意程式在內部網路掃描及橫向感染其它主機時，是否會引起警覺；
3. 駭客試圖往外建立連線時，是否會被發現；
4. 當機敏資料遭外傳時，是否會被攔阻等。

必須體認的是，企業投注了很多資源在建構一個完善的防護機制，然而這些防護機制在真正事故發生時是否奏效、資安人員是否有足夠的警覺、緊急應變計畫是否如實執行，與企業在事後所需付出的代價息息相關。

企業對事故偵測的能力有多少，取決於對威脅者的手法了解有多少。經驗豐富的鑑識團隊可從威脅者的角度來看企業的運作是否存在可被利用的弱點，並且可能透過何種手法規避資安偵測，有助於提升企業在事發當下的事故偵測及反應能力。

事前防禦

不可否認的，臺灣企業在事前的防禦與事後災害復原機制都已經相當成熟。然而在災害復原前的緊急應變還有相當大的進步空間。如能注重「點、線、面、體」收集並檢視既有的風險處置方法是否妥善、入侵跡證是否能回答事故發生的原因、所造成的損失及該負責任的人，並從事故偵測角度評估威脅者可能使用的策略、技術和程序，進而了解目前整體防禦能力的現況，將有助於企業針對皇冠上的寶石，設計主動安全措施以保護敏感的企業資產。



企業應考量的方向包括：

1. 從人力資源、資料流通、資訊作業及實體環境管控等層面，因地制宜設計主動安全措施以保護敏感的企業資產，並適時保存所留下的資料軌跡。

2. 員工教育訓練與機敏資料保護文化的養成。員工的資安意識是防護機制成敗的關鍵，企業應認知惟有組織上下一體了解關鍵資產保護攸關企業與員工的切身利益，方能養成企業資安的保護文化。

3. 以企業關鍵資產保護為目標帶動績效管理方向，設定部門整體與個人績效指標，從結果產出、行為表現及事故應變演練等面向，進行目標績效管理與追蹤，並適時回饋改善。

營業秘密法及個人資料保護法的視角

概述

數位時代的資訊流通更為簡易快速，企業對於自身資訊的流向也更不易查知，產業界因此意識到資訊保護的重要性。然而，企業應如何辨識資訊的性質、掌握資訊保護的目的，以及如何針對不同性質的資訊提供不同程度的保護，則是企業要採取資訊保護措施應評估的前提事項。

資訊保護的目的

企業對於所持有的資訊應如何進行保護，基於該等資訊的來源與性質不同，可從二個不同的法律視角進行觀察。其一是企業自身產出或基於契約關係合法自其他企業取得的營業祕密相關資訊，此類資訊是企業依自身營運需求所研發或自外部取得的資產，因此，在此視角下，企業當然會基於確保自身資產不受他人以不當方式取得或接觸，以避免導致資產發生價值減損的不當影響之目的，致力於建立一妥善而完整的保護制度；其二是企業在營運時可能會直接或間接蒐集到來自終端消費者的個人資料，此類個人資料並非企業的自有資產，但企業會基於營業流程而取得相關資訊，且必須依照個人資料保護法等強制性規定，採取符合法定要求門檻的個人資料保護措施，以避免消費者的個人資料遭洩漏或被濫用，進而導致企業可能需負擔違反營業秘密法及侵害消費者隱私權之責任。因此，在此視角下，企業會基於法律遵循的要求，建立一符合規範門檻的最低標準保護制度。

換言之，企業對於營業秘密此類資訊的保護，是出於自發的保護自身資產，則在符合成本效益的前提下，企業即願意採取高規格的妥善保護措施；然而，企業對於個人資料此類資訊的保護，則是基於外來的法律強制要求，企業當然只願採取符合法律要求的最低保護密度。因此，資訊的性質將影響企業所採取的資訊保護措施強度。然而，附帶言之，在數位經濟的科技演進衝擊之下，各國主管機關已發現個人資料的保護越來越不容易，從而，各國所要求企業須採取的個人資料保護措施強度，均有日漸上升的修法趨勢。

資訊保護的方式

完整的資訊保護，不僅僅是來自企業IT部門提供的資訊安全技術保護措施，還需要依據企業整體營運策略建立完善保護制度，並將制度精神內化至企業文化之中，藉以落實保護機制。除了過往較為人知的資安技術層面之外，尚可分別由組織面、制度面、流程面等不同面向切入觀察：

首先，在組織面，要落實資訊保護制度，涉及企業集團組織的所有內部人員及外部合作夥伴等不同對象，因此，資訊保護不僅僅只是資安部門的責任，而是所有利害關係人都參與其中，企業將資訊保護的執行單位置於何階層，也影響了企業如何看待資訊保護的重要性。例如，董事會是否瞭解公司對於資訊保護是如何落實以及整體執行情形，有無專職專責的資訊保護單位，如何統籌內外各單位的資訊保護需求及規劃。

其次，在制度面，應如何制定資訊保護的相關制度，並確保落實執行，能將制度精神內化至整體企業文化中，亦為重點。資訊安全技術的導入僅能防止外賊，但是享有資訊優勢的內部人，即難僅以資訊安全系統防止其不當取得企業營業秘密等重要資訊，此即為建置完善資訊保護制度之目的，也就是如何將資訊保護的重要性深植於企業管理者及其他內部人員之認知，並確保各相關人員的遵循及落實。

再者，在流程面，企業內部作業流程都應該考量資訊保護所可能產生的衝擊，在工作流程、系統開發、產品設計或其他上下游供應鏈等合作廠商之間的作業程序中，均應預先考量如何滿足資訊保護原則的設計目的，也就是在流程設計之初即內建「始於安全的設計」或「始於隱私的設計」(Security by Design/Privacy by Design)的保護機制，而不只是倚賴事後追溯性的資訊安全稽核作業，而上開「始於隱私的設計」也是現行的歐盟一般資料保護法規 (GDPR)所導入的核心要求。

基於上述，企業要完善資訊保護機制，除了傳統認知應購買先進之資安軟硬體設備外，尚必須著重於制度的建立、文化的養成、流程的規劃與組織的調整等面向。然而，不論是何面向的機制建立都要投入資源，在資源有限的現實之下，企業可以先辨識主要所面臨的資訊安全風險為何，再行擬訂以風險為導向之資訊保護管理策略，判斷資源投入的優先順序。

資訊外洩的亡羊補牢

關於營業祕密的保護

營業秘密外洩對高科技企業造成的傷害甚鉅，如何有效防患營業秘密之侵害於未然，是企業治理的嚴峻課題。營業秘密外洩的風險雖可能來自外部（例如駭客入侵），但更多時候是因企業內部人員的故意或過失所導致，因此，企業應認識營業秘密暴露的風險源，並採取符合成本效益的保密措施，防患未然；而在面對營業秘密流出事件時，應及早警覺並處理，避免損失擴大。

1. 事前預防機制的建立

   要談營業秘密的保護，首先應釐清的是，究竟甚麼樣的資訊屬於「營業秘密」。「營業秘密法」所保護的營業秘密，係指非一般涉及該類資訊之人所知的資訊，即具有所謂的秘密性；而且該資訊必須因其秘密性而擁有實際或潛在之經濟價值。最重要的是，秘密的所有者必須依實際情況盡合理之努力，對其認知的秘密資訊，採取合理的保密措施。因此，如從營業秘密法的角度架構保護策略，即應聚焦在「事前預防」上，亦即合理保密措施及制度之建立，而事後的停損與舉證，其實也是繫諸於事前保密措施及制度建立的完善性。

   建立預防營業秘密外洩的事前保密措施，亦如前述，大致可分為組織性、制度性、流程性及技術性。例如，擇定適當的營業祕密管理者，以誘因機制將秘密持有者的個人利害與公司相互連結，將可較有效的避免營業秘密所託非人；確保營業秘密資訊的建檔及儲存，促使員工落實工作或研發日誌的填具；採取合理妥適的保護措施，如防火牆、專門電子傳輸通道、資料庫權限限制，以及採取充分的教育訓練、引入監督稽核或獎懲機制等。企業若能識別風險來源並預先建立保密措施，在營業秘密保護上，即能獲得事前及事後的雙重保護效果。此外，企業也應致力於營造維護營業秘密的組織文化。在管理制度成形之後，透過定期稽核及檢討會議等，形成營業秘密保護的風氣，進而落實對營業秘密的保護。

2. 事後處理機制 - 停損及舉證

企業面對營業秘密的流出，首要工作當屬避免損害擴大。透過檢調機關的法律手段，如搜索扣押、限制出境等，可能達到某種程度的停損，並有警惕作用。但企業想要促使檢調機關發動該等手段，至少必須提供檢調機關一定的資訊，例如營業秘密之內容、使用情況，以及可能的洩密管道等，則事前預防機制落實到何程度，將會決定企業可舉證自身享有的權利範圍為何，以及促使檢調機關發動偵查的機率高低。此外，高科技資訊對於檢調人員來說可能較不易理解，故有必要透過企業內部人員與外部律師間溝通配合，協助檢調人員釐清案情，加速檢調機關偵辦的速度。

關於個人資料的保護

何謂個人資料，各國法令或有範圍不等的定義，大致而論，能藉以直接或間接辨識個別自然人身分的資料即屬個人資料，如姓名、護照號碼、聯絡方式等。數位時代下，個人對於自身個人資訊遭企業蒐集處理利用的情況，實不易掌握，因此，為確保隱私權的保護，各國主管機關紛紛透過個人資料保護法規強制要求企業依法蒐集處理利用個人資料，企業因此負有保護個人資料的義務。

1. 事前預防機制的建立

個人資料並非企業的資產，企業之所以需要保護個人資料，實係基於法律規範的強制要求，而須建立符合法定門檻的基礎保護制度，因此，在建立個人資料保護的事前機制時，企業首要應先辨識所蒐集取得之個人資料為何，該等個人資料將受到何處法律的保護，始得釐清須符合什麼樣的保護機制。如企業僅聘僱有台灣員工，且僅於台灣境內營運或銷售，並不蒐集或取得台灣居民以外的自然人資料，則只須將台灣的個人資料保護法納入考量。然而，如企業聘僱有歐盟居民員工或在歐盟境內有營運或銷售行為，而可能取得歐盟居民之個人資料時，企業即須將歐盟的一般資料保護法規 (GDPR) 納入評估，據以制定遵法的隱私政策並加以執行。

2. 事後處理機制

如前所述，企業應如何對於所蒐集取得的個人資料進行保護，應視該等個人資料受到何地法律的保護，因此，當個人資料不幸發生外洩事件時，企業應如何處理，亦端視所需適用之法律規範。

以GDPR為例，當發生個人資料侵害事件，且有造成個人資料當事人的權利或自由受侵害的風險時，控管該個人資料的企業應於知悉後 72 小時之內，向監管機關通報，通報之內容則應包含：個人資料侵害事件的情形、個人資料保護長的姓名及聯絡資訊、個人資料侵害事件的可能結果、控管該個人資料之企業已採取或欲採取的措施等。

結語

當企業與競爭者在世界版圖中持續較勁，威脅者也跨越企業安全防護邊界與國界快速發展。站在這個高度變動的時代且攻防成本不對等的大環境下，企業一方面積極尋求創新轉型，另一方面卻又飽受來自內外部的各種資訊保護威脅，如何在持續變動的全球競爭中找出未來道路，正視且重視資訊安全保護問題是解決難題的第一步。

良好的資訊保護策略應該從事前的預防角度出發，將企業的有限資源投注在最關鍵的地方，降低資訊外洩風險，同時建立良善的事故緊急應變措施，審慎評估如何保留關鍵跡證以利事後數位鑑識調查程序的進行，減少事後的衝擊影響；而經驗豐富的資訊保護規劃團隊及數位鑑識團隊可協助企業瞭解威脅者可能使用的策略、程序、技術及手法，並在事前協助企業辨識內部最須受保護的核心資訊、設計保護機制、培養員工資訊保護意識，以建立企業內部的資訊保護文化，並促使員工能及時感知及掌握外洩事故，防止損害擴大。企業在決定資訊保護策略時，宜由上開觀點進行評估。

服務團隊

若您希望深入了解資訊安全與數位鑑識，或有相關服務需求，歡迎與以下專業人員聯繫：

資誠智能風險管理諮詢公司

張晉瑞　執行董事
+886-2-27296666 ext. 26916
chin-jui.chang@tw.pwc.com

鍾松剛　協理
+886-2-27296666 ext.23538
alex.chong@tw.pwc.com

唐雍為　協理
+886-2-27296666 ext. 23567
yung-wei.w.tang@tw.pwc.com

普華商務法律事務所

蔡朝安　主持律師
+886-2-27295200
eric.tsai@tw.pwc.com

張馨云　副總經理
+886-2-27295200 ext.23613
rebecca.h.chang@tw.pwc.com

鄧萍玟　協理
+886-2-27295200 ext. 23824
susan.teng@tw.pwc.com

鍾詩敏　律師
+886-2-27295200 ext. 23409
sylvia.chung@tw.pwc.com

www.pwc.tw