科技高速創新競爭的 3 個反思

就算我們缺乏市場，但可以放眼全球，即使我們缺乏外來人才的誘因，但可以淬鍊本土人才，在科技高速創新競爭上，仍大有可為

蒲樹盛

臺灣資安及稽核業界領導風險管理的資深專家
現任 BSI 英國標準協會臺灣分公司總經理
具備國際主導稽核及國際註冊講師資格、
大學講師及中華民國電腦稽核協會常務理事等職務。

猴年真的像猴一樣好動，才一開年就變化不斷。全球經濟快速動盪、能源價格劇烈波動、恐怖組織橫行依舊、天然災害不斷重創……不知如何是好！而科技的高速創新也造成另一股全球競爭與威脅，所以想藉由一些見聞感想跟大家談談我們的現象，不只是談資安。

政策與資源的反思

一月去了趟英國開會，抵達希斯洛機場，發現 T5 航站的接駁是透過一種稱作 Heathrow Pod 的無人駕駛艙（已啟用幾年，但之前都沒注意），旅客透過螢幕操作，可於 4 ～ 6 分鐘內抵達航站。該系統採無人駕駛設計，並透過紅外線偵測周邊環境，而且完全是電力驅動，方便又環保。

跟英國同事聊天，才知道英國政府很清楚地宣告，要發展無人駕駛產業，並於國會通過 1 億英磅（約臺幣 49 億元）預算，發展相關技術與應用。挺遺憾的，又證實有錢才能實現理想，空有想法是沒用的（反之，光有錢但沒及時正確掌握方向，恐怕也只是個敗家子而已）。想想我們，產業政策好像不大明確，嚴格來說，想做的多，但沒錢，只好每一種產業象徵補助一點點，結果就一事無成。

因工作關係，接觸到為數不少且包羅萬象的組織，發現到同樣的現象：組織缺乏明確的政策（包括資安政策），高層也視政策為 Paper work（許多都是照抄的）或只是部門層級的工作，沒有合理的預算去支持政策，也缺乏結合核心營運能力的前瞻性。英國將無人駕駛產業視為明日之星，結合研發與應用預算，將快速群聚人才，大量連結 ICT 技術應用（IoT、Big Data、Cloud Computing、Hardware & Software），朝向更遠大的智慧城市政策與商機邁進。雖然面對機場巴士駕駛的示威抗議，但政府還是從宏觀眼光，毅然確定發展方向。

政策及預算有了，路就出來了，企業及人才就有方向，自然有機會 Make It Happen。這是我的第一個體驗，我們似乎缺乏「聚焦」的政策及預算。

風險與落實的反思

小年夜高雄美濃發生了芮氏 6.4 大地震，造成 116 人死亡，許多災民無家可歸，令人唏噓與同情。此事件直指問題在施工不實與監督不力。

想起另一個例子，美國太空梭挑戰者號曾經有一次發射過程中爆炸，事後找到問題係出自於一片用於連接引擎及燃料噴嘴的橡膠墊片破裂。工程師認為此墊片的測試項目已包括耐熱測試，不解為何會破裂？物理學家及諾貝爾得主 Richard Feynman 進行簡單實驗，模擬當天溫度（當天弗羅里達州的氣溫偏低），將墊片先後置入該低溫環境與發射狀態之高溫環境中，結果墊片因溫差

英國希斯洛機場 T5 航站的接駁，是透過一種稱作 Heathrow Pod 的無人駕駛艙，旅客透過螢幕操作，可於 4 ～ 6 分鐘內抵達航站。該系統採無人駕駛設計，並透過紅外線偵測周邊環境，而且完全是電力驅動，方便又環保。圖片來源／ Ultra Global

過大而應聲破裂。這才發現，測試項目並未考慮到低溫狀態。

這令我想到資安風險管理與落實的現況。多數組織對資安風險的認知是片面與單點的，缺乏完整的風險管理流程或跨部門的投入，僅交由少數業管部門（如 IT 或甚至外部顧問）鑑別組織風險，並擬定控制措施。殊不知這樣的過程將導致部門因資源或績效等考量，而便宜行事。就像偷工減料的大樓，用不合理的預算草率完成攸關人命的建案，而主管機關也怠忽職守，未掌握借牌建造與工程品質，所有的代價都留在日後發生。

損害發生了，多數組織的 BCP 營運持續計畫，普遍過於簡化及形式，劇本及關鍵流程沒有經過嚴謹的分析過程，而演練的過程也過於理想化或次數不足，極有可能導致真正危機發生時的無法應變及復原。例如雖有 UPS 或發電機，但從未進行切換演練或演練時間過短，無法測試出合理的營運持續能力；工作區失效（火災、地震等），應擬真進行逃生、異地切換或遠端營運等演練。只要多用點心，不一定會增加成本，就可多一份考慮及獲致更有保障的結果。就像太空梭爆炸般，若能多一道簡單的測試，就可避免因缺乏完整的測試而付出可觀的成本。

如何掌握科技風險？臺灣多屬中小企業，資源及規模有限，建議定期參考國際組織所發布的各種專業報告，作為了解與掌握全球商機與風險的方法之一。

科技面之國際標準（列舉）

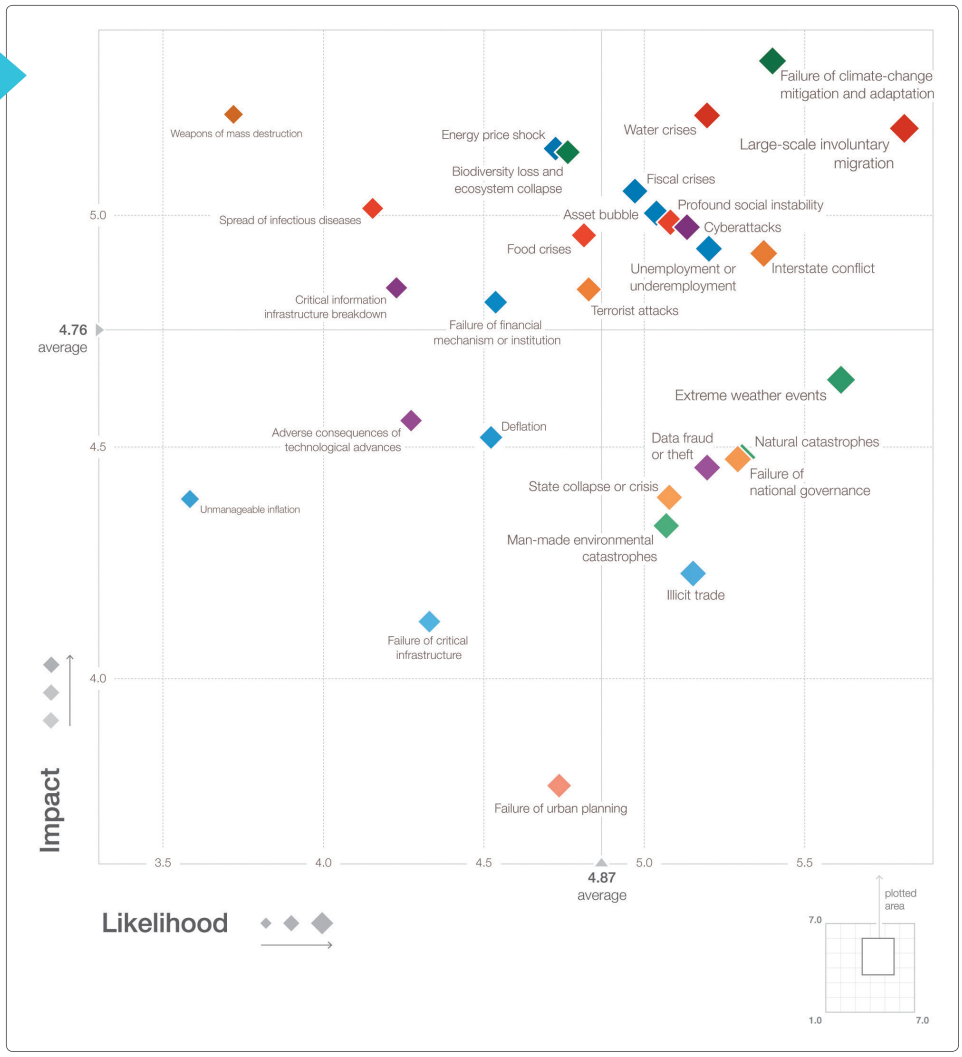
標準編號	標準名稱	標準說明
ISO 27001:2013	資訊安全管理系統	全球最受歡迎的資訊安全管理系統。用以減少資訊遺失或誤用的風險，並確保機密資料的安全，以取得利害關係人和客戶的信任。
ISO 27018:2014	公有雲之個人可識別資訊保護指南	Code of practice for protection of personally identifiable information（PII）in public clouds acting as PII processors。
ISO 22301:2012	營運持續管理系統（BCM）	確認並管理可能造成營運中斷的風險。瞭解自身企業所面臨的威脅並確立優先順序，訂定預防性解決方案計劃以迅速從意外中復原。
其他產業或區域之資安或隱私標準: HIPPA、PCI DSS、TRUSTe、US Laws Compliance White Papers（FedRAMP, FISMA）、European Privacy Seal（EuroPriSe）		

資料來源：蒲樹盛，2016 年 2 月

依據 2016 世界經濟論壇（WEF）發佈的全球風險報告，指出全球正面臨包括經濟面（財政危機、能源價格衝擊、失業及未充分就業）、環境面（氣候變遷、極端氣候、生物多樣性消失），及科技面（網路攻擊、資料外洩、關鍵基礎設施中斷）等重大風險。從每年的報告差異中，可以判斷出風險的變化與趨勢，作為管理的重點方向，及資源配置的參考。而從各年度的風險變化軌跡趨勢來看，科技風險絕對是風險值竄升最快的項目，前三名分別為網路攻擊、資料外洩、關鍵基礎設施中斷。

這些全球重大風險所導致的各種環境及緊急事件，都極可能導致了企業營運中斷。而這些日益複雜且快速的風險變化，也使企業更加清楚地意識到營運持續管理的重要性。中小企業管理階層 / 董事會必須正視營運持續管理並採取行動，為全球政經不穩、競爭環境丕變、科技高速進步、及營運模式創新等可能情況做好準備。

英國營運持續協會（BCI）的研究指出，大型或小型公司都一樣，差不多有四分之一的公司不曾設想如何因應供應鏈或委外供應商中斷的情況。在堅稱其供應商有 BCM 的公司當中，18% 的企業會直接採信供應商的片面說詞，而不進一步求證，27% 的公司只會要求看一下計畫，又有 27% 的企



在 2016 世界經濟論壇（WEF）全球風險報告中指出，全球正面臨包括經濟面（財政危機、能源價格衝擊、失業及未充分就業）、環境面（氣候變遷、極端氣候、生物多樣性消失），及科技面（網路攻擊、資料外洩、關鍵基礎設施中斷）等重大風險。圖片來源／世界經濟論壇

業不了解該如何證實那些計畫是否有效。BCI 對此現象的評論是：「對許多行業的營運持續計畫來說，這是個令人擔憂的缺陷。」

參考上列標準，將可協助企業建立制度，有效管理相關風險，增強國際競爭力。

認知與文化的反思

有一次至澳洲稽核，發現其控制措施及風險處理計畫相對簡單，與其同仁交談後，發現先進國家因為從小教育及守法觀念的養成，普遍具備較正確的預防觀念，而較少完全以防弊防賊的角度看待控制措施。包括：門禁管制、帳號密碼的使用（極少共用帳號或詢問他人密碼等行為）。這令我想起破窗理論，許多組織因同仁缺乏資安意識或紀律，而未遵循資安規定，但組織放任不管，導致多數同仁放棄紀律，隨波逐流放任風險及弱點存在於各個流程中。我看過一個組織，每次舉辦資安教育訓練時，多數同仁僅簽到後便離場。於是高層決定增加訓練時數要求，以為這樣就多少能增加資安認知。實際情況是，簽名的人變多了，到課的人數更少了！

我們目前的教育制度，坦白說，國小階段尚可真正著重於德智體群美等均衡發展（因為較沒有升學壓力），還有機會養成正確的道德與價值觀。但到國中以上階段，恐怕多數都已背離教育本質，而僅為升學考試目的在努力。因果關係下，我們很難有機會將專業所賴以支撐的道德與價值觀扎根，自然將苦果留給下一代。

我們的人才其實不少，優秀大學培養出許多傑出學生。例如全球發展迅速的 Big Data 技術，過去幾年，我們的某大學團隊參加全球最頂尖資料探勘比賽 ACM KDD Cup，參賽七次，就獲得五次世界冠軍，這是多麼傲視全球的成績啊！但是缺乏人才延續機制，許多人才被國際挖角或未能持續精進而漸被超越。

新年快樂，迎向未來

分享到這，其實我們並沒有悲觀的權利，雖然有許多值得改善的地方，但依舊要發揮臺灣人的勤奮堅毅與熱情。我們缺乏市場，但可以放眼全球；我們缺乏人才誘因，但可以淬鍊本土人才。

擬定策略、發展政策與提供資源；強化風險，腳踏實地；重視教育，邁向永續！**文⊙蒲樹盛**