中華警政研究學會

警政與警察法相關圓桌論壇（十二）

【企業安全與風險管理】論壇會議紀錄

時間：2018 年 12 月 27 日

地點：智邦科技 台北辦事處

主持人

中華警政研究學會林德華理事長：

各位與會的學者專家及貴賓大家好，延續我們上個月在台新金控主辦第一場「企業安全與風險管理」論壇之後，今天來到智邦科技台北分公司舉辦第二場「企業安全與風險管理」論壇。感謝黃董事長百忙之中親自出席共同主持這場會議。學會的同仁過去大多都在警大開會，本次進入企業體系中舉辦論壇，讓我們有機會開拓視野，討論的時候能更有共識、更能聚焦。上一場會議談論到企業被害、預防以及管理，當天在台新金控的會議上，發言非常踴躍，氣氛熱絡，大家針對不同的領域來探討企業安全與風險管理。以往學會的論壇主要著眼於警政，像是社會治安、警政管理政策等相關議題，然而因為整個時代與社會環境的改變，警政課題不能忽視企業安全問題，所以經過學會幾位同仁研究討論之後，決定在十一月、十二月、一月舉辦有關企業安全與風險管理的學術論壇，希望能藉在不同領域的專家、學者提供專業的見解。

當然一兩次的論壇沒有辦法完整論述企業風險管理的整個領域，所以日後將持續深入探討。企業安全與風險管理的範圍相當廣泛，在最近的討論中可歸納成兩點，一是內部的問題，包括內部系統設備安全、內部資安、企業貪污以及企業核心幹部管理等，以上對成長中的企業影響重大，像是先前台積電發生駭客入侵，就是一種企業安全風險管理的例子。二是企業外部的問題，包含投資風險、經濟景氣、政治影響、職場災害等等。今天希望藉由各位的專業及知識，整合內外部的問題並不斷地檢討，在將來能夠對企業安全與風險管理架構出一個因應模型，這也是本論壇的最終目的，請各位專家踴躍發言。

智邦科技公司黃安捷執行長：

感謝各位貴賓與學者的蒞臨，我過去曾跟理事長一起共事，清楚理事長做人做事的精神，對警界貢獻良多。警察是臺灣社會安定的力量，所以個人感謝

理事長從警界退休之後仍持續奉獻社會。理事長對警界有深厚的情感，累積了豐富的實務經驗，再結合中央警察大學的理論基礎，相信學會在他帶領之下，一定會開創不一樣的新局面。

對長期經營網路資安的公司來說，企業安全風險的議題並不陌生。不久前就發生某公司員工竊取 6 萬筆資料，幸好公司在員工離職前察覺到異狀，事後對該員工及相關人員予以懲處，也寫悔過書，但檢察機關卻是以證據不足不予起訴。經歷此事後，顯現安全風險管理對企業是非常重要。傑出的主管或幕僚，就應該有風險意識，每個月都要演習幾次。例如從事李前總統的隨扈便須演習救護、擔架如何通過樓梯、需要多少救護車及救護員、到達醫院需要幾分鐘、事先通知醫生準備，以便不時之需，果然最近即順利用上。可惜的是臺灣企業對安全風險管理的觀念太過缺乏。若政府無法幫忙，可與風險管理委員會合作連結。

我以一個老百姓、生意人的角度來看，安全風險管理很重要，但也感到很無力，因為整個社會對此並不在意，唯一能做的就是與相關單位互相交流，累積知識，防患於未然。另一方面可從消防、公安角度檢視，包含 101 大樓失火危機處理。若有可能，甚至可成立相關的公司或企業。各位都是專家，藉此向各位報告一些心得，感謝各位。

引言人

中央警察大學消防學系黃俊能副教授：

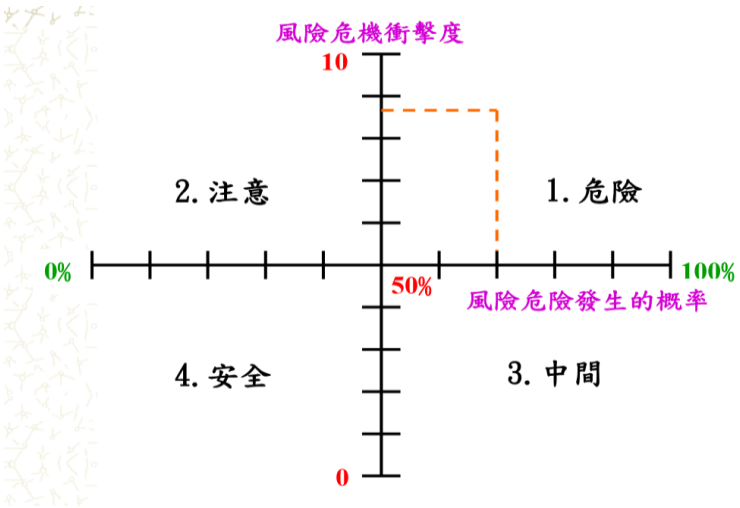
談企業風險的核心思維，不能以公共財(public goods)來討論，以全臺警察約 7 萬多人爲例，光陳雲林來台事件就出動了 7 千多警力，此事件就用了十分之一的全台警力，依企業成本而言，是不符合成本概念，但卻在政府對後續的群眾運動有所變化與改革。除了人為事件以外，天然災害台灣 921 大地震，也造成兩千四百多人死亡，此次災害，也因電力供給不足，導致臺灣經濟重大損失。再以高雄氣爆為例，地下管線破裂導致氣體外漏，而部門之間的資訊沒有妥善分享，如中央經濟部工業局沒有將詳細的管線資訊(如丙稀有害物質)告之高雄市政府，造成重大人員傷亡及財物損失。2010 年颱風重創南臺灣，連日大雨造成大規模淹水，重重影響當地經濟。不管是人為疏失或天災影響，都是難以預測，所以風險掌握、發現危機或隔絕危機是安全風險管理的主要挑戰。企業體若能做好風險管理與防患未然，當危機發生時能夠快速復原，降低自身損失，達到企業永續發展。在高度競爭下，企業以維持永續發展為先；政府組織則是對民眾環保意識、平權運動、不景氣、高失業率等等權利要求下，盡可

能滿足民眾期待。

企業持續營運(BCM)是一連串的整合流程內容應包含風險管理(Risk Management)、災害復原(Disaster Recovery)、設施管理(Facilities Management)、供應鏈管理(Supply Chain Management)、品質管理(Quality Management)危機管理、安全管理、安全建康(Heath and Safety)、知識管理(Knowledge Management)、緊急應變(Emergency Management)、危機處理(Crisis Communication)、安全管理(Security Management)等等，可以看出，BCM 的程序是一項高度整合之科學與手段。亦不應只侷限於災害復原之單一目的。國際研究指出導入 BCM 架構的企業體較能夠達到永續發展。風險定義是在安全控管下仍發生的無法預測的危機事件，像是災害造成實際損失、生產線停擺、產品瑕疵、人員傷亡、法律訴訟、財產損失等等都含蓋於風險基本概念，在風險掌控框架下所有組織都要考量利害關係人。風險概念可分為頻率與後果，如何掌握發生的頻率與發生產生的後果，過去以保險的被動方式來預防風險發生，而現今是主動發現問題並解決。在統計學上來看，風險像是機率，譬如飛機、核電廠的失事率，因內部控管非常精細，促使發生災害事情的機率趨近於零，所以會發生事情有可能是由內部人員所造成問題而致，稱之為內部威脅(insider threat)，但這只是風險一小部份，仍然有不可預測的因素存在。風險又能區分成純粹風險與投機風險，純粹風險如火災、水災或人為疏失，可以藉由保險來預防，對於市場與政治帶來不可預測的風險稱為投機風險，則無法轉嫁風險。

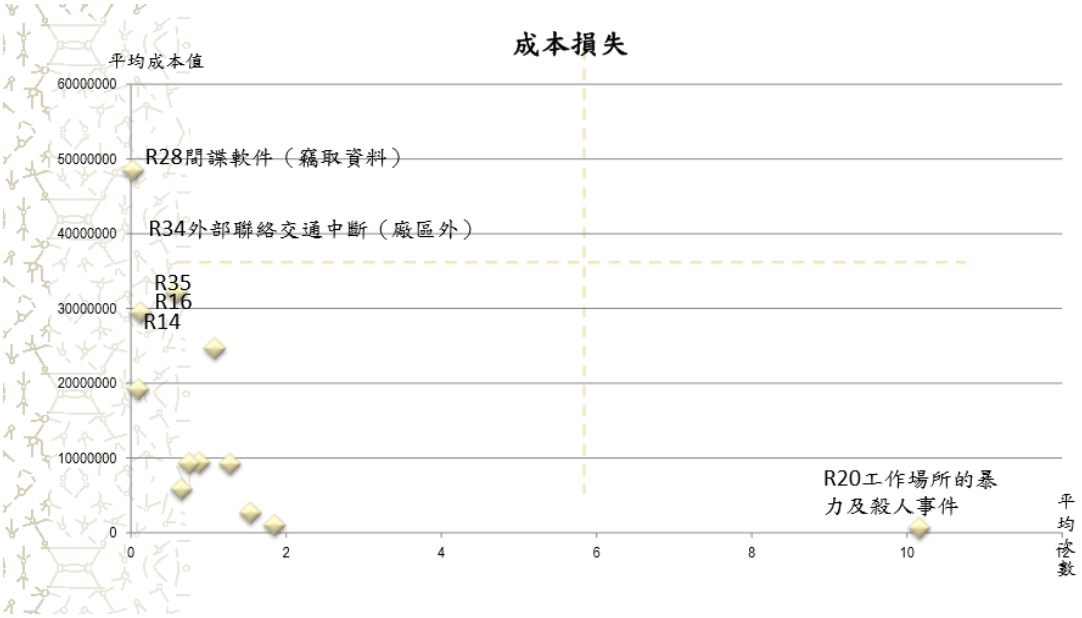
從英國經濟學人研究來看，企業裡總共分八類共七十三種指標可以做風險參考，今天的主題聚焦在員工的欺騙、非法的行為、未授權、員工的安全或者是災難的損失這部分。另外還有人為的部分包含貪汙、舞弊、洩露資訊、恐怖攻擊等，其他還有自然事件，包含地震、颱風、水災，而風險管理的作用，就是讓災難快速復原的能力，這是一個企業體必須有的能力。

根據風險衝擊度與發生的機率可以製成風險危機嚴重程度量表，需要嚴密管理的是衝擊度跟發生機率都很高的第 1 象限，第 2 跟 3 象限可以做風險轉嫁、外包、保險等方式來處理。以上就是典型風險管理架構，而風險流程，包含風險來源分析、風險辨識、風險評估、及風險處理手段，包含風險承擔與風險轉嫁(例如保險)等。



接下來針對學會去年到大陸進行合作電子大廠所做有關企業大陸設廠投資風險方面的研究，向各位分享，風險評估可分為巨觀分析(大陸投資環境)、微觀分析(研究對象廠房各項風險)兩類，巨觀分析排名前五項風險因子有 1、勞工成本增加及生產力下降；2、電力供應穩定性不足；3、市場景氣衰退；4、匯率變動產生企業損失；5、生產技術上游能力與支援不足，微觀分析部分，在廠區總共辨識出 40 種風險災害因子，如下表，依合作廠商之高階主管問卷調查後，依據平均發生次數與成本損失做成下圖:

編碼	風險因子
R1	地震
R2	地層下陷
R3	洪水
R4	乾旱
R5	暴風雪
R6	熱帶氣旋（颱風、超大豪雨）
R7	塵暴/沙塵暴
R8	極端溫度（熱、冷）
R9	雷擊
R10	食物中毒
R11	流行性疾病(如H1N1)
R12	傳染性疾病(如SARS)
R13	有害物質洩漏（瓦斯/毒氣）
R14	爆炸/火災
R15	交通運輸事故（廠區內）
R16	建築物/結構倒塌
R17	員工意外死亡
R18	罷工或勞資糾紛
R19	犯罪活動（破壞、縱火，搶劫，盜竊、詐欺，貪污，瀆職）
R20	工作場所的暴力及殺人事件
R21	騷擾事件
R22	不平等待遇/歧視
R23	造反/叛亂
R24	運行中斷/當機（資訊系統）
R25	硬體故障
R26	失去網路連結（外部互聯網或內部區域網）
R27	電腦病毒/蠕蟲（使電腦癱瘓）
R28	間諜軟件（竊取資料）
R29	電信中斷或故障（無法通話、上網）
R30	部分斷電或停電
R31	水供應（全面中斷）
R32	電力供應（全面中斷）
R33	瓦斯供應
R34	外部聯絡交通中斷（廠區外）
R35	供應鏈中斷（上游原物料）(DRAM、CMOS)
R36	國際關係波動
R37	教育與知識的不足
R38	人力資源不足
R39	決策錯誤（建廠、宿舍、空間不足）
R40	NG電池起火



依問卷結果，該電子大廠其最嚴重的風險，所造成的成本損失項目為間諜軟件竊取資料，此部分損失成本可以高達 50 億人民幣，接下來是外部交通中斷，因合作廠商的廠房規模甚大，總員工人數高達 10 萬人，每天人員上下班交通若中斷造成的成本損失非常可觀，另外，工作場所的暴力及殺人事件這個項目，平均發生次數是最高的，但造成的損失成本相對是低的。

最後針對該企業體做出幾點焦點座談的成果，如下：

★ 供應鏈中斷是 IT 產業極大風險之一。

★ 火災是廠區極大風險（大過地震）。

★ 利用外部專家協助辨識內、外部風險。

★ 網絡社群媒體已成為難以掌握的風險管道。

★ 公司主要以火災、颱風和化學品洩露、爆炸、地震、 食物中毒、外來人員入侵、內部人員不明原因聚集、 傳染病防疫為預想風險因子威脅對象。

★ 臺北總公司訂定永續經營(BCM)規範，持續改進。

★ 政治風險最大，勞力跟勞工教育水準次之

★ 內部竊案造成商譽及廠區安全問題。

★ 爆炸(火災)雖頻率低但損害大

與談人

新光三越公司馬振華安控長：

延伸黃教授引言的重點，發現危機因子的途徑，特別強調有四點。

一. 天災難測，人禍難防。「風險掌控」「發現危機」「隔絕危機」是未來風險與安全管理的挑戰。

二.企業持續營運架構，有十大要務，其中風險管理、災後復原、健康與安全、緊急事故管理、安全、危機處理，就佔了六項，其餘四項與風險間接有關。從這點能夠得知企業的永續經營跟風險是一體兩面，若沒做好風險就無法談企業永續經營。

三.過去風險管理，偏重保險的觀點，被動等待發生；現在採危機管控，主動消除危機因子。

四.風險管理基本步驟　1.辨識　2.評估　3.分析決策　4.管控。

第四點不是單純的一個先後步驟，是一個循環，在最後也許發現新的風險再去做辨識、評估、分析，是首尾相連的，另外，在第一個步驟辨識之前應該還要有一個步驟是發現危機，在發現危機之後才有後續的步驟開始，因此這次主題就在於發現危機因子的途徑。

目前新光三越有 18 個分公司、22 個館體、18 個營業務部門、2 萬 5 千名員工、總營業面積 150 萬平方米、每年來店人數 1 億 3 千萬人次、2 千 6 百個品牌、推測年營業額 1 千億元以上。從如此龐大的企業為例，可以推測 20 個發現危險因子的途徑，組織內過去事故歷史、外部案例、外部專家意見、政府主管機關指導、現地訪視、安全與風險圓桌會議、業務檢查、無預警檢查、委外專業檢測、客訴管道、自陳管道、秘密客、演練、觀摩、同業聯防、自主風險評估、專案問卷研究、書面篩檢紀錄、事件調查、自動檢測。

各位學者未來在研究企業安全與風險管理，若能具備洞察力、想像力、專業能力、創造力以上特質，就能對發現問題有所幫助。在企業體中發現問題時，實行改善措施可能引起價值觀衝突帶來的質疑，所以在發現問題時要讓企業體有以下的願景；強化預防意識、改進工作制度、創新安全設施、增加全體安全感、提升安控的企業附加價值。

真理大學法律學系蔡震榮教授：

美國ＣＯＳＯ委員會對公司內部制定一套內控制度，內控制度可分為企業風險管理、內部控制與嚇阻舞弊，為合理達成組織目標而建立的一切政策與程序。早期的內控是一種財務控制的報告，２０１３年時美國委員會定義內控的範圍也涵蓋非財務報告，如內部控制聲明書、永續經營報告；或是供內部決策使用的年度預算表與客戶滿意程度報告。

內部控制是一種能消彌弊端的綜合管理制度，由管理階層規劃設計，經機關首長核准，可透過興利、制度管理提升績效並提高資源運用效能；而管理制度的推動需考量法規規定、組織組成、技術面向與內部人員的溝通；董事會選

出經理人，執行由上而下的內部控管 。企業內控法規可分成政府面規與企業面，政府法規面向上，國內對於內部控制及內部審核之現行法令及定位，明定於預算法、會計法、決算法、審計法、政府採購法、內部審核處理準則及其他有關政府內部控制及內部審核審核之法令規章內，法令遵循制度在國外及國內金控、銀行、保險、信合社及票券業已實施多年。

內部控制制度的組成要素應包括控制環境、風險評估、控制作業、監督，各個公司再依照實際需要增加項目，包括人員管控、產品輸出等。過去企業建立內控制度的目的多在於防弊，但是面對新世紀的來臨，資訊科技之突飛猛進，瞬息萬變的競爭環境與日新月 異的經營方式，內部控制對企業的時代意義，應是如何降低企業內不合理的浪費，提高效率與競爭力，以爭取商機，進而創造出企業最大利潤之利器，另外還有增加一個預防的工作，在危害還沒發生時透過內控制度做預防工作，就像警察法理中除了防止危害以外，還有預防犯罪預防危害，現今內控的目標往前邁進，且科技進步以利簡化內部程序。

內控跟風險管理是息息相關的，內部控制是風險管理的一部分，內部控制本身無目標，主要是幫助企業整體達成目標，所以內控是動態的，包羅著企業整體層級和所有作業層級的動態過程，凡生產、銷售、 研發、公關、採購和財務等各項業務，均應有合理之控制，以減少任何不必要成本之發生與資源的浪費。從企 業經營與管理的角度而言，它更囊括了所有管理與經營的控制、會計控制與電腦資訊控制等制度。內控制度應是動態的，務實的，同時也會因企業、部門、作業內容之不同而有所差異，它需要隨著時空環境變遷與依據內部稽核執行情形持續不斷的評估與修正。

開南大學法律學系鄭善印教授：

企業的安全管理面相多元，其中一個重要的就是「資安與通安」，故想以此為題，與談日本企業的安全管理。

資安與通安首先牽涉到的就是，企業內營業秘密與顧客資料的保護。因為資訊技術的發達，這類機密很容易被駭客或內部員工擷取，例如駭客以藏有病毒的軟體進入公司的官網瀏覽，並侵入系統以擷取所需資料，或員工以 USB 等硬碟盜拷顧客資料等。一旦發生這種情形，企業將遭到莫大的損失或喪失長年累積的信譽。如 2011 年因駭客攻擊，使得索尼公司洩漏 7700 萬件的顧客個資，據說共損失 2 兆日圓。

第二個問題是，企業資訊系統受害後，將導致與其交易的所有企業亦遭受感染。例如東京都都政府 2015 年 7 月即有員工電腦 9 臺遭受病毒感染將個資 2

萬多筆洩漏出去，其路徑係員工觀賞動漫及電子遊戲時，駭客利用 Adobe Flash Player 的脆弱性，將病毒隱藏其中以致系統感染，接著與其接觸的其他各機關系統也都紛紛感染。

第三個問題是，有一本「小企業資安脆弱性之調查書」指出，佔日本企業87%的小企業，由於資金及人手不足，其資安的脆弱性十分明顯，若予放任非但這些小企業將被弱肉強食，並且與其接觸的所有人員，都將遭受個資洩漏的危險。

經 IPA 該機構調查所知中小企業主有關資通安全最大困擾在：

一、不知如何著手

二、應該做到哪裡

三、無經費可聘僱專門人員

四、安全預算不足

為此有五個重點行動方案來因應：

一、保持軟體的最新狀態

二、使用防毒軟體

三、強化密碼更換

四、檢討共通設定制度

五、了解威脅或攻擊手法

永豐金控李相臣資安長：

企業安全跟使用者業務主管、公共或稽核人員、檢舉人有關，這些負責風險管理的人員通通可以由ＩＧ處理，而ＩＧ的概念因變化速度快導致不能靠以往的經驗來判斷，從聯發科、台積電、富士康、友達等案例，資料外洩的來源可能是能夠接觸資料的人、電腦或郵件，也可能是使用者帳密被盜取，若要杜絕資料外洩，從企業周遭環境、資料庫存取記錄、員工間的通訊等等都要納入考量。

從網路上可以獲得大量資訊及現代區域學習可以將資料客制化，在便利的過程中，往往也是個資洩漏的開始，內部舞弊、外部駭客等都源於網路科技不當的應用。而內部控制很重要在執行的一點就是預先的防範；由多方面的資訊監測來得知惡意程式的 IP 位置，惡意程式的目的及作法；監測內部 USB 異常下載頻率來推測內部資料竊取行為，應用電腦資訊反向追蹤，從而達到預防危機的動作，這些都是目前科技水準能夠做到的。以我們企業為例，電腦資訊統計與公司外部連線異常頻繁的ＩＰ國家是俄羅斯，目前公司在俄羅斯根本沒有

客戶，這就是一個典型的木馬程式，因為木馬程式在執行時會與植入者做連線，大多木馬程式攻擊後約會在三個月左右達成目的造成損失，透過設立監控點預先防範，這就是我們透過電腦大數據能夠做的危機預防。現下企業情況很多都是有能力做數據監測，沒能力做判讀，電腦ＡＩ判讀將是未來的趨勢，依照先例數據特點從而判斷異常執行預防。

國立陽明大學張佩嫈博士候選人：

美國知名企業家Frank Argenbright創立風險管理及安全查核公司始於一台測謊儀器；在以色列，民間企業公司廣泛委託測謊機構來查核面試人員的背景，在既有履歷文件、各類電腦化問卷檢測外，能再搭配測謊儀測，除了能對新進人員忠誠度進行篩選，大幅降低商業間諜進入企業的風險，另經過測謊人員深入的晤談，往往可以更深入瞭解該人員的成長背景、素行、交往與個性等等，提供客觀意見給企業主管聘用人之參考。

根據美國測謊協會(APA)以及ASTM國際標準，對於測謊均訂有嚴謹的施測程序規範，而臺灣司法單位的儀測部門亦與國際同步，在遵循規範下的測謊結果，不論在國內外都是能具有法律效益的。今天若發生內部資料遭竊取事件，公司在警察介入之前的內部調查，可以先透過測謊篩選可能涉案人員、縮小調查範圍、追查資料是否已經釋出，以及有沒有共犯等情事，當然，測謊人員也必須有專業素養，晤談中如有涉個人隱私、無關調查中案件的資訊，並不提供予公司。

根據目前國際上研究，測謊如以目前研究腦科學熱門的磁振造影、腦電波、腦磁波等儀器，其準確度仍不及測謊儀Polygraph，且Polygraph儀器費用相對便宜、體積輕巧。目前國內雖然已經有民間公司在執行測謊工作，但應用在企業還是很少。美國雖在1988發布施行EPPA法案，約束民間企業對於新進人員或者現職人員不得運用測謊來影響其工作權益，但是對於跟國家安全、與政府相關連、涉及安檢、公安、藥品相關、甚至接觸重要機密等等工作，企業還是能透過測謊進行人事查核，多一層安全防護網。但在EPPA法案裡，如已有事件發生時，對於事件的內部調查，企業可運用測謊來協助，能夠在初步調查時，蒐集保全更多相關證據。

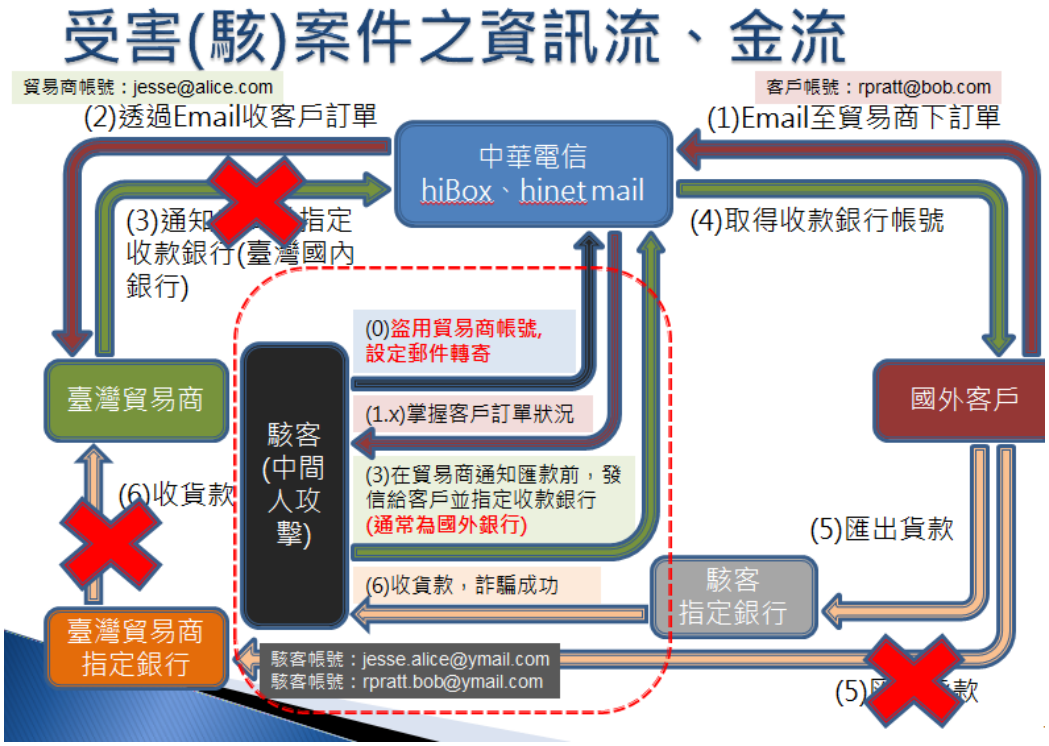
測謊儀測查核篩檢可以提供企業用人三大成效：1、揭露(過去曾有如竊取公司機密等行為)；2、嚇阻(避免未來犯罪行為)；3、偵測(調查公司內部已發生事件涉案情形)。

刑事局科技中心羅國良股長：

根據美國 FBI 旗下網路犯罪申訴中心的 2014 年網路犯罪報告：「變臉詐騙是一場複雜的網路詐騙活動，目標是經常執行電匯付款的外國供應商或企業合作伙伴，主要透過社交工程手法，以及入侵商業電子郵件帳戶等方式，進行未經授權的轉帳。

在 20 多種網路費罪類型中，以電子郵件為攻擊途徑的變臉詐騙（Business Email Compromise, BEC）已經占總企業損失的四分之一，可以歸納出 BEC 詐騙的攻擊流程是鎖定目標→社交工程攻擊→潛伏監控→執行詐騙。

正常貿易金流與受害詐騙金流資訊流如下圖示：



常見案例分享，不明犯嫌必定能攔截或轉寄國內貿易商與國外客戶往來的郵件，因此能夠得知郵件內容，精確掌握出貨及匯款等資訊，利用外部電郵信箱如 hotmail 或 ymail，註冊與貿易商及客戶相似的電郵帳號，對客戶實施社交工程手法，通知客戶將貨款匯至犯嫌另行申請之金融機構達成詐騙目的。

藉由郵件登入紀錄來分析網路詐騙，從 webmail 登入紀錄顯示，特定日期持續有非國內 IP 登入，且在國外 IP 登入紀錄同一天有短時間多次登入失敗，之後成功登入系統之樣態，表示該帳號遭密碼猜測攻擊，也能從 pop3 收信紀錄觀察到徵兆，譬如期間內多次出現短時間國內外的 IP 下載貿易商與客戶端的郵件。當郵件寄出時 TCP 通訊協定於資料傳輸前會針對檔頭來認證雙方 IP 存在，確認存在後才會將郵件發送，所以整個郵件中檔頭是最真實的存在，藉由郵件檔頭資訊分析，能夠得到更多詐騙者的資訊。

防範網路變臉詐騙的秘訣為詳細檢查所有電子郵件、強化員工防詐觀念、建立廠商變更的匯款資訊流程、建立另以非電子郵件為管道之雙重認證機制。

中央警察大學推廣中心蔡庭榕主任：

企業風險管理是企業安全與發展的重要基礎，能夠分成風險鑑別、風險評估、對策選擇與施行，以及成效評估四個通用階段，風險鑑別又分風險種類、威脅來源；風險評估考量到威脅、可能性、弱點與緊要性；對策選擇與施行如

門禁管制、ＣＣＴＶ、警衛巡邏、警報系統、防毒軟體、權限管理等等；成效評估則由巨觀與微觀來衡量。統合各位的分享，在案件之前能夠前瞻預防，案件之中要能縮短處理時效，案件之後則延伸至法律責任上。

企業風險特性具多元多樣、各有不同、大小殊異、變化快速、政策法令、源自內外，例如員工竊取營業機密、企業間諜、洗錢防制、豬瘟控管等等，只要有關降低風險的因素都能納入考量。企業體需訂立能夠復原的關鍵設施保護機制（ＣＩＰ）、標準處理程序（ＳＯＰ）或導入人工智能（ＡＩ）及掃描分析回應評估機制（ＳＡＲＡ），並重視企業安全窗口的重要性，譬如聯絡官掌控整個流程使效率提高。

中央警察大學法律學系許福生教授：

藉由發現危險因子來確認及分析風險，從人、事、物上去分析，確認後才能擬訂政策或排除風險。作為犯罪預防實務人員，為了提供有效的犯罪風險服務給顧客，犯罪預防實務人員必須從事下列事項：1. 犯罪型態分析：了解時下最流行普遍的犯罪型態，可從下列著手了解與考量：(1)犯罪發生率(某犯罪類型的當地受害者人數÷當地居民總人數)。(2)犯罪方法分析。(3)犯罪時間分析。(4)嫌犯特徵分析。(5)報案型態分析。(6)損失類型與數量分析。2.實施安全調查研究：安全調查的主要目的在促使犯罪預防實務人員經由了解顧客的硬體安全設備、出入程序、活動、可能遭受犯罪攻擊的目標、犯罪型態等資訊後，分析出顧客目前可能面臨哪些特殊的犯罪風險。3. 系統設計：當犯罪預防透過安全調查辨識出顧客所有的及可能的最大損失之犯罪風險後，便可試著利用下列的五個風險管理原則，進行犯罪風險管理系統的設計：(1)避免風險。(2)降低風險。(3)分散風險。(4)轉移風險。(5)接受風險。4.成本分析：成本效益分析，是風險管理的基礎。換言之，作為犯罪預防實務人員，需要清楚了解犯罪的型態，包含犯罪發生率、嫌犯特徵、報案型態、損失類型與數量，這些能藉由科技進行大數據的分析，之後實施安全調查，了解硬體安全設備、出入程序、活動可能遭受侵害的可能性，接者進入系統設計，以避免、降低、轉移、接受、成本分析為風險管理原則，企業風險也能從類似的流程進行分析。

美國欺詐交易委員會將企業風險管理分成八個概念；內部環境、目標設定、事項識別、風險評估、風險應對、控制活動、信息與溝通以及監控等八個要素構成。目前市場環境可分成七種風險；投資風險、經濟合同風險、產品市場風險、存貨風險、債務風險、擔保風險、匯率風險。雖然企業風險管理與犯罪學並無直接關係，但是藉由學會同仁針對風險的討論，足以架構成初期模型。

警政署秘書室廖訓誠博士：

在上一次論壇中提到人在企業安全與風險管理上佔了非常重要的因素之外，操作工具也是其中因素之一，現今科技的先進，促使我們能藉由工具使用，將風險管理更加系統化、步驟化，例如 ORMIT 風險管理工具，強調六項運用模組：危險識別、風險評估、風險控制、下達控制決策、建立模型、風險指標，目前大多應用於政府機關或重大事件上，往後若能導入企業體，應能為企業帶來很好的效益。雖然科技的發達，能夠將大數據系統化管理，但最後還是要回歸於人的因素上。

詮理法律事務所陳佳瑤所長：

關於企業安全與風險管理，我會於下一次論壇會以南港輪胎回扣案及德士通電信企業資料外洩案為例，用真實的案例讓各位同仁了解企業面臨的風險。

與談總結

中央警察大學行政警察學系章光明教授：

警察大學共有１４個系，與安全領域都有關係，若能將研究成果和企業安全與風險管理結合，想必成果可以讓企業受益。統合今天所有演講者的論點，都能回歸於安全意識，從三個層面來談，若企業主本身不具有安全意識的話，安全在企業的價值就無法反映，不重視風險與安全管理的企業，很難達成永續經營，因此希望能透過學會向企業宣導；政府在企業安全與風險管理上佔重要地位，政府具有安全意識，實行良好的政策能促進企業體發展；企業體所有員工都要具有安全意識，不是依賴特定安全部門，當安全責任落實到員工上對企業是非常好的。

當同一個概念被重複提到，那麼此概念就非常重要，許多問題都是由內部衍生出部，所以資安大多都為人安生成，如何辨識員工也變得非常重要，測謊方法對於企業體或許是可行的，針對分析大數據其實是一種人的行為分析，許多例子最後回歸到人本身的問題。

科學分析與評估的運用，只能夠作為輔助，要能更進一步發展，當找到每一個影響企業安全與風險的因子，針對這個問題要如何解決，但並非發生後才去處理，而是著重在預防的防治措施，然後提出解決之道，並且不斷的演練，才能從中知道方法是否可行；或在演練過程中，發現更多的漏洞，經過多次的改善讓方法的可行性提高。

最後結論出三個論點，如何從企業主、政府、企業員工三方面提升其安全意識；如何從人安測謊、大數據分析，發現問題因子；如何在評估之後提出預防的解決之道，訂立ＳＯＰ並落實操作。

結語

中華警政研究學會林德華理事長：

非常感謝黃董事長盛情邀請，今天下午我們學會在智邦台北分公司舉行第二場「企業安全與風險管理」圓桌論壇，也感謝在場教授學者及專家大家熱心參與，會議進行三個多小時，發言立論精闢，分析見解獨到，討論也是欲罷免不能！感謝大家用心專注，這是我們學會從社會治安的學術研究、管理策略探討，跨足到企業安全治理的一大步，期待大家繼續共襄盛舉，加速蒐研國內外專業知識，並瞭解企業營運的實際需求，大家集智研究發展，期待能發展出具體可行的行動策略方案。再次感謝大家，尤其特別感謝黃董事長全程參與及長年對我們警政工作的支持！感恩！