資訊風險之量化與安全性
Quantifying Information Risk and Security

作者: **Ed Gelbstein, Ph.D.,** has worked in IT for more than 40 years and is the former director of the United Nations (UN) International Computing Centre, a service organization providing IT services around the globe to most of the organizations in the UN System. Since leaving the UN, Gelbstein has been an advisor on IT matters to the UN Board of Auditors and the French National Audit Office (Cour des Comptes) and is a faculty member of Webster University (Geneva, Switzerland). A regular speaker at international conferences covering audit, risk, governance and information security, Gelbstein is the author of several publications. He lives in France and can be reached at ed.gelbstein@gmail.com.

譯者: 劉其昌, 立法院教育及文化委專門委員 中華民國電腦稽核協會 編譯出版委員會委員

吾人進行資訊活動之風險性平郭以及如何計算資訊安全投入之回收報酬率係頗具挑戰性者，ISACA架構下所定義的資訊科技性風險[1]係指企業經營營運過程中，因使用、擁有、牽涉、影響和採用了資通訊科技因素，對公司營運上所行成之風險[2]，當然任何幸值風險之因素管理必須倚賴主客觀性之預測、假設、及猜測在內。

COBIT 5®有關資訊安全性之內容增補瞭若干在以往之出版品揭示之資安準則，和資安實務作業面上所缺漏之資安治理內容，COBIT 5®所提出支資安安全量化與資訊計量式安全性之若干指標內容，但以企業營運之觀點而言，資安之量化仍有少許之困難。

資訊安全事故對於企業個體之衝擊程度，取決於企業經營個體之衝擊程度，取決於本身對此意外事件之了解程度，資通訊科技制度在於支應企業營運過程上提供基本之服務，同時平和誤用資訊科技於企業作業活動時將產稱司不利影響，獲取這項不利影響產生之損失數據將有賴於企業經營者自身才知道，因為他門是唯一得以將上述阻斷干擾因子對 企業財務活動，何管制性行為作為造成衝擊時可加以評估進而於以量化的人。

一項資安事故對企業衝擊的周延完整性 分析(BIA)應當反應包括其對企業營運活動所遭受之衝擊度，以及這種衝擊本身所具備之時間影響效果，在時間影響面上它顯然不是一種線性函數關係，或許 10 分鐘 的資訊中斷服務可被忽視其影響衝擊，然而當這種中斷服務狀態持續達 3 天以上時，足可證實它會對企業帶來相當大之災難，BIA 建基於熟悉特定企業領域過程者，個人以其可信度之資料為基礎，以趨近真實態度來評估企業遭受資安之衝擊，雖然不足以確保評估數據之完整正確，但屬於足可被信賴而接受者。

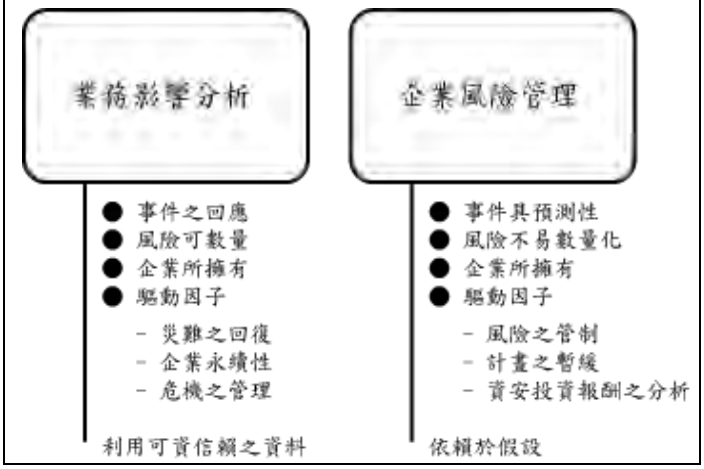
BIA之評估成果應當係屬一種經過良好規劃設計檢測 ，同時與時俱進更新之企劃(對因應意外事件之回應、災變之回復、企業營運之永續、和危機之管理等) ，這類計畫之有效性族已決定區分企業持續生存與失敗之不同差異。

企業風險管理(ERM)係指建基於以企業風險為基礎所涉及之各種不同面向的資訊風險，並給予不同之關心與管理工作，這將整合包括內部控制、以及涵蓋其他各種層面，例如對管制性之遵循方面，就如同對資訊風險之衝擊影響，ERM當然應由企業營運經理階層來負責掌控管理，圖1則展示BIA與ERM二者間之主要差別性：

資訊風險管理以及資訊安全這二項規範已從其原先專注之範圍領域，轉於到企業營運管理之廣泛層面，資訊安全之風險評估和相關ROI值之計

算必聯結特定問題，相關討論指出；資訊安全之啟使者被期望非常熟練上述二項攸關資訊科技運作之規則規定，而本文旨在企圖論述相關議題，存在資訊風險及安全問題時所可能遭遇之困難，何面臨之陷阱詐欺。

圖1 BIA與ERM間領域之差異



資訊風險之管理

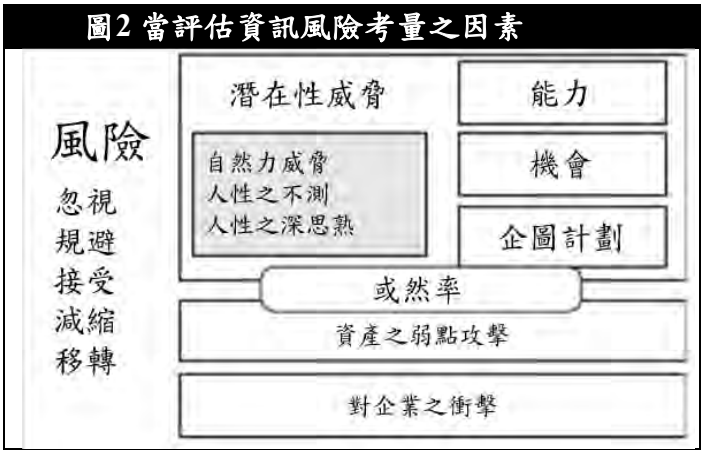
資訊風險管理(IRM)藉由下述各種因素逐漸引起企業經營階層之注意力：

- 企業之營運層面持續過度依賴於資訊科技之使用
- 若干之資訊體制和服務據有關鍵重要性之使命特性
- 依賴於開放性下全球網絡連結及其產出效果(著名之網際網路犯罪何來源不明之惡意軟體攻擊)
- 網際空間之武力軍事化和潛在的網際戰爭和網際恐怖威脅性問題

不斷受到關注

ISACAS 有關資通訊科技架構之風險和資通訊科技風險之先驅指導者，提出了一項概括完整周詳經過深思熟慮之藍圖和清楚地執行組合，資通訊科技風險指導手冊第四章介紹致力於瞭解和傳達資通訊科技內涵，執行資通訊科技作業之品質性評核供作比較， 簡單易於執行，但是有關所需之數量化評估資料則不易取得，圖 2 顯示處理個別性資通訊風險的五項策略及其相關之風險評核組成因素，這是一種屬於比較簡化和簡潔地處理資訊風險之評估問題，至於對這類問題比較完整性的觀點論述，可見諸於資訊科技架構風險之專論中。

圖2 當評估資訊風險考量之因素



威脅

迄至 1990 年代資通訊科技風險之先趨者開始將焦點轉移至自然界之威脅包括暴風雨和地震，當資訊科技記述行同無所不在時，由於人性之意外事件活動(諸如未正確配置一項設施將無法偵測出軟體之錯誤)，所導致之資訊風險變成非常容易發生，必須採取審慎熟慮之對策，俾得以節省時間資源避免詐欺，和破壞行為之發生，這些均屬資訊使用之威脅內容，當吾人忽視這類風險因子將非屬謹慎細心的行為過程，計畫性地人性資訊弱點攻擊，或許會是最大的威脅挑戰，尤其針對關聯性的基礎建設更是如此，因為：

- 這類屬性之行動不具可預測性亦非隨機，因此以往事件資料之統計分析無法提供任何協助。
- 這種威脅性之背後所隱含之個人通常並不易知悉，也甚少認證個人本身，不論屬內在或外在性因素舉備良好的智能係屬基本者，但

它難以實現。

- 長期以來(或許以被偵測出來的)資訊內部之惡意人士挾其潛能、 動機和機會不斷干預擾亂資訊體系，和資料庫之使用且未能偵測出結果。

在缺乏提供足夠之資料用以計算和數量化資訊科技之風險，面對人類經過精心設計用以攻擊企業資訊資產之各種可能，資訊風險之評估者最多只得信賴他們對於企業資訊治理之知識瞭解。處於此種資訊攻擊在缺乏可資信賴的智能情況下，當取決於社會文化、民族人性、和以往相關之經驗等因素，有關資訊之品質性評估多少取決於推估之情報，無論何種企業所具之不同性質、類別、主觀性、或屬於正確性否，均依個別企業之本身狀況而異。

資產之弱點攻擊

資通訊科技產業之快速創新發展，大大增加了資訊資產弱點之遭受攻擊機會，資訊安全之管理方面亦增其複雜程度主要係基於下述之理由：

資訊科技產品複雜程度之增加

當 IBM 在 1967 年所引入的 360 系統其作業運作體系(OSS)就是一個實例，在當時它係最大的電腦軟體設計，大約總計有一百萬條信號線路裝製，推出一年之後其成本為當初預算額度之 4 倍，其在運作中所發現之錯誤約耗費一年于時間去消除[3]，至 1969 年 IBM 公司了解到每次消除電腦系統軟體時大約存在有 1000 個錯誤，而這個數據屬合理且穩定的[4]。

微軟公司在 2009 年推出視窗 Windows 7 (在 2012 年則為 Windows 8 用以替代資訊軟體)，先前所推出之 Windows 7 中大約包括了 5 千萬條信號線路(係 360 電腦系統規模大小之 50 倍)，微軟公司並未揭露原先雖出軟體系統 Windows 7 版本作業系統出現之錯誤，同時本文亦無法 重其他來源獲知任何可資信賴之相關資訊，不過 Windows 7 版本軟體成為熱門維修調控之狀況，以及在以每週為維修基礎所發出之訊息中[5]，採用緊急標籤之標示作法也透露了其實況。

事實上每一項之資訊產品包括伺服器、路由器、平板電腦、及智慧型手機等，皆具有相當之複雜性存在，對於企業在使用下載之行動應用資訊(APPS)時，亦存在有若干之複雜性，吾人認為每一項資訊設備和其軟體本身弱點均可能遭受攻擊(若干以被察知和其餘未被發現者)，同實在惡意企圖攻擊下將造成損失與犧牲。

回歸問題本質當前系統軟體之生態環境系微小的，因為在全球均共同使用若干相同內容組成之軟體(例如 Windows 微軟、Android 、Java 系統等) ，上述這些系統之運作失誤會經常被查覺且有系統地報導出來，而這些有關之報導內容對於潛在的攻擊者則有相當知助益與方便處，由於系統設計安裝具有複雜度，同時欲全盤修正測試之錯誤，必將甚為耗時，事實上也未全盤地執行完畢。

市場時間

資通訊科技產業之競爭性本質驅使了最近的資訊創新趨勢，資通訊科技產業本於創新之文化本質鼓勵了研發設計，並促使賣方儘早將產品之注意力聚焦於潛在之顧客方，某些創新表現於商業展覽會中所加以陳列展示者至多僅屬貳流者，某些已早在市場上市了或許並未將全部之系統軟體線路完全檢視校正、測試、或完成其他的確保品質程序。

智慧型手機和平板電腦之消費端使用者下載安裝數以百萬計的 APP 軟體應用程式，將使得使用這類資訊行動裝置設施支安全性評估變得時分複雜。

終端用消費使用者之執照協議(EULAS)針對套裝軟體之使用者限縮了賣方應負之責任，內容為當套裝軟體之使用對消費端使用者電腦，或資料造成損害時得以免除其責任，上述協議內容頗為繁複不易閱讀瞭解，且無法進行協商溝通尤其當安裝軟體時被視為已屬同意之條件，創新產品旨在於滿足個人對財貨之慾望，近年來各機構組

織皆有壓力促使其員工選擇與其工作相關之室內和移動性裝置設施有關技術之偏好，但這將逐漸地對公司企業之技術和安全性結構產生損壞。

資通訊科技技術面之不完整性諸如設計和製造上之誤差已逐漸呈現，也有若干尚未被察覺(一旦被查覺將變成立即維修)，典型地說當賣方所經常提供之解決方案會引發出新的 系統偏誤。

受責難性

除了系統性缺點導致使用者運用了不完備的資通訊科技，通常使用之資通訊科技必須有賴於眾多的電腦運算過程(有關之詳細資料，可參考 COBIT5 和其相關之出版品 COBIT5 有關資訊安全面問題)，有關之資訊弱點攻擊來自於：

過程執行之程度 (較少之單位利用內部資源甚少能夠執行完成 COBIT 所規定之全部系統過程，那些已完成執行者亦無法充分滿足高水準所需之要求，和所需完成之條件)

執行相關過程中應遵循以建立之良好實務指導準則之程度，諸如遵守資通訊科技基本架構之規定(ITIL)，智識本體之資料管理(DMBOK)，智識本體軟體工程(SWEBOK) ，以及智識本體之計畫管理(PMBOK) 等之妥適性。

在實務上遵循上述過程之能力程度，當與適用遵循條件內容大小和範圍寬窄有關，在時間之壓力下和較缺乏智識之配合下，往往導致圖謀設立可用之捷徑，其實每一項例外之事件將被視為可受責難弱點之處，當然企業組織文化背景、 遵循法令之能力、推動政策之動機、和對試用過程努力奉獻之程度等皆具有影響力，再次評核弱點受攻擊之時可責性，在於資訊技術之過程和執行人員知本身，這些對有效率地評估資訊風險實皆是不可或缺者，此種弱點之責難性必與企業之資訊執行過程其精確性有關聯，以及當遭受特定威脅時所產生損害引發之衝擊影響程度有關。

或然率性

一項廣受接受的資訊風險定義係指：一項特定性之威脅對企業資產弱點攻擊造成之潛在性損失，若干發行刊物對資訊風險之顯示公式表達為：

風險=或然率× 衝擊程度 ，但是或然率一詞通常會被用希望性之類觀念加以取代，不過小心這貳個名詞所替代之意義是不相同的，或然率值可藉統計分析予以推導出數值，統計學是一門正式之學科，經常使用若干複雜之數學工具，在相關之統計學訓練方面未使學習者完全了解認識其真正函意，同時統計值也常遭至誤用表達，這個部分在 19 世紀之專論" 謊言、 責難謊言和統計"[6] 中之敘述已足以區別認知統計之說明。

統計學科基本上包括二大部分，其一為敘述性統計另一為推論性統計，敘述性統計在於反應過往之事件分析，這當有賴於需要足夠之資料樣本，才可以滿足特定之需要，推論性統計則藉助於以往歷史資料和數學公式計算出可預測性資訊，用以支持其未來之目標，推論性統計包括在某種程度上可精確計算之部分，這就是機率遊戲下之情況，諸如擲骰子或賭輪盤的遊戲，賭博遊戲場長期以來依賴上述這些統計學資料，賭博名聲令企業十分厭惡，企業並部樂見因為賭博原因而聲名大噪具知名度[7]。

推論性統計和事件之資訊消息也常被保險公司用來計算其共同案件(例如車輛肇事 、竊盜、死亡等案件)保險費費率之計算基礎，保險公司選擇將較特殊案件之風險移轉予再保險公司，或同業之相關公協會，而後者可能肇因於統計資料上之限制性以致於損失巨額之資金，因為針對如此罕見發生之事件，以往根本沒有任何可資信賴之資料可供分析預測(例如超級火山之爆發事件之機率)，創投資本家和投資者藉諸壓注得以成功致富者，係因瞄準打賭創新者早期之創作多屬成功之賭註機率甚大使克有之。 例如 1998 年 GOOGLE 網際網路之成功出現即屬一例[8]。

最佳的資訊安全係處理伴隨者出現頻率和大

小程度不確定性時事件之發生情形，因此這需要採用某種程度之臆測(更甚者為一睹注) ，這將去決於評估者本身對不確定性事件處理之智慧 經驗判斷和堅持之程度。資訊威脅之程度有低中高之分，吾人可以建置一個伴隨不同顏色之資訊風險距陣，以綠色、 黃色、 或紅色等不同之顏色代表小區域，這是首先的第一步---當所有不同任務之參予者皆了解其主觀本質，同意相意假設內容和所給予之評等級別後，這些資訊風險距陣將會變成甚具參考之熱點地圖，不過另一方面也可能引發他們之誤解。良好的實務作法為希望熱點地圖必須與組織之風險標準間建立相關性，俾得以決定某一風險水準情況應否被接受(亦即及風險之偏好程度) 。

資訊風險距陣可被用來建立風險之紀錄，評估風險衝擊之大小程度(這當然需要有健全的 BIA 用以提供所需之資訊) ，提出明確而合適的風險因應策略(包括忽視 、接受、 規避、 減緩 、移轉等)，伴隨採取策略之可責性，當採取選擇一種緩合措施時之效果，在此同時亦連結出對執行減緩措施時 ROI 值估計之影響性。

一項對立之觀點：在實務上有時採取官僚式的方式來評估資訊風險之程度大小，例如：

- 引入顧問群以短期研討工作會方式訓練企業經營階層，了解如何建立資訊風險距陣。 ．要求企業經營階層執行一項資訊威脅易受攻擊弱點性分析，俾確認對其負責營運部分阻斷影響之程度，以一頁之文件篇幅表達對未跨越不同風險組別，諸如屬低中高之風險狀態下之風險衝突評估，而對於巨大災難遜 參考資訊亦甚缺乏。
- 此外個人(通常微風險之經理者)則蒐集所有這些一頁文件資訊，並將它們用一個厚厚的資料夾家已歸檔存放，將可非常容易地確認明瞭資訊之依賴性或可數量化及其衝擊影之程度大小。
- 彙集厚厚的資訊檔案同時告知企業審計長已進行完成一項全盤性地資訊風險評估工作。
- 不必進行任何資安管控作為直到發生資安事件，此時得以找出誰是應該受責難歸究者。當資安事件發生時或許應備歸責之人，他本身並非官僚式資安方法論之創始或支持者。當缺乏用以支持正確性計算或數量化資料時，有關資訊資產安全性攻擊之可能性評估，恐怕仍然有賴於風險之評估者本身對企業經營之認知，尤其是關於企業之文化與人們作業之習性，數量化資安風險之評估多少有採用臆測之成分在內，不過這總比以不變應萬變要好，他總是一個重要的起步。

衝擊性

有關企業資訊安全事件之分析係屬企業風險管理方面重要之一項基本要素，就如高階管理者可以財務性用語來表達管理產生之效益情形，並可對問題提出顯著性之解答一般，例如：

- 一項資訊安全事件的發生對企業造成多少成本之支出，對產業供應鏈中其他構成因數之影響為何？
- 一項資訊安全事件對企業組織、營運能力、公司名譽和所需伴隨之依從成本影響有若干？

本文期盼有關發生資訊事件災難之回復，企業之永續經營和危機之管理方面以及在未來之發展過程中，BIA 皆預先可扮演一個重要且必須不可或缺之角色，BIA 得以顯著成功運作之因素包括有：

- 係被企業擔未或具功能性經理階層所掌握
- 具可數量化性
- 持續不斷更新
- 有效地被執行
- 經審計委員會簡是和核定

若干機構藉蒐及資安事件有關資料，運用以往資料去評估資安事件之衝擊性，例如對時間成本面之節省，在過去數年中除了因智慧財產權因遭竊所損失之成本外，有關資安事件之成本問題一直受許多出版刊物所廣為討論之主題，而這類成本損失在有關領域中之估計係屬困難者，或者至少是不容易正確估計者，實務上若所估計之數

字會經過企業高階管理階層代表之認可同意，那就表示一種進步了，不過這不代表估計值係完全精確者。

資訊安全投資之報酬

資安事件之發生必會對企業之營運經營產生因果關係，企業組織明瞭必須採取適當之行動，俾得以阻止、防止或減輕其衝擊之影響效果，而這需要有包括員工、過程、及技術等資源之配合投入，而企業應當投入多少經費用於資訊安全藉以保護其訊息資產？這恐怕是一個衍生性的老問題 ，也就是說企業個體應當投入多少資源用於資訊之技術升級，俾得以順利執行其營運活動？

盡管過往友有許多的發行刊物和組織架構(包括 ISACA 有關資訊安全之運作模型〔BMIS〕)，此一問題迄今仍然存有爭論，其原因主要導因於大多數對於資安環境領域在內之投資效益多屬無形以及具有投機性之本質，同時對於不確定性之事件本身就難以處理。吾人無法反對企業為資通訊科技安全之投入應計算 ROI 之問題，這好像在一個建築物內安裝門鎖管制物和安全性阻斷設施，這類性質之計畫會有巨額之成本開支(耐用期限)他係十分可預見者，這當然均需要企業組織性以及在程序上的改變和配合。

針對企業所關心問題即欲就不同之計畫方案，提出比較性之評估結果計算其投資報酬率(ROI)係最佳之方法，有關之計算方式得出可資比較結果者，成本因子應包括在內以外，尚可就不同計畫方案評估其利得，諸如個別所具有之不同功能性、成本金額、和涵蓋之時間範等。

單就單一選項計算之 ROI 比較不具有參考價值，因為它十分容易與支出聯結，以證實所具之正當性，最終決策之構成因子除了 ROI 之因子外，應尚有例如在其他組織之間相似投入裝置之經驗、賣方之支持力量，以及相關根據之理由等。

資訊安全支出增加一項哲學性空間之因數：

- 資通訊資本支出是真正的投資亦或只是企業營運中之一種成本支出？
- 將企業辦公室所投保險之成本加以區分為它屬於一種 投資是否正確？
- 選購防阻電腦病毒軟體程式係一種選項內容？

在許多資訊安全之專業化論著中顯示已將資安支出視為企業之營運成本，雖然資安支出不斷被要求應提供有關資安投資之回報率(ROSI) ，才可以符合企業預算上之需求規定。

已有相當多論述此一問題之刊物專論已發表[8 10 11]，但是彼此之間所獲致之結論亦有所矛盾，例如在英國著名的資安專家 Bruce Schneier 在其所公開發表，且直得尊敬的若干篇論文中指出，在理論上(ROSI)是一個相當好的觀念作法，但在實務上大多數之作法係將其棄置不採[12] ，暫時拋開資安支出在企業營運成本中之比率，另一項對立之論點反應者為企業長久以來，營運之經驗主要係專助於財務面之數據，而非在意何者事實上會對企業之經營比較有利，或許因信賴或是過於天真，企業在實際營運執行層面上往往疏于驗證上述這些數據之真實性，同時非常可能這些皆是錯誤之資料。

首先評估過程中比較簡單明顯的組成因素為成本部分，對那些熟悉資通訊科技深具相關經驗者而言，完全明白了解通常對時間和成本支出之效益評估多屬比較樂觀態度，此外除了產出與服務之原使成本外，針對企業營運時在計算分析其 ROI 或 ROSI 時非常容易忘記許多其他之成本因數，例如：·準備一項計畫提案或計畫要求時之前置成本，及其後續之評價(有時係因顧問之堅持) 。

- 有關採購過程作業上包括法律核閱費用之內部性成本支出。
- 採購項目之事後運輸、安裝以及結構配置之支出。
- 針對採購品項未來營運、維護和支援人員之教育訓練支出。
- 項目計畫之生命周期性支出(反映快速的退化過程，和許多賣方對產品偏短之生 命周期

短期)。
- 循環性不斷發生項目之一欄表諸如執照之更新費用、維護、安裝及隨時不斷測試之支出。

具有實務經驗之執行者應當能夠提出一個全盤性伴隨數據之表列內容，並樂觀地表示大約有30%上下之利潤空間(且甚少會被低估)，有關資訊品項利益(實際報酬)之評估，主要依賴於創新能力，儘管創新不論在未來或現在皆不乏臆測，或實際上示無法預估的，而未來之不確定性將使未來會出現許多非計畫之因果關係存在，這當然取決於下述若干假設之是否具有效性而定，例如：

- 所運送和安裝之資訊項目其品質內容，以及賣方所介紹之項目，其功能性是否可完全且真實地發揮，同時其產出不得有任何偏誤或缺失瑕疵。
- 資訊設備項目已被合適地配置，這在實務上多係熱切之盼望勝於事實之證明。
- 資訊設備項目已被證實具有單一分散式或多重集中式風險因素，資通訊安全對企業之營運衝擊影響，可提出因使企業曝露於資安風險時有關財務性定量化數據予以評估分析。
- 防止資通訊安全之利益由被資安認證之企業所有者獲得，並對資安之防護行動負有說明之責任義務。
- 此類資安之利益與時間數軸長短有關。

實際行動之執行者應當了解當要求藉諸資安投資報酬率值大小，用以確認資安投資活動之正當性時，有關之評估數據質未必精準，或許尚可能會有一些錯誤。

結論

本文顯示二種不同觀點之論述方式，俾提升資通訊科技較多的能見度和所引發之資通訊安全問題，在實務執行層面耗費相當多的時間，在尋找執行實務上遭遇問題之解決方案，用以減少企業經營決策階層決定計畫性投資支出時得以減少資通訊之風險，此舉必會有若干正常之質疑被提出，而大多數最受歡迎採用的資安風險管理方式，事實上也不會比傳統占星學作法更佳(對閱讀占星學有關內容者有一些抱歉)。

因此實務執行者勢必面臨相當大之挑戰：無法以精確具體之數字用以顯示正確地評估資通訊科技使用之訊息風險，適當地採取周全審密方式，強化資通訊科技安全體系之策略，以有助於對企業體價值增加，而下述二種行動方案有助於因應上述之資通訊安全挑戰：

- 對資通訊安全技術、運作過程和參與工作人員等易受攻擊之弱點，允以健全詳細之評核建議作法，就資通訊安全技術風險之有效評估是預先就應有，屬不可或缺的前提，這些易遭受攻擊之弱點與企業營運過程有密切之關聯性，以及因遭受此特殊性資安威脅所導致影響後果之攻擊程度。
- 對資通訊安全事件之回應、資通訊災難之回復、企業之永續經營和經營危機之管理計畫等方面之發展，應如何提供與時俱進和正當有效性之分析，在先驗上均係不可或缺者，這些應當必須有效地依序加以檢視規範，例如因環境因素改變時，當須倚賴從以往事件之教訓中所學習之經驗，將之融入到相關結果之分析中，因此包括對資通訊安全計畫之修正在內，倘若執行之情況並非如此，針對將資通訊安全事件予以分割獨立處理之企業將無法繼續存活下去。

本文亦論及若干資通訊安全因子雖然它係無法數量化，不過在與企業高階管理階層商討時，也認為下述資訊應當被明確地表示出來：

- 在人性經過深思熟慮下對企業資通訊資產發動之攻擊，在缺乏足夠資料用以計算和數量化風險因子時，就資通訊安全之評估者而言，至多只能依賴於其對企業 本身之認知了解智慧，尤其是有關企業之文化與從業之員工們，而通常所提供之數量化評估資料，也多少存有資通訊訊息臆測之可能。
- 資通訊設備在先天設計與製造時之偏誤會逐漸顯現其缺失

- 風險，或許有些偏誤仍然尚未被發現(一但被發現將遭抵制)，典型地說資通訊設備之賣方所提供之解決方案，有時多少又引入另一項新的錯誤 。
- 欲以統計上之或然率理論和其他統計技術方法，將資通訊資料予以數量化，截至目前由於欠缺足夠之資料，這不是一個可行有用之方法，因此只能繼續使用近似概略估計法，不過不應該忘記它多少總比單純之猜測要好。
- 當吾人評估資通訊安全之投資報酬率（ROSI）時，進行這類分析時應該存有相當可創造力之想像空間，對具有實務執行經驗之執行者可能會問：任何企業之經營階層在其心目中，對此問題是否存有特定之數據標準？
- 任何預測並非具十足精準性之科學。

ENDNOTES

1. *With the release of COBIT 5 in 2012, key elements of Risk IT have been incorporated in COBIT. COBIT for Risk is expected to be released in September 2013.*
2. *ISACA, The Risk IT Framework, USA, 2009,www.isaca.org/riskit*
3. *Ensmenger, Nathan; The Computer Boys Take Over (History of Computing), The MIT Press, 2010*
4. *NATO Science Committee, Software Engineering Techniques, in a report of a conference, April 1970, p. 15*
5. *Cowart, Robert; Brian Knittel, Microsoft Windows 7 In Depth, Que Publishing, 2009*
6. *Twain, Mark; "Chapters From My Autobiography," 1906,*
7. *in which Twain attributes the phrase to Benjamin Disraeli (UK Prime Minister)*
8. *Bierce, Ambrose; The Devil's Dictionary, 1906*
9. *This is the essence of the book The Black Swan by Nassim Taleb.*
10. *Gordon, L.; M. Loeb; Managing Cybersecurity Resources: A Cost-benefit Analysis, McGraw-Hill, 2005*
11. *10 Singh, Jaspreet; "Pay Today or Pay Later: Calculating ROI to Justify Information Security and Compliance Budgets," Information Systems Control Journal, vol. 3, 2008, www.isaca.org/archives*
12. *Anderson, Kent; "A Business Model for Information Security," Information Systems Control Journal, vol. 3, 2008, www.isaca.org/archives*
13. *Schneier on Security, "Security ROI," 2 September 2008, www.schneier.com/blog/archives/2008/09/security_roi_1.html*