強化資訊安全治理
Strengthening Information 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 also a faculty member of Webster University, Geneva, Switzerland. He is a regular speaker at international conferences covering audit, risk, governance and information security and is the author of several publications Gelbstein lives in France and may be contacted at ed.gelbstein@gmail.com

譯者: 劉其昌, 立法院教育及文化委員會主任秘書
中華民國電腦稽核協會 會員服務委員會主委、編譯出版委員會委員

資訊安全治理機構和國際電腦稽核協會，係在眾多單位最先頒布資訊安全治理指標的單位，他們發表的各式出版物[1、2]；也獲得其他資訊治理機構的補充，包括尚未發行的國際標準 ISO 27014[3]，以及資訊安全論壇最新修正的優良實務準則[4]。此外，例如顧納(Garter)群體[5]，在有關工業顧問服務方面，亦提議其他方式之資訊安全架構。

在晚近的一、二年中大凡是在足以增加資安可見度與敏感性領域者，大致上皆是到支持歡迎，在資訊產品生命循環縮短之情況下，很明顯地是任何一個組織皆會無法避免地遭受創新科技浪潮之影響。

比爾蓋茲(Bill Gates)和艾倫(Paul Allen)這些微軟電腦公司之先驅者，曾經夢想在每一個家庭的每一張桌子上都應會有一部電腦設備放置，他們的構想沒有錯，但是它耗用 30 年之時間才達到目標境界，當蘋果電腦發表 iPAD 平板電腦時，在資訊產業之需求面上並無先例，但也只不過一夜的時間，iPAD 卻變成一項人民必備之手持裝置，若無資訊部門和安全之主管們會被視為不合格，而訴諸在政策面上你必須持有手持裝置，否則在執行部門者而言，你將落後其他許多朋友們，此外，無可避免地沒有任一機構組織不會受到資訊之攻擊影響。

嫌疑罪犯包括相當範圍內之行動者，從個人式的駭客延伸到有組織式的群體(諸如匿名者)，以及其他具高度競爭性而無法證實身分之群體，他們採取各式組合之偵探方式(例如在產業上之間諜或是其他)，採取有組織方式犯罪和知悉內部情資之人。

最近發生比較重大的資安缺口包括在倫敦、瑞士商業銀行之疏漏、詐欺，以及在伊朗因疏忽不小心引入鈾元素到其設備之中，當然這些也僅是因其有名而被揭露，當屬各層冰山中的一角而已，網際空間之攻擊每天皆有不同方式呈現出來，其中發生許多，但並沒有出現在媒體之爆料，因為它的嚴重性尚不足以構成媒體之頭版新聞。

通常夜間之防盜警報裝置皆運行妥當，除非他們的保險公司堅持要這麼做，否則多數民眾皆是被偷竊之後才會去安裝警報設備，請問我們的資訊安全治理是否也落入這種同一屬性類別中?

資訊安全治理(ISG)述言:係不具優先性亦遭忽視，且資訊安全治理(ISG)之目的其架構各種方向以敘述地非常清楚，可以匯總如下加以評估，指導管理和監視資訊安全之範圍，包括:

1. 確保符合企業之需求
2. 強化資訊安全保證之能力
3. 確保資訊風險已經持有人之證實
4. 降低不依從之風險
5. 降低被訴訟之風險
6. 達成可證實的信任、誠實、完善和有益性(CIA)。

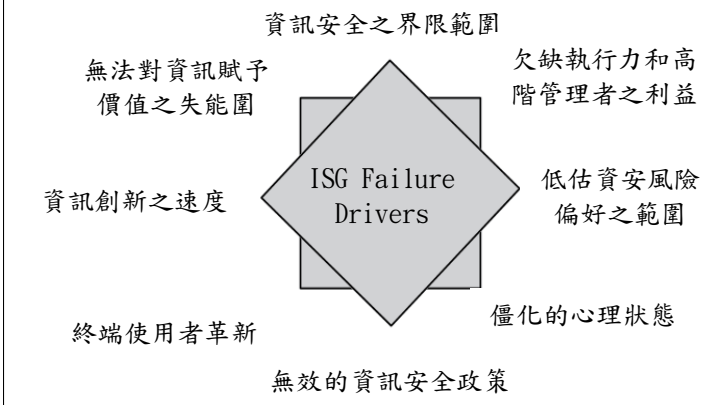
資訊技術面涵蓋之安全要素中，具有若干共同之元素，皆存在於各種組織中，幾乎不論組織其活動之特性為何，這對於電腦中之伺服器、儲存裝置和網際網路皆是正確地，人們將它應用在企業資源管理(ERP)和顧客關係管理(CRM)以及諸如電子郵件和遠地接曲之行動服務中。

不過組織文化之歧異程度對於個別資訊安全有差異，即期可承受之安全性非常不同，其中一個極端為社會非常依賴的重要性，資訊基礎理論(例如公用事業、緊急服務、國家安全)，至於另外一個極端則存在於當有一個巨大偶發事件發生，但他對社會之衝擊傳播不會超過圍牆之外---亦即最壞狀況沒有人會在意他們的信譽會短期間遭受到負面影響。

本文反應出非營利機構過去幾年執行安全審計時之發現，包括在歐洲、中東和非洲等地區有關之資訊安全論壇會議，討論時所獲取之看法意見以及其他事業機構所蒐集之結果，雖然樣本或許不具有統計上之顯著性，其結論指出在評核明知資訊安全治理(ISG)重要性的排名上，董事會成員和執行階層並沒有將資訊安全治理，納入他們最關心在意的最前十個領域中。

在過往的十年中本文作者所蒐集的發現結果，以資安失敗的導因方式呈現導致資安信息治理缺失、失能、或欠缺者之主要因素，在有限之資源和不是論壇中討論個案之情況下，提供業務執行面上執行者認為最妥適的方法。

圖 1 顯示匯總的資安治理失能的八個主要動因



資訊安全治理失能的動因 1:資訊安全之界限範圍

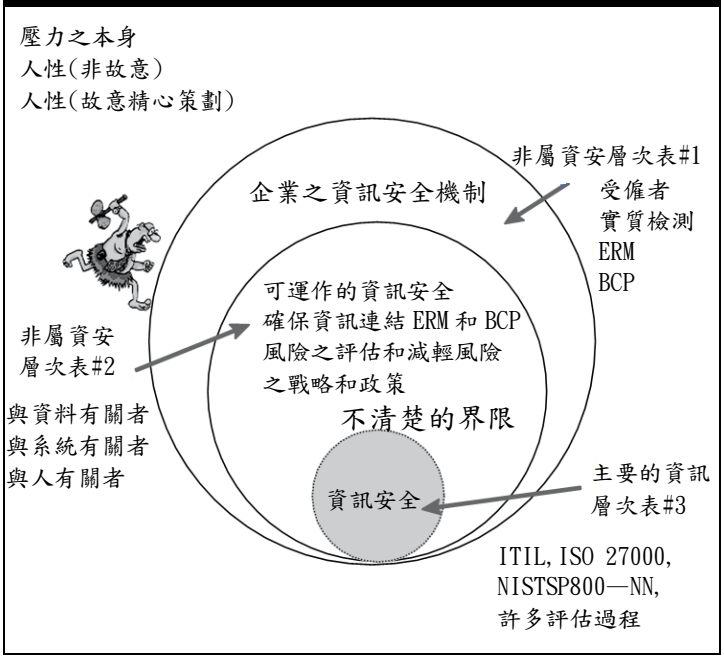
高階行政階層和資深經理們通常都認為資訊安全係企業資訊部門之責任，當吾人相信資訊之服務供應者時，以機關之身分而言這就是構成一個處理資訊安全治理的外部性責任。

這或許也只有部分地正確，如圖 2 內容所示，其實應定義為那些得以接近存取系統資訊者，因為他們擁有使用資料的權限，因此這些任務型之經理們也應當伴隨負擔資安治理之責任。

有關在資料確認(認證)和存取管理，安排資訊安全簡報和培訓員工的循環期中，這也是同樣真確的，比較重要的是這取決於企業經理人致力於評估資訊風險和管理，對企業衝擊分析，以及對企業永續經營計畫之影響，這反應了個人化體制和電子化設備所扮演之角色。

同樣地，當資訊部門提供了有關政策輪廓方向資安治理安全訊息時，它必須被其他部門團體們進行檢視和評核同意，這當中可能包括人力資源部門(HR)、法規顧問部門等，這也取決於組織幕僚所代表的成員多寡，以及其他之部門團體等，再者除非上述部門間之檢視評核係可付諸實踐者外，只靠資安部門之資訊治理之投入會變成白費力氣。

圖 2 資訊安全性之背景環境



資訊安全治理失能動因 2:欠缺執行力和高階管理者之利益

無論公私部門經與許多主要的執行長們(CEO)、部長、外交官和高階管理階層藉工作和夥伴關係，舉行資安治理會議商討問題後，獲得一個十分明確地結論，上述這些高階管理主要階層們工作之時間都十分寶貴值錢，各種壓力只會驅使他們將注意力集中在當前、當下最具重要性之問題上，而部門之資訊和其安全程度，通常並不會被它們納入這個層次中處理，除非資安已經造成偌大之錯誤時，而當這發生時他們的反應也只是去整修處理而已。

在某些不大可能發生之情況下，當他們決定去參加資訊或資訊安全治理之研討會上，這時他們可能會發覺資安問題重要，且公開的表示願意接受正視它，不過私下任為資安只是一個浪費官階管理階層寶貴的時間而已。因為資安之重點非企業業務行銷所重視者，他僅是一個技術面之問題，但若同時有另外一個會議，他們很可能會派不具有資安專業權威的另外一個代表去參加。

欲以如果資安發生不知會造成甚麼衝擊，來請公司高階主管思考一下問題，這個理由不再具有任何藉口，只有當高階主管們深切了解資訊系統之安危，足以對其組織營運活動構成相當之巨大影響衝擊時，他們才會十分樂意地去正視此一問題，此時對於任何潛在之資訊安全漏洞皆不會放過----至少會持續到找出資安漏洞之後為止。

當資安漏洞發生時且造成巨大衝擊效果者-----例如 2007 年在法國之 Societe Generilo 之資安損失達美金 70 億元以上，以及於 2011 年在英國倫敦的瑞士信貸(UBS)資安漏洞損失美金 20 億元以上等，這兩個案例皆係因控管風險進行不當，進行未經合法授權之交易所造成者------這些事件已迅速地強化升級了資安管理之問題層次。

一旦短期之問題獲得解決後，即刻之利益消失後，吾人相信資訊本身並重視安全之信念，已經被建置完成了。

這個情況處境對資訊科技安全經理者而言，早已司空見慣好多年了，他們渴望能夠榮登於主舞台，但是通常皆在未受邀請之列，這或許部分原因是因資安人員通常用的是技術空泛特殊語言，而非企業營運行銷之語法，此外,資訊安全有時感知被認為係企業創新發展思想上的一項障礙。許多資訊科技安全之經營階層在企業組織中和創新產業常是有名的”非”博士級水準。

行政階層期望獲得最近非常流行的科技裝置(在 2011 年為平板電腦)，但是資訊部門會以基於資訊安全議題之理由，不能分配科技裝置於有關人員，這種觀點不大可能獲得支持，尤有進者甚或會因而導致企業發生利益之損失。

資訊安全治理失能之動因 3:低估資安風險偏好之範圍

國際電腦稽核協會(ISACA)在所論及之資訊科技之風險架構時，表示資訊風險範圍涵蓋，不只限於對企業營運與服務層面之負面衝擊影響。它尚包括企業因喪失商機，所伴隨之風險損失價值，以及藉資訊科技之技術來增強，或強化企業之營

運機制(註 6)，在第五章之風險治理基本條件章中，內容有多次使用到風險偏好性向趨勢和風險容忍程度之用語，但是這兩者間對資訊風險之真意，仍存有潛在性十分高的誤解，這兩個詞語是不應該被交互使用的。

有關圖 3 列示資訊科技架構之風險，從資訊安全治理的觀點觀察，它描述了採用資訊安全對企業之利益，作為行政執行管理團隊了解資訊風險管理所扮演之角色，更甚於重視行政管理職責之責任，資訊科技風險之應用對於企業策略目標影響，和如何有效使用資訊科技來降低策略運作上將衍生之風險。

資訊風險偏好性向趨勢規範衡量，一個組織可以願意接受多少的風險壓力，在採取減輕風險動作之前，企業之資源必須可用於執行支持這類行動，資訊風險偏好性向趨勢的一個廣義說明內容，不應有資源賦予對風險持有者甚少助益之必要行動。

資訊安全治理傾向挑戰探索永無止境追求企業成本下降，和所需資源用以減輕不確定規則下環境之風險間之差距，在此有關過往歷史和統計工作所能提供之助益有限，有關成本下降，或延遲不落實之作為等，皆會提升組織之風險偏好性向之趨勢。

當偶發意外事件之影響程度大於風險之性向趨勢時，其所遭受責難之人，將非當時核准抑制減少成本者。

資訊安全治理失能之動因 4 僵化的心理狀態

以最寬廣意念欲確保資訊安全機制，必需有賴於企業個體外許多資訊科技單位部門其提供之功能與之服務者，以及負責資訊安全之主要官員們(CISO)之首肯承諾，這些主要的參與者包括:

- 系統及資訊之擁有者—主要之參與必需(至少)為資料之分類負起責任，在確保必需知悉的最基本權利前提下，應定議資訊存取之權利，有關權責部份應建置合適的區隔觀念，提供投入資源對企業衝繫之影響分析。
- 應用發展層面—提供確保資訊之安全，唯其實際應用面上不包括系統內崁入之邏輯炸彈，後門程式或其它設施，這些可提供以接存取所產生之資料。
- 人力資源—確保指引資訊發展和落實資訊安全政策時，會對機構人員產生一個直接之衝繫，人資部門因了解資訊之發展提出支持人力培訓計劃資安之部分，同時強化企業 之資訊安全文化與落實在企業之組織實務上。
- 採購功能—確保確信與供應勞務之賣方向採購契約之有效性，包括如何合適地規避資訊軟體最易受責難之弱點的防禦功能，以及保証資安之漏洞缺口
- 法津顧問—藉由所有法規程序和應遵守之行政規章來指導企業之職工和其它使用者，承擔為獲取目標所需具備之規定，和一連串針對資安之監督，管理作為確保相關安全政策有效地運作。
- 內部審計—針對資安管理提供一個獨立且客觀的確定保護方法
- 其他部份—益及設置有關貿易結盟/員工組織協會，預算辦公室等之設置當取決於各個組織結構之性質而定。

就核心之活動而言，上述任何一項的功能可能皆會處於十分忙碌之狀態，而資訊安全治理在潛意識上今被視一種混亂分心的作法，在最極端之情況下會認為資安治理並不在我的工作職掌範圍內(亦即僵化的心態)這種無可避免的辦公室政治哲學，是另外一項會更進一步惡化資訊安全治理的因子。

圖 3 聽取觀眾和利益	
角色	**採用和適應資訊風險架構下之利益和理由**
1.董事會和經營管理階層	應多瞭解資訊科技管理之責任以及所扮演之角色，應用資訊科技到策略性之目標計劃，和如何善用資訊科技來降低策略性採用時之風險。•存取朋友清單與網路取得公開的履歷並允許使用搜尋功能擷取
2.公司管理者之風險(有關 ERM)	協助經管資訊科技風險，調和接受一般化通用 ERM 原則。
3.管理者之營運風險	將企業經營風險與資訊科技風險架構相互連結，確認營運之損失或關鍵性風險指標之發展
4.資訊科技管理	妥善了解如何確認和管理資訊科技之風險，和如何導引將企業資訊科技風險應用到企業決策之中者。
5.資訊科技服務經理	強化營運資訊攸關風險的論點，應當其使適合於整體企業資訊風險管理架
6.企業永續經營管理者	與 ERM 建行整頓(因為在評估風險上它係責任的一個主要觀點)
7.資訊科技安全經理者	在所有各類資訊科技風險之中，予以定位安全之風險程度
8.資訊長們	獲取有關資訊科技風險較佳之觀點，和其為投資和投資組合管理目的之財務性應用內容
9.企業治理官	支持其論點同時監視其資訊治理之責任，以及其它資訊安全治理扮演之角色
10.企業經營階層	了解和管理資訊科技之風險-許多企業的風險之一，應當全體同心協力合作
11.資訊科技審查者	妥善分析風險內容，和支持審計計劃及審計報告
12.管理階層	支持且評核管制性企業之資訊科技風險管理之步驟與方法
13.外部性審計者	增加對資訊攸關風險水平之監理，同時建立內部控制品質方面之意見回饋
14.保險業者	支持建立合適的資訊風險保險涵蓋範圍，同時針對不同風險水平追尋一致化標準
15.機構之評等	與保險業者合作提供對企業內部處理資訊科技風險治理實之客觀評核與評等機制
資料來源　ISACA，資訊風險之架構，USA 2009 年	

資訊安全治理失能之動因 5:無效的資訊安全政策

資訊安全政策內容係一大堆或一套可做與禁止做的作業規則，在大多數的國家皆與法津調和，企業組織負責人以代表全體持股人身份有責任建立一套確保企業資產安全的義務，在一個理想的世界裡，資安政策之發展應使公司資深高階層經理階層明瞭且涉入資訊安全之管理中，同時使資訊安全治理居於合適之優勢地位。

為規範一個組織企業有關資訊可信度、有效度、完整性政策等相關資訊體系之經營哲學、營運策略、政策法規、和執行實務等方面之文書應該被分開保管，發行公布、據以遵行，當資安治理良好設計實行後妥善用運行時，將可以產生下述多項功能:

- 他規範資訊體系與資料之可接受範圍區間和使用時之權責
- 他定義處理資訊安全事件之委任權威(限)
- 他對於全體所關切的資訊安全治理提供實務上之指導.
- 他對於顯示資安實地查核過程提供一般性步驟和有關電子與紙本之查核 軌跡路徑。
- 他提供符合國際性查核一致性必要之查核標準 諸如 ISO27001

備妥成套的資訊安全政策說明書後，想要簡單亦可非常簡單，如果視為十分困難也會如想像般地困難，資訊安全政策的樣板標準可免費地從甚多來源處免費加以下載，針對政策大綱、摘要、或每一個條款非常詳細小心之技術性規範的資訊安全對策，皆可價購獲取(有關後者尚陷於熱中具有追求策略完美止境的誘惑)。

不論資訊安全治理之對策，係經由何種路徑來發展，僅完成文書之配置顯然是不夠的，為達有效化境界針對每位履行承諾者，皆必需充分瞭解資安政策內涵之意義，其得以有效地配合執行（避免有一種從未接觸之反應）更重要的是這些都應屬於強制性之規定（註 7），上述這些沒有一件是十分容易可以達成的，情況最壞的是在許多機構單位中，誰擁有對資安政策執行之創制權、傳播宣導權、和監視遵從性的機制等其實均不明確清楚。

此外依據最近之審計經驗顯示，許多機構單位之作為已落後於時代之潮流，因為他門尚沒有針對終端使用者需求革新(參見資訊安全治理失能動因 6)的因應對策。

資訊安全治理失能動因 6：終端使用者革新

當機構單位為其營運工作力選定安裝，提供妥當電腦硬體資訊設備和軟體之安裝後，企業營運生命週期本身並非困難之事，在此一情景下針對軟體之安裝和系統本身服務之存取，從資安角度而言，在合理範圍內當具有可控制者，通常這個在數位環境之下的所作所為，皆可能會被監控治理的。

當家庭之辦公室中皆可購置之電腦設備出現之後，以及體積小具移動性之輕便資訊裝置出現之後，使得資訊安全問題變得難複雜了，就個人而言，用途具實用性之寬廣和直接對消費個人設備價格之不斷下跌－如筆記型電腦、平板電腦、智慧型手機電話，口袋大小具高儲存能量的裝置，所導致消費者迫不及待地採用，其結果造成機構單位產生資安之壓力，迫使允許員工可以伴隨攜帶他們使用之自有技術內容（ＢＹＯＴ）軟體。

上述這些作為皆會導致機構單位公司之資訊架構。不易掌控而產生安全性問題，而當企業之員工必需使用存取企業之電腦資訊系統，和用他們自身使用之資訊軟體裝置使用資料時，將不易被適當地作好系統安全防護機制，因此會產生下述的若干問題包括：

- 智慧型電話／平板電腦 ＡＰＰＳ程式中是否包含粗心大意漏洞？
- 是否所有之資訊裝置皆置於保管安全處，倘若如此誰持有鑰匙？
- 是否公司之資訊已被儲存於某處所，但是公司組織並不知道其實際處所？

- 是否有資訊裝置遭至遺失？

除了消費者持有之本身軟體技術外，Ｗｅｂ 2.0 技術之出現產生了新的挑戰；他們傳播專業化與個人化活動之間的界限差異，第一個問題是如何合適使用社會網路、部落格、和有關論壇中意見之自由表達，這是一個配量之基準，第二是有關雲端科技之事務。

最近由本書作者主導的審計工作，確保公司之資料包括若干敏感性之文件，已經被上傳到雲端資料庫（在這個特殊之情況係指Ｇｏｏｇｌｅ Ｄｏｃｓ上和Ｇｍａｉｌ電子郵件) 而使機構單位之使用者發現，可以遠端地存取令人麻煩的資料之處理程序，而執行他們的工作，文字訊息之快速傳播是十分容易簡單地，而接下來會不斷地會蔓延傳播開來。一旦這種（類）處理實務被建立認定，未來將會十分困難去清除。

資訊安全治理失能之動因 7：資訊創新之速度

資訊創新（亦即科技之技術、服務和設施）之速度和與生俱有數字化（Ｙ世代青年）之熱情，已將資訊創新速度被視為他們人生中的一大部份，這就好像伊索寓言中的野生兔子一樣（註８），而組織個體在建立資訊創新政策，和規範有關運作之方式十分緩慢，則宛如龜速般地在進行中。

較不幸地是資訊安全問題涉及三方面對象運作之競賽，這三方之參與者們屬眾多行動者中的任何一個，在排除奇妙心理，自己滿自大、情緒和敵意；財務性利得、或政治動機外，仍有處心積慮心態破壞企業單位之資安防禦措施，扮演這種角色者包括或至少會不斷提升對資安治理之危脅程度：

- 大部份年青熱心的駭客和他們如小孩般的劇本，皆屬於Ｘ令人討厭者，
- 資訊科技中的惡棍以其專業智能和經驗運作，宛如網際空間的為金錢而工作之圖利者。
- 網路行動主義者和駭客們找一個藉口組呈匿名集團 (他們即使皆擁有臉書)
- 內部人士獲取智識與經驗之動機與欲望
- 工業性間諜以獲取智慧財產權和其他可資信賴資料者為目標 ．
- 與組織犯罪無關連之惡意軟體設計者(非有意犯罪)
- 與組織犯罪有關連之惡意軟體設計者(有犯罪故意)
- 惡性殺手級的軟體設計者(藉由州政府、軍隊或非州政府之行動所贊助者)

正如本論文在一開始所敘述者，沒有任何一個組織單位之資安不會受到影響，若以比較樂觀之經驗來觀察或可說，從未有如此糟糕之情況，資訊安全治理不可能變得更為惡化。

資訊安全治理失效動因 8 ：無法對資訊賦予價值之失能

重要的資訊基礎建設原則上應足以擔負衡量資訊不安全時之衝擊影響程度，以計量方式收集許多資料諸如在商業區內一項特定活動之成本開支(例如一家銀行會持有其交易往來對象之資料)，這類成本正常的情形將會包括組織單位之直接性成本以及有關顧客之法律義務成本和名譽之損害等。

有關資料之完整性損失程度比較難以估計衡量，除非未經合法授權更正資料之詐欺行為被偵測發現，如 1994 年之霸菱銀行損失(註 9)、2007 年的 SOCIETE GENERALE 事件(註 10) 以及 2011 年的瑞士信貸(UBS) 犯罪等皆是在其中最有名的內部人士未經合法授權修正資料，所產生的重大網路詐欺犯罪事件。

在各個不同產業間供開揭露資訊(外洩)之成本代價差異非常之大，例如 2009 年杜邦公司在法庭上主張一家韓國公司 Kolon 廠商有竊取杜邦公司 Kevlar 品牌產品之商業交易機密資料，在 2011 年 9 月間美國維吉尼亞地區法院宣判應賠償杜邦公司大約近 9.2 億美元之損害賠償(註 12)。

在 2007 年杜邦公司發生一個令人不甚愉快的有關經驗，因為公司內部員工從其電子資料圖書館中大量下載數以萬計之文件資訊，當檢方搜索該員工之住家時，在其各部電腦中發現未經保護的高級機密文件，以及好幾袋以被撕程粹片的技術性文件，該員工最後被宣判處以 18 個月之監牢，同時必須應支付將近美金 5 萬元之賠償罰金，依據該公司之評估表示遭失竊之資訊價值在美金 4 億元左右(註 13)。

另外有一個極端情況是有許多之組織單位(依作者之論點)根本尚未評估它們本身持有企業資訊資產之價值究竟值多少？資訊審計者指出：

- 我們偏好資訊之透明度和揭露而不進行任何隱藏，當有不少問題之思索引起類似無法持那種想法觀的答覆之後。
- 在這裡網路欺詐不是一個問題，因為吾人之工作同仁接致力於此，且在潛意識裡十分相信網路之安全性信任他 ，就好像網路欺詐本身從來沒有發生過一般。

結論

當資訊安全治理機制處於脆弱或不足情況下，此時資訊安全治理之指導，則僅賴於一些個人基於其全心努力之方式維持，這種在本質上效果是有限地，處於此種情節之下，組織單位本身顯然沒能好好地準備妥當適用，以阻止任何來自網路網際空間之任何攻擊行動。

缺乏資訊安全治理周全準備下的主要徵兆，包括有下面:

1. 有權責的管理階層、執行單位和董事會成員們對資安治理缺乏足夠智識或興趣使然。
2. 資料之所有在體制中權責不清楚，有關資訊安全治理缺少可責性。
3. 相信資訊安全治理僅屬資訊科技本身的問題而已。
4. 資訊安全治理政策組合本身不具完整性，無法涵蓋所有情況，沒有軌跡追蹤同時也無法與時俱進。
5. 有關資訊風險之評核作業不完整或根本不存在，對資安治理本身風險本身沒有任何登載，亦無任何減輕資安風險之計畫。
6. 提供予資訊安全治理之資源不足(包括人力、工具和資金)
7. 企業員工職司負責數位化行為者，缺乏合適之指導方針。
8. 使用終端設備使用者所持有之設備，沒有任何法規之限制與規定。
9. 資訊安全治理政策及其執行，被視為是一種障礙物。
10. 有關企業營運項目欠缺任何安全之計畫標準。

下面的方法被用來以分數評估組織單位，對資訊安全治理之準備程度良窳，針對所指定適用稽核項目的每一項徵狀給予一個記點分數，所計得知分數若介於。

- 8 至 10 分者表示組織單位在資訊安全治理上，存有一個十分嚴重的安全問題，請問執行單位知悉嗎?
- 5 至 7 分表示該組織單位欲獲取較佳之 CIA，必須留意更加努力做好才可獲得，此時那一種徵狀現象應當被優先地處理?
- 1 至 4 分者表示該組織單位係在一良好狀態下，處理資訊安全治理問題，此時是否還有任何人願再努力作業來調降分數值?
- 0 分者表示可加以恭喜，該組織單位對資訊安全治理問題處理地十分良好，不知資安治理審核者，是否同意此項評估結果?

ENDNOTES

1 IT Governance Institute (ITGI), Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, USA, 2006

2 ITGI, Information Security Governance: Guidance for Information Security Managers, USA, 2008

3 International Organization for tandardization (ISO), ISO 27014 Information Technology—Security Techniques—Governance of Information Security, publication planned for release in 2012
4 The Information Security Forum (ISF), Standard of Good Practice, 2011
5 Gartner Group Research, The Gartner Information Security Governance Model, 2010
6 ISACA, The Risk IT Framework, USA, 2009
7 Creech, Jason; Matthew Alderman; "IT Policy Compliance for Dummies," J. Wiley and Sons, 2010, www.qualys.com
8 Aesop; "The Hare and the Tortoise," Aesop's fables, available from several publishers
9 BBC News staff reporters, "How Leeson broke the Bank," BBC News, 22 June 1999, http://news.bbc.co.uk/2/hi/business/375259.stm
10 Fraser, Christian; "Societe Generale Trader Kerviel Jailed for Three Years," BBC News, 5 October 2010, www.bbc.co.uk/news/business-11474077
11 Financial News staff reporters, "Meet Kweku Adoboli,"Financial News, 15 September 2011, www.efinancialnews.com/story/2011-09-15/kweku-adoboli
12 Business Week, "Kolon Loses 920-million Verdict to Dupont in Trial Over Kevlar," Bloomberg, 15 September2011, ww.businessweek.com/news/2011-09-15/kolonloses-920-million-verdict-to-dupont-in-trial-over-kevlar.html
13 The Kaspersky Labs Security news service, "Infamous Insiders: Eye-popping Heists by Insiders," 2011,http://threatpost.com

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 2, 2012 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：

ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2012,Volume 2中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。

Copyright

版權聲明：

Disclaimer:

The ISACA Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

免責聲明：

ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每年出版的ISACA Journal。

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal 則無法保證內容的原創性。

若為非商業用途之課堂教學，則允許教師免費複印單篇文章。若為其他用途之複製，重印或再版，則必須獲得ISACA的書面許可。如有需要，欲複印ISACA Journal 者需向Copyright Clearance Center(版權批准中心，地址：27 Congress St., Salem, MA 01970) 付費，每篇文章收取2.50元美金固定費用，每頁收取0.25美金。欲複印文章者則需支付CCC上述費用，並說明ISACA Journal 之ISSN 編碼(1526-7407)、文章之出版日期、卷號、起訖頁碼。除了個人使用或內部參考之外，其他未經ISACA或版權所有者許可之複製
行為則嚴明禁止。