淺談資安風險與網路保險之發展

李珍穎

一、前言

伴隨著網際網路的加速發展、金融科技的應用以及資訊通訊基礎建設的普及，更多的個人、企業和政府機構紛紛的在網際網路上應用以及提供服務，也促進了電子商務的發展。由此可知，網際網路在現代社會中已經融入個人的日常生活、企業的商業行為、政府機關資料到跨國的資訊傳輸，成為了不能缺少的角色。互聯網已經成為國際交流合作的重要橋樑，也讓世界緊密的連結在一起，同時也會帶來資訊風險的問題。世界經濟論壇 2018 年發佈之全球風險報告指出，全球十大風險中，其中網路攻擊、數據詐欺或竊取即與資訊風險有關，其發生之機率與影響逐年增加，可以看出企業面臨的資訊安全威脅越來越險峻，只要受到攻擊，就有可能導致嚴重的損失，因此不少企業也開始尋求移轉風險的解決方法。產業顧問公司 Frost and Sullivan 於 2018 年 5 月的研究報告指出，企業遭受網路攻擊的經濟損失常被低估，台灣 2017 年總計因資安威脅造成 270 億美金（約新台幣 8,100 億元）的經濟損失，將近台灣 GDP 的 5%，其中由於攻擊手法的快速迭代，有 97% 的惡意攻擊來源都是首見，沒有被列在過去的黑名單中，顯見網路安全需要更智慧的情資分析，化被動為主動防禦。其中直接損失最顯而易見，包括營收與生產力的損失、罰金與訴訟費用以及修補工作費用，但這只占總體損失冰山一角，還應包含客戶轉移與商譽影響等間接損失以及對整個生態系影響的延伸損失。

二、近年來重大資安事件及資安相關法規

近年來全球就有不少和資訊安全問題相關的事件，橫掃全球的 Wanna Cry 網路勒索讓台灣發生史上最大的資安事件，2018 年 8 月，台積電在安裝新機台時未事先隔離確認病毒狀況，造成 Wanna Cry 入侵，使機台當機及重複啟動，造成竹科、中科與南科廠區停工，損失五十二億元。根據統計，Wanna Cry 事件，台灣是全世界第五大受害者。今年 8 月台灣又發生 56 家醫療院所電腦主機遭「勒索病毒」攻擊，全台無數病患及員工個資和醫療數據全被挾持，駭客要求以比特幣作為贖金。因此可知資訊風險存在損失幅度偏高的特性，對企業的永續經營影響甚鉅，以下為近年來全球重大駭客攻擊的重大事件。網路世界所面臨的風險，已經不遜色於真實世界的危險性，在各種惡意程式或是可供利用之漏洞層出不窮的情況下。各國政府也陸續意識到數位軍火的強大，不僅要設法理解網路風險對於國家、政府、企業甚至民眾可能帶來的重大損害外，更紛紛透過制定各種資安專法的方式，延伸政府對於網

路世界的風險管控能力。美國在 2015 年 12 月 18 日通過新版的《網路安全法》，就是希望透過《安全資訊分享法》的修正，建立一個獲得早期資安預警的資安分享框架。另外一個影響全球甚鉅的資安法規，就是歐盟歐洲議會在 2016 年 4 月 27 日公布的《歐盟通用資料保護規則》（GDPR），不僅因應科技發展，將許多現在科技的資訊列為個人資料（PII）的一環，例如：IP 位址、Cookies 或者是地理定位系統 GPS 的位址等，更將違法外洩歐盟民眾個資的罰則，依照情節輕重，從 1 千萬歐元或全球營收 2%，提高到 2 千萬歐元或全球營收 4% 不等。而 GDPR 在 2018 年 5 月 25 日正式實施，對於全球以及許多台灣企業在內，因應歐盟 GDPR 的個人資料保護規範，已經成為國內企業界資安重大挑戰之一。在國內，2012 年個人資料保護法修法之後，企業提高對客戶之個人資料的保護意識。而 2015 年政府修正新的個人資料保護法，強調資料保護的重要性，也懲罰企業發生資料外洩事件時，需要繳交罰款來警惕企業未善盡資料保護的責任。再則於 2016 年 8 月成立國家級專責資安單位「資通安全處（Department of Cyber Security）」，並於 2018 年 5 月 11 日完成「資通安全管理法」，規範公務機關、公營事業及政府捐補助的財團法人，並廣納能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關，以及高科技園區 8 大領域的關鍵基礎設施提供者，都須向政府提報資安維護計畫，且發生資安事件時，應立即通報中央目的事業主管機關，藉此強化我國資安防護網。

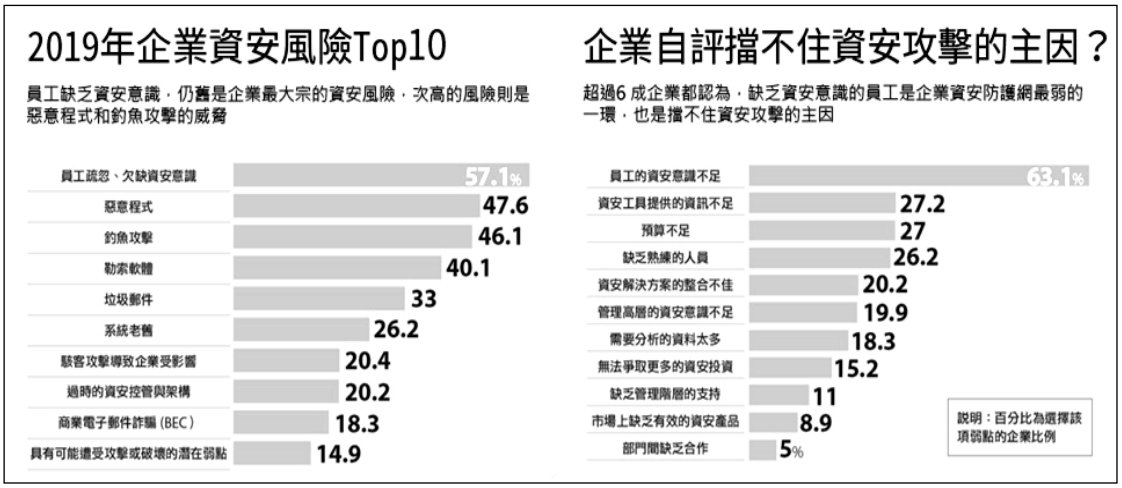
資料來源：現代保險新聞網

圖 1　全球重大駭客攻擊事件

三、主要之資訊安全風險

資訊安全包含電腦設備、機房，以及系統和資料的安全。但是，隨著科技的普及應用，企業對資訊科技應用的重心，逐漸從資訊部門擴展到使用者部門。資訊科技已被普遍應用於企業與客戶及供應商的互動合作以及企業內部作業流程等活動上。因此對於企業資訊安全控管議題必須涵蓋企業的市場、財務、人力資源、客戶、產品、內部運作、安全控管以及商業機密、程序科技知識等專屬資訊或是軟體、硬體、基礎設備、資訊技術專家、使用者知識等各種資訊資產的控管安全之上。資安風險是指易受威脅的資訊資產，在資訊系統運作過程中，遭受到外力威脅時，因資訊資產本身存在的弱點所可能引發的各種威脅，例如資料處理錯誤、網路損壞、設備/資料遭竊、軟體錯誤、電腦詐欺、未經授權的存取、電腦元件故障、被人蓄意破壞、自然環境災害、設備誤用、病毒木馬，或是資訊服務停機等。尤其當資訊系統愈趨複雜，也會同時強化資訊風險問題的嚴重性。這些風險可以進一步歸納成系統面與管理面兩部份。基本上，系統面的資訊風險就包括軟體、硬體、資料與網路四個部份；管理面的資訊風險則有實體、人為，以及管理層面的問題。

根據 2019 年 iThome 資安調查的問卷，該調查對象涵蓋台灣 2 千大企業，結果發現台灣企業資安風險比例前十，由高比例依序排序，分別是，員工疏忽欠缺資安意識、惡意程式、釣魚攻擊、勒索軟體、垃圾郵件、系統老舊、駭客攻擊導致企業受影響、過時的資安控管與架構、商業電子郵件詐騙、和具有可能遭受攻擊或破壞的淺在弱點。然而企業們自評擋不住資安攻擊的主要因素員工仍舊是企業最大的資安風險，也是企業 IT 主管自認擋不住外部攻擊的主因，4 成企業還擔心惡意程式、釣魚攻擊和勒索軟體的威脅。有關台灣資安風險及企業自評擋不住資安風險主因圖 2 所示。



資料來源：iThome 2019 資安大調查

圖 2　台灣面臨十大資安風險及企業自評擋不住資安風險主因

根據 iThome 2019 資安大調查中的數據顯示，員工的疏忽及資安意識不足會導致輕易讓惡意程式（惡意軟體）及勒索軟體進攻、釣魚攻擊、及垃圾郵件氾濫。惡意程式指的是病毒間諜軟體，它的目的是在於破壞電腦程式而釣魚攻擊是設計出巧妙的陷阱在郵件中，使員工感到興趣甚至是去訂閱開啟，此時個人的個資或帳密可能已經在不知不覺中被竊取。而惡意程式和勒索軟體的進攻會導致電腦中毒或電腦被鎖起來，使得受害者可能需要用「贖金」來取回電腦控制權。上述這些威脅都會導致駭客的攻擊進而造成企業受到影響，因此對於企業而言，除了自身防護系統要做足還是需要一個強而有力的守衛把守企業網路入口，才能確保資訊安全。因此，真正的資訊安全除了設備以外，還需要政策與人員的積極整合。

四、資訊風險管理與企業預防

隨著新興科技的崛起、法規環境的轉變，商業模式和客戶體驗不斷地演化與創新，科技發展所面臨的風險管理議題，包含策略風險、營運風險、網路安全與資料風險、作業與財務風險等各個面向，都將更加複雜，因此，數位時代下企業的風險治理將從單點管理走向整合性價值鏈生態圈治理。運用法遵科技，亦即 RegTech（Regulation Technology）強化風險管理或為解決之道，例如企業佈建資料風險分析平臺應用藍圖，針對企業內部（資訊安全、資料保護、內控迴圈）及外部（競爭者資訊、協力廠商資料、以及開放資料），從單一領域深度分析進展至跨領域的綜合分析，同時建置有效的異常存取規則（人、事、時、地、物），藉由網路威脅情資分析平臺，自動蒐集外部威脅資訊，整合內部情資，產出資安趨勢及風險分析報告，並針對稽核軌跡進行主動管理，賦予數據應用嶄新視野，強化數據分析於風險管理的地位。

然而，風險管理策略中風險控制與風險理財為重要的管理工具，資訊安全的工作需要防範於未然，預防勝於治療，一般而言，在企業資安領域所執行的事前防範比起事後補求，可節省至少十倍至上百倍的資源耗費。如風險控制中的加強「網路的安全」、「IT 基礎防護」、「強化員工資安意識」、「災難的復原」及事故發生後的風險理財工具-保險

(一) 加強網路的安全

網路的安全包含網路裝置安全、網路資訊安全、網路軟體安全。駭客通過基於網路的入侵來達到竊取敏感資訊的目的，也有人以基於網路的攻擊見長，被人收買通過網路來攻擊商業競爭對手企業，造成網路企業無法正常營運，網路安全就是為了防範這種資訊盜竊和商業競爭攻擊所採取的措施。從控制的角度來看，不論架設防火牆，或是實施權限控管，都是為了防止某些會影響組織業務的事件發生，以便降低風險。就控制而言，又可以分成三類，預防性控制（Preventive Controls）、偵測性控制（Detective Controls）以及矯

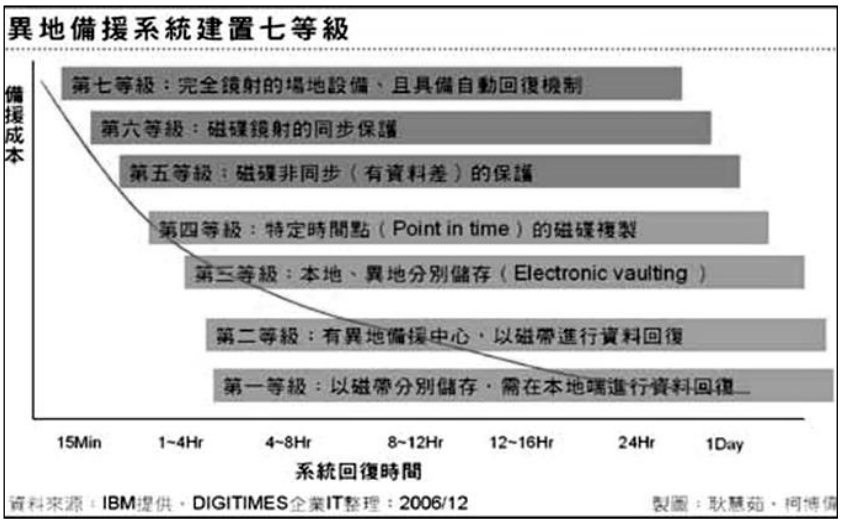
正性控制（Corrective Controls），所謂預防性控制，就是在事件尚未發生以前，所事先採取的一些行動。舉例而言，定期舉辦員工教育訓練，就是要提高大家的認知程度，以免在不知情的狀況下導致資安事件發生。甚至對於敏感性的資料，需要使用權限控管軟體，限制人員的使用，這些都是屬於預防性控制的一種。

(二) 強化員工資安意識的四個要點分別為

（1）確保員工了解重要性，（2）提升目前資安危脅的意識，（3）專注於關鍵的策略-網路釣魚和社交工程攻擊及（4）能存取公司重要系統的人都可能存在弱點，包括所有用戶主管、顧問和供應商，非只有一般員工會成為社交工程攻擊，網路釣魚以及其他駭客攻擊的受害者。高階主管、經理、合作夥伴以及廠商等可以存取公司重要系統的人都可能存在弱點，必須要有提升防範第意識。

(三) 災難的復原

災難復原系統可依照對系統保護的程度與等級，分七個層次，七個等級之分別如下附圖。這七個層級基本上可以區分為非在線系統、伺服器層次、儲存設備層次。層次由零到七，依照這個定義下的分類，被訂為等級 0 的企業，就是完全沒有備份或備援的相關設備與策略。第一層級所需的恢復時間最長，但成本最少；而第七層級正好相反，恢復系統運作的時間幾近於零，不過建置成本相對來說非常高。到底要做到哪一層次的備援，企業最重視的仍然在總體持有成本。決定異地備援系統成本的兩個重要因素，為回復所需時間和資料損失量。回復所需時間計算的是系統中斷到重新啟動間所經歷的時間；資料損失量則是指在系統中斷時間間隔中，資料損失的狀況。圖 3 為災難復原異地備援系統建置七等級。



資料來源：科技網

圖 3　災難復原異地備援系統建置七等級

(四) 保險

根據在 2019 臺灣資安大會的議程中，第一次有保險業者開使表達對於網路保險（Cyber Insurance）的看法，雖然企業購買網路保險最主要的目的，是要轉嫁風險發生時的損失，然而，實際遭遇網路攻擊時，企業當下也可遭受重大損失而亂了陣腳，不曉得從何因應，因此，在網路保險的服務內容中，應該也要有相關的配套項目，以協助企業妥善處置所遭遇的事件。綜觀數位安全的未來發展，網路安全技術與網路安全保險的整合將是重要的趨勢，企業未來規劃網路安全發展策略，除了投入資源建構更安全的網路安全防衛系統外，投保網路保險也是保障網路安全重要的選項，甚至將成為一個不可或缺的保護措施。

五、網路保險市場現況

美國網路保險之發展主要為法令要求（隱私漏洞）及網路隱私權重視而促使保險市場發展，1996 年該產品始出現於美國保險市場，爾後加州開始有隱私漏洞相關的法規，盡而提升網路安全保險的需求，依據加州所訂定的相關法規，其餘 47 州也跟進，促使美國網路保險市場的成長，2006 年網路隱私權之重要性日益漸增，2014 年「網路安全」被寫進超過 60 個承保人合約內容，並產生約十億元的保險營收，2015 年「網路安全法」與「網路安全資訊分享法」及 2016 年「國家資訊安全行動計畫」強化國家資安中說明網路保險推動重要性，而使其該保險順利推展，2017 年全球年保費收入約為 30 至 40 億美元，預計於 10 年（2027）內達到 200 億美元。

(一) 國內網路保險現況

目前國內相關的網路保險依據保險事業發展中心的分類，目前在國內產險市場，有關資料保護、資訊安全等之保險商品，主要可以分為資料保護保險、資料及網路錯誤或疏漏責任保險、資訊系統不法行為保險和資訊服務業專業責任保險，其中前三項主要是企業發生資安事件時，保險公司能夠轉嫁企業損失，以及提供理賠服務的險種，最後一項則是針對資訊人員因為作業疏失，而遭他人提出損失賠償，保險公司可以彌補相關損失的險種。其中，資訊系統不法行為保險承保對象只限於銀行、券商及投顧等金融機構，補償被保險人因其電腦系統遭第三人入侵並詐欺性輸入、竄改、銷毀電子資料，而直接遭受的資金或財產損失。例如，一銀 ATM 被駭事件損失 8,390 萬元，即可由這類保險轉嫁。而資料保護保險，只就個資外洩的第三人責任賠償做保障，包含抗辯費用及和解金，或法院判決金。此商品適用所有產業，主要是因應《個資保護法》的實施而推出的。資料及網路錯誤或疏漏保險則為資料保護責任保險的升級版，除包含第三人的求償金及訴訟費用，還可擴大承保網路中斷保險、電腦勒索保險、媒體內容責任及其他費用（電子資料修復、重置費用、鑑識服務費及名譽修復等費用），以及營業中斷損失，都適用這張保單。有關國內產險市場主要網路保險整理如表 1。

表 1　產險市場目前網路保險主要險種

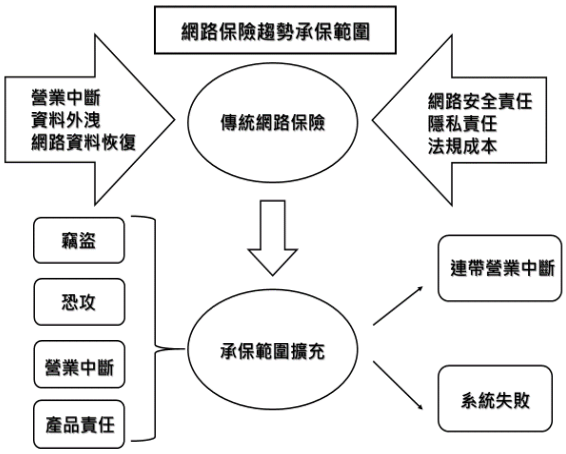
保險名稱	承保對象	定義	承保範圍
資料保護保險	不限	發生違反資料保護或違反資料安全之情事，致第三人受有損害。	企業如果發生個資外洩，能夠提供第三責任賠償，包含和解金、訴訟費、判決金和抗議費，包括外包場將客戶資料流失。
資訊及網路錯誤或疏漏保險	不限	因勒索或犯罪行為或內部管理疏失等造成相關損失。	提供被保險企業之營業中斷損失、危機管理成本、駭客竊盜、網路勒索等針對被保險企業直接之損失保障，以及隱私洩漏、機密洩漏之責任保障。
資料系統不法行為	金融機構（銀行、證券）	企業電腦系統遭到入侵而遭到金錢或財產的損失	資訊輸入竄改或銷毀、電腦指令之偽造或變造、電子資訊及媒體之毀損滅失、電子訊息之誤傳或竄改、資訊系統服務之失誤、電子傳送之導誤，電腦病毒侵害，口頭撥款指令之偽造。

資料來源：本研究整理

我國網路相關保險自從推出以來，市場反應並沒有預期中熱絡，反應冷淡，但從 2015 年個人資料保護法修法後，2016 年行政院通處成立，且在歷經 2016 年後全球網路程式開始有攻擊事件及 2017 年時銀行遭受網路攻擊，導致資訊安全保險的企業詢問度逐漸攀升，逐漸被重視，使得越來越多相關的網路保險商品在這幾年中持續推出，保費及承保件數也明顯提高。

(二) 網路保險未來發展趨勢

由於網路風險趨勢造成原有之相關保險由傳統的網路保險，逐漸的發展變化成為承保範圍的增強與擴大，這些包含普遍承保範圍持續擴大（如目前市場上的次限額經常要求到足額）、開放系統風險故障（如被保險人電腦系統的任何意外或者無意中斷）、增加連帶的營業中斷損失（如承保範圍可以全面擴展，以前僅限於指定的供應商等）等，相關網路保險之趨勢及承保範圍請詳圖 4 所示。



資料來源：Trans Re, North Asia Workshop 與本研究整理

圖 4　網路保險之趨勢及承保範圍

六、結論

2017 年全球花費在網路安全的經費達 930 億美元，預計到 2022 年會成長到 1970 億美元。網絡攻擊所造成的各種損失達到 3 兆美元，遠遠超過了自然災害。如果目前這種趨勢持續下去，到 2021 年每年的損失可能高達 6 兆美元。為了因應以上的狀況，網路保險（Cyber insurance）或

許是有效的解決方案。茲將我國未來網路保險發展相關的建議如下：

1. 根據不同類型產業特性設計不同的網路保險（EX:教育機構、醫療單位等），以符合企業不同的需求及特性，如此可以提升不同產業業對資安風險的需求。
2. 對大型企業量身訂做網路保險保單，並結合資安專家提供資訊安全服務以加深保險公司的服務價值，共同創造低資安風險雙贏局面。
3. 將資訊安全管理與網路保險的購買列為公司治理評鑑的一環，以利保險公司推行上市上櫃公司的網路保險，以強化公司的資訊安全保障，來增進利害關係人的利益。

本文作者：
實踐大學風險管理與保險學系
助理教授