金融業的資安實況剖析：《臺灣企業資安曝險大調查》

KPMG安侯數位智能風險顧問(股)公司 副總經理⊙林大馗

關於臺灣企業資安曝險報告

KPMG透過調查機構，觀察到2019年在產業運用數位科技的趨勢，請參圖1。

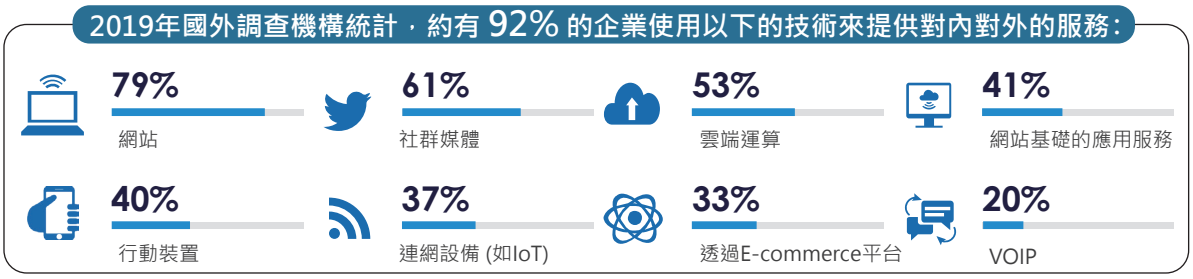

圖 1、2019 年產業運用數位科技的趨勢圖

也是因為數位科技於企業中運用的如此蓬勃發展，為了協助企業了解這些數位科技背後所隱藏的數位風險，及數位風險的曝險程度，所以KPMG著手蒐集有關臺灣指標企業有關網路安全環境的資料，KPMG調查的面相包含項目如圖2。

圖 2、KPMG 調查臺灣指標企業有關網路安全環境面相

同時也結合了近年重點產業的趨勢、組織網路曝險的現況等，於2020年底彙整並製作成曝險調查報告，期待為臺灣金融產業帶來以下的效益：

1. 量測全面網路風險：不同於市面上一般的技術性量測工具，本報告除了資訊安全的檢測外也包含了可量化的財務評估，讓企業了解其有形及無形的風險。
2. 比較產業資安現況：依據企業營運特性，將檢測的大型企業區分為五大產業，可以結合產業趨勢做出更精準地分析，真的得比較同產業、委外及合作廠商所屬產業，了解各自曝險控管的優劣。
3. 配置合理資安預算：了解指標產業若發生資安事件的平均財物損失風險，讓相關產業能有依據的在其組織做網路風險評鑑，並在人力、預算許可的範圍內，訂定合理的可接受風險值，有助於替潛在的風險訂定改善計畫，並在考量所需預算、優先順序、時程與負責人員後，以投入最少的資源降低、轉移或接受這些風險。
4. 部署資安防禦策略：呈現內外部各面向的風險因子，在針對普遍有待加強的項目進行深入剖析與提供建議，輔助制定內外部網路管理的策略。

臺灣金融業的資安實況

2020年新冠肺炎造成全球巨大衝擊，企業爭先恐後導入雲服務、智慧物聯網、遠距工具等新興科技。但依據KPMG最新公布的《臺灣企業資安曝險大調查》結果，抽樣的50家本土大型企業中，在網路防護方面，僅繳出尚可的C級成績單，具備一般能力的專業駭客，就有可能進行入侵。

KPMG報告所調查的臺灣大型企業中，包含了五大產業，除了金融業的87分外，其餘產業平均皆與金融業有很大差距，呈現「一好四壞」的現象。特別是電子零組件製造業、通訊業與電腦及周邊設備製造業，亦即通稱高科技業的「護國群山」們，於本次調查中的網路防護安全性分數，平均只有68分，除少數公司可以擠身領先群外，多數落後於臺灣產業平均分數。

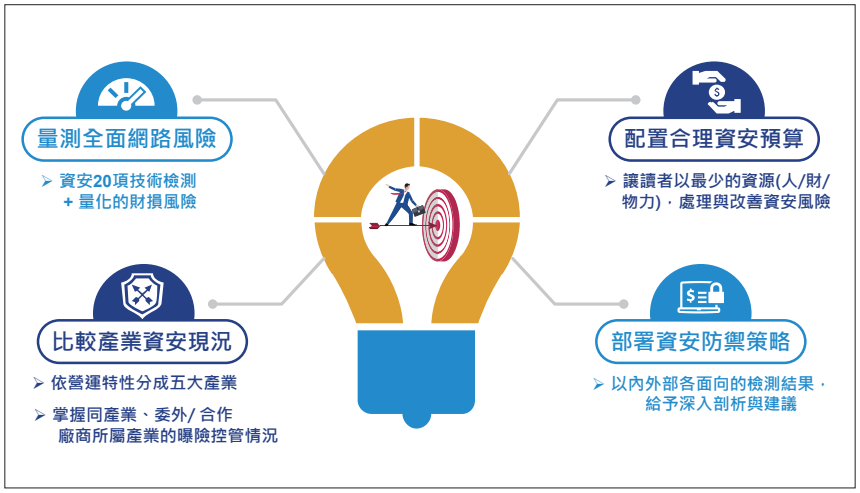

圖 3、資安曝險調查效益示意圖

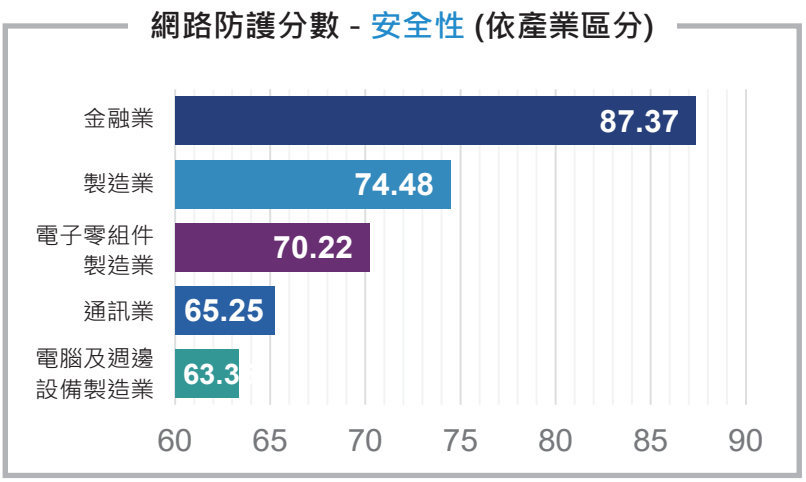

圖 4、臺灣大型企業網路防護安全性分數
資料來源：KPMG《臺灣企業資安曝險大調查》

另依據調查工具中的財損模型推測，臺灣高科技業潛在平均資安財務損失風險超過每年3,000萬新臺幣，比整體調查平均高出5成，成為駭客眼中標準的「肥羊」。

金融業在調查報告的網路防護分數四大面向中，不論是隱私性、安全性、韌性、聲譽皆為全產業表現最優異，且平均成績都接近A級（只有世界一流駭客才能侵害）。我們認為，國內金融業能普遍成為「績優生」，是因為近年主管機關的高度監理。在違反金融相關法規時，除了將遭重罰，信譽下降、創新服務無法順利上線等因素都將造成重大營收損失，成就了金融業成為臺灣企業的資安標竿。但也要提醒金融業者，金融產業擁有豐富且價值高的金流資訊，因此，迄今仍為駭客集中精力攻擊之標的。根據國際研究機構的報告指出，金融業受到網路攻擊的可能性為其他業的300倍，且每年攻擊數都在攀升，因此，臺灣金融業只能持續精進資安能力，沒有鬆懈的理由。也是因為金融業者持續將數位科技帶入金融服務中，我們也可稍微一窺目前數位科技在金融業的應用（請參圖5）。

圖 5、現階段數位科技在金融業的應用

我們必須深切體認到「數位轉型、風控先行」，資訊安全當然是數位風險中重要的一環，但我們如果用更宏觀的角度來剖析數位風險，其實包含如網頁排名、搜尋引擎最佳化（Search Engine Optimization, SEO）等數位能見度，也是屬於數位風險中的一環。比如我們今天透過搜尋引擎搜尋A期貨公司，但卻因為SEO、Hashtag等因素，造成B期貨公司出現在排名的首位，這樣對金融機構於數位空間中，形成新的數位議題挑戰，再針對金融產業更深入探討與研析，可以發現目前金融業可能存在下列的數位空間潛在風險，包含：

1. 臺灣金融業的網頁排名指標偏低，品牌行銷與搜尋引擎最佳化（Search Engine Optimization, SEO）指標，也落後於平均產業分數，雖帶來較低的潛在財損風險，但也間接造成客戶流失與偽冒品牌使用的風險；更是影響了金融機構運用 Fin Tech 與數位化的推廣。

> 數位品牌的露出於現今時代更形重要，特別在純網路銀行加入競爭，與開放銀行形成廣域金融生態應用趨勢下。KPMG 建議：臺灣金融業應更積極應用新興科技，同步提升數位影響力與資安防禦能力，才能創造金融科技的價值。

2. 臺灣近年金融業遭受駭客覬覦的比例明顯高於其他產業，但相關防禦能力並未顯著領先，甚至部分金融業還落後產業平均值。包含：

(1) DNS防護：我們常見到的DNS攻擊類型，包含DNS挾持（DNS hijacking）跟DNS中毒（DNS poison）。這類攻擊會將偽造的 DNS 資料作為 DNS 解析URL的解析程式中，造成DNS客戶端解析URL時傳回不正確的網域 IP 位址。造成DNS客戶端流量可能會被導向到惡意中繼站或攻擊者想要的其他任何IP位置，而不是前往正確網站。

(2) DDoS緩解措施：近幾年金融機構常見的DDoS緩解措施，通常為採用電信服務供應商（Internet Services Provider, ISP）所提供的流量清洗（Clean pipe），而此一措施被駭客突破的方式，最常見的即為使用組合型網路流量，讓資安設備無法即時識別其特徵，造成需要人工介入撰寫規則，進而延長駭客攻擊的時間，造成服務中斷時間恢復的延宕。

> KPMG建議：金融機構應立即梳理本身對Internet服務之屬性、網際網路負載平衡節點及DNS等架構與防護標的，並評估部署相關如內容遞送網路（Content Deliver Network, CDN）、流量清洗與DNS監控等安全管控機制。其中採用CDN解決方案時，需特別注意不可洩漏原有DNS紀錄，否則可能造成CDN機制失效。

3. 依據本次調查報告顯示，臺灣歷史越悠久之企業（包含金融機構），因設立時間長，其遺留於網際網路上的數位足跡（Digital footprint）更為廣泛且紊亂，相關留存於網際網路資訊缺乏妥善管理，而駭客亦可能透過類似本文的手法撈取相關資訊。

> KPMG建議：金融機構應立即著手針對下列方向精進：
> (1) 梳理現有外部數位足跡資訊（如WhoIS、社群等），盤點並校正其數位足跡資訊。
> (2) 定期審視外部情資，找出日常資安管理分工盲點。

金融業的意料之中

對於金融業資安較整體平均高的現象，是個初看「意料之外」，但細想在「意料之中」的成績。

一般人對金融業的印象，都是櫃枱親切待人，許多事情追求程序與規範，且門禁森嚴，但仔細觀察實際的金融網路環境可以發現，凡事講求生產效率與成本的臺灣大企業，在金融業者的網路環境中非常罕見，甚至可以說並不存在，而是金融業者所有的網路連接、系統設計開發與交付、資安控管與資料加密，乃至個資保護等需求，均須與主管機關法令法規密切接軌對齊。以銀行業及保險業每年資安部門的重頭戲，電腦系統資訊安全評估作業項目來說，單以網際網路服務檢測的範圍辨識作業，就需要下足功夫。比如，如何確認金融業者網際網路均已被辨識、DNS中相關A紀錄（A Record）是否詳實等，就需要資安部門偕同資訊部門一同合作，來將此一任務完成。

故完全符合且落實主管機關的法規要求乃為金融業者最基本條件；然而除金融業外，臺灣其餘產業對資安的重視普遍程度不高，通常都是頭痛醫頭、腳痛醫腳的個案處理方式來應對全面性的資安風險，加上疫後遠距科技的多元應用，就造成了網路安全高曝險結果。

近期駭客對高科技產業的狙擊更加猖狂，常見事故不僅包含科技供應鏈的上中下游廠商的電腦綁架勒索事故，其他如電郵偽冒詐財、機密竊取等上不了熱門新聞的「日常資安事件」，都反映數位風險挑戰日益嚴峻。若高科技產業不加速提升資安控管和自身防護能力，駭客將有機會進行更大規模的屠殺。更甚者因供應鏈的網路環環相扣，很容易因單點、單一系統，或單一公司遭入侵，而對整體供應鏈產生巨大衝擊。而此一風險與危機也非常值得金融業者借鏡。

誰是下一個可能的受駭者？

本文之調查報告自調查時間起，已經經過了接近一年半的時間，以常見的電腦綁架勒索通案為例，科技業要預防事件一再重演，必須要深入了解綁匪的「選案邏輯」，與被駭者的「脆弱特徵」。

駭客下手選取對象的取樣方式，通常與企業內部自我診斷、弱點掃描或資安稽核的手法差異很大。惡意的攻擊者，偏好採用狙殺鍊架構（Kill Chain Framework），從挖掘、分析暴露於網路的公司情報，來判斷具備攻擊「CP值高」的對象，所以**當數位足跡越多，網路防護通常有越大的危機。**

另從近期多起被駭企業的脆弱特徵分析，科技業被入侵綁架的原因，多是一個員工小疏失（最常見的就是隨意點選來路不明內含木馬程式的釣魚郵件），加上一個漏洞（未及時修補的系統漏洞，例如Windows或電子郵件主機的漏洞沒有即時更新）。或是，員工無意間採用公司電子郵件信箱註冊了某個電子商務，且密碼設定與公司相同，當此電子商務店家不幸受駭時，採用公司電子郵件註冊的員工，就無意間提供了駭客非常多可利用的資訊（包含網域名稱、帳號、密碼等）。同時，疫後遠距科技的多元應用、及科技業遍布全球但防護程度不一的多產線體系，更提供了更多入侵管道給駭客。根據報告結果，平均每四家臺灣大企業，就有一家在漏洞修補管理「抱鴨蛋」被評測為零分，成為了企業資安大破口。

除了從曝險報告中持續強化防火牆，期貨業者還應該做的事？

從駭客攻擊發起的步驟與觀點分析，除了不斷提升強度網路防禦工事外，以下「三多」技能，可以提供企業的資安網路防護程度，特別是降低外部駭客覬覦的機率。第一招、主動進行多元弱點情資蒐集：包含情蒐來源要豐富（如：社群媒體、供比對的弱點資料庫等）、檢測弱點的範圍要廣（如：物聯網、雲端、IT、OT），漏洞修補或其他補償性控制措施要確實與即時。第二招、多因子驗證：防止不肖人士未經授權的連線，避免錯誤的資訊裸露於網路世界。第三招、多進行檢測與演練：透過與外部可靠信賴的團隊，多進行網路與系統評測與演練切磋，才能真正洞悉自身資安問題，淬鍊出具備高防禦能力的數位企業。

除了上面的觀點外，另外，我們自然也需要關注主管機關對期貨業者的資安相關的法規要求，比如「新興科技資訊安全自律規範」就是一個很好的例子。

在「新興科技資訊安全自律規範」中，同時間關注到了下列新興科技，我們也同步將法規對該新興科技的定義納入本文：

1. 雲端運算服務：透過網路技術達成共享運算資源之前提下，提供使用者具備彈性、可擴展及可自助之服務，惟本自律規範定義之雲端運算服務不包含建置組織內部且僅對內提供服務之私有雲。
2. 社群媒體：一種結合科技、社交互動與內容創造之網路應用，允許創造或交換使用者產出內容；且透過此高度互動的平台，個人及群體可以分享、共創、討論並修改使用者產出內容，惟本自律規範定義之社群媒體不包含組織內部溝通使用之社群媒體或平台。
3. 行動裝置：一種具有資料運算處理、儲存

與網路連線功能之可攜式設備，包括智慧型手機、筆記型電腦、平板電腦與 PDA 等裝置，惟本自律規範定義之行動裝置僅限可用於處理組織內部定義之敏感性事務且可直接連接組織網路設備、服務之行動裝置。

4. 員工自攜行動裝置（BYOD）：非屬組織行動裝置用於處理組織事務、直接連接組織網路設備或服務。
5. 物聯網設備：指具網路連線功能之嵌入式系統設備及其周邊連網之裝置（如：感測器）。

在其中，我們要注意上述新興科技對我們期貨業者可能造成的四大外部曝險因子，包含：

1. 雲端運算服務：依據OWASP的定義，錯誤的組態設定通常是使用不安全的預設值，或者是錯誤配置像是HTTP標頭或者是系統顯示的錯誤資訊已經包含敏感性個資所造成的，除了要安全設定所有作業系統、框架、函示庫以及應用程式外，更必須做到系統更新與升級，以確保系統安全與時並進。但是在雲端的環境中，會造成雲端服務上重大災害的，通常都是錯誤的組態設定（Misconfiguration），比如說將私人的（Private）設定為公開的（Public），而此一風險通常是人為造成的疏失。

> KPMG建議：透過四眼原則（4 eyes principle）等其他重複確認機制，確認相關組態異動，並持續監控託管於雲端服務供應商之服務是否正常運作。

2. 雲端運算服務：金融機構時常無意間採用了雲疊加的架構，什麼是雲疊加？就是可能租用的A廠商的PaaS服務，在上面放了B廠商的SaaS服務，而這樣的架構，除了簽定合約內相關歸責性外，也容易造成金融業者於查核時容易疏漏。

> KPMG建議：雲端環境建議於使用初期盡可能將管理透明化、扁平化。更要辨識相關須遵循的法令，如銀行業的「金融機構作業委託他人處理內部作業制度及程序辦法」，並於合約簽訂時明訂相關資訊安全管理責任與相關服務水準（Service Level Agreement, SLA）。

3. 社群媒體：最讓企業煩躁的，有心人士所成立的”偽冒粉絲專頁”絕對是排名第一，偽專頁除了可能偷取客戶的登入資訊、個人資料外，更可能透過如偽冒的行銷活動，造成企業名譽的損失。

> KPMG建議：建議定期於社群媒體上搜尋與企業相關資訊，並確認該專頁是否為企業所有。另亦建議建立社群媒體異常通報與處理機制，避免造成客戶權益損害。

4. 物聯網設備：通常物聯網設備都是提供企業內部的服務，如CCTV、IP Phone及多功能事務機等。但我們也時常看到如某學校的列表機直接連接網際網路（INTERNET），除提供列印服務外，且未變更預設管理帳號密碼，造成駭客大量列印勒索信件，校園人心惶惶。

> KPMG建議：梳理目前企業對外服務的服務埠是否均納於相關資安管理框架中，另外亦須辨識物聯網相關服務是否有不當設定而暴露於網際網路（Internet）中。若因業務所需，須開放至網際網路（Internet），建議透過防火牆規則，以點對點開通及服務埠限縮的原則進行管理。

疫後新現實，我們應該怎麼辦？

依據KPMG【2021臺灣銀行業報告】中所提，金融業者在新興科技的導入後，提供智能金融服務、遠距作業與雲端應用、開放銀行（Open banking）等潮流，金融業者勢必正視且聚焦上述新興科技導入所產生的潛在風險，過去靠著金融科技結合營運模式，將「流量變現」的「重創新、輕風險」、「重數據、輕隱私」、「重效能、輕安全」時代已經過去。

在可見的未來，各國金融監理機構，都將經由各類數據治理、金融監管、資安與隱私保護的新法規，建立新的數位經濟世界規範與新的數位貿易屏障，金融業者也必須在創新與風險的天平上，求得平衡點。

另外，我們更需深切的體認到不只有COVID-19的病毒會變種，駭客所釋出的網路惡意病毒及攻擊手法也是日新月異。在「高頻寬、廣連結、低延遲」的5G智慧世代來臨之際，企業需更加重視與強化資安，才不會讓駭客餐餐都有豐盛的佳餚，成為「高贖金、廣被駭、低反應」的受駭企業。

附註：關於《臺灣企業資安曝險大調查》

KPMG於2020第四季全球疫情正熱，同時遠距科技、雲端服務等數位工具應用急速擴張的期間，針對臺灣包含金融、製造、電子零組件、通訊、電腦製造等50家大型企業，以智慧工具網路情資探測方法，由資安技術、財務曝險等不同面向，呈現臺灣大型企業所面臨的真實資安風險。同時KPMG於本調查也提出我們的觀點與建議，俾協助企業更密切關注組織內部的資安管理政策，同時制定因應策略。在數位發展多變的世界中，我們期盼給予企業協助，一起更有自信且可靠地應用各種智慧科技、降低科技風險、保護企業資產，提升臺灣企業整體的競爭優勢。