出國報告（出國類別：研究）

網路威脅情資(Cyber Threat Intelligence)之預警分析與管理研究

服務機關：臺灣土地銀行

姓名職稱：宋麗華　領組

派赴國家／地區：英國、荷蘭

出國期間：107年9月3-23日

報告日期：107年11月22日

摘要

本次奉派赴英國、荷蘭研習「網路威脅情資 (Cyber Threat Intelligence) 之預警分析與管理研究」，出國研究期間，主要目的在於瞭解國外資安相關產業因應網路科技發展，針對網路攻擊事件層出不窮之狀況，如何將網路攻擊事件之情資有效地蒐集、分析、運用及管理，藉由參訪勤業眾信聯合會計師事務所英國倫敦及荷蘭海牙之網路威脅情資中心 CIC (Cyber Intelligence Center) 、英國標準協會 BSI (British Standards Institution) 、英國營運持續管理協會 BCI (Business Continuity Institute) ，透過會議簡報及實地參訪等方式了解上述企業對於網路威脅情資之應用及發展，參酌其如何將以往事件發生後被動處理的模式，逐漸改變為於事件發生前主動偵測預警的模式，有效運用威脅情資進行分析，把外部各種資安情資、內部資訊架構所遭受的攻擊與潛在弱點，統一彙整做為預警參考並有效維持企業持續營運之目標。以期本行汲取相關經驗以因應現今數位環境的資安風險並進行相關處理及防禦。

網路威脅情資(Cyber Threat Intelligence)之預警分析與管理研究

目次

壹、 緣起及目的

網路科技發展日新月異，網路攻擊事件層出不窮，且攻擊手法不斷翻新，大部分企業投入大量的資源及成本強化資訊安全，像是定期進行滲透測試、弱點掃描、內部稽核、加強安控措施、了解網站弱點等等，甚至建置企業內部的資安事件管理平台 (SIEM, Security Information Event Management) 蒐集相關網路攻擊事件，但要在數以萬計的事件中辨別出真正的攻擊並做出正確的回應就像大海撈針，企業投入的這些高成本的資安架構，其大部分的效用著重在強化企業的資安防禦及了解本身的潛在弱點，但卻沒辦法知道想要攻擊自己的敵人會以何種形式出現，因此，在當前已無國界的網路世界裡，開始有企業關注網路威脅情報 (Cyber Threat Intelligence, CTI) 的應用。

孫子兵法有云：「知已知彼，百戰不殆」，在虛擬的網路世界裡，同樣適用這樣地智慧，因為從攻擊者的角度來看，耗費心力研究出來的攻擊手法，通常不會只用一次，而是會找尋類似的目標或環境重覆發動攻擊，如果有企業願意投注資源將蒐集到的攻擊手法加以分析、整理，甚至有效運用後提出防禦手法，並提供相關產業，透過這種網路威脅情報的應用，那麼網路戰爭的形態，企業即可能從被動地仰賴資安廠商提供的各種資訊安全公告後才開始著手相關的防護措施，轉變為主動且有效於最短時間內進行防禦的模式。面對瞬息萬變的網路攻擊手法，傳統且被動的資安防禦模式，已不足以應付最新的網路攻擊和威脅，應考量將傳充資安防禦模式，強化為主動運用各種網路威脅情資，除了可提升企業對於攻擊事件的反應速度，並可增加對於外部威脅的掌控能力。

因此，本次奉派赴英國、荷蘭參訪歐洲資安相關產業，瞭解國外資安研究單位因應網路科技發展，針對網路攻擊事件層出不窮之狀況，如何將網路威脅事件之情資有效地蒐集、分析、運用及管理，進而檢視本行目前資安

事件管理平台(SIEM)對於網路威脅情資之運用，考量本行業務之特性，加以調整或改善，以期提升本行資安防護能力，降低資安事件發生時所帶來之衝擊及營運被迫中斷之風險，更進一步可把外部各種資安情資、內部資訊架構所遭受的攻擊與潛在弱點，統一彙整做為預警參考，並可提供主管相關資訊以掌握威脅概況，達到掌握情資，制敵機先的目標。本次研究期間自民國一〇七年九月三日至一〇七年九月二十三日

貳、 參訪單位簡介

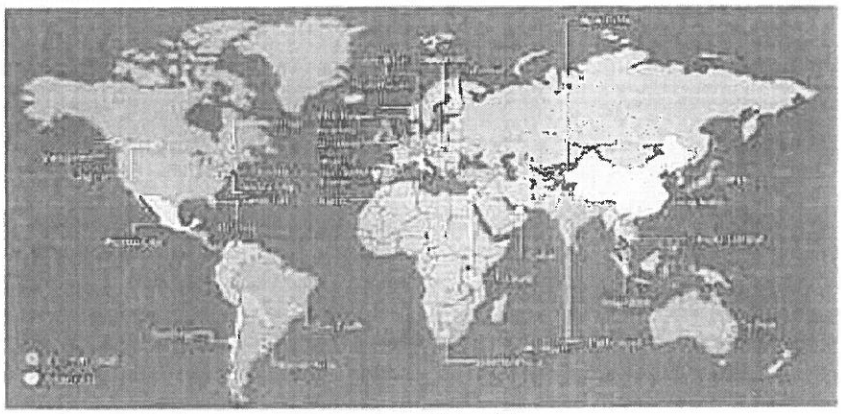
本次奉派赴英國、荷蘭參訪 4 家歐洲資安相關產業，瞭解國外資安相關產業因應網路科技發展，對於網路威脅情資的應用。分別參訪勤業眾信會計師聯合事務所位於英國及荷蘭之網路威脅情資中心 CIC (Cyber Intelligence Center)，主要負責歐洲地區之網路威脅情資蒐集、分析，定期與整個歐洲地區網路威脅情資中心聯繫交流，並將分析結果與全球勤業眾信網路威脅情資中心彙報，即時更新網路威脅情資，並提供合作企業進行瞭解及防禦；另安排參訪英國標準協會 BSI (British Standards Institution)、英國營運持續學會 BCI (Business Continuity Institute) 等資訊安全國際標準發行機構及學術研究單位，目的在於瞭解歐洲資安研究單位因應網路科技發展，如何將網路威脅事件之情資有效地蒐集、分析，進而因應網路世界的攻擊趨勢，訂定資訊安全相關標準以有效降低企業之網路資訊安全所造成的營運中斷風險。參訪單位簡介如下：

一、 勤業眾信聯合會計師事務所網路威脅情資中心 CIC (Cyber Intelligence Center)

勤業眾信聯合會計師事務所（以下簡稱勤業眾信）於 2003 年由「勤業」及「眾信」兩個會計師事務所合併成立，為全球四大會計師事務所之一，其服務除傳統會計外，也包含了審計、稅務、財務諮詢、法律諮詢及管理顧問服務，近年來因應資訊安全日漸受到重視，亦成立了風險諮詢相關部門，提供資訊安全及數位科技風險等服務，其中透過作業流程及資料內容特性之分析，為企業制定妥善之資訊安全政策與規劃配套之資訊技術，以有效保護企業資訊安全，而隨著資訊科技的普及，大多數的企業越來越仰賴位數位科技，而其發展又遠較於資訊安全技術來的迅速，也因此，勤業眾信針對數位科技風險提供了數位科技策略、數位科技安全、數位風險預警與數位

防禦等服務，協助企業於面對這些重大數位科技威脅時，可以找出自身的弱點並進行必要的強化，而網路威脅情資中心也因此蘊育而生。

勤業眾信之網路威脅情資中心遍佈全球各大重要城市，像是歐洲就於英國倫敦、荷蘭海牙、西班牙馬德里...等大城市設有網路威脅情資中心，分別針對不同之地區進行網路威脅情資蒐集，並將分析結果與全球之網路威脅情資中心進行彙報及研究，進而彙整至共用之網路威脅情資平台，提供全球客戶瞭解新興之網路攻擊手法並進行相關之防禦措施。



圖一　勤業眾信之網路威脅情資中心全球分佈概況

（資料來源：勤業眾信提供）

本次參訪英國倫敦及荷蘭海牙之網路威脅情資中心：

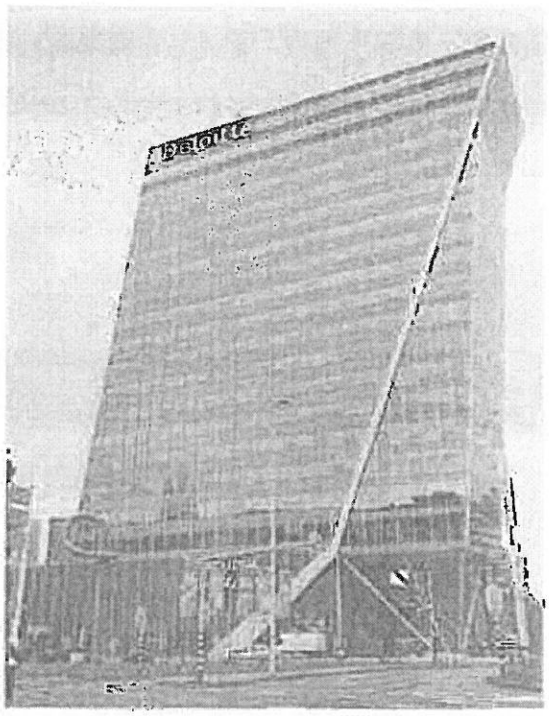
(一)　英國倫敦網路威脅情資中心 CIC (Cyber Intelligence Center)

為勤業眾信於英國倫敦成立之網路威脅情資中心，負責於高度安全工作環境中提供 7*24 小時的網路威脅分析、解讀、處理，提供反 APT 程式、網路惡意軟體、多沙盒惡意軟體分析、情報分享平台、行動裝置 APP 警惕及網路威脅情報

等事件之蒐集管理，主要提供英國地區之企業高度資訊安全專業的服務。

(二) 荷蘭海牙網路威脅情資中心 CIC (Cyber Intelligence Center)

為勤業眾信於荷蘭海牙成立之網路情報中心，負責於高度安全工作環境中提供 7*24 小時的網路威脅的分析、解讀、處理，提供反 APT 程式、網路惡意軟體、多沙盒惡意軟體分析、情報分享平台、行動裝置 APP 警惕及網路威脅情報等事件之蒐集管理，主要提供荷蘭地區之企業高度資訊安全專業的服務。



圖二 勤業眾信

（資料來源：自行整理）

二、 英國標準協會 BSI (British Standards Institution)

英國標準協會 1901 年成立於英國倫敦，經過數次沿革，主要負負

各項國際標準（如資訊安全標準 ISO 27001、資訊科技服務管理標準 ISO 20000、營運持續標準 ISO 22301…等）之發佈，為英國皇家特許之國家標準制訂機構與百年歷史的國際性標準發行機構，更是全球第一個國家驗證機構和國際標準化組織的核心成員，每年發佈超過 2,500 項標準，跨足領域包括航太、汽車、營造、能源、工程、金融、醫療保健、資訊科技、食品、貿易與零售等產業，致力協助客戶提高效能，降低風險及永續經營，提供一致、獨立且公正的專業資訊、稽核、驗證、查證及訓練服務於全球；並於 1996 年 2 月正式成立臺灣分公司，以發展大中華地區之標準驗證服務，經過數十年的經營，已樹立良好口碑於各產業，目前所推行的各項標準更為政府及業界所推崇；所制定的標準除被國際 ISO 組織所認可，更是臺灣制定符合國內現況標準時所引用的標準。

圖三　英國標準協會

（資料來源：自行整理）

三、 英國營運持續學會 BCI (Business Continuity Institute)

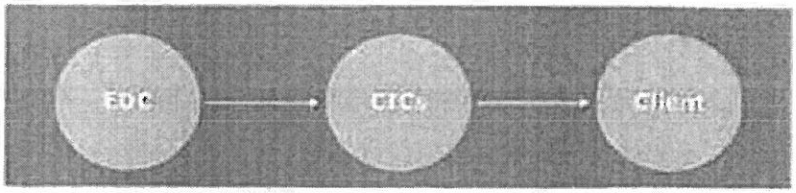
該協會為 1994 年成立於英國之專業學術組織，主要研究如何讓企業面對困難處境下，仍能維持服務且有效運行，協助企業維持營運持續與打造組織韌性，並提供專業且有效的實際營運持續專業課程，輔以實務分析經驗，強化對於營運持續的認知，並能有效回應外在威脅。該協會在英國標準協會 BSI 的協助下，已連續 7 年完成地平線掃描調查 (Horizon Scan Report)，調查內容包含企業所面臨的主要威脅，營運持續專業人員的觀點，以及採取哪些方法加以克服等之研究，被視為企業擬訂營運持續策略的重要資訊來源

參、 研習過程及內容

為瞭解網路威脅情資之預警分析與管理之應用現況，以作為本行網路資安事件管理之發展參考，本次奉派赴英國勤業眾信聯合會計師事務所網路威脅情資中心 CIC (Cyber Intelligence Center)、英國標準協會 BSI (British Standards Institution)、英國營運持續學會 BCI (Business Continuity Institute) 及荷蘭勤業眾信聯合會計師事務所網路威脅情資中心 CIC (Cyber Intelligence Center)參訪，目的在於瞭解歐洲資安研究單位因應網路科技發展，針對網路攻擊事件層出不窮之狀況，如何將網路威脅事件之情資有效地蒐集、分析、運用及管理，進而有效降低企業遭受網路資安事件所造成營運中斷之風險。

一、 參訪英國勤業眾信聯合會計師事務所－倫敦網路威脅情資中心 CIC (Cyber Intelligence Center)

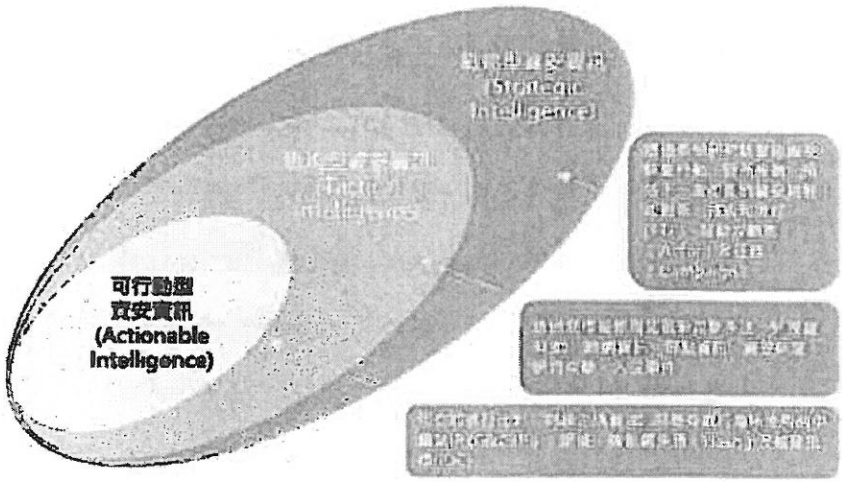
由於近年網路威脅事件的演變愈來愈複雜，迅速且複雜的特性已使許多企業已無法單獨應對網路威脅的挑戰，於是藉由第三方的專業技術，像是勤業眾信的網路安全管理服務，提供網路資安事件的監控、威脅事件的分析，並提供相關的事件解決方案，而隨著服務客戶的增加，蒐集到的資安事件、網路威脅事件愈來愈多，面向也就愈來愈廣且多元。目前網路威脅情資主要來源為勤業眾信之 EMEA Delivery Centre (EDC, Europe, Middle East and Africa Delivery Centre)，經由網路威脅情資中心專業資訊技術團隊彙整這些來自各方的網路情資並加以分析、運用及管理後，發展出面對各種網路威脅的防禦或解決方案，再將網路威脅事件之相關經驗、防禦方式或解決方案提供至客戶端，即是目前網路威脅情資中心前最主要的任務。



圖四　勤業眾信網路威脅情資中心發展流程

（資料來源：勤業眾信提供）

網路威脅情資係指一種以情資為主導的對抗策略，勤業眾信將其分為三大類別：可行動型資安資訊 (Actionable Intelligence)、戰術型資安資訊 (Tactic Intelligence)、戰略型資安資訊 (Strategic Intelligence)，若能將這三大類別的情資依循威脅情形生命週期有效運用的話，不但可以讓企業了解網路攻擊者使用的攻擊手法、策略及程序，更可以依據不同的需求，提供即時有效的告警機制，並可協助企業發展出有效的防禦策略



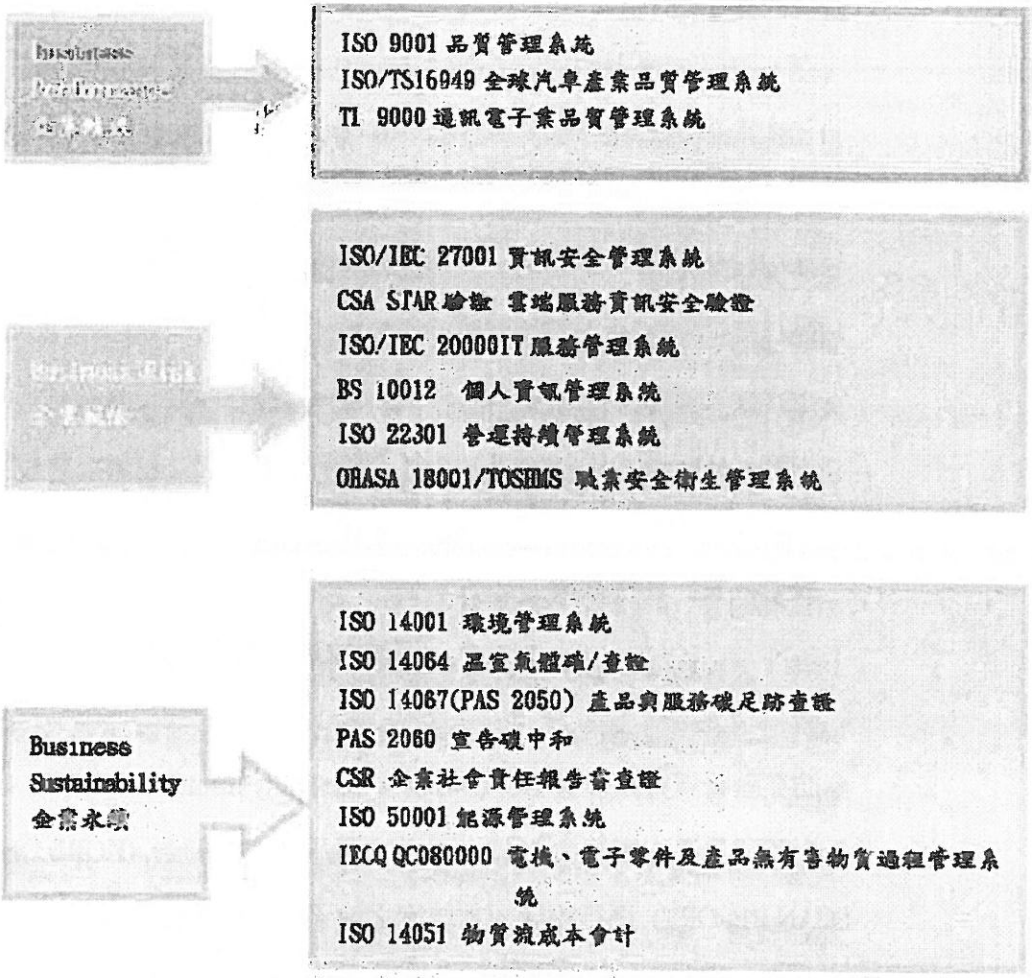
圖五　網路威脅情資分類

（資料來源：勤業眾信提供）

二、 參訪英國標準協會 BSI (British Standards Institution)

主要目的為瞭解標準制定之架構及運作方式。英國標準協會為英國皇家特許之國家標準制訂機構與百年歷史的國際性標準發行機構，每年發佈超過 2,500 項標準，目前至少發佈了 37,834 項標準，而這些標準的制定，並非完全由英國標準協會獨立完成，而是由英國標準協會召集對於主題事務有興趣和專長的企業學員組成技術委員會來共同研議草擬標準，經由不斷的討論及審查程序確保標準的合理性、權威性，且每項標準完成制定的時間不定，所需的時間可能從一年到四年不等，須視該項標準的複雜性和牽涉到的利害關係人範圍而定，且每項標準制定完成後，並非就是結束了標準制定的作業，之後還須不斷的審視並依據現況持續的將標準進行更新，以確保各項標準的適用性，所以每項標準均是花費大量時間及人力的成果。

英國標準協會除了是國際性標準發行機構外，也是國際公認的標準驗證機構，並以最高水準的品質與服務在全球各處營運，為協助企業的永續經營，提供了全方位國際標準驗證作業。



圖六 英國標準協會全方位國際標準

（資料來源：英國標準協會提供）

英國標準協會針對資訊安全議題方面，提出了與企業風險相關的各項標準，如 ISO 27001、ISO27017、ISO 27018、ISO 22301、ISO 20000、BS 10012 等國際標準，並發展資訊韌性 (Information Resilience)架構，若能在企業整個資訊發展的生命週期中，從源頭到銷毀的各個階段能進行有效的管理，符合愈多的標準要求或取得第三方驗證，即能有效保護使用者安全及有效率的儲存、取得及使用資訊，除可符合法規遵循，保護客戶，提升競爭優勢及服務外，更可增加客戶對於

企業的信任感。

圖七　資訊韌性架構

（資料來源：英國標準協會提供）

三、參訪英國營運持續學會 BCI (Business Continuity Institute)

針對英國營運持續學會 2018 年公佈之地平線掃描報告 (HORIZON SCAN REPORT) 進行說明。本年度之地平線掃描報告係針對 76 個國家 657 個組織進行調查彙整而成的一份營運持續策略參考，而 2018 年調查結果，網路攻擊、資訊外洩及無預警的資訊中斷是目前企業經營所面臨最重大的威脅，而這項調查結果，並沒有讓該學會感到太大的意外，因為這些威脅已連續 3 年在地平線掃描報告被各組織視為前 5 大威脅項目，且不論是依地區／國家調查、依產業別調查或是依營運規模調查，網路攻擊皆是名列第一的重大威脅，網路攻擊所造成營運中斷的影響不容小覷，就以近年來發生的 WannaCry 勒索軟體事件來看，即影響範圍偏及全球，影響層面非同小可

2016	1. 網路攻擊 2. 資料外洩 3. 無預警的資訊與通訊中斷 4. 恐怖主義行動 5. 安全事件
2017	1. 網路攻擊 2. 資料外洩 3. 無預警的資訊與通訊中斷 4. 公共服務中斷 5. 勒索病毒
2018	1. 網路攻擊 2. 資料外洩 3. 無預警的資訊與通訊中斷 4. 公共服務中斷 5. 勒索病毒

表一　近年來組織面臨之重大威脅

（資料來源：2018 HORIZON SCAN REPORT）

英國營運持續學會依據產業別比較的結果提醒，網路攻擊、資料外洩、無預警的資訊與通訊中斷等威脅與衝擊，對於身處金融業且負責資訊領域的我們，更應重視網路攻擊的影響，如何有效的即時或事先告警，並能在短時間內找到解決方案或防禦策略，應是我們目前應大力投入資源進行的一項發展趨勢，另一項不可忽略的威脅即是隨著新興科技的多元發展，物聯網裝置的數量大增，透過使用互聯網進行惡意攻擊的手段必然成為駭客的新興手法，因此，網路攻擊的範圍在未來將更加廣泛且更為頻繁，不再單純的僅有電腦裝置存在風險，物聯網的各項設備都存在風險發生的可能，面臨這樣的新興趨勢與不確定性，我們更應該小心應對。

	金融與保險服務	資訊與通訊
前 3 大威脅	1. 網路攻擊 (62%) 2. 資料外洩 (54%) 3. 無預警的資訊與通訊中斷 (48%)	1. 網路攻擊 (58%) 2. 資料外洩 (47%) 3. 無預警的資訊與通訊中斷 (35%)

前 3 大衝擊	1. 無預警的資訊與通訊中斷 (75%) 2. 惡劣氣候 (53%) 3. 網路攻擊 (39%)	1. 無預警的資訊與通訊中斷 (58%) 2. 惡劣氣候 (51%) 3. 網路攻擊 (45%)
前 3 大趨勢	1. 使用互聯網進行惡意攻擊 (78%) 2. 新法規和更嚴謹的監管審查 (58%) 3. 社群媒體的影響 (55%)	1. 使用互聯網進行惡意攻擊 (82%) 2. 新法規和更嚴謹的監管審查 (56%) 3. 社群媒體的影響 (50%)

表二　金融與保險服務產業與資訊與通訊面臨之威脅及衝擊

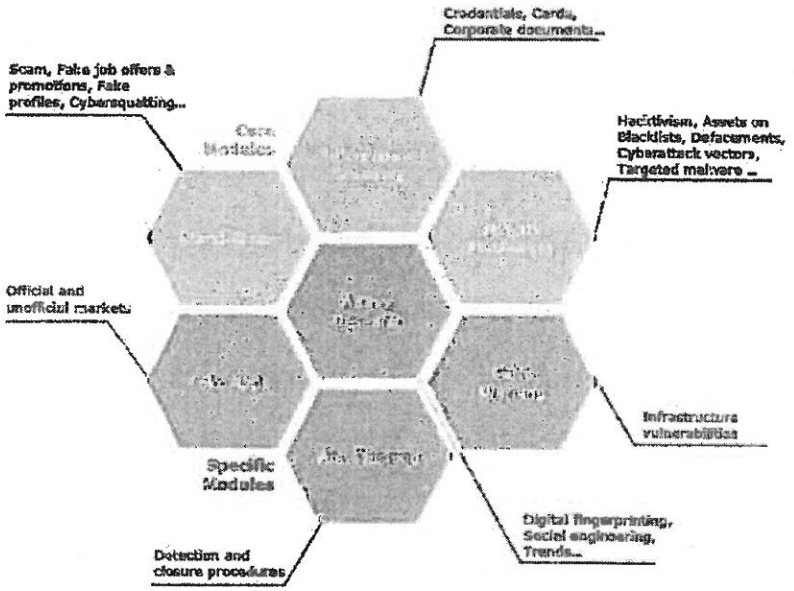
（資料來源：2018 HORIZON SCAN REPORT）

四、　參訪荷蘭勤業眾信聯合會計師事務所－海牙網路威脅情資中心 CIC (Cyber Intelligence Center)

海牙網路威脅情資中心之架構與倫敦網路威脅情資中心類似，根據說明，位於各大城市的網路威脅情資中心負責的工作幾乎是相同的，最大的差別在於蒐集情資的範圍來源與提供解決方案或策略的客戶端不同。

勤業眾信在資訊安全管理部分，提供了客戶端資安事件管理平台服務(SIEM)，建置的方法係於客戶端的網路環境中加裝設備，用以蒐集客戶端發生的網路異常事件，協助客戶了解自身發生的問題及辨別真正的攻擊，找出弱點及風險，並利用這些網路異常事件的資訊加以分析、運用，提供客戶事前的告警以及相關的防禦措施，以降低對於威脅的回應時間。而勤業眾信因為服務的企業組織眾多，對於資安事件管理平台於各客戶端蒐集到的網路異常事件之資料量龐大（前提當然是各客戶端願意分享網路異常事件資訊），而網路

威脅情資的重要基礎，即是必須擁有足夠且強大的情報來源，而勤業眾信即擁有這樣的資源及支援，藉由與各企業間的情資交流，以及內部資訊安全、網路分析專業人員的技術分享，加上專業研究人員不間斷的分析過濾所蒐集的資料，經由持續的資訊回饋，才能將情資分析做的更好更精準，而長期累積下來的分析經驗，自然而然地建置此豐富且多元的網路威脅情資中心。



圖八　網路威脅情資架構示意圖

（資料來源：勤業眾信）

	SIEM	CIC
資料來源	企業內部蒐集之資訊為主	各企業間的情資分享等外部資訊
功能	著重於資料蒐集，並整合企業內部各項設備之日誌紀錄，以發現威脅	著重於各企業間情資之分析、運用，以找出威脅及風險，並協助提供

	事件	相關之回應措施
優點	了解企業本身的弱點	了解攻擊者可能的手法
缺點	單純的蒐集資訊，容易產生過多且不必要的錯誤警示	須花費大量的分析資源，才能解析不同的情資

表三　SIEM 與 CIC 之差異

（資料來源：自行整理）

本次實地參訪海牙網路威脅情資中心，發現其與想像中冰冷嚴肅的工作環境完全不同，以下針對四大部分進行說明：

(一) 環境：網路威脅情資中心隱身於一棟辦公大樓中，進入勤業眾信的辦公區域後，經由負責人員的簡單介紹及說明，隨即進行實地的參觀，惟考量網路威脅情資中心之機密性，僅對部分環境進行說明。不意外地，網路威脅情資中心如同一般的機房重地戒備森嚴，要進入該中心，須經過一道一次僅容一人通過的安全門禁，而且不只須要門禁卡，還須輸入密碼確認身分後才可進入，而訪客則還需要管理階層授權後才可進入。而進入該中心後，亦顛覆了我對網路威脅情資中心的想像，原以為映入眼簾的會是一大片螢幕牆，牆前坐者一堆專業人士正在進行監控及分析，結果不然，走進中心後，發現牆上掛著專業團隊的照片，負責人員可以一一唸出員工的名字且負責的項目，頓時覺得這中心是個很有溫度的地方，而後看見的是一間間不透明的辦公室，經負責人員說明，每一間辦公室都有不同的用途，而且每個辦公室也都有嚴實的門禁控管機制，首先參觀的是負

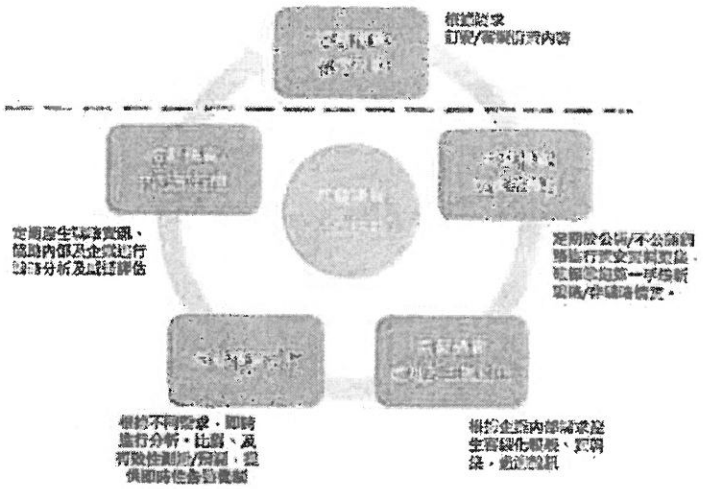
責監控的辦公區域，該區域不大，約有十來部電腦及 3、4 名人員，這間是 24 小時的監控中心，每天不同的時段由不同人員負責監控，主要透過建置於客戶端的託管平台進行客戶端的日誌蒐集，或通過現場部署的網路風險分析和行為分析工具進行日誌蒐集，並採用從日誌蒐集和關聯到行為分析的各種概念進行研究，如果有發現異常，則即時進行相關的通知；除了監控區域外，當然也有存放重要設備的機房，該機房需要三方密碼擁有者分別輸入密碼後才能開啟進入，是整個網路威脅情資中心中控管最嚴謹的區域；硬體設備研究室裡頭則擺滿了電腦相關的硬體設備和零件，負責人員說明，他們鼓勵員工多汲取電腦相關的知識，而這些零件即是電腦組成的基礎，資訊人員必須由基礎紮根，即使是平凡的小配件，也應該有相關程度的了解，而且拆解這些零件，對他們來說有時也是個紓解壓力的方式，其他研究室、分析室主要提供專業團隊進行威脅情資的分析，並每週定期進行經驗分享，除了該網路威脅情資中心的研究外，另外還有可以與各大城市網路威脅情資中心共同視訊討論的研究室。

(二) 專業團隊：該中心的技術團隊包含了各方面的專業人材，除具備專業能力外，還具備豐富的實務經驗，成員包含資訊安全專家、網路技術專家、情資分析專家、社交媒體分析師、技術駭客等顧問團隊，尤其技術駭客的部分，勤業眾信認為，要了解駭客的心態及手法，最佳的方法是讓自己也成為駭客，所以網羅了許多網路高手，培養自己的一組駭客軍團，以利進行相關的研究。雖然團隊成員的工作時間、地點不一，但會定期進行內部及外部的資訊交流及經驗分享，不定期的舉辦聚會，培養

團隊間的合作默契，且積極培訓員工參與專業技術課程，取得專業證照，例如：國際電腦稽核師 (CISA) ，資安系統專家 (CISSP) 和資訊安全經理人 (CISM) 、資安分析專家 (ECSA) 、道德駭客 (CEH) 、網路封包安全分析 (NSPA) 等各種資訊安全國際證照，以增長專業技術，並於國際各項資安比賽中，鼓勵成員組隊參加各項競賽，勤業眾信的駭客團隊已於近幾年的駭客大賽中取得優秀的成績。

(三) 服務策略：當今企業面臨的最大挑戰是難以專注於那些構成最高風險的網路威脅事件，如何使用先進的方法來分析當前的網路威脅，並確定哪些是可能的潛在影響加以進行防護。傳統的資安防禦模式似乎也愈來愈無法應付新興的威脅趨勢，勤業眾信期望能協助企業將傳統的資安防禦模式，提升為主動威脅情資的運用。首先協助企業由內部蒐集之資訊進行識別（如網路設備日誌），透過事件管理監控和行為分析內部威脅的主要來源，而由於安全漏洞不停的公佈，駭客們透過這些安全漏洞尋找獲取系統權限的方法，即是企業所面臨的主要威脅，而要降低威脅的發生，漏洞管理是不可或缺的一環。而企業內部的資訊蒐集、分析，僅能協助企業了解本身的狀況及問題，無法了解駭客可能使用的手法，解決方案大多只能採用被動的防禦。而隨著網路威脅的不斷發展，了解網路威脅形勢日趨困難，識別威脅不可或缺的方法就是利用大量資源來蒐集、過濾和分析來自各種來源的網路威脅資訊，才能將網路威脅情資發揮最大的價值，而若要需要大量的網路威脅資訊，單純蒐集單一企業的事件，是不足以了解新興的網路威脅形勢，因此透過網路威脅情資的專業團隊，將各個企業的事件彙整，再蒐集各企業外

部發生的潛在威脅事件，針對可行動型資安資訊 (Actionable Intelligence)、戰術型資安資訊 (Tactic Intelligence) 、戰略型資安資訊 (Strategic Intelligence) 等不同面向的威脅情資加以分析，透過網路威脅情資生命週期的概念，建立多元的網路威脅情資中心，並透過此中心的事件管理運用，預測新興形態的威脅手法，提供相關的告警回饋給客戶端，使各企業能夠在短時間內了解新興的威脅手法及適應未來的威脅，進一步提供各企業解決方法或相關對策，以防止或減輕潛在威脅對於企業的影響，即是網路威脅情資中心主要的服務策略，另可針對企業中不同層級之需求提供不同面向之威脅情資，客制化網路威脅情資之管理模式，也是此服務的另一項附加價值。



圖九　網路威脅情資生命週期

（資料來源：勤業眾信提供）

(四) 效益：透過網路威脅情資中心的有效運用，可為企業帶來以下的優勢

1. 快速識別內外部網路安全現況：企業能對內外部環境進行掌控，有效設計及部署相關的資訊安全防護措施及設備。
2. 縮短應變時間：透過看似互不相關的威脅事件情資進行相互的關聯分析，可能預測出新興的威脅手法，確認事件發生的可能及風險，供企業規劃對應的策略及解決方案。
3. 有效提高防禦強度及靈活度：企業可依據內外部現況的攻擊模式、技術及程序進行偵測並加以應對，將防禦模式由被動改為主動。
4. 提供管理階層做出適當的決策：透過網路威脅情資中心提供的資訊，可供管理階層有效掌握網路威脅趨勢，做出明確、有效的資訊安全策略。
5. 降低資源及成本的耗費：透過網路威脅情資中心分享網路威脅手法及解決方式，可降低的企業獨立對抗網路威脅所需耗費的資源、人力及各項成本

肆、 心得與建議

本次參訪了 4 家資訊相關產業後，進一步地認知，隨著網路的蓬勃發展及新興科技的多元趨勢，網路威脅事件也與日俱增，且具調查臺灣已屬於網路攻擊最嚴重的國家之一，加上因應金融科技發展下，金融業必然會是駭客組織或有心人士威脅覬覦的對象，以往企業內部的資訊安全防護措施僅能達到被動式防範，已不足以應付未來的網路威脅，要能有效明顯的減少網路威脅，採取主動式的預防，則需要仰賴完善且健全的網路威脅情報才能做到，也因此，合縱連橫的防禦架構，已是未來資訊安全的重要趨勢。對於身處金融產業的我們，因為本身的業務特性，網路威脅的資訊相對無法透明化的公開，僅能依賴現有的網路安全設備進行相關的防護

本行現況分析：

一、 依據英國標準的資訊韌性架構，本行的資訊業務範圍符合資訊安全管理 (ISO 27001) 、資訊科技服務管理 (ISO 20000) 、個人資料管理 (BS 10012) 及營運持續管理 (ISO 22301)等國際標準要求，並通過英國標準協會的認證且取得證書，對於行內的資訊系統，已訂有制度化、文件化的管理機制，有效維持資訊系統的安全管理，並降低營運中斷的風險。

二、 而針對網路威脅部分，本行已建置資安事件管理平台，24 小時不間斷的蒐集各種設備的事件資訊，做為日誌的處理、告警、分析與報告的工具，並透過監控機制，確保各系統的運作安全，但目前僅主要運用在日誌的處理及告警，礙於人力及專業技術的考量，目前還無法達到將事件進行分析的目標，這亦是本行目前的一大挑戰。且依目前資安防護運作現況，僅能達到內部異常事件警示及立即處理之作業，缺少主動洞悉外部威脅以預防事件發生的機制。

如何將現行傳統資安防禦能力，提升為主動利用威脅情資，並把外部各種

資安情資及內部資訊架構所遭受的攻擊與潛在弱點，統一彙整、分析並提供管理階層進行決策，以期有效因應數位科技帶來的資安風險，並將威脅情資淬煉為戰略策略，提升內部事件反應速度及增加外部威脅掌控能力，真正達到掌握情資，制敵機先之目標，亦是本行未來資訊安全發展的重要趨勢。

Team T5 公司創辦人暨執行長蔡松廷就曾經發表，關於第一銀行 ATM 遭盜領現金事件，就是沒有確實掌握威脅情資的直接範例。因為，類似的 ATM 盜領事件在國外已經發生過了，但臺灣的企業總認為攻擊者距離很遠，而一直沒警覺，而且就算看到這樣的消息，也認為與己無關，直到某天真的不幸發生，企業也措手不及而無法因應。因此，企業若要規劃完整的資安威脅應變及防禦機制，一方面可依組織架構按事件管理、網路支援、系統管理、資料庫應用等功能分類，建立資安威脅應變的組織，另一方面針對重要業務活動，考量外部威脅情資，設計與實施攻防演練；總括而論，企業必須全力將威脅情資淬鍊為有效的防禦策略，提升面對威脅時的應變能力。

針對本行網路威脅情資運用建議如下：

一、 強化資安事件管理平台 (SIEM, Security Information Event Management)

現行的資安事件管理平台僅能達到異常事件監控、警示，如果發現問題須立即採取處理措施，僅能被動式的在發現問題後尋找解決方法，而這對網路威脅情資來說，我們已經踏出了第一步，已有蒐集內部事件的機制，但更一進步地，我們應加以檢視，是不是所有的日誌紀錄均有被完整收納，不只是網路設備，還包含了作業系統資訊、應用系統資訊等等，建議可對資訊系統進行盤點，將所有的系統、設備之日誌紀錄予以蒐集，但很重要的一點，蒐集並非是單純

的將所有資訊倒入資安事件管理平台中，毫無規則的資訊反而容易造成平台的負擔及發出錯誤的警示，最好的方式是在資料納入平台前，有一定的正規化機制，先將多餘且不必要的資訊過濾，才能建立有效的事件管理機制，提供最正確的警示訊息及攻擊資訊。

二、 積極培養網路威脅事件分析人材

現行資安事件管理平台的運用，在於企業內部發生異常事件時的監控與警示，一個高效能的事件管理平台，是須要經過不斷的蒐集、分析並提出有效的建議，以本行目前的狀況，僅能達到蒐集的目標，尚無能力將這些蒐集到的事件資訊與以分析、彙整，原因在於現行的人力不足，且沒有足夠的專業知識、技術及經驗，因此，要提升事件分析的能力，得要從人員的專業知識著手，建議安排人員多參加資訊安全相關課程，並鼓勵同仁取得國際證照，提升專業能力，當專業能力提升後，我們有能力善用本身蒐集的資訊分析屬於自已的情報，建立應有的解決方案，更能提升本行的資訊安全優勢。

三、 善用金融資安資訊分享與分析中心 (Financial Information Sharing and Analysis Center , F-ISAC)

金融業的業務特性，將威脅資訊公開於網路上可能存在敏感資訊外洩的風險，因此相較於一般企業無法透明化的公開，若要蒐集金融業的威脅情資單靠一家銀行的力量是難以完成的，幸而金融監督管理委員會為提升金融體系資安防護能量，於 106 年底成立了金融資安資訊分享與分析中心 (F-ISAC) ，針對金融產業包含銀行、保險、證券期貨、投信投顧等各業別金融機構，提供「通報」、「情資研判分析」、「資安資訊分享」、「協處資安諮詢與評估」、「研討會、教育訓練及國際交流」、「資安專題研究分析」、「協助資安事件應變處理」、「金融機構資安演練」、「協助資安規範評估與建議」等 9 大服務，

並與資訊安全專家共同合作，協助進行資安控管和漏洞評估，以及針對資安事件進行分析，並研究策略提供緊急應變的處理，以建立一個強而有力的金融資安聯防體系，維繫金融市場的資訊安全。

以本行現行的狀況，單打獨鬥的應戰方式，是不足以對抗外部多元化的威脅，而金融監督管理委員會設置了金融資安資訊分享與分析中心 (F-ISAC) ，確實對金融業提供了很大的幫助，善用金融業合縱連橫的提供威脅情資，透過金融資安資訊分享與分析中心的情資分享，提供新興威脅的防禦方式，聯手低禦外部威脅，不但強化土地銀行本身的資訊安全，更是金融業整體資安防護的一項優勢。

依本行的現行資訊安全架構及運作狀況，且已取得多項資訊安全相關的國際標準認證，再再顯示本行具有一定的資訊安全防護能力，且有對應的機制降低營運中斷的風險，但若能依上述建議進行強化資安事件管理平台、提升人材專業能力及善用金融資安資訊分享與分析中心，相信可以協助本行提升對於內部事件的反應速度及增加對於外部威脅的掌控能力，真正做到善用情資，強化資訊安全防護，達到制敵機先的目標

伍、 結論

網路威脅情資就如同天氣預報，準確的預測天氣，可以讓人們在出門前就做好萬全的準備，大晴天時就該做好防曬，下大雨時就得準備好雨具，避免造成曬傷或淋雨的損害。而管理完善的威脅情報，就是讓企業做好萬全的準備，面對已預測到狀況，找出相對應的預防方式，讓攻擊者無從發動攻擊，讓企業避免不必要的損失。但是威脅情資的應用，是一項長遠的投資，需要靠企業之間不斷的交流及投入資源，協同資安專家的分析評估，才能建置完善的網路威脅情資中心，且這不是獨立的一項服務，而是必須和企業現有的防禦機制整合，透過企業的有效運用，才能發揮網路威脅情資中心最大的價值，降低企業面臨的資安風險及營運風險

陸、 參考文獻

[1] 吳佳翰、陳威棋、白哲豪，”次世代資安防禦－網路威脅情資淺談”，https://www2.deloitte.com/tw/tc/pages/risk/articles/cyber-threat-intelligence.html.

[2] BCI 地平線掃描報告 2018 HORIZON SCAN REPORT

[3] BCI 業務持續性管理實施－全球最佳實踐指南

[4] 金融資安資訊分享與分析中心(F-ISAC)揭牌 邁向金融資安聯防時代，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201712220001&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News