2020 金融趨勢關鍵議題

資安挑戰與金融業資安聯防之趨勢

TABF

台灣金融研訓院 金融研究所編製
AIWAN ACADEMY OF BANKING AND FINANCE

2020
May

本輯摘要

資訊系統可說是現代化金融服務的大腦與神經系統。一個金融機構能否順利營運，與其資訊系統是否妥善建置與維護息息相關。就是因為資訊系統扮演如此重要角色，以至於往往成為惡意人士攻擊的重心，一有疏漏除了造成直接的財物損失外，登上媒體版面往往會影響商譽或消費者信心，造成更大的損失。特別是我們的日常生活對資訊作業的依賴日深，網路、物聯網、雲端及大數據應用更為普及下，可被惡意攻擊的弱點也就越來越多。

由於金融業已面臨資訊科技所帶來之風險與衝擊，因此 2017 年 3 月 G20 財長與央行總裁會議宣言中提到，惡意的使用資通訊科技(Information and communication technologies, ICT)可能癱瘓掉一國或國際金融體系，破壞金融的安全與民眾的信任，並危及到金融穩定[1]。這也是為什麼新上任的金管會黃天牧主委，將金融資安列為「六大興利方案」之一。

目前大部分國家在銀行間或與監理機關間已有資安資訊交換機制，有的是自願性，有的是強制性，其目的就是共同抵抗越來越嚴重的資安威脅。台灣的資安聯防也已經上路，研究國外經驗應有助於建立更為完善的聯防體系，提升資安的抵抗力。

陳鴻達 副研究員 Honda Chen
研究領域：監理科技、宏觀審慎管理、開放銀行
聯絡方式：honda@tabf.org.tw

註 1：Bank for International Settlements, “Cyber-resilience: Range of practices”, 2018

CONTENTS

壹 資安風險趨勢與影響

資安風險有多大

世界經濟論壇的「全球風險報告，WEF Global Risks Report」[2]，針對當前全球所面臨的各種風險進行**「發生的可能性」與「發生後的衝擊」**分別進行排序，而資安問題經常是名列前茅。在 2020 年的報告中，「身分被冒用或資料被竊取」以及「網路攻擊」兩項分別高居十大可能風險的第 6 與第 7。而「網路攻擊」與「關鍵資訊基礎建設被毀」之風險，也高居十大衝擊之第 8 與第 6 位。雖然 2020 年資安問題的排名較 2019 年下降，但在世界經濟論壇所訪談的專家眼中，仍屬於發生率與衝擊性同時存在的高風險。

Top 10 risks (可能性)	Top 10 risks (衝擊影響)
1. Extreme weather	1. Climate action failure
2. Climate action failure	2. Weapons of mass destruction
3. Natural disasters	3. Biodiversity loss
4. Biodiversity loss	4. Extreme weather
5. Human-made environmental disasters	5. Water crises
6. Data fraud or theft	**6. Information infrastructure breakdown**
7. Cyberattacks	7. Natural disasters
8. Water crises	**8. Cyberattacks**
9. Global governance failure	9. Human-made environmental disasters
10. Asset bubbles	10. Infectious diseases

【圖 1】世界經濟論壇十大可能風險與十大衝擊風險之排序

資料來源：WEF Global Risks Report 2020

註 2：WEF，“Global Risks Report”，2020

同時接受WEF訪談的專家中，有76%的人認為網路攻擊造成基礎設施服務中斷的風險將增加。也有75%的人認為在未來新的一年中，網路攻擊、身分被冒用與資料被竊取的風險將更嚴重。這兩個資安問題分別高居風險將增加的第5與第8名，因此許多國家包括我國的蔡英文總統都曾公開表示，資安問題就是國安議題。

Short-Term Risk Outlook

受訪專家認為在 2020 年風險將會增加的項目以及認同的百分比

Economic confrontations	78.5%
Domestic political polarization	78.4%
Extreme heat waves	77.1%
Destruction of natural ecosystems	76.2%
Cyberattacks: infrastructure	76.1%
Protectionism on trade/investment	76.0%
Populist and nativist agendas	75.7%
Cyberattacks: theft of money/data	75.0%
Recession in a major economy	72.8%
Uncontrolled fires	70.7%

【圖2】認為未來風險將增加的項目

資料來源：WEF Global Risks Report 2020

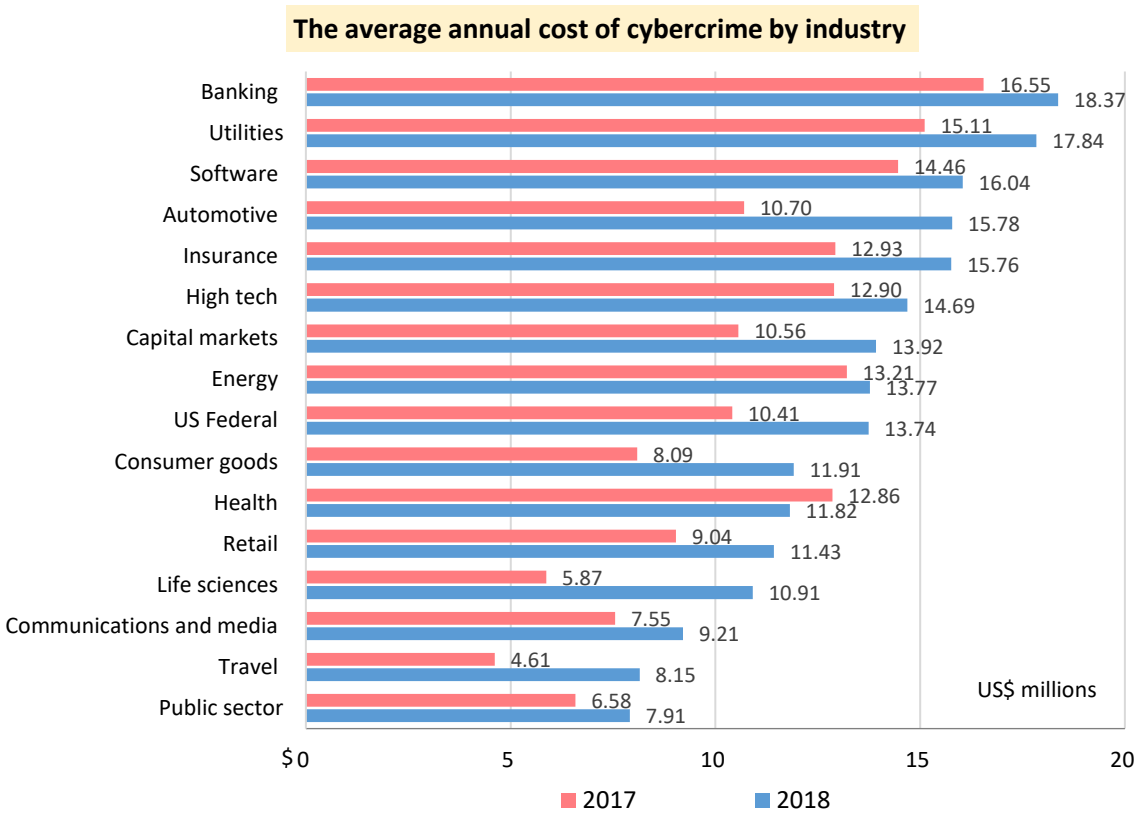
資安事件造成的損失

雖然要將網路犯罪的成本貨幣化不容易，但根據美國華府著名智庫CSIS的報告估計[3]，全球網路犯罪所造成的直接與間接成本高達6千億美金，約占全球GDP的0.8%。該智庫納入統計的項目包括：企業機密資訊與智慧財產的損失、身分冒用與個資竊取、竊取企業營收或規劃資料，進而影響併購等財務操作、因資安造成工作暫停的時間損失、網路勒索贖金、修護成本、保險費用、商譽與庫存損失。

另外根據Accenture針對來自11個國家355間企業的2,647位主管的訪問結果顯示[4]，網路犯罪對銀行業所增加的成本最大，保險業也擠上第5名。在2018年平均每家銀行為因應網路犯罪的成本為1,837萬美金，較2017年增加182萬美金。

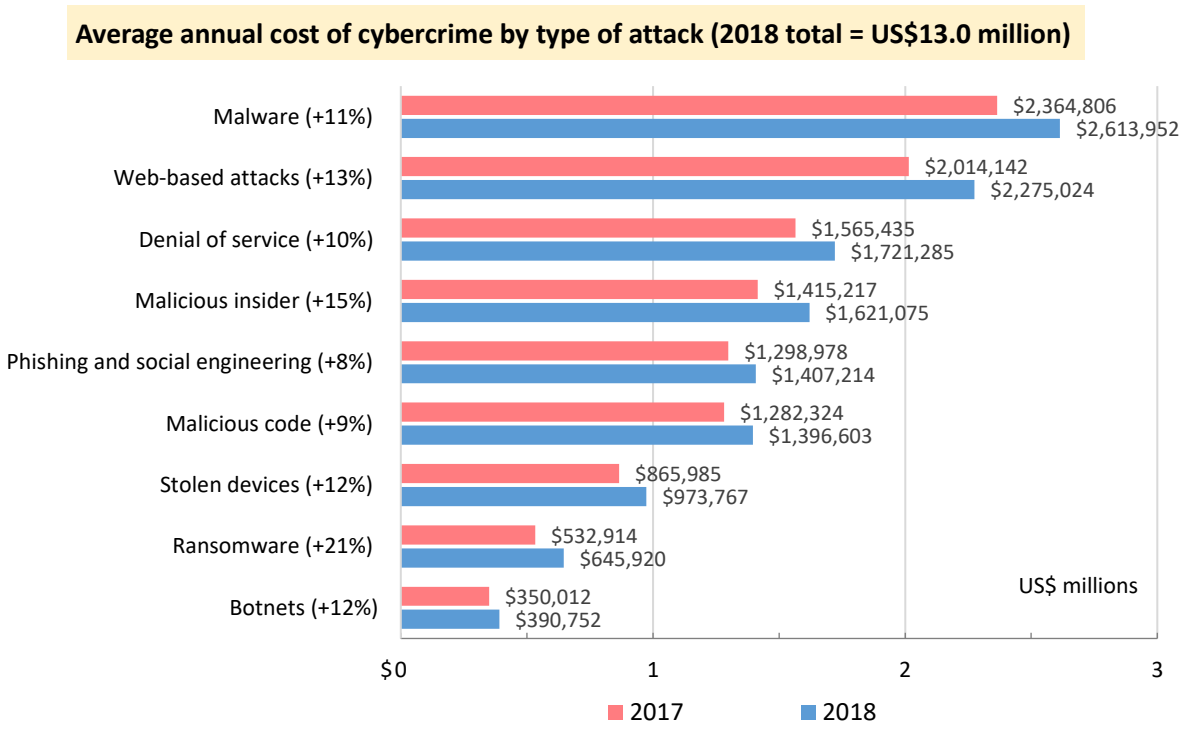
註 3：CSIC，“Economic Impact of Cybercrime-No Slowing Down”與 McAfee 合作, 2018

註 4：Accenture，“The Cost of Cybercrime”與 Ponemon Institute 合作, 2019



【圖3】行業別平均每年每家受訪公司為因應網路犯罪所增加的成本

資料來源：Accenture, 2019



【圖4】平均每家受訪企業每年因各種網路犯罪所增加成本分析

資料來源：Accenture, 2019

貳 資安攻擊類型分析

1. 進階持續威脅攻擊(APT)

卡巴斯基 2015 年公布一份名為「最大銀行搶案」指出，Carbanak 駭客集團利用 APT 已入侵約 100 家金融機構，其中半數有財物損失，受害銀行遍及全球，較集中於俄羅斯、烏克蘭、德國與中國。其中某受害者的 ATM 被動手腳自動吐錢，損失約七百萬美金。另一個受害者被盜轉一千萬美金。[5]

2016 年駭客入侵孟加拉中央銀行 SWIFT 系統，取得系統登入憑證，盜轉了八千一百萬美金。導致總裁 Atiur Rahman 為此下台，隨後越南、菲律賓與我國某銀行也陸續傳出 SWIFT 系統遭攻擊。

2. 分散式阻斷服務(DDoS)

2017 年 2 月台灣券商首次集體遭到 DDoS 攻擊勒索，全台 79 家券商中有 13 家遭到攻擊，這 13 家的交易量約占全國總交易量的三分之一。券商集體遭 DDoS 攻擊事件公開後，署名 Armada Collective 的駭客勒索信曝光，要求 7～10 個比特幣。並表示這只是試探性的攻擊，券商若不付款將發動更大規模的攻擊。[6]

2018 年 5 月調查局破獲台灣首家提供 DDoS 攻擊的網站，宣稱可提供穩定且強大的攻擊流量。要購買此服務者須將比特幣匯到國外的指定帳戶。

3. 勒索病毒軟體(Ransomware-as-a-Service, RaaS)

2017 年 5 月全球逾一百個國家陸續遭到名為「想哭(WannaCry 或 Wcry)」的勒索病毒軟體攻擊，中毒電腦的所有檔案將被強制封鎖並加密。一旦用戶點擊檔案，畫面即會跳出對話框，逼迫用戶購買「比特幣」來交換解密程式。被勒索人須購買三百到六百美元不等的比特幣，並匯入指定帳號。用戶若遲未繳付「贖金」，所有檔案將遭到刪除。台灣雖然也有人中鏢，但金融業因普遍不能隨意安裝軟體，資訊安全防護標準較高，同時網路銀行、ATM 等都放在伺服器，因此未有災情發生。

註 5：Kaspersky, "CARBANAK APT --THE GREAT BANK ROBBERY", 2015

註 6：台灣金融研訓院，「金融科技力」第 14 章資訊安全與風險管理，2019

參 國際資安聯防之經驗

美國金融服務業資訊分享與分析中心(FS-ISAC)

該中心成立於 1999 年，是一個非營利性的自願性組織。蒐集金融業資安弱點的資訊，並即時提供資安威脅的警告給會員。其目的在分享關鍵的聯防團隊資訊，用以評估或回應金融業之實體的或網路的資安危機。這些資訊有助於掌握情況；分析威脅、弱點與衝擊；協調政府各機關與相關業者。其目標是提高金融業各部門，甚至國家與全球對資安威脅的抵抗力。以避免資安危機造成大規模的中斷資訊作業，衝擊到金融運作的安全、穩定或聲譽。但這個架構不是要取代原先監理機關對各業者關於資安的監理要求。

其會員包括：銀行、信用合作社、保險公司、投資公司與金融監理機關。除了最為資訊交流平台，FS-ISAC 舉辦研討會、教育訓練課程，並規畫進行跨部門的演練。其他工作或效益如下：

1. **快速回應**。FS-ISAC 藉由 (Critical Infrastructure Notification System, CINS)即時取得會員間遇到的資安威脅資訊，並加以分析。

2. **資訊分析與分享**。FS-ISAC 全年無休，每日 24 小時從各種管道取得各種資訊，經確認後進行分類與分級，並即時透過 CINS 給各會員，必要時 FS-ISAC 還會發出危機通知。

3. **匿名資料**。由於不管是 FS-ISAC 蒐集的，還是其發給各會員的資訊都具有機密性，因此都必須 secure portfolio，避免被猜到是哪一個機構遇到的問題。因為隱私獲得保障，所以各會員願意分享資訊。

4. **會員主導**。因此在運作上會滿足會員的需求。

5. **被監理機關認可**。Federal Financial Institutions Examination Council 認可 FS-ISAC 是一個主要提供資安威脅情報來源的機構，以減輕資安威脅與脆弱性。

英國網路安全資訊分享夥伴計畫 (CiSP)

有鑑於資安威脅日益複雜與頻繁，英國在 2016 年成立獨立的國家網路安全中心(NCSC)，提供即時資安威脅分析、提供技術建議、對重大資安事件之回應，以減輕資安事件的損失。特別要強調的是 NCSC 不是監理或管制機構，他們提供免費與機密的資安建議。每個業者能獲得多少的資源或協助，完全取決於這些資安衝擊對國家利益的危害程度。資安事件發生時，NCSC 提供技術建議或指引，某些狀況也會直接提供技術支援。

而為了提升資安績效，NCSC成立一個網路安全資訊分享夥伴關係倡議(CiSP)，結合政府與民間業者的力量，即時交換資安威脅的資訊，同時又保有個別業者的機密，提高群體的資安意識，以降低對全英國的威脅。每個在英國登記的公司行號，或是有立案的機構都可以登記參加CiSP。線上登錄參加的手續非常簡便，號稱五分鐘就可填好申請表格，送出之後五個工作天之內便可接到正式參加CiSP的邀請。

參加會員的好處包括：得到早期資安威脅的預警、可獲得其他人過去成功或失敗的經驗、可尋求專業建議、可免費獲得適合自身行業屬性的資安監測報告者，以提升本身及整個行業的防護力。

肆 我國金融業資安聯防體系的建立

有鑑於資安聯防已經成為國際趨勢國際上，並取得顯著成果，因此金管會從2016年開始也陸續推動相關工作。初期由臺灣證券交易所以證券期貨業者為範圍，先行試辦證券期貨資安分享中心。2017年2月幾家證券商遭受到國外駭客分散式阻斷服務(Distributed Denial of Service, DDoS)攻擊期間，證交所試辦的資安分享中心即發揮聯防功能，協助業者建立對網路下單服務之即時監控，並導入流量清洗機制，也建立遭受攻擊的緊急應變處理程序。

2017年12月正式成立「金融資安資訊分享與分析中心」，以之前證券期貨業為基礎，將服務範圍擴大涵蓋銀行、保險、證券期貨、投信投顧等金融業別，目前已有3百餘家金融機構加入成為會員。目前規劃該資安分享中心有六大功能，包括情資研判分析、資安資訊分享、通報服務、資安諮詢與教育訓練、資安事件應變處理機制及建立資安事件改善的良性循環等六大功能。讓金融業在防範酸客攻擊上，化被動為主動，有效提升防護能力。

【表1】金融資安聯防體系六大功能

六大功能	說明
情資研判分析	金融資訊安全的情資蒐集、分析與研判，並發出警訊給金融機構。
資安資訊分享	建置金融機構間和與行政政院的「政府資安資訊分享和分析中心」交換與共享資安情報。
通報服務	接收金融機構通報資安事件，並可發布緊急資安情資通報金融機構事先防範。
資安諮詢與教育訓練	提供資安諮詢與漏洞評估服務，辦理相關資安研討會、座談會等專業訓練課程。
資安事件應變處理理機制	就金融機構資安事件，提供相關之技術及鑑識支援。
建立資安事件改善的良性循環	就國內外重大資安事件，探究問題發生原因、事件應變處置程序等，動態檢討可供借鏡改善之處。

資料來源：金融監督管理委員會，本研究自行整理

伍 結語

除了資訊交換之外，國際上越來越多進行紅藍實際演練。專人扮演駭客假想敵來進行模擬演練，找出缺失以利改進。另外由於駭客的攻擊往往是跨國性的，因此國際上越來越重視跨國間的資安聯防合作，例如美國的 FS-ISAC 與新加坡的 MAS 就有合作計畫；香港的 HKMA 與新加坡 MAS 也有合作備忘錄。這都可供我國未來建立更完善資安聯防體系之參考。

TABF

台灣金融研訓院 院本部
地址：(10088)台北市中正區羅斯福路三段 62 號
總機：(02)3365-3666
傳真：(02)2363-8968
研究所辦公室：(10646)台北市大安區羅斯福路三段 37 號 10 樓
金融研究所專線：(02)3365-3677