淺談資安政策與資安治理成熟度評估

蘇柏鳴 / 金融聯合徵信中心 資安部

資安風險

世界經濟論壇（World Economic Forum，WEF）每年都會出版全球風險報告(The Global Risks Report)，2020年的報告[1]中顯示Cyberattacks在Likelihood 項排名排名第七，Impact項排名第八，由此可見，資安風險所造成的衝擊已經是各機構的決策者(decision-makers)在風險控管層面不能忽視的主要風險項目，而資訊安全的討論已不僅停留在管理與技術層面，近年來已提升至法律及治理層面。

為了因應這股世界風潮，「資通安全管理法」已於2019年1月1日正式施行，依其子法「資通安全責任等級分級辦法」之管理面應辦事項，資通安全責任等級A級與 B 級之公務機關，每年應辦理一次資安治理成熟度評估作業，而金管會為強化金融業資安防護能力，達成安全、便利、營運不中斷目標，也在2020年8月6日今日發布「金融資安行動方案」，並提出四大後續策勵方向，強化資安監理、深化資安治理、精實金融韌性及發揮資安聯防。

表1、Top 10 risks in terms of Likelihood

1	Extreme weather (極端氣候)
2	Climate action failure (氣候行動失敗)
3	Natural disasters (自然災害)
4	Biodiversity loss (生物多樣性喪失)
5	Human-made environmental disasters (人為環境傷害)
6	Data fraud or theft (數據詐欺或竊盜)
7	Cyberattacks (網絡攻擊)
8	Water crises (水資源危機)
9	Global governance failure (全球治理失靈)
10	Asset bubbles (資產泡沫)

1 2020年全球風險報告，http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

圖1、 The Global Risks Landscape 2020

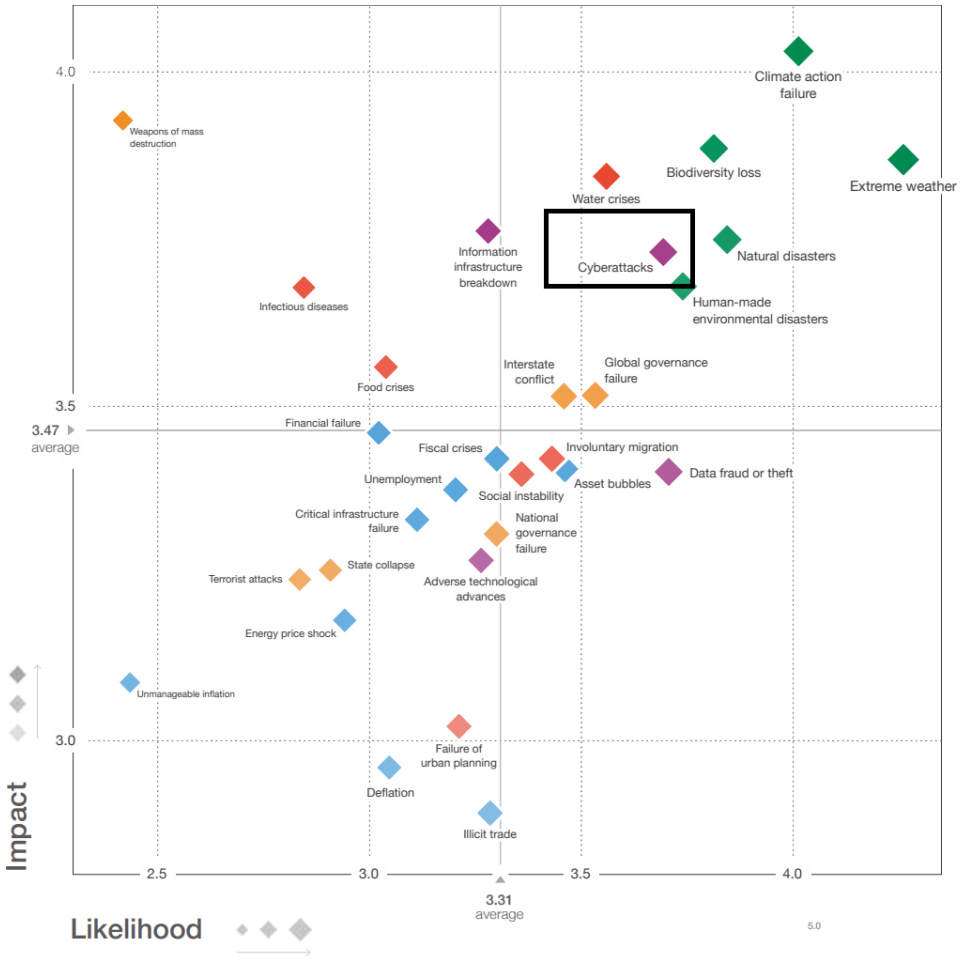


表2、Top 10 risks in terms of Impact

1	Climate action failure (氣候行動失敗)
2	Weapons of mass destruction (大規模殺傷武器)
3	Biodiversity loss (生物多樣性喪失)
4	Extreme weather (極端氣候)
5	Water crises (水資源危機)
6	Information infrastructure breakdown (信息基礎建設故障)
7	Natural disasters (自然災害)
8	Cyberattacks (網絡攻擊)
9	Human-made environmental disasters (人為環境傷害)
10	Infectious diseases (傳染性疾病)

資通安全管理法

公告日期為2018年6月6日，並於2019年1月1日正式施行。

表3、臺灣資通安全管理法架構

		說明	子法[2]
資通安全管理法	第一章 總則 §1～§9	立法目的、用詞定義、規範對象、資通安全產業之推動、行政院職責、委任或委託、資安責任等級分級、情資分享機制、資通委外監督	• 資通安全責任等級分級辦法 (第七條 第一項)。 • 特定非公務機關資通安全維護計畫實施情形稽核辦法 (第七條 第二項)。 • 資通安全情資分享辦法(第八條 第二項)。
	第二章 公務機關資通安全管理 §10～§15	資通安全維護計畫之訂定、資通安全維護計畫實施情形之查核、資通安全事件通報應變之訂定、資通安全長之設置、獎懲辦法	• 資通安全事件通報及應變辦法(第十四條 第四項)。 • 公務機關所屬人員資通安全事項獎懲辦法(第十五條 第二項)。
	第三章 特定非公務機關資通安全管理 §16～§18	資通安全維護計畫之訂定、資通安全維護計畫實施情形之查核、資通安全事件通報應變之訂定、行政檢查	
	第四章 罰則 §19～§21	行政處分	• 資通安全事件通報及應變辦法(第十八條 第四項)。 • 公務機關所屬人員資通安全事項獎懲辦法(第十九條 第二項)。
	第五章 附則 §22～§23	施行細則、施行日期	• 資通安全管理法施行細則(第二十二條)。

金融資安行動方案

1.願景：因應層出不窮的資安事件(圖二)，追求安全便利不中斷的金融服務。

2.目標

(1)建立業者重視資安的組織文化

(2)提升業者資安治理能力與水準

(3)確保系統持續營運與資料安全

3.推動策略

(1)強化資安監理

- 建立業者重視資安的組織文化：設立資安長、遴聘具資安背景之董事。
- 完備資安規範：訂定資通安全防護基準、新興金融科技資安規範及供應鏈風險管理規範。
- 強化資安監理職能：提升中高階主管資安知能。

2 資通安全管理法子法最新公告，https://nicst.ey.gov.tw/Page/D94EC6EDE9B10E15/8c1e32e1-f068-4cab-a97d-865d5524d705

- 加強金融資安檢查：因應新興業務調整資安檢查重點及提升資安檢查人員專業技能。

(2)深化資安治理

- 加強資安管理：導入國際資安管理標準(ISMS)及取得驗證、推動金融資安治理成熟度、鼓勵金融機構自評。
- 強化資安監控：建置資安監控機制(SOC)。
- 加強資安人才培育：訂定金融資安人才職能地圖、鼓勵金融資安人員取得國際資安證照、推動攻防演練訓練課程。

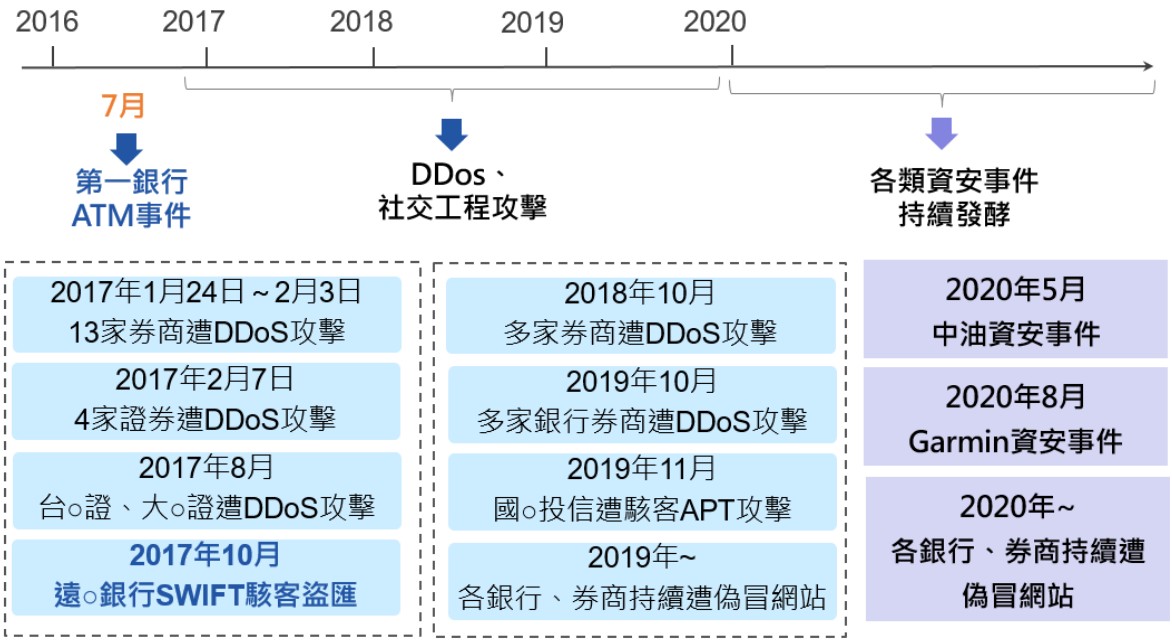
(3)精實金融韌性

- 增進營運持續管理量能：訂定強化作業韌性參考規範、導入國際營運持續管理標準(BCM)及取得驗證、實際作業之營運持續演練。
- 加強資安演練：辦理金融資安攻防演練、辦理金融資安攻防競賽、辦理重大資安事件應變情境演練。
- 建構資料保全避風港：推動成立資料保全中心。

(4)發揮資安聯防

- 資安情資分享與合作：建立資安情資關聯分析平台，提供金融機構早期預警與防護。
- 建立金融資安事件應變體系：建立電腦資安事件應變小組、建立金融資安應變體系(F-ISAC)。
- 建立金融資安事件監控體系：訂定資安監控作業標準，透過 協同運作，以即時有效關聯分析資安風險。

圖2、近年國內資安事件



政府資安治理成熟度

行政院國家資通安全會報技術服務中心提出之「資安治理成熟度評估」，共三個面向(策略、管理及技術)、11個流程構面及41個檢核項目，而每個檢核項目分成「Level0 未執行流程」、「Level1 已執行流程」、「Level2 已管理流程」、「Level3 標準化流程」、「Level4 可預測流程」及、「Level5 最佳化流程」，經由檢核項目的評分可以瞭解該面向中哪個流程構面為短版(木桶理論[3])，進而改進流程來強化該面向。

圖3、資安治理成熟度三個面向

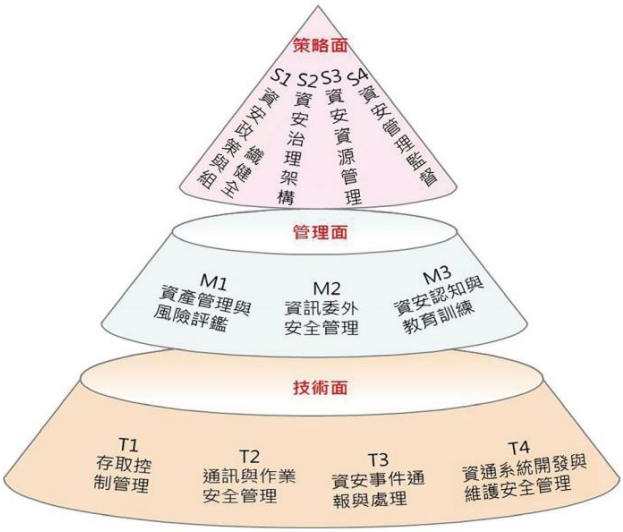


表4、檢核項目41個細項

面向	流程構面	檢核項目
S策略	S1資安政策與組織健全	1. 建立資安政策與標準作業程序
		2. 具備資安推動組織與執行管理審查
		3. 落實資安法令與規範
	S2資安政策與組織健全	4. 納入資安新興議題於年度業務項目
		5. 落實利害相關者溝通方式
		6. 揭露重要資安資訊
	S3 資安資源管理	7. 規劃資安資源
		8. 配置資安專職人員
	S4 資安管理監督	9. 執行資安內部稽核
		10. 落實資安管理制度 (ISMS)驗證
		11. 訂定業務持續運作計畫與執行演練
M管理	M1 資產管理與風險評鑑	12. 盤點資訊資產與執 行風險評鑑
		13. 執行資通系統分級與落實資安防護基準
	M2 資訊委外安全管理	14. 評估委外廠商資安專業能力
		15. 確保委外廠商資安 管理
		16. 確保委外廠商資安稽核
	M3 資安認知與教育訓練	17. 訓練資通安全及資訊人員應具備資安技能
		18. 訓練一般使用者與主管應具備資安認知
		19. 取得資安專業證照
		20. 宣導資安政策與相 關資安要求

3 木桶理論，https://wiki.mbalib.com/zh-tw/%E6%9C%A8%E6%A1%B6%E5%8E%9F%E7%90%86

面向	流程構面	檢核項目
T 技術	T2 通訊與作業安全管理	21. 落實網路安全管理
		22. 管理資通系統權限
		23. 落實機敏資訊之加 密管理
	T3 資安事件通報與處理	24. 執行惡意軟體之偵測與預防
		25. 執行遠距工作安全控制措施
		26. 落實電子郵件安全管理
		27. 落實機房管理
		28. 執行資料與資通系統備份
		29. 執行儲存媒體之防護措施
		30. 落實資通安全監控
		31.落實資通安全防護
		32. 執行政府組態基準
		33. 執行資通安全健診
		34. 執行網站安全弱點 檢測
		35. 執行系統滲透測試
		36. 執行資安事件通報應變
		37. 保存資通系統與資 安設備日誌紀錄
	T4 資 通系統開發與維護安全	38. 執行資通系統開發 之安全需求設計
		39. 執行資通系統開發之安全性測試
		40. 執行源碼安全管理
		41. 區隔系統開發、測試、實作的環境與設備

總結

全球主要國家數位科技風險法規推陳出新，2015年5月，澳洲金融監理署(Australian Prudential Regulation Authority)公告CPG234資訊及資訊技術安全管理指南，作為其轄下監管機構之資訊安全管理參考指南；歐盟為於2019年4月17日通過網路安全法（Cybersecurity Act），並自2019年6月27日生效。並授權成立一常設之歐盟網路安全專責機構-歐盟網路與資訊安全局（European Union Agency for Cybersecurity，ENISA）。；美國紐約州金融廳(NYDFS)發表「銀行業交易監控與制裁名單過濾機制之規範與聲明」(簡稱Part 504)與「金融服務業網路安全要求規範」(23 NYCRR Part 500)相關規則與法案並於2017/3/1正式生效，數位科技風險法規已成世界潮流，目前國內資通安全法在實務上執行尚有進步空間，期待未來政府能吸取各方意見持續優化法規，讓台灣資安治理持續建全。