

上市櫃企業資安治理 - 從合規到競爭優勢

陳志明

安永諮詢服務股份有限公司 副總經理

2025年4月17日



The better the question. The better the answer. The better the world works.



講者簡介



陳志明
副總經理
安永諮詢服務股份有限公司

Mobile +886 936 169 800
Tel +886 2 2757 8888 #67836
Email Jemmy.CM.Chen@tw.ey.com

背景介紹

學歷

- ▶ 中山大學 資訊管理研究所 碩士
- ▶ 中山大學 資訊管理學系 學士

專業資格

- ▶ CISSP
- ▶ CISA
- ▶ ISO 42001 LA
- ▶ ISO 27001 LA
- ▶ BS 10012 LA

相關工作經驗

- ▶ 具備金融、高科技、電信等產業商業及資訊流程的風險管理經驗，在資訊安全、機敏資料/個人資料/隱私權保護相關領域有超過15年的工作經驗
- ▶ 協助多家金控、銀行、保險及證券公司建構資訊安全風險管理架構，並取得資訊安全管理制度 (ISO 27001)及個人資料保護管理制度(PIMS)國際認證
- ▶ 協助多家半導體、資訊電子業公司執行資訊安全風險管理，資訊安全架構設計、資訊系統安全評估（包含弱點掃描、滲透測試），建置ISO 27001資訊安全管理制度，並取得國際認證
- ▶ 負責過20個以上資訊安全/機敏資料保護/個人資料保護專案，協助客戶建置資訊安全管理制度、個人資料保護管理制度，並取得國際認證
- ▶ 主要的客戶群包含半導體、資訊電子、電信、金控、銀行、證券與保險、汽車、零售等產業

專業能力

- ▶ 資訊安全風險管理制度建置
- ▶ 資訊安全架構設計與評估
- ▶ 資訊安全解決方案設計
- ▶ 機敏資料保護與管理
- ▶ 個人資料保護/隱私權管理
- ▶ 供應鏈風險管理評估
- ▶ 資訊科技環境控制諮詢
- ▶ 一般資訊循環及應用系統查核
- ▶ 資訊循環控制制度設計及覆核

上市櫃公司資安相關法規重點



2022年分享的内容

CYBERSEC 2022
臺灣資安大會

9.20 ~ 9.22
臺北南港展覽二館

CHANGE

年報揭露資安管理作為的實務議題

ITHome

EY

資本額百億以上公司資安作為揭露分析 (1)

上市櫃公司資本額達百億以上公司 119 家，其中取得 115 家公司年報

年報頁數 平均 317 頁 最薄 66 頁 最厚 709 頁	資安作為揭露頁數 平均 2.5 頁 最薄 0.5 頁 最厚 6~7 頁	揭露內容最豐富 兆豐金控 中華電信 中信金控 中國鋼鐵
揭露資安架構 113 家	揭露資安政策 113 家	揭露管理方案 113 家
揭露科技改變及產業變化對財務業務之影響及因應措施 111 家		

第14頁

EY

觀察重點(1) - 主管機關的意向

資通安全管理架構
資通安全政策
具體管理方案
投入資通安全管理之資源
重大資通安全事件之損失、可能影響及因應措施
科技改變及產業變化對公司財務業務之影響及因應措施
資通安全事件

公開發行公司
年報應行記載
事項準則
年報
企業官方網站

評估標準
時間與方式
內容
確保可靠
度的機制
目的

法令、法規規範
證交所、櫃買中心查核

鼓勵
要求
強制(?)

第28頁

EY

資本額百億以上公司資安作為揭露分析 (2)

揭露資安人數 27 家 資安人數最多 台積電 500+ 資安相關 1000+ 警勤資安	揭露資安經費 13 家 資安經費最多 ▶ 台積電：10 億元 ▶ 玉山金控：3 億元 ▶ 聯發科：2.4 億元 ▶ 富邦金控：資安經費 占資訊經費5%	揭露重大資安事件 14 家 最高損失金額 元大金控 1950 萬
--	--	---

第15頁

EY

資本額百億以上公司資安作為揭露分析 (3)

取得ISO 27001認證 68 家 其他資安相關標準 NIST CSF ISO 27701 BS 10012 ISO 22301 ISO 15408 ISO 62443 FFIEC CAT TISAX	揭露資安會議次數 52 家 會議型態 審計委員會 PIP委員會 資訊安全管理委員會 處務會議 ISMS例會 金控資安主管會議 風險管理會議 資安聯防會議	揭露教育訓練計劃 82 家 投保或評估資安險 12 家
--	---	--------------------------------------

第16頁

EY

董事會關注資安議題 - EY Fortune 100大揭露調查 (2018-22)

Fortune 100 cybersecurity disclosures, 2018-22
How they plan, implement, and disclose cybersecurity risks included in the 2022, 2021, 2020, and 2019 disclosures.
Note: The data represents the 2022 disclosures, unless otherwise specified.

Disclosure	Score	2022	2021	2020	2019
Board oversight	100	100	100	100	100
Board expertise	100	100	100	100	100
Board independence	100	100	100	100	100
Board diversity	100	100	100	100	100
Board composition	100	100	100	100	100
Board effectiveness	100	100	100	100	100
Board engagement	100	100	100	100	100
Board communication	100	100	100	100	100
Board transparency	100	100	100	100	100
Board accountability	100	100	100	100	100
Board responsibility	100	100	100	100	100
Board integrity	100	100	100	100	100
Board ethics	100	100	100	100	100
Board culture	100	100	100	100	100
Board values	100	100	100	100	100
Board mission	100	100	100	100	100
Board vision	100	100	100	100	100
Board strategy	100	100	100	100	100
Board goals	100	100	100	100	100
Board objectives	100	100	100	100	100
Board priorities	100	100	100	100	100
Board focus	100	100	100	100	100
Board impact	100	100	100	100	100
Board legacy	100	100	100	100	100
Board reputation	100	100	100	100	100
Board image	100	100	100	100	100
Board brand	100	100	100	100	100
Board identity	100	100	100	100	100
Board personality	100	100	100	100	100
Board character	100	100	100	100	100
Board temperament	100	100	100	100	100
Board disposition	100	100	100	100	100
Board nature	100	100	100	100	100
Board quality	100	100	100	100	100
Board quantity	100	100	100	100	100
Board value	100	100	100	100	100
Board worth	100	100	100	100	100
Board price	100	100	100	100	100
Board cost	100	100	100	100	100
Board benefit	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss	100	100	100	100	100
Board gain	100	100	100	100	100
Board revenue	100	100	100	100	100
Board income	100	100	100	100	100
Board expense	100	100	100	100	100
Board cost	100	100	100	100	100
Board profit	100	100	100	100	100
Board loss					

資本額百億以上公司資安作為揭露分析

	110年年報	111年年報	112年年報
揭露家數	115	117	116
年報頁數	平均：317 最厚：709 最薄：33	平均：327 最厚：719 最薄：31	平均：319 最厚：707 最薄：21
資安作為頁數	平均：1.9 最厚：5 最薄：0.5	平均：2.1 最厚：5 最薄：0.5	平均：2.2 最厚：6 最薄：N.A.

年報揭露資安管理作為範例 - 中華電信

112年年報



111年年報



■ 表格化呈現投入資安資源，容易識別與分析其效果。



年報揭露資安管理作為範例- 中鋼

(四)投入資通安全管理之資源

112年年報

112 年資訊安全措施推動執行成果：

政策	認證
維護 27 個資安管理規定和作業標準，修訂 14 個項次。	111 年通過 ISO/IEC 27001 資訊安全管理系統審查，112 年認證持續有效。
訓練/宣導	
1.辦理 112 年新進員工資訊安全教育訓練，共 365 人受訓，皆完成資訊安全教育訓練，並通過測驗考核。 2.112 年完成 ECIH 資安危機處理課程，共 9 人受訓。	每月執行 1 次資安宣導，共辦理 12 次，宣導內容包含資安新知、弱點修補資訊及重要資安宣導等
資安檢測	
138 個站台滲透測試檢測與執行弱點掃描檢測 每年執行2次電子郵件社交工程釣魚郵件演練，抽樣演練人數2,000人	

(四)投入資通安全管理之資源

111年年報

111 年資訊安全措施推動執行成果：

政策	認證
維護 24 個資安規範	111 年通過 ISO/IEC 27001 資訊安全管理系統審查，認證持續有效
訓練/宣導	
1.辦理 111 年新進員工資訊安全教育訓練，共 513 人受訓，皆完成資訊安全教育訓練，並通過測驗考核。 2.111 年完成 CHFI 資安鑑識調查專家訓練，共 9 人受訓。	每月執行 1 次資安宣導，共辦理 12 次，宣導內容包含資安新知、弱點修補資訊及重要資安宣導等
資安檢測	
135 個站台滲透測試檢測與執行弱點掃描檢測 每年執行 1 次電子郵件社交工程釣魚郵件演練，抽樣演練人數 1,000 人	

(四)投入資通安全管理之資源

110年年報

110 年資訊安全措施推動執行成果：

政策	認證
新增/修訂 22 個資安規範	通過 ISO/IEC 27001:2013 資訊安全管理系統驗證
安全教育訓練，並通過測驗考核	修補資訊及重要資安宣導等
資安檢測	
20 個站台滲透測試檢測	113 個站台執行弱點掃描檢測
每年執行 1 次電子郵件社交工程釣魚郵件演練，抽樣演練人數 700 人	

■ 表格化呈現投入資安資源，容易識別與分析其效果。

年報揭露資安管理作為範例- 中國信託

112年年報

認證

通過	通過	通過	通過
ISO 27001:2013 資訊安全管理系統 認證	ISO 22301:2019 營運持續管理系統 認證	BS 10012:2017 個人資料管理系統 認證	PCI DSS 支付卡產業 資料安全標準認證

第三方評估

個資保護 破信查核	電腦系統 資訊安全 評估	資訊安全 整體執行 情形評估	SWIFT 客戶安全 計畫評估	電子支付 機構查核	資訊系統 滲透測試	紅隊演練	DDOS 攻防演練
--------------	--------------------	----------------------	-----------------------	--------------	--------------	------	--------------

教育訓練及宣導

39,000 小時宣導課程 1,400 小時專業訓練 24,000 人次參與模擬挑戰 28 份資安宣導函 5 場資安事故演練

所有員工均須完成年度個資與資安認知教育訓練，課程內容包含：社交工程、上網安全、辦公環境安全等議題。針對資訊安全專責單位人員提供專業課程訓練或職能訓練，訓練主題包含：雲端安全、安全開發、數位鑑識等。宣導成效：辦理 2 次資安情境模擬挑戰，透過模擬真實情境的互動式問答，強化製作 28 篇資訊安全宣導函，持續傳達資訊安全重要規定與事項。業務單位及資訊管理等單位於年度內辦理資安事故演練，以促使同仁熟悉事故應變流程。

社交工程演練

156,000
餘封社交工程演練信件

每月均參考當下時事設計釣魚郵件主題，對海內外全體同仁進行無預警演練，並於演練後公告演練成績。另辦理 4 次針對釣魚郵件，透過展示真實攻擊樣貌及風險，強化辨識可疑郵件能力。

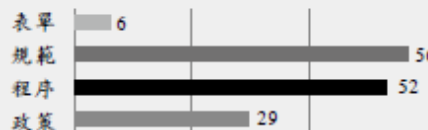
資安人力配置

29 人資安一道作業
30 人資安二道作業

除在資訊安全專責單位配置 30 名資安專業人力，綜理全球二道防線作業外；另配置 29 人辦理安控系統、帳號管理及資安設備維護等一道防線作業。

規範增修

143 份制度文件增修



參考國際最佳實務，定期審閱資訊及資安相關政策及作業管理規範，並依風險趨勢及最佳實務增修相關管理要求。

KPI 指標

47 項資安 KPI 指標

透過企業資安委員會轄下資安工作小組分別針對弱點管理、資安防護和監控應變等面向完成分析作業，並依據分析結果建立檢核機制及 KPI 指標，以達到持續監控及改善目的。

表格及視覺化呈現投入資安資源，容易識別與分析其效果。

111年年報

認證

通過 ISO 27001:2013 資訊安全管理系統 認證	通過 BS 10012:2017 個人資料管理系統 認證	通過 PCI DSS 支付卡產業 資料安全標準認證
-------------------------------------	------------------------------------	---------------------------------

第三方評估

個資保護 破信查核	電腦系統 資訊安全 評估	資訊安全 整體執行 情形評估	SWIFT 客戶安全 計畫評估	電子支付 機構查核	資訊系統 滲透測試	紅隊演練	DDOS 攻防演練
--------------	--------------------	----------------------	-----------------------	--------------	--------------	------	--------------



參考國際最佳實務，定期審閱資訊及資安相關政策及作業管理規範，並依風險趨勢及最佳實務增修相關管理要求。

教育訓練及宣導

36,000 小時宣導課程 1,300 小時專業訓練 41,000 人次參與資安週 18 份資安宣導品 5 場資安事故演練

所有員工均須完成年度個資與資安認知教育訓練，課程內容包含：社交工程、上網安全、辦公環境安全等議題。針對資訊安全專責單位人員提供專業課程訓練或職能訓練，訓練主題包含：雲端安全、安全開發、數位鑑識等。宣導成效：辦理 2 次資安情境模擬挑戰，透過模擬真實情境的互動式問答，強化製作 28 篇資訊安全宣導函，持續傳達資訊安全重要規定與事項。業務單位及資訊管理等單位於年度內辦理資安事故演練，以促使同仁熟悉事故應變流程。

社交工程演練

144,000
餘封社交工程演練信件

每月均參考當下時事設計釣魚郵件主題，對海內外全體同仁進行無預警演練，並於演練後公告演練成績。另辦理 3 次針對釣魚郵件，透過展示真實攻擊樣貌及風險，強化辨識可疑郵件能力。

資安人力配置

29 人資安一道作業
28 人資安二道作業

除在資訊安全專責單位配置 28 名資安專業人力，綜理全球二道防線作業外；另配置 29 人辦理安控系統、帳號管理及資安設備維護等一道防線作業。

推動工作

53 項資安 KPI 指標

透過企業資安委員會轄下資安工作小組分別針對弱點管理、資安防護和監控應變等面向完成分析作業，並依據分析結果建立檢核機制及 KPI 指標，以達到持續監控及改善目的。

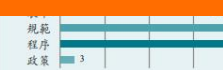
110年年報

認證

通過 ISO 27001:2013 資訊安全管理系統 認證	通過 BS 10012:2017 個人資料管理系統 認證	通過 PCI DSS 支付卡產業 資料安全標準認證
-------------------------------------	------------------------------------	---------------------------------

第三方評估

個資保護 破信查核	電腦系統 資訊安全 評估	資訊安全 整體執行 情形評估	SWIFT 客戶安全 計畫評估	電子支付 機構查核	資訊系統 滲透測試	紅隊演練	DDOS 攻防演練
--------------	--------------------	----------------------	-----------------------	--------------	--------------	------	--------------



參考國際最佳實務，定期審閱資訊及資安相關政策及作業管理規範，並依風險趨勢及最佳實務增修相關管理要求。

社交工程演練

12 個月
每月 12,000 餘演練對象

每月均參考當下時事設計釣魚郵件主題，對海內外全體同仁進行無預警演練，並於演練後公告演練成績。另辦理 4 次針對釣魚郵件，透過展示真實攻擊樣貌及風險，強化辨識可疑郵件能力。

資安人力配置

29 人資安一道作業
27 人資安二道作業

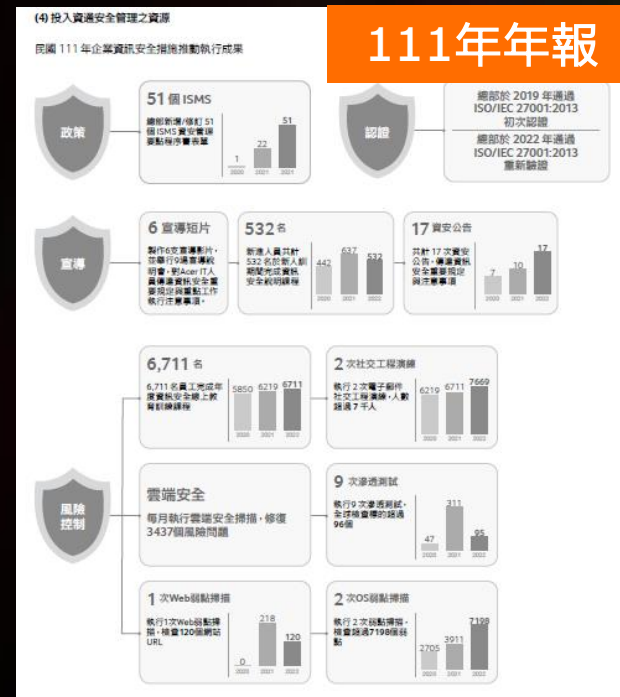
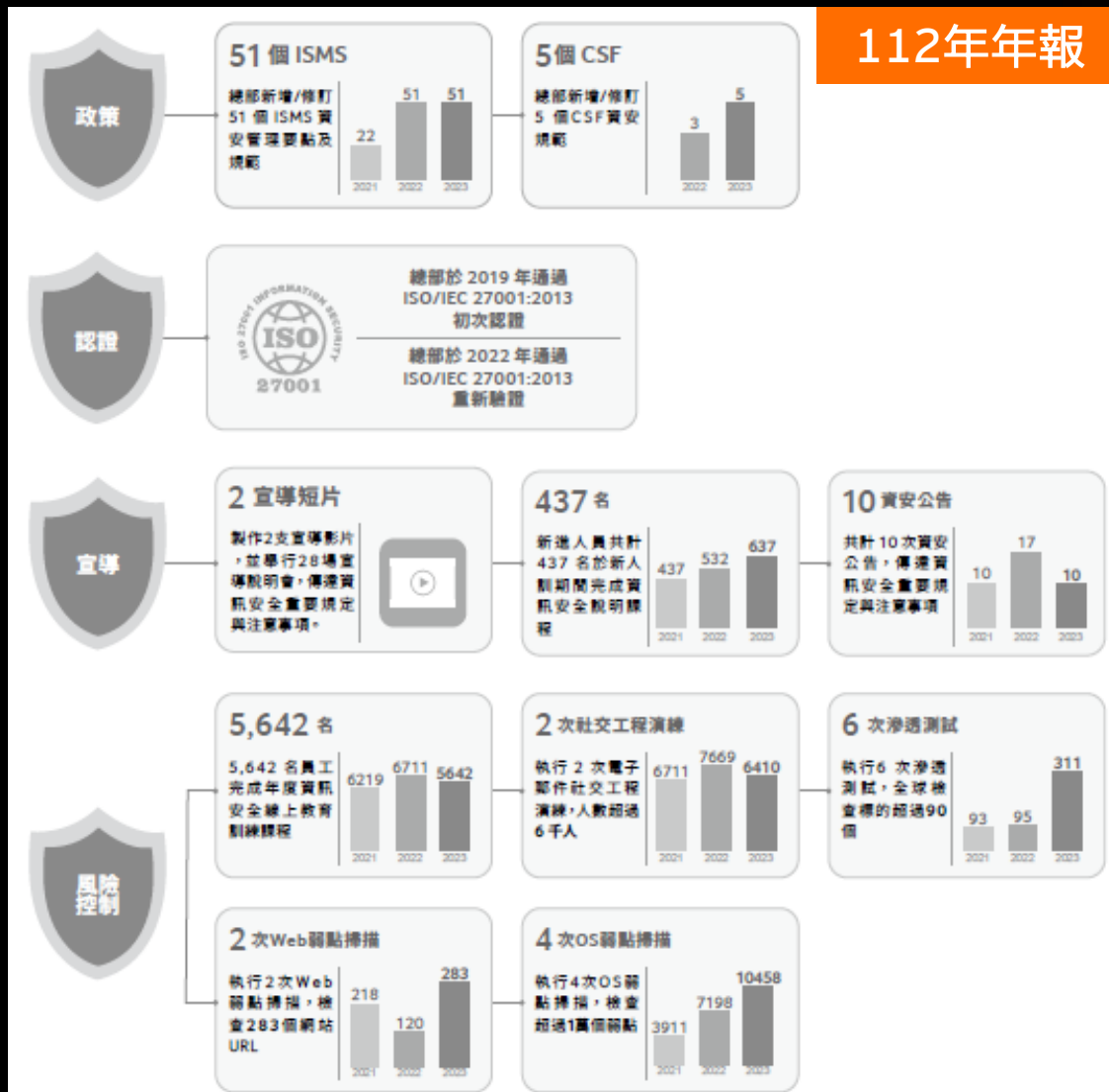
除在資訊安全專責單位配置 27 名資安專業人力外，另配置 29 人辦理安控系統、帳號管理及資安設備維護等一道防線作業。

推動工作

30 餘項資安 KPI 指標

透過企業資安委員會轄下資安工作小組分別針對弱點管理、資安防護和監控應變等面向完成分析作業，並依據分析結果建立檢核機制及 KPI 指標，以達到持續監控及改善目的。

年報揭露資安管理作為範例- 宏碁



■ 圖像及視覺化呈現投入資安資源，容易識別與分析其效果。

年報揭露資安管理作為範例- 長榮航空

4.投入資通安全管理之資源

112年年報

資訊安全模擬演練

社交工程演練
進行超過 41,000 人次之社交工程郵件演練。

資安演練
個資外洩演練、資安事件演練、營運持續演練共 33 次。

稽核作業

內外部稽核
ISO 27001 外部稽核及資訊安全內部稽核之驗證範圍人數總計 658 人。

主管機關及利害人查核
總計 5 個機關進行 7 次資訊安全查核。

訓練/宣導

全體員工
全體員工實施資訊安全線上訓練課程、新進人員、晉升基層主管及外派人員資安課程共超過 12,200 人次。

資訊人員
272 人接受共 544 小時以上資訊安全專業相關課程。

供應商
供應商接受資訊安全相關課程共超過 2,800 人次、1,600 小時。

資安宣導
於資訊安全暨個資保護委員會開辦資安講座，另針對中層及基層主管辦理資訊安全暨個資保護講座，總計受訓超過 200 人次。

資訊技術投入

執行超過 19 個資訊安全相關專案，投入金額超過新台幣 6,000 萬元。

資訊安全指標量化評估

量測包含核心系統可用性管理、一般系統可用性管理、權限控管、防止駭客攻擊、資訊安全事件管理、資訊安全持續改善、人力資源安全及供應商安全等八個管理目的，共 16 項指標，達成率為 100% 以上。

資訊安全風險評鑑

執行超過 12 項內外部資安議題風險評估及管理作業。

資訊安全通報管理

接獲超過 127 件疑似資訊安全通報，進一步問題釐清處理超過 24 件。

資安管理制度文件及法令法規遵循

檢視資安政策及 54 件管理制度文件；針對 4 項新增法令規範進行後續合規作業。

4.投入資通安全管理之資源

111年年報

資訊安全模擬演練

社交工程演練
進行超過 35,000 人次之社交工程郵件演練。

資安演練
個資外洩演練、資安事件演練、核心業務系統營運持續演練共 23 次。

內外部稽核
ISO 27001 外部稽核及資訊安全內部稽核之驗證範圍超過 1,316 人次。

主管機關查核
針對 6 個受查單位進行資訊安全查核，查核內容超過 20 項。

訓練/宣導

全體員工
全體員工實施資訊安全線上訓練課程、晉升基層主管資安課程及外派人員資安課程共超過 10,088 人次。

資訊人員
250 人接受共 500 小時以上資訊安全專業相關課程。

資安宣導
於資訊安全暨個資保護委員會開辦資安講座及分專資安案例，國內外部門進行年度資安研討會共超過 50 場次。

資訊技術投入

執行超過 22 個資訊安全相關專案，投入金額超過新台幣 6,600 萬元。

資訊安全指標量化評估

量測包含核心系統可用性管理、一般系統可用性管理、權限控管、防止駭客攻擊、資訊安全事件管理、資訊安全持續改善、人力資源安全及供應商安全等八個管理目的，共 16 項指標，平均達成率達 90% 以上。

資訊安全風險評鑑

執行超過 19 項內外部資安議題風險評估及管理作業。

資訊安全通報管理

接獲超過 103 件疑似資訊安全通報，進一步問題釐清處理超過 18 件。

資安管理制度文件及法令法規遵循

檢視 54 件資安政策及管理制度文件；針對 4 項新增法令規範進行後續合規作業。

4.投入資通安全管理之資源

110年年報

資訊安全模擬演練

社交工程演練
進行超過 40,000 人次之社交工程郵件演練。

資安演練
個資外洩演練、資安事件演練、核心業務系統營運持續演練共 14 次。

內外部稽核
ISO 27001 外部稽核及資訊安全內部稽核之驗證範圍超過 1,000 人次。

主管機關查核
針對 4 個受查單位進行資訊安全查核，查核內容超過 29 項。

訓練/宣導

全體員工
全體員工實施資訊安全線上訓練課程、晉升基層主管資安課程及外派人員資安課程共超過 11,000 人次。

資訊人員
24 人接受共 300 小時以上資訊安全專業相關課程。

資安宣導
國內外部門進行年度資安研討會共超過 50 場次，發布超過 30 則資安新聞及資安案例或新知。

資訊技術投入

人力/金額
執行超過 10 個資訊安全相關專案，投入超過新台幣 4 千五百萬元及 2,300 人日之人力。

資訊安全指標量化評估

量測包含核心系統可用性管理、一般系統可用性管理、權限控管、防止駭客攻擊、資訊安全事件管理、資訊安全持續改善及人力資源安全等七個管理目的，共 18 項指標，平均達成率超過 99%。

資訊安全風險評鑑

執行超過 15 項內外部資安議題風險評估及管理作業。

資訊安全通報管理

接獲超過 94 件疑似資訊安全通報，進一步問題釐清處理超過 71 件。

資安管理制度文件及法令法規遵循

檢視 41 份資安政策及管理制度文件；針對 4 項新增法令規範進行後續合規作業。

■ 表格化呈現投入資安資源，容易識別與分析其效果。

年報揭露資安管理作為範例- 科技改變（包括資通安全風險）及產業變化對公司財務業務之影響及因應措施

開發金

兆豐金

合庫金

第一金

英業達

中華電信

[illegible][illegible][illegible][illegible]

1. 中国作为发展中国家和社会主义国家,在对外开放的过程中,必须始终坚持独立自主、自力更生的原则,同时又要积极引进国外先进技术和管理经验,以促进国内经济的发展。在引进外资和技术的过程中,必须坚持平等互利、双向交流的原则,既要引进资金,又要引进技术,既要引进人才,又要引进设备。在引进外资和技术的过程中,必须坚持国家主权原则,既要维护国家主权,又要尊重外国投资者的合法权益。在引进外资和技术的过程中,必须坚持经济效益原则,既要提高经济效益,又要兼顾社会效益。在引进外资和技术的过程中,必须坚持可持续发展原则,既要发展经济,又要保护环境,既要提高人民生活水平,又要促进社会进步。

[illegible][illegible][illegible]

                   	                   	                   	                   	                   	                   	                  
--	--	--	--	--	--	---

[illegible]

- 確實分析產業及科技變化對公司資通安全的影響及提出因應之道

上市櫃公司因發生資安事件需發佈重訊的相關規定

母公司需替發生資安事件子公司發佈公告	發生資安事件需揭露	規範資安事件重大性標準	更新資安事件重大性標準	更新資安事件重大性標準
上市櫃公司之未上市櫃或未登錄興櫃之重要子公司，遇有第4條第1項各款情事者，視同上市櫃公司重大訊息，上市櫃公司應代為申報	明訂發生資通安全重大情事需揭露於重大訊息。損失達金額三億元或股本的20%，應召開重大訊息記者會說明	公司之 核心資通系統 、 官方網站 或 機密文件檔案 資料等，遭駭客攻擊或入侵，致無法營運或正常提供服務，或有 個資外洩 之情事	公司之 核心 資通系統、官方網站等，遭駭客攻擊或入侵，致無法營運或正常提供服務，或有 個資 、 內部機密 文件檔案資料外洩之虞等情事	公司之 重要 資通系統、官方網站等，遭駭客攻擊或入侵，致無法營運或正常提供服務，或有 致個資 、 大量 內部文件檔案資料有外洩之虞等情事

100年/5月 103年/6月 105年/8月

110年/4月

112年/8月

113年/1月

5月

114年/1月

違反重訊規定罰則

可處違約金3萬至500萬元

重訊發佈時間

事實發生日起**次一交易**日交易時間開始**兩小時**前

重訊內容不得偏頗

重訊內容與對外說明之內容應一致

近年遭受駭客攻擊或勒索病毒資安案件發佈重訊的上市櫃公司已超過百家

120+ 家

109年

110年

111年

112年

113年

114年

盟立 力成 中油 金積	及嘉 日勝生 東元 聯泰	台達電 健鼎 台豐虎航 新油	廣宏 永發 華航 國泰 中華航 中石化 雄獅 國泰航空	京鼎 恩德 柏文 富野 鴻昌 GOGOLOOK 藍天 環球晶	華銀 廣豐 廣隆 松上 第一金 青雲 鴻發 台塑化 聯華 廣豐 廣發 KY 神隆 正新 世昌	美利達 豐利 KY 華新科 台船 力隆 三通工業 國巨 廣研 宏昌 廣發 新天德 神隆 廣研 廣發	群光 自強 世昌 KY 大眾控 欣泰科技 華航 遠東新 聯益 宏發(興發) 美發 廣發 廣發 華發 新龍 科達 青雲 華發 永通光 同益 同利 聯發 宏發 廣發光電 神隆 世昌風電 國隆	鴻華 廣發 廣發
--	---	---	---	--	---	--	---	--

觀察與分享

- 駭客無差別攻擊，不分產業類型與公司規模
- 事件型攻擊的比例有增加的趨勢
- 發生資安事件後，對股價並無直接影響！？
- 攻擊發生後，不影響企業的營運！？

資安事件重大訊息內容分析(1/2)

■ 112年發佈的21則重大訊息分析

營運影響	攻擊手法	應對措施模式	對外公告措辭
▶ 機敏資料外洩 ▶ IT 系統中斷 ▶ 製造/產線受影響	▶ 駭客網路攻擊伺服器與內部系統 ▶ 勒索軟體攻擊	▶ 立即斷網與切斷系統 ▶ 通報主管機關 ▶ 委外資安團隊協助	▶ 已採取資安應變措施 ▶ 事件對營運影響有限 ▶ 已通報主管機關，持續調查中

註：使用Chatgpt 4o協助分析

資安事件重大訊息內容分析(2/2)

- 113年發佈的56家/63則重大訊息分析

營運影響	攻擊手法	應對措施模式	對外公告措辭
▶ 短暫性系統停機 ▶ 生產調度受阻 ▶ 多表示「對公司營運、財務無重大影響」	▶ 駭客網路攻擊 ▶ 加密（勒索病毒）攻擊 ▶ 部分涉及釣魚郵件或社交工程	▶ 關閉系統 ▶ 啟用備援 ▶ 啟動事件調查流程 ▶ 報警並通報主管機關	▶ 後續仍將持續提升網路與資訊基礎架構之安全管控以確保資訊安全相關資安防護機制 ▶ 目前已足以因應此事件，後續將持續密切監控

註：使用Chatgpt 4o協助分析

年報應記載事項對重大資通安全事件之要求

《公開發行公司年報應行記載事項準則》

■ 第十八條 營運概況應記載下列事項：

六、資通安全管理：

- (一) 敘明資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等。
- (二) 列明最近年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實。

別浪費一次危機 (Never let a good crisis go to waste)

掌握資安事件的
損失項目與計算

善用產創條例之
資安投資抵減

建立與強化資安
聯防體系

平時演練，累積
應變能力

降低駭客勒索的
損失



建立資安事件應變與調查程序，充分瞭解潛在損失項目

《上市公司重大訊息發布應注意事項參考問答集》

公司發生資通安全事件造成損害或影響之評估範圍，包括但不限於財務損失、商譽或智慧財產權之損害、顧客或供應商關係之影響、競爭優勢之喪失、修補漏洞及未來加強資安保護措施之成本，暨其未來可能伴隨之訴訟調查等。

事發當下

財務損失（勒贖贖金）

業務中斷損失（營收、客戶流失）

資訊系統還原與重置成本

資料還原與重置成本

員工生產力降低

事後復原

資安設施強化費用（升級、新增）

員工培訓

事件調查、法律諮詢與訴訟費用

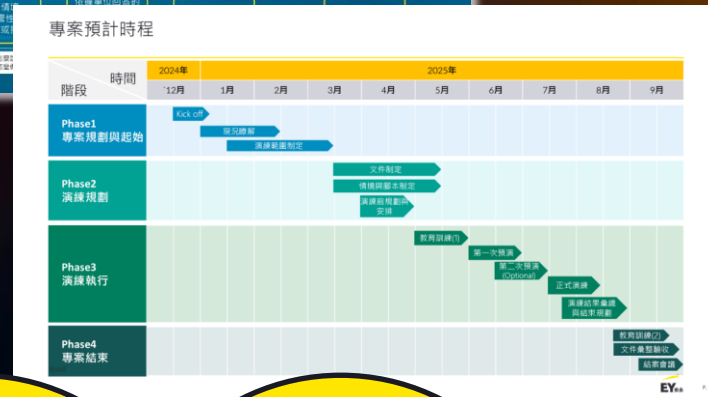
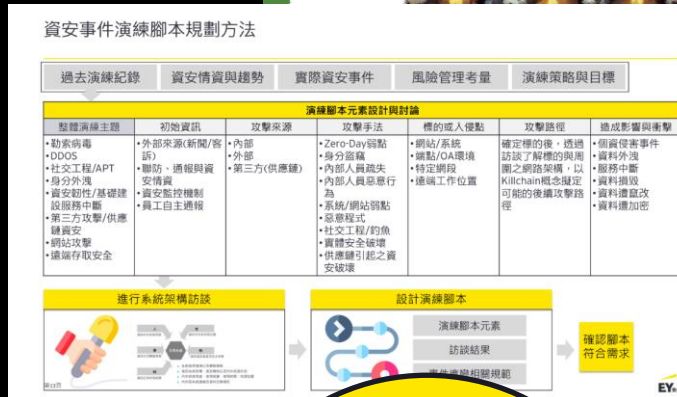
違約賠償

違規裁罰

商譽損失

理賠金額 / 保費調漲

透過資安演練，強化內部應變能力



與政府資安調查單位進行區域聯防與交流

王道銀行與臺北市調查處簽署國家資通安全聯防與情資分享合作備忘錄

提要

公私部門協力啟動資安聯防機制 強化數位金融資安防禦能力



王道銀行與臺北市調查處完成「國家資通安全聯防與情資分享合作備忘錄」簽署 攜手強化數位金融資安防禦能力。

法務部調查局與新光金融控股股份有限公司簽署 國家資通安全聯防與情資分享合作備忘錄

法務部調查局與新光金融控股股份有限公司簽署 國家資通安全聯防與情資分享合作備忘錄

發布日期 112-04-20 17:59:07 更新日期 112-04-20 18:03:11 公共事務室

法務部調查局與新光金融控股股份有限公司(下稱新光金控公司)於今(20)日假新光摩天大樓43樓簽署「國家資通安全聯防與情資分享合作備忘錄(MOU)」,簽署儀式由新光金融控股股份有限公司董事長許澎主持,調查局王俊力局長代表調查局與新光金控公司簽署合作備忘錄,資安長孫承一主任秘書、臺北市調查處吳富梅處長、資通安全處張尤仁處長、洗錢防制處藍家瑞處長及經濟犯罪防制處高聰明處長暨同仁共同觀禮,場面隆重。



法務部調查局與新光金融控股股份有限公司(下稱新光金控公司)於今(20)日假新光摩天大樓43樓簽署「國家資通安全聯防與情資分享合作備忘錄(MOU)」,簽署儀式由新光金融控股股份有限公司董事長許澎主持,調查局王俊力局長代表調查局與新光金控公司簽署合作備忘錄,資安長孫承一主任秘書、臺北市調查處吳富梅處長、資通安全處張尤仁處長、洗錢防制處藍家瑞處長及經濟犯罪防制處高聰明處長暨同仁共同觀禮,場面隆重。

法務部調查局與臺灣銀行簽署 國家資通安全聯防與情資分享合作備忘錄

法務部調查局與臺灣銀行簽署 國家資通安全聯防與情資分享合作備忘錄

發布日期 113-06-05 10:42:26 更新日期 113-06-05 10:42:36 公共事務室

法務部調查局與臺灣銀行股份有限公司(下稱:臺灣銀行)於113年6月4日假臺灣銀行公署「國家資通安全聯防與情資分享合作備忘錄(MOU)」,簽署儀式由臺灣銀行呂桔誠董事長主持,調查局陳白立局長代表調查局與臺灣銀行簽署合作備忘錄,資安長吳富梅副局長、臺北市調查處吳富梅處長、資通安全處張尤仁處長、經濟犯罪防制處何復生處長及洗錢防制處吳月萍處長共同觀禮,場面隆重。



法務部調查局與臺灣銀行股份有限公司(下稱:臺灣銀行)於113年6月4日假臺灣銀行公署「國家資通安全聯防與情資分享合作備忘錄(MOU)」,簽署儀式由臺灣銀行呂桔誠董事長主持,調查局陳白立局長代表調查局與臺灣銀行簽署合作備忘錄,資安長吳富梅副局長、臺北市調查處吳富梅處長、資通安全處張尤仁處長、經濟犯罪防制處何復生處長及洗錢防制處吳月萍處長共同觀禮,場面隆重。

兆豐金控創公股之先 與調查局簽署「國家資安聯防MOU」

2023-10-03 15:35 聯合報/記者朱漢強/台北即時報導



圖說:兆豐金控集團創公股之先,與調查局簽署「國家資安聯防MOU」,今與法務部調查局王俊力局長(右)代表簽署合作備忘錄。圖/兆豐金控提供

國泰金攜調查局建資安防護網

國家資通安全聯防與情資分享合作備忘錄



國泰金控與法務部調查局共同簽署「資安聯防與情資分享合作備忘錄」,藉由互相交流資安聯防情資與做法,共創公私協作的資安防護網。由法務部調查局王俊力局長(圖右)及國泰金控總經理李長庚(圖左)共同出席簽署儀式。國泰金控/提供

台新金攜調查局聯防資安

提要

簽訂數位金融合作備忘錄 將分享情資強化防禦 提高客戶資產保障



台新金控與調查局簽訂資安聯防合作備忘錄,成為國內首家金融機構簽署合作,台新金控董事長吳東亮(右四)親自出席表示支持,簽約儀式由法務部調查局局長王俊力(左四)與台新金控總經理林維俊(右二)代表簽署。其餘由左至右分別為調查局資通安全處處長余尚賢、臺北市調查處處長孫承一、主任秘書吳富梅、台新銀行總經理尚瑞強、台新金控資安長孫一仕。台新金/提供

法務部調查局與遠東銀行簽署資通安全聯防與情資分享合作備忘錄

張孝義
2023年4月6日

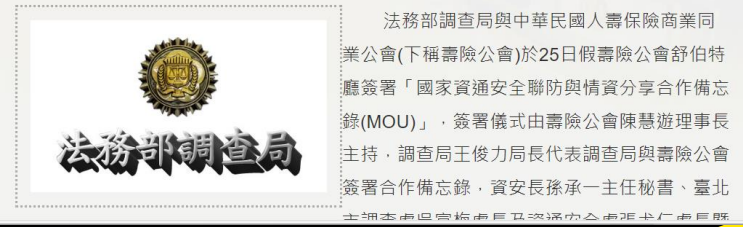


法務部調查局與中華民國人壽保險商業同業公會簽署 國家資通安全聯防與情資分享合作備忘錄

法務部調查局與中華民國人壽保險商業同業公會簽署 國家資通安全聯防與情資分享合作備忘錄

發布日期 112-08-26 08:37:20 更新日期 112-08-26 09:00:05 公共事務室

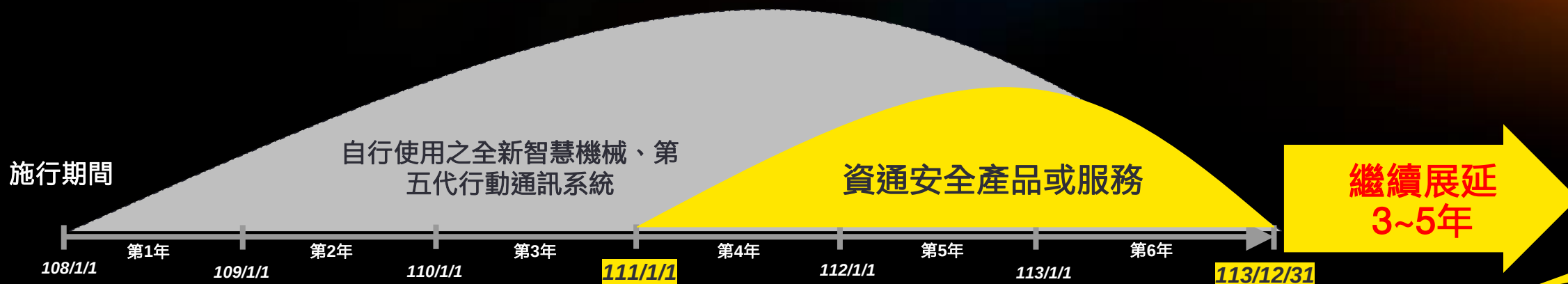
法務部調查局與中華民國人壽保險商業同業公會(下稱壽險公會)於25日假壽險公會舒伯特廳簽署「國家資通安全聯防與情資分享合作備忘錄(MOU)」,簽署儀式由壽險公會陳慧聰理事長主持,調查局王俊力局長代表調查局與壽險公會簽署合作備忘錄,資安長孫承一主任秘書、臺北市調查處吳富梅處長及資通安全處張尤仁處長暨各保險公司董事長、總經理等會員代表共同觀禮,場面隆重。



善用產創條例抵減，降低資通安全產品與服務投資費用

產業創新條例第10-1條

適用項目	如何申請	投資可抵減額度	投資抵減上限
購置(1)智慧機械、(2)第五代行動通訊系統以及(3)資通安全產品或服務相關全新硬體、軟體、技術或技術服務。	公司或有限合夥事業購置後提出投資計畫，經主管機關專案核准，每一個課稅年度以申請1次為限。 申請限制 最近三年內無違反環境保護、勞工或食品安全衛生相關法律且情節重大情事。	其核定支出總金額在同一課稅年度內<u>達新臺幣(以下同)100萬元以上，不逾10億元為限。</u> 抵減方案二擇一 方案1： 支出金額<u>5%限度內，抵減當年度應納營所稅額。</u> 方案2： 支出金額<u>3%限度內，3年內抵減各年度應納營所稅額。</u>	1. 不超過當年度應納營所稅額<u>30%</u>為限。 2. 合併適用投資抵減及其他抵減，當年度合計抵減不超過當年度應納營所稅額<u>50%</u>為限。 3. 依其他法律規定當年度為最後抵減年度且抵減金額不受限制者，不在此限。



資通安全產品或服務適用抵減範疇

- 資通安全產品或服務：
為防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，確保其機密性、完整性及可用性，運用於終端與行動裝置防護、網路安全維護或資料與雲端安全維護，並具有下列五大構面之一之硬體、軟體、技術或技術服務(參考美國國家標準暨技術研究院(NIST) 提出以下網路安全框架五大構面)：

辨識 (Identify)：

建立資安管理規則以管理人員、裝置、網路設備、雲端資產、數位資料之網路安全風險，並符合下列功能之一：

1. 資安治理及風險評估
2. 資產管理

保護 (Protect)：

建立和實施適當之資安措施以確保重要服務、設備、企業營運的運行，並符合下列功能之一：

1. 端點裝置防護
2. 網路安全防護
3. 資料加密與保護
4. 應用服務保護

偵測 (Detect)：

制定並實施適當的作為以識別資安事件的發生，並符合下列功能之一：

1. 端點網路偵測/回應
2. 使用者行為分析
3. 網路威脅情資運用

回應 (Respond)：

對偵測到之資通安全事件，規劃並實施適當的行動，包括但不限於資安事件之後的：

1. 數位證據保存
2. 數位鑑識
3. 數位資產監控追蹤

復原 (Recover)：

制定並實施適當的措施以修復因資安事件受損的功能和服務，並符合下列功能之一：

1. 異地備援
2. 資料備份

- ▶ 所稱技術，指專用資通安全產品或服務之專利權或專門技術；所稱技術服務，指提供與技術有關之規劃、設計、檢驗、測試、專案管理、系統整合或其他服務。
- ▶ 前項規定之資通安全產品或服務，屬安裝於個人電腦之防毒軟體或防火牆者，不適用之。
- ▶ 智慧機械或第五代行動通訊系統及資安產品或服務投資抵減申辦系統-常見問題-抵減申辦作業 (idbtax.org.tw)

面對駭客勒贖，該如何思考因應對策？

受害者選擇	支付贖金	部分支付贖金	不支付贖金	拖延與執法合作
駭客履行承諾(取得金鑰)	-損失金額大但恢復業務	-損失金額小，測試履約能力與誠意	-無經濟損失，解密成功	-解密成功，駭客失利
駭客不履行承諾	-損失金額大且無法恢復	-損失金額小，但依舊無法解密	-無經濟損失，但資料丟失	-爭取時間恢復或降低損失
駭客升級威脅 (再次攻擊或資料外洩)	- <u>資料公開且損失金額大</u>	-資料公開，但損失金額較小	- <u>無經濟損失，資料丟失且公開</u>	-爭取時間減少公開影響

資料來源：法務部調查局資通安全處

後續觀察重點

- 重大訊息公布時限內能理解多少的資安事件內容與估計損害？
- 對於發生資安事件的公司，在年報的揭露要求是否有更多指引？
- 商業電子郵件詐欺（BEC）是否列為重大資安事件？

別只「獨自升級」，我們一起升級！

2025年4月13日 / 星期日

資安署長 蔡福隆 強化台股資安 帶動升級

擴大內需市場 提供各行各業更多誘因 使用資安產品



（記者徐子苓／台北報導）從金管會主委轉戰資安署長，蔡福隆上任至今滿兩個月，喊出要壯大台灣資安產業。他近期積極拜會立委與產業公協會，並首次接受媒體專訪，向本報透露下一步規劃。蔡福隆表示，資安署未來會擴大內需市場，提供各行各業更多誘因來使用資安產品，其中一個措施是強化上市櫃的資安內控，藉此帶動資安業者升級技術，達到正向循環。

曾有資安業者建議，政府應整點國家須掌握的「關鍵技術」，確保戰爭或危機時，台灣能自給自足，不用仰賴國外。蔡福隆說，資安署會透過國際研調機構，了解資安產業的全球趨勢，藉此盤點哪些技術的國際提供者較少，且是台灣獨有的需求，例如身為製造業大國，IC（營運技術）資安、工控設備就有商機。

企業資料遭駭頻傳，數發部資安署長蔡福隆近期積極拜會立委與產業公協會，並首次接受媒體專訪，向本報透露下一步規劃。
（記者廖振輝攝）

資安署4招壯大台灣資安產業



- 01 上市櫃資安內控
- 02 供應鏈資安管理
- 03 資通產品安全
- 04 國產資安產品

- 擬加強資安防護應辦事項，擴大市場需求
- 攜手產業公協會，由龍頭公司帶動供應鏈中小企業
- 推出「國家級漏洞獵捕計畫」，號召白帽駭客測試資通產品是否有漏洞
- 鼓勵補助案部分採用本土產品
- 公務機關採購契約中，優先曝光本土產品

資料來源：採訪整理 製表：記者徐子苓

（記者徐子苓／台北報導）從金管會主委轉戰資安署長，蔡福隆上任至今滿兩個月，喊出要壯大台灣資安產業。他近期積極拜會立委與產業公協會，並首次接受媒體專訪，向本報透露下一步規劃。蔡福隆表示，資安署未來會擴大內需市場，提供各行各業更多誘因來使用資安產品，其中一個措施是強化上市櫃的資安內控，藉此帶動資安業者升級技術，達到正向循環。

曾有資安業者建議，政府應整點國家須掌握的「關鍵技術」，確保戰爭或危機時，台灣能自給自足，不用仰賴國外。蔡福隆說，資安署會透過國際研調機構，了解資安產業的全球趨勢，藉此盤點哪些技術的國際提供者較少，且是台灣獨有的需求，例如身為製造業大國，IC（營運技術）資安、工控設備就有商機。

企業資料遭駭頻傳，數發部資安署長蔡福隆近期積極拜會立委與產業公協會，並首次接受媒體專訪，向本報透露下一步規劃。
（記者廖振輝攝）

資安署4招壯大台灣資安產業



- 01 上市櫃資安內控
- 02 供應鏈資安管理
- 03 資通產品安全
- 04 國產資安產品

- 擬加強資安防護應辦事項，擴大市場需求
- 攜手產業公協會，由龍頭公司帶動供應鏈中小企業
- 推出「國家級漏洞獵捕計畫」，號召白帽駭客測試資通產品是否有漏洞
- 鼓勵補助案部分採用本土產品
- 公務機關採購契約中，優先曝光本土產品

資料來源：採訪整理 製表：記者徐子苓



A woman with blonde hair tied back, wearing a red lanyard and a patterned blouse, is speaking into a microphone. She is gesturing with her right hand. In the background, several people are seated, listening attentively. The setting appears to be a modern office or conference room with large windows and indoor plants.

報告完畢
謝謝聆聽

安永 | 建設更美好的商業世界

安永的宗旨是致力建設更美好的商業世界。我們以創造客戶、利害關係人及社會各界的永續性成長為目標，並協助全球各地資本市場和經濟體建立信任和信心。

以數據及科技為核心技術，安永全球的優質團隊涵蓋150多個國家的業務，透過審計服務建立客戶的信任，支持企業成長、轉型並達到營運目標。

透過專業領域的服務 - 審計、諮詢、法律、稅務和策略與交易諮詢，安永的專業團隊提出更具啟發性的問題，為當前最迫切的挑戰，提出質疑，並推出嶄新的解決方案。

安永是指 Ernst & Young Global Limited 的全球組織，加盟該全球組織的各成員機構都是獨立的法律實體，各成員機構可單獨簡稱為「安永」。Ernst & Young Global Limited 是註冊於英國的一家保證（責任）有限公司，不對外提供任何服務，不擁有其成員機構的任何股權或控制權，亦不作為任何成員機構的總部。請登錄ey.com/privacy，了解安永如何收集及使用個人資料，以及個人資料法律保護下個人所擁有權利的描述。安永成員機構不從事當地法律禁止的法律業務。如欲進一步了解安永，請瀏覽 ey.com。

安永台灣是指按中華民國法律登記成立的機構，包括：安永聯合會計師事務所、安永管理顧問股份有限公司、安永諮詢服務股份有限公司、安永企業管理諮詢服務股份有限公司、安永財務管理諮詢服務股份有限公司、安永圓方國際法律事務所及財團法人台北市安永文教基金會。如要進一步了解，請參考安永台灣網站 ey.com/zh_tw。

© 2024 安永諮詢服務股份有限公司。
版權所有。

APAC no. (請填上SCORE number)
ED MMY Y [填寫圖片版權到期日，若無到期日請寫上 ED None; 若無圖片請刪除]

本材料是為提供一般信息的用途編製，並非旨在成為可依賴的會計、稅務、法律或其他專業意見。請向您的顧問獲取具體意見。

ey.com/zh_tw

加入安永LINE@好友
掃描QR CODE，獲取最新資訊。

