CYBERSEC 2021
臺灣資安大會

ORGANIZED BY iThome

TRUST:redefined

信 任 重 構

MAY 4-6 臺北南港展覽二館

CYBERSEC 2021
臺灣資安大會
ORGANIZED BY iThome

TRUST: redefined

金融資安行動方案焦點座談

110年5月6日

MAY 4-6 臺北南港展覽二館

簡報大綱

壹、政策制度

貳、實體安全管理及網路安全管理

參、資安監控與人才培育

肆、事件管理與營運持續

伍、外部監督及回饋

陸、結論

壹、政策制度

政策制度

- 建立內部控制制度，持續辦理內部稽核作業及自行查核作業。
- 104年4月16日列為「資安責任等級A級機構」;108年6月26日屬金管會非資通安全法納管機關(構)之資通安全責任等級範疇。
- 資通安全法特定非公務A級機關相關規定註
  - -資通安全責任等級分級辦法
  - -資通安全事件通報及應變辦法
  - -特定非公務機關資通安全維護計畫實施情形稽核辦法
  - -資通安全情資分享辦法

註:「資通安全管理法」及相關子法於108年1月1日施行。

貳、實體及網路安全管理

	構面	項目內容
實體安全管理	終端機操作室	門禁管制、錄影監控、限制連線、無儲存及輸出設備之精簡型端末機(Thin Client) ，供授權、變更作業使用
	辦公區	精簡型端末機(Thin Client)連線營運環境作業
	環境	大樓24小時保全，各樓層設門禁、錄影監控、防火警報及消防系統
	人員	廠商人員、物品管控
網路安全管理	內部環境	實體隔離(營運區、OA測試區、管制區、終端機操作室)、電腦防毒系統(Anti Virus) 、 微軟更新服務系統(WSUS) 、設備管控系統：管制個人電腦之USB儲存及無線通訊傳輸裝置、電子郵件過濾、APT防禦系統及客製化放行系統、網站存取防禦系統(上網採取正面表列管制、阻擋可疑網站)
	外部環境	入侵防禦系統(IPS)、網站應用程式防火牆系統(WAF)、電子郵件防護系統(SPAM)、DDoS防護系統
	資安監控系統	資安監控中心(SOC)

叁、資安監控與人才培育

導入國際及國內資安管理制度

- 導入並驗證通過資訊安全國際標準(ISO 27001)、個人資料保護管理制度(TPIPAS)

強化資安監控

- 強化網路異常行為之監控機制。如日誌蒐集、加入F-ISAC。

加強資安人員培訓

- 每年派員參加國際資安研討會，擴大資安資訊來源，與國際接軌。
- 藉由外部攻防演練，強化第一線人員的防守能力。

肆、事件管理及營運持續

事件通報

- 法源依據:資通安全法之「資通安全事件通報及應變辦法」、金融監督管理委員會之「銀行業通報重大偶發事件之範圍與適用對象」。
- 訂定事件通報暨處理作業，依影響標的範圍及服務中斷時間，定義事件等級及通報對象。

營運持續

- 依據資訊中斷對營運衝擊分析結果建立備援措施(同地備援機制、異地備援機制)。

資安演練

- 訂定網路攻擊、個資外洩等資安事件應變演練作業並定期辦理。

伍、外部監督及回饋(1/2)

外部監督

金管會檢查局金融檢查

外部紅藍白實際攻防

-國內白帽駭客

-國際資安團隊

資訊安全遵循之相關法令與規章

-資通安全法

-個人資料保護法及施行細則

伍、外部監督及回饋(2/2)

第三方稽核驗證

資訊安全管理制度(ISO 27001)驗證

(1)範圍：全中心。

(2)頻率：每年1次續審；每3年重審。

(3)98年11月通過ISO 27001驗證，101年11月通過3年期滿重審，104年8月通過ISO 27001:2013轉版暨三年重審，109年7月通過續審。

個人資料保護管理制度(TPIPAS)驗證

(1)範圍：全中心。

(2)頻率：每年1次續審；每2年更新驗證。

(3)104年8月通過「台灣個人資料保護與管理制度（TPIPAS）」驗證。108年11月通過更新驗證。109年11月通過續審。

陸、結論

- 沒有100分，只有努力往前跑

- 遵守政策，董事會要導入專業董事及投入資源

- 設置資安長

- 掌握市場被攻擊的最新情況

- 和外部專業團隊，時時互動、交流

TRUST: redefined

Q&A

感謝您的聆聽