證券商
資安案例分享

臺灣證券交易所
券商輔導部

大綱

一、證券商資安風險

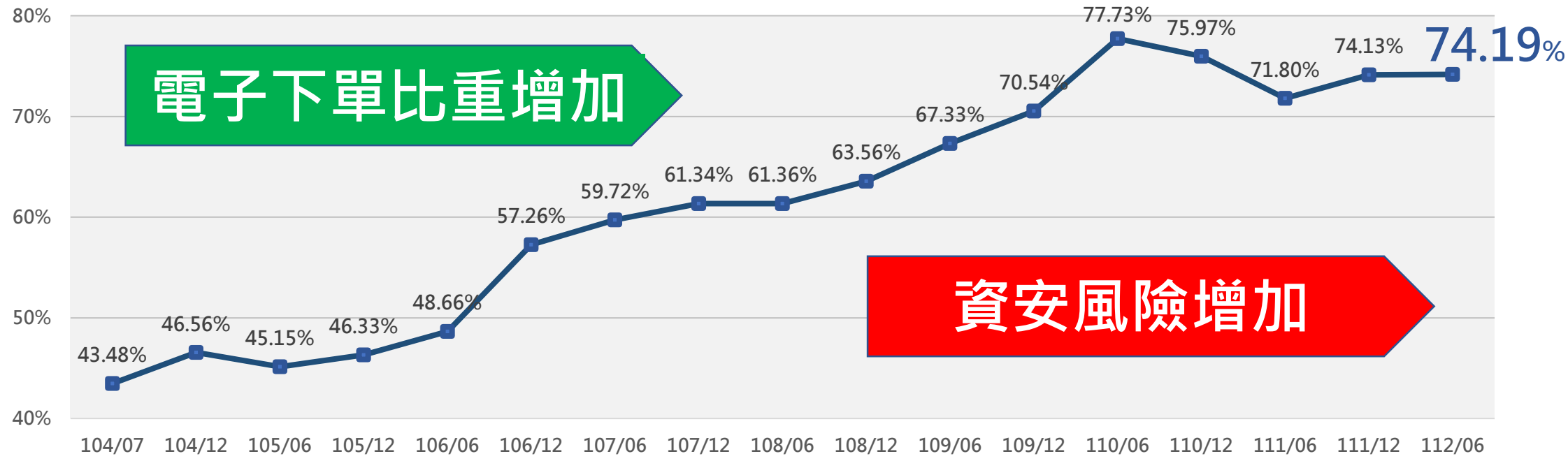
二、因應資安風險之監理措施

三、資安通報類別統計

四、案例分享

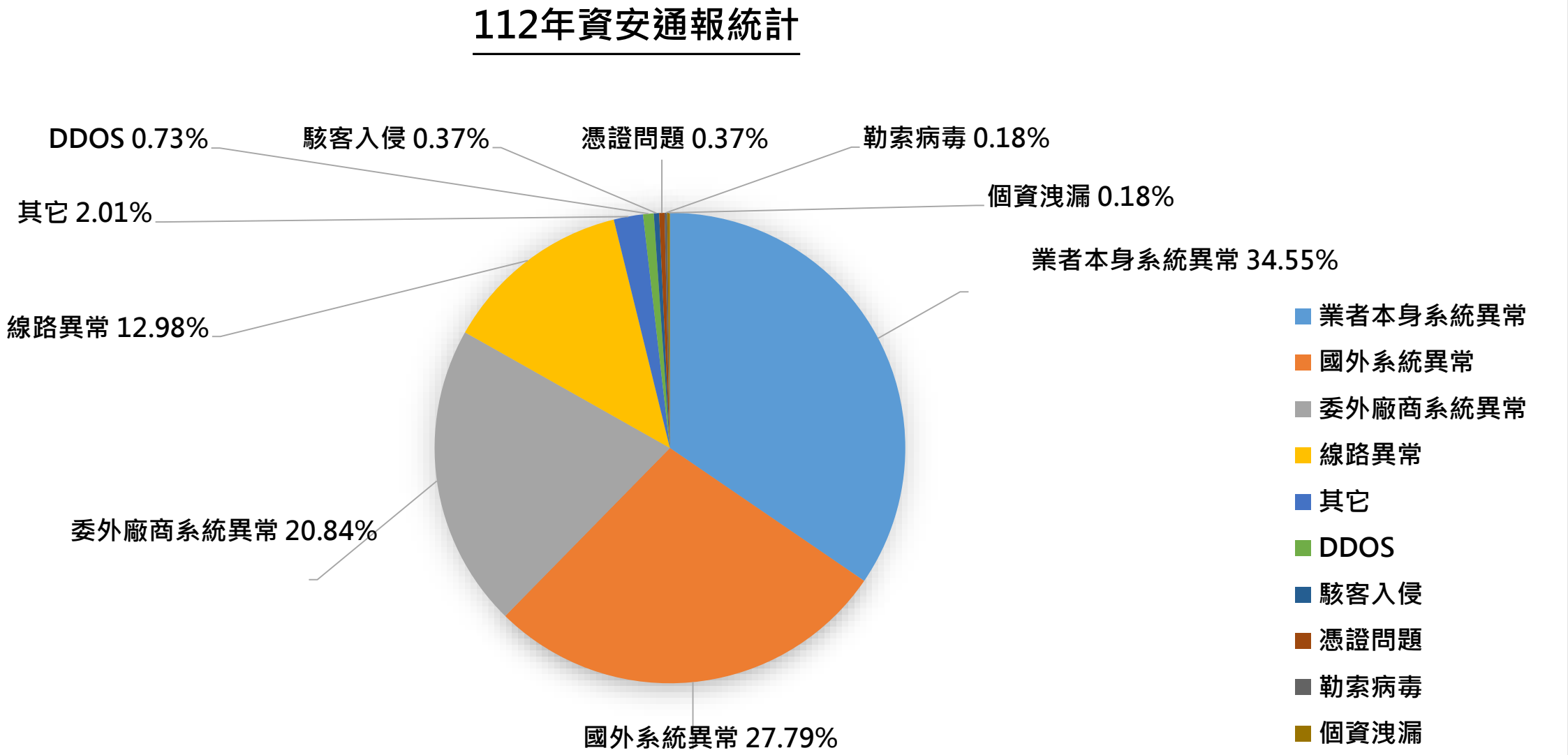
五、結語

證券商資安風險



107.2	109.10	110.11	111.8	112.7
DDos攻擊	主機共置	撞庫攻擊	網頁置換	當機事件

資安通報類別統計



資安案例1：委外廠商系統異常 (1日內發生2起同類)

1.APP電子下單主機異常，無法登入

- 經查下單主機相關設定均無異常，最後將主機中內建的「Windows Defender防火牆」關閉後，連線即恢復正常。

2. AP電子下單系統，連線異常

- 因中台主機作業系統更新後，內建的防毒軟體導致連線異常，後續將作業系統回復舊版，連線即恢復正常。

資安案例1：委外廠商系統異常 (1日內發生2起同類)

強化措施

- 關閉自動更新
- 更新後應作完整測試(重要系統可於測試或備援環境先進行更新)
- 定期備份(更新失敗時可以回復)

資安案例1：委外廠商系統異常 (1日內發生2起同類型)

廠商報價系統異常

- 外國期貨PATS報價異常。

資安案例1：委外廠商系統異常 (1日內發生2起同類型)

強化措施

- 報價系統備援措施
- 評估系統容量(capacity)

資安案例1：委外廠商系統異常

憑證系統驗章回應緩慢，造成電子交易平台無法登入

- 經查資料庫資源使用正常，係因憑證系統應用程式無法提供連線服務，將憑證系統主機重開機、重啟服務之後，連線即恢復正常。

資安案例1：委外廠商系統異常

強化措施

- 系統整體資源評估(前中後台與憑證系統)
- 落實營運持續計劃

資安案例2：委外廠商控管問題

廠商系統中毒，病毒轉傳至證券商

- 經查廠商系統中毒，經由線上維護將病毒傳送至證券商。
- 證券商採獨立網段並有監控，尚無造成損害。

資安案例2：委外廠商控管問題

強化措施

- 加強異常行為監控(如登入失敗)
- 落實網段區隔
- 禁止使用預設高權限帳號使用及簡易密碼

資安案例3：委外廠商控管問題

證券商未將測試與正式系統隔離

- 證券商對測試系統與正式系統未隔離，並提供廠商高權限帳號及遠端登入功能，廠商於盤中進行系統下單測試。
- 造成1.4億元鉅額錯帳，回補後證券商虧損113萬，並被課35萬元違約金。

資安案例3：委外廠商控管問題

強化措施

- 落實網段區隔
- 帳號控管應依職掌配置妥適權限
- 測試計劃應完整(目的、方法、紀錄、結果)

資安案例4：程式測試不完整(本身系統異常)

證券商上版程式測試不完整

- 下單程式上版後未詳細檢查正式上線結果。
- 出現測試資料、對帳單寄錯對象、程式有問題無法及時下架。

資安案例4：程式測試不完整(本身系統異常)

強化措施

- 程式應有完整測試計劃
- 個資處理應依規範辦理(非公務機關個人資料檔案安全維護辦法)

資安案例5：暗網販售證券商客戶資料

暗網販售證券商客戶資料

- 暗網販賣宣稱某幾家券商客戶資料。
- 資料來源不明、正確性待查。
- 通報、舉證無個資外洩(第三方驗證)、向客戶加強宣導、報案。

資安案例5：暗網販售證券商客戶資料

強化措施

- 落實網段區隔
- 客戶資料系統應避免透過網際網路進存取
- 個資使用存取應有軌跡，並防範異常存取

資安案例6：證券商下單程式遭冒用

網路商店出現非證券商上架之APP

- 進行網路搜尋，找出異常APP。
- 報案、網站警示公告、找第三方鑑識及查核單位協助處理。

資安案例6：證券商下單程式遭冒用

強化措施

- 防範詐騙釣魚並積極通知客戶
- 於官網揭露相關訊息並提供軟體服務下載點
- 向警察局報案及軟體平台提報下架偽冒程式

結語

公司價值，駭客攻擊

新興科技，攻擊翻新

資安防護，成本效益

結語

未來資安法規發展

- 委外作業
- 金融業運用人工智慧
- 雲端架構
- 零信任架構

簡報結束
敬請指導