保險業資安監理重點說明

保險局

109年12月4日

題綱

一、提升保險業對資訊安全之重視

二、督導產、壽險公會定期檢討自律規範

三、強化資安防護措施

四、提升電子商務交易安全之控管效能

五、近期保險業資安缺失裁罰態樣

六、未來推動重點

一、提升保險業對資訊安全之重視

(一)完備資安內控規範

修訂保險業內部控制及稽核制度實施辦法，包括：

- 建立資訊系統各項內部控制作業
- 將自律規範納入內控制度重要環節
- 設置資安專責單位及主管
- 要求高階管理人員出具聯合聲明
- 從業人員教育訓練

一、提升保險業對資訊安全之重視

(二)資安風險因子鼓勵誘因

於「人身保險及財產保險安定基金計提標準」增列「資訊安全管理指標」之評等

保險業資本計提因資訊安全缺失違反相關規定時，得採取加重計提作業風險資本

一、提升保險業對資訊安全之重視

(三) 配合「金融資安行動方案」執行措施

- 推動一定規模保險業增設資安長，統籌資安政策與協調資源
- 鼓勵遴聘具資安背景之董事、顧問或設置資安諮詢小組，透過第三方外部專業人員協助董事會決策過程
- 鼓勵導入國際資安管理標準及取得驗證，如：資安管理 ISO27001、個資管理ISO27701
- 鼓勵導入國際營運持續管理標準及取得驗證，如：導入ISO22301；鼓勵一定規模保險業於異地備援演練時，納入實際業務運作驗證
- 適時參考F-ISAC資安防護建議，並配合於110年度辦理資安治理成熟度評估
- 鼓勵保險業建置資安監控機制(SOC)

一、提升保險業對資訊安全之重視

(四) 培育保險資安人才

主管機關

- 加強資安監理人才培育
- 提升中高階主管資安知能

保險業者

- 請保發中心開辦董監事資安教育訓練課程
- 請保發中心開設資安人員專業課程
- 鼓勵資安人員取得國際資安證照

二、督導產、壽險公會定期檢討自律規範

(一)最新版本經本會於109年5月26日同意備查，規範重點包括：

- 參考F-ISAC資安情資及防護建議，以防範駭客及社交工程攻擊
- 因應防疫期間異地辦公之資料傳輸加密機制、機敏資料防護、視訊設備安控、異常行為監控等遠端作業安全措施
- 依電腦系統重要性進行資安評估
- 明定核心資訊系統範圍及訂定開發置換作業程序
- 依行動應用程式重要性進行檢測作業
- 網路投保密碼之設計安全原則、物聯網設備管理規範

二、督導產、壽險公會定期檢討自律規範

(二)未來檢討方向

網路安全防護及資訊系統安全防護基準內容

行動應用程式、雲端服務、物聯網、網路身分驗證新興科技安控

核心資訊系統供應商及跨機構資訊服務風險評估及查核管理機制

訂定保險業資訊作業韌性參考規範

三、強化資安防護措施

- 請產壽險公會及保經代公會每半年彙整保險業資安風險評估表，以評估現行資安管理機制是否足以因應面臨之風險
- 每年均督導保險業參與本會及F-ISAC辦理金融業DDoS攻防演練，並請業者依演練結果檢討改善其資安防護措施
- 防堵釣魚網站假冒金融機構名義，不當蒐集個人資料或涉有詐騙之情形
- 依據「保險業通報重大偶發事件之範圍與適用對象」規定，如發生資通安全事件，其結果造成客戶權益受損或影響健全營運，需依規定向本局通報

三、強化資安防護措施

- 請保險公司及目前辦理網路投保業務之20家保經代公司加入F-ISAC，藉由F-ISAC分享資安警示及獲取防護建議
- 參考F-ISAC建議，並督導業者防疫期間啟動異地辦公或遠端工作管理、視訊會議設備等安控作業
- 針對近期駭客攻擊等資安議題，如：F-ISAC近期發布「駭客組織偽冒金融機構往來企業人員寄送電子郵件給金融機構要求轉帳至特定帳戶」之訊息，請保險業宣導防範社交工程手法，提醒人員確實遵循內部規範及標準作業流程

四、提升電子商務交易安全之控管效能

◎ 本會為因應數位化趨勢，訂定保險業辦理電子商務應注意事項，以確保交易安全，保障消費者權益。

建置網路投保平台

- 經由保險公司建置網站專區、網頁或行動應用程式(APP)。
- 保險業與異業合作辦理網路投保業務，相關投保平台應由保險業負責管理維護並揭露相關資訊。

強化資訊安全

- 保險業應取得資訊安全管理系統國際標準認證(ISO 27001)之認證、建立DDoS網路流量清洗機制。

身分驗證防護機制

- 消費者應提供足資驗證其身分之個人基本資料，辦理首次註冊及身分驗證作業，並由保險業發送一次性密碼(OTP)，以確認身分。
- 為確認要保人之網路投保意願，保險業依規定執行電話訪問。

保險商品上架限制

- 財產保險商品採負面表列；人身保險商品則考量商品屬性較複雜，因此採正面表列，以確保消費者權益。

遵循核保及通報規範

- 保險業依相關法令及內部核保、保全、理賠內部控制作業進行審核及通報，且於完成審核時通知保戶辦理結果。

五、近期保險業資安缺失裁罰態樣

資安管理面
委託外部資安廠商之網路監控服務，對於控管服務延宕情形
資料庫存取授權管理未落實最小授權原則
弱點掃描作業，未依時限完成弱點修補
弱點掃描結果未建立後續風險評估及處理情形之追蹤管理機制
原始碼檢測作業，未規範應對檢測級別風險評估及採取後續處理措施
伺服器之異地備援區無防火牆設備區隔控管
對外寄送電子郵件之資料外洩防護系統欠嚴謹

五、近期保險業資安缺失裁罰態樣

個資管理面
個資檔案及資料庫複製至開發測試主機作業，未去識別化
資料庫個資存取軌跡留存有欠完整
未訂定資安情資或警訊通報處理標準程序及作業規範
未就外部網路入侵及非法或異常使用行為所致個資外洩情境，定期演練及檢討改善

五、近期保險業資安缺失裁罰態樣

電子商務系統管理
網路投保之個資複製至個人電腦，無稽核軌跡及管控措施
電子商務系統之安全設計涉及個資，未妥適隱碼顯示
APP上架、安全性檢測、發布與更新等作業規範，有違分工牽制原則
未依內部規範，定期辦理APP程式原始碼檢測、發行用密碼變更、憑證備份與封存等作業
提供業務員使用之行動投保APP系統設計欠妥適

六、未來推動重點

目標：確保保險服務安全性、便利性及營運不中斷

配合本會109年8月6日發布之「金融資安行動方案」，以差異化管理精神，為期1至4年循序推動

推動方式：持續與各保險公會、保險周邊單位及保險業合作，提升保險業整體資安防護能力

簡報結束

感謝聆聽