資安保險說明

2024/03/07

簡報內容

- 資安風險及相關法規
- 資安保險商品說明
- 資安事件案例
- 資安保險核保審核標準

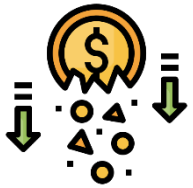
資安風險及相關法規

資安風險年年增加

台灣2023年上半年受網路攻擊次數在亞太地區佔比55%

資料來源：Check Point Research

全台每週有8.5%機構受勒索軟體攻擊



台灣每秒就有將近1.5萬次攻擊發生

政府法規規範

個人資料保護法§12, 27,29

個資外洩的法律責任義務

- §12通知義務，應通知當事人
- §27為防止個資外洩義務，應採行適當之安全措施
- §29違反個資安全應負損害賠償責任，被害人若不易或不能證明
  每人每一事件得求償NT$500 ~ NT$20,000；單一事件合計最高NT$2億

證交所、櫃買中心重大訊息處理程序修訂(2021/04)

- 上市櫃、興櫃公司發生重大資安事件時，需發布重大訊息對外揭露

金管會「公開發行公司建立內部控制制度處理準則」(2021/11/28)

- 明訂上市櫃公司需設置資安長以及資安專責單位，並採分級的方式給以不同資安編制要求
  - 2022年底前設置資安長及專責單位：資本額100 億元以上、台灣 50 指數成分公司、電子銷售平台等。
  - 2023年底前設置資安專責主管及人員：最近3年稅前純益無連續虧損且最近1年度每股淨值未低於面額者。

資安保險商品說明

資安保險商品說明

法定責任

- 資料保護責任
- 資訊安全責任

費用損失

- 資安專家費用
- 通知費用
- 官方調查費用
- 復原費用
- 抗辯費用

資安保險商品說明(續)

法定責任

1. **資料保護責任**
   承保企業因違反資料保護，致第三人受有損害而依法應負之賠償責任。

2. **資訊安全責任**
   承保企業因違反資訊安全，致第三人受有損害而依法應負之賠償責任。

資安保險商品說明(續)

名詞定義:

◆「違反資料保護」：

係指企業對於第三人個人資料之蒐集、處理及利用時，**違反中華民國個人資料保護法或我國及其他國家規範內容相似之法令**。

◆「違反資訊安全」：

係指企業所有或承租之電腦系統遭受未經授權之入侵、使用、修改、毀損、刪除、惡意程式碼感染或阻斷式服務攻擊。

資安保險商品說明(續)

費用損失

1. 資安專家費用

因聘請資安專業人員確認電腦系統之安全狀態、判斷發生之原因所產生之費用。

2. 通知費用

依法令規定應向資料所有人發出通知所致之費用。

3. 官方調查費用

因遭受主管機關調查所需之法律諮詢費用及為回應主管機關所支出之費用。

資安保險商品說明(續)

費用損失

4. 復原費用

為回復、重新蒐集或重置遭受破壞、毀損、修改或刪除的電子資料或軟體，使其回復原狀所產生之費用，但不包括為提升或改善資料保護或資訊安全而產生之費用。

5.抗辯費用

因違反資料保護、違反資訊安全責任進行抗辯所發生之費用。

資安保險商品說明(續)

重要除外不保事項

- 機械故障、電力故障(電力中斷、停電、電壓下降或突波)、通訊系統(包括網路服務)或衛星系統故障、錯誤、干擾或中斷所致者。
- 因交易損失、交易責任或帳戶價值變動；被保險人照護、保管或控制中的任何金錢(包括虛擬貨幣)、有價證券或其他有形資產遺失、移轉或遭竊所致者。
- 營業秘密、著作權、專利、商標或其他智慧財產權之盜用、抄襲或侵害

其餘不保事項，詳如保單不保事項。

資安事件案例

美國最大燃油管道系統Colonial Pipeline遭到駭客勒索攻擊，支付近500萬美元贖金

資料來源：yahoo!新聞 張子清 | 2021-05-13

美國東部最大的燃油管線「殖民管線」(Colonial Pipeline)公司5月7日遭到駭客勒索攻擊，被迫關閉數日，直到12日開始陸續恢復運作，但仍要再經過幾天調整才能恢復正常供油。**這起事件凸顯美國基礎設施體系的漏洞，也就是主要由私營企業營運的燃油管線不需強制執行安全網絡防護，給予惡質的駭客團體可趁之機**。

資料來源：iThome 林妍溱 | 2022-05-10

Colonial Pipeline 於2021年5月遭到勒索軟體攻擊，波及所有管道作業，由於Colonial Pipeline**負責美國東岸多達45%的燃料供應，公路運輸大亂，**讓美國政府一度宣布緊急狀態。駭客加密了該公司系統檔案，竊走近100GB的資料要脅，該公司據傳為此支付了500萬美元的贖金。

可能啟動的承保範圍:

資安專家調查費用、官方調查費用、復原費用

印度國營瓦斯公司遭爆資安漏洞，近七百萬用戶個資可用Google搜尋取得

資料來源：TWCERT/CC | 2019-02-19,
iThome 陳曉莉 | 2019-02-20

Indane為印度國營石油暨天然氣公司IndianOil旗下的瓦斯（LPG）品牌，也是全球第二大的瓦斯供應商，在印度有超過9,000萬個家庭是Indane的客戶。

又是缺乏身分認證機制惹的禍！法國資安研究人員披露，印度國營的瓦斯服務Indane所設立的網站因完全不設防，而讓任何人得以存取用戶的個人資料，包括數位身分證號碼，估計影響逾670萬名的印度民眾。

可能啟動的承保範圍:

資安專家調查費用、官方調查費用、通知費用、資料保護責任、抗辯費用

微風百貨90萬會員個資遭駭 經濟部喊查：未改善將開罰

資料來源：TVBS新聞網 呂欣芷 | 2023-02-25

國內知名百貨微風集團驚傳90萬筆客戶個資疑遭駭客竊取，對此，經濟部表示，23日已派員前往了解，並於昨(24)日成立調查小組，前往微風集團子公司微風數位時代股份有限公司調查，要求業者釐清事故原因及執行改善措施，並通知會員知悉，同時也要求業者落實《個人資料保護法》相關規定，如屆期未改正，將依法處以罰鍰。

……為儘速釐清個資外洩情形，由經濟部商業司、數位發展部國家資通安全研究院、資訊工業策進會及內政部警政署組成行政調查小組，共同前往微風數位時代股份有限公司進行行政調查。

微風集團表示…內部資安團隊已完成軟體及作業系統安全性更新，同時提高資安防護層，並以簡訊通知會員修改密碼，目前已委請資安公司調查事故原因中。

可能啟動的承保範圍:

資安專家調查費用、官方調查費用、通知費用、資料保護責任、抗辯費用

個資外洩客戶遭騙判決出爐，在個資法賠償外，業者並需負起7成過失責任

資料來源： IThome | 2019-10-07

在2017年，有民眾提告某電商個資外洩，致使受害者遭騙25萬元，二審判決在2019年9月出爐，指出業者也應付起7成部分責任，最終裁定賠償18萬3,274元。這起判例，也將影響未來個資外洩事件的判決。

(略)

在詐欺侵權行為損害的賠償方面，對於張女遭詐騙的25萬，在這次判決結果也有相關說明，判決內容指出，個資外洩與後續遭詐騙而造成的損害，有相當因果關係，如果沒有這些明確資料，民眾應不致於陷於錯誤而遭詐騙，另外，XX公司雖抗辯盡到適當的安全防護與個資保護之責，但法院認定其網路平臺之內部及外部風險控制存有諸多缺陷，並且未能完全落實其個人資料保護的管理。

(略)

可能啟動的承保範圍:

資料保護責任、抗辯費用

資安保險_核保審核標準

資安保險 – 費率因子

包含但不限於:

✓年營業額

✓個資筆數

✓行業類別

✓資安管理及防護措施

✓過去五年是否有發生資安事件

(以上供參，實際狀況依各家保險公司審核辦理)

瓦斯及燃氣供應業核保審核 – 最低資安標準

包含但不限於:

✓安裝防毒軟體、防火牆及惡意程式阻擋軟體

✓有長而複雜的密碼

✓關鍵系統有即時更新

✓遠端存取需有多因子認證

✓員工及管理員使用者須有資安訓練

✓個資須加密

✓資料須備份

✓儘速安裝關鍵補丁與系統更新

(以上供參，實際狀況依各家保險公司審核辦理)

電力及燃氣供應業核保審核 – 進階資安措施

包含但不限於:

- ✓專責資安負責單位
- ✓國際資安認證，如ISO27001
- ✓需有反阻斷式服務攻擊解決方案
- ✓需有特權帳號管理，例如PIM、PAM解決方案
- ✓需有涵蓋所有關鍵系統之SOC/資安事件管理平台
- ✓每年需有第三方資安廠商執行滲透測試
- ✓敏感資料於傳輸及留存時需點對點加密

(以上供參，實際狀況依各家保險公司審核辦理)

資安保險參考保險條件

單位: NTD

	項目	保險金額	保險金額
法定責任	資料保護責任	200萬	500萬
	資料安全保障責任		
損失費用	資安專家費用	20萬	50萬
	官方調查費用		
	通知費用		
	復原費用		
	抗辯費用		
年營業額1000萬以下		保費 1萬 ~ 2萬	保費 2萬~3.5萬
年營業額1000萬~3000萬		保費 1.5萬~2.5萬	保費 2.5萬~4.5萬
年營業額3000萬~5000萬		保費 2萬 ~ 3萬	保費 3.5萬 ~ 5萬

說明: 以上僅供參考，實際保險條件及保費依各家保險公司審核為準。

如有保險需求，請逕行洽詢各家保險公司

謝謝聆聽，敬請指教