數位經濟×資料保險

發展趨勢

科技會報兼任研究員
王仁甫

2018年3月13日

大 綱

- 數位經濟創新所造成的資安風險
- 網路資料保險之需求與發展
- 全球網路資料保險概況
- 我國資料保險制度未來發展之建議

數位經濟與資安課題

未來拓展至智慧城市、智慧聯網
巨量資料
連結資安網路保險
前瞻科技
資安課題
雲端服務
智慧聯網
行動裝置
人工智慧
沒有資料哪有AI

巨量資料資安課題之四大面向

巨量資料資安課題可彙整成四大面向加以探討:

- **基礎設施安全性**
  - 分散式程序設計框架之安全計算
  - 非關聯式資料儲存的安全最佳方案
- **資料的保密**
  - 可擴充性和可合成性隱私權保護資料探勘與分析技術
  - 密碼學強化的資料中心安全技術
  - 漸進式的存取控制
- **資料管理**
  - 安全的資料儲存與交易記錄檔
  - 漸進式的審核
  - 資料來源
- **資料完整性和被動的安全**
  - 端點輸入驗證和過濾
  - 即時的安全監控

大 綱

- 科技創新所造成的資安風險
- 網路資料保險之需求與發展
- 全球網路資料保險概況
- 我國資料保險制度未來發展之建議

網路資料保險推動緣起(1/2)

- **網路安全保險定義**：美國國家國土安全部將網路安全保險定義為，為減緩各種資安事件的發生所帶來的損失所設計的保險。
- **網路攻擊晉升全球最擔心議題**：根據WEF「2016年全球風險報告」指出，數據造假與偷竊風險是全球風險發生機率的第八名。
- **智慧連網(IOT)發展後，資料保險之重要性**：根據KerbsonSecurity調查2016年10月，駭客使用Mirai病毒控制了美國大量的IP攝影機和相關的DVR攝影機等超過百萬台物聯網設備，以DDoS攻擊Twitter、Paypal、Spotify等，也導致這些網站被迫中斷服務，超過半數人無法上網。
- **2017年勒索軟體橫行，資料保險需求將逐漸增加**

資料來源：美國國家國土安全部、 KerbsonSecurity、Aite Group及本研究彙整

網路資料保險推動緣起(2/2)

- 伴隨雲端服務應用、行動裝置、巨量資料、電子商務平台及智慧連網（IOT）的發展趨勢，資料外洩風險亦隨之增加；同時個資法規範及資安管理法即將上路，資料需要更強化的保護，恐將阻礙雲端、智慧連網（IOT）、電子商務產業發展；因此需加速推動網路保險市場，提出相關配套措施。

網路資料保險優點

- 分散資安風險
- 提供更深層的保護
- 降低資安事件發生後企業所遭受到的損失
- 減免法律程序相關費用負擔

CYBER保險推動之重要性

提出我國網路保險制度發展之建議與配套措施，加速網路保險市場發展

推動網路資料保險之重要性大幅提升

個資法上路資安管理法送立法院 ＋ IOT快速發展 ＋ 電子商務平台成立 ＋ 全球虛擬財產保險崛起

資安問題恐阻礙產業發展

2012年個資法上路，公務或非公務機關都得採取適當措施保護個資，以防止被竊取等問題發生。伴隨意識抬頭，企業對網路保險之需求勢必提升。

多數公司發展IOT科技應用，提升產品和服務競爭力，但也衍生出更多的資安保護相關議題，資料洩漏風險提高。

伴隨電子商務的蓬勃發展，鑑於網站成立門檻不高，資安防護能力薄弱等問題恐製造出多的資安問題。

中國網路保險市場發展趨勢快速，延伸出更廣泛的服務，例如將之運用於保護遊戲當中的裝備與虛擬幣等。

巨量資料與網路資料保險

對於巨量資料，除了需要安全框架以預防資安問題產生外，透過資料保險能夠獲得資安保護、偵測、資料洩漏極小化

大 綱

- 科技創新所造成的資安風險
- 網路資料保險之需求與發展
- 全球網路資料保險概況
- 我國資料保險制度未來發展之建議

網路保險歷史發展

美國產品發展

法令要求(隱私漏洞)+網路隱私權→促使保險市場發展

- 1996：網路安全保險初作為產品出現在美國保險市場
- 2003：加州開始有隱私漏洞相關的法規，盡而提升網路安全保險的需求
- 2000s：依據加州所訂定的相關法規，其餘47州也跟進，促使美國資安保險市場的成長
- 2006：網路隱私權之重要性日益漸增
- 2014：「網路安全」被寫進超過60個承保人合約內容，並產生約十億元的營收
- 2015：「網路安全法」與「網路安全資訊分享法」
- 2016：「國家資訊安全行動計畫」(6,261億台幣)(設立聯邦隱私權議會)(強化國家資安會議中說明資安保險推動重要性)
- 2017：「網路安全總統令」1.保護聯邦網路 2.保護CIIP 3.保護民眾網路

歐洲產品發展

法令要求(資料保護)→促使保險市場發展

- 1995：1.歐盟開始實施資料保護指令 2.將資料保護作為歐盟市民的權力
- Mid 200s：對IT依賴性與駭客事件的增加，使得網路保安全保險需求漸增
- 2012：歐盟修改資料保護法，其中增加對資料漏洞法規的罰鍰已集相關的資料保護要求
- 2013：歐盟發布網路安全指令，並要求企業最低安全量
- 2013/14：承保人開發國際相關保險，在倫敦已開發了25-30個市場
- 2014：歐盟金融機構網路支付安全綱領(2014EBA)
- 2015：支付服務新修正指令(2015、PSD2)
- 2016/4：通過資料保護規則規範資料跨境傳輸，需有充足保護水準(2018/5執行)

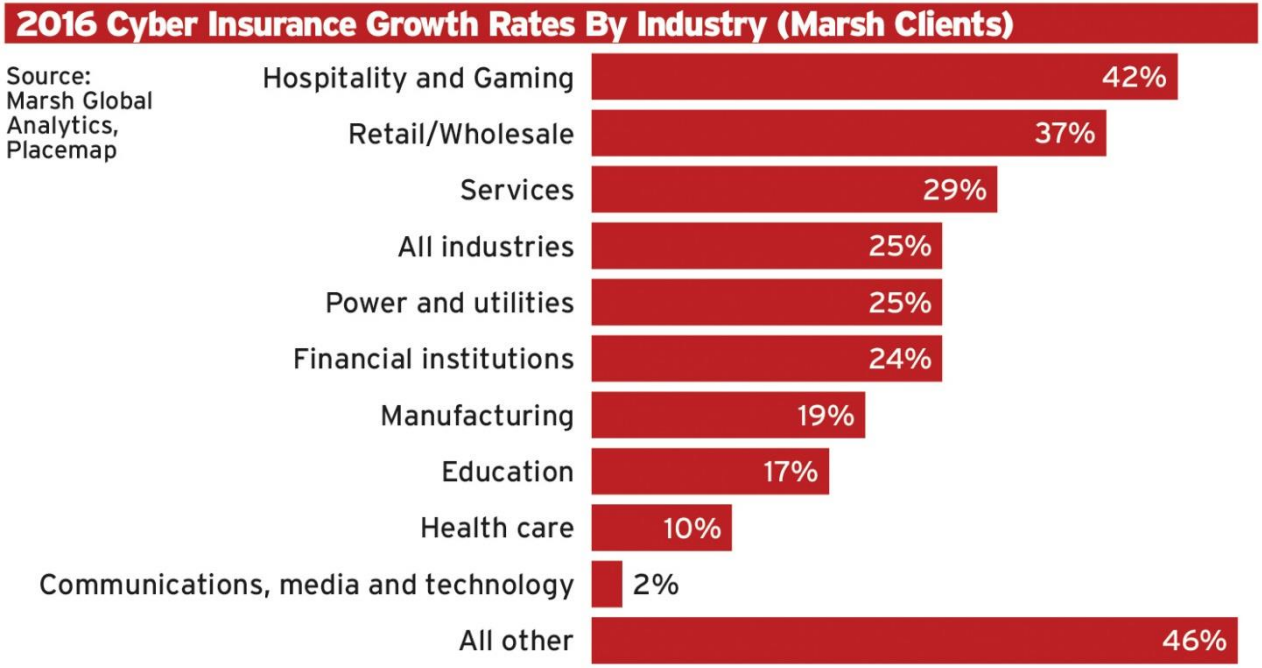
資料來源：Historical Development Of Cyber Insurance與本研究彙整

全球網路保險平均保費收入

2017年全球年保費收入約為30至40億美元，預計於10年(2027)內達到200億美元：國際金融協會2017年12月7日發布調查報告，指出醫院及零售業需求增幅最高。

2021年全球網路犯罪成本將高達六兆美元：

Herjavec 集團（Cyber Venture）委託的研究報告中，預測2021年全球網路犯罪成本將高達六兆美元。



不購買網路保險的原因：

1. 經銷商、保險公司與被保險人間溝通問題
2. 投資在預防措施而非購買保險
3. 保險範圍太多限制也不夠清楚
4. 資訊不足無法做決策
5. 保費過高
6. 申請程序過於複雜
7. 保險承保範圍外之費用過高
8. 損失難以量化

資料來源：Cyber Risk insurance: A growth market adapting to changing Risk，國際金融協會2017年12月7日發布調查報告，本研究彙整

各國網路保險市場概況

美國與英國網路保險發展概況

需求市場背景

1. 在ICT投資快速成長，且重度依賴網路的商業活動、消費性產品，與服務、資訊交流等發展，使經濟與社會暴露在包括資料、資訊被竊取，拒絕服務與網路入侵等風險下，而造成這些情形產生往往歸咎於不完善的資訊安全管理。
2. 可能的風險包括聲譽損害、商業或企業機密損失、成本增加等。
3. 推動需求市場的因素：隱私或資料洩漏通知的危機管理措施、補救措施及聲譽風險等產生的成本，可能包括罰款、損害賠償、和解、法律費用等。

供給

保險業者	經銷商 / 承銷商	律師

- 英國目前有AIG、ACE、Kiln、Brit 、Barbican 、QBE、CNA、Beazley、XL、Hiscox等家業者提供網路保險。（相對美國則約有30-40家保險業者提供網路保險保單）

資料保險應考慮六項關鍵項目：

1. 承保類型與有限責任範圍
2. 承保範圍
3. 承保責任啟動時機
4. 承保之資料類型
5. 承保之處理費用（發生資料外洩之處理成本）
6. 承保之處理服務

需求

政府、地方主管機關	零售業、醫療業、旅館業者、金融業等企業	民眾

- 英國網路保險市場規模（包括賠償）約2.5億美元；美國則是約8億美元。

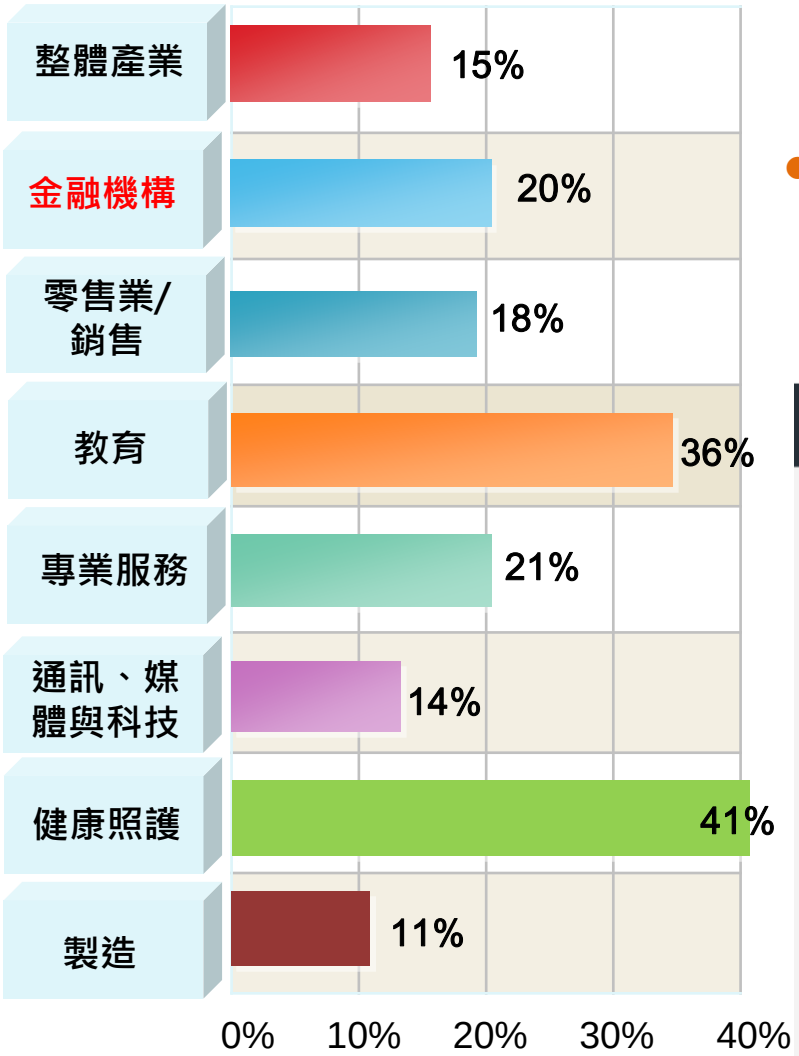
目前認為消費者認為其購買保險有包含網路風險的原因：

1. 一般商業綜合責任保險（CGL）或包含網路風險的商業綜合責任保險
2. 採用其他政策（如業務中斷）
3. 單獨式的網路政策

- 對面新興網路風險，傳統商業保險（如產物保險、責任保險、犯罪保險政策、企業主保險等）皆較偏向第一方風險造成的直接損失（如業務中斷、數位資產損失等），但未來第三方責任的重要性逐漸受到重視（驅動因素：歐洲與美國的洩漏通知制度），因此資料外洩產生之**第三方責任相關費用**，成為網路保險未來成長的契機。

美國網路保險市場概況

2015年購買資安保險增加比例

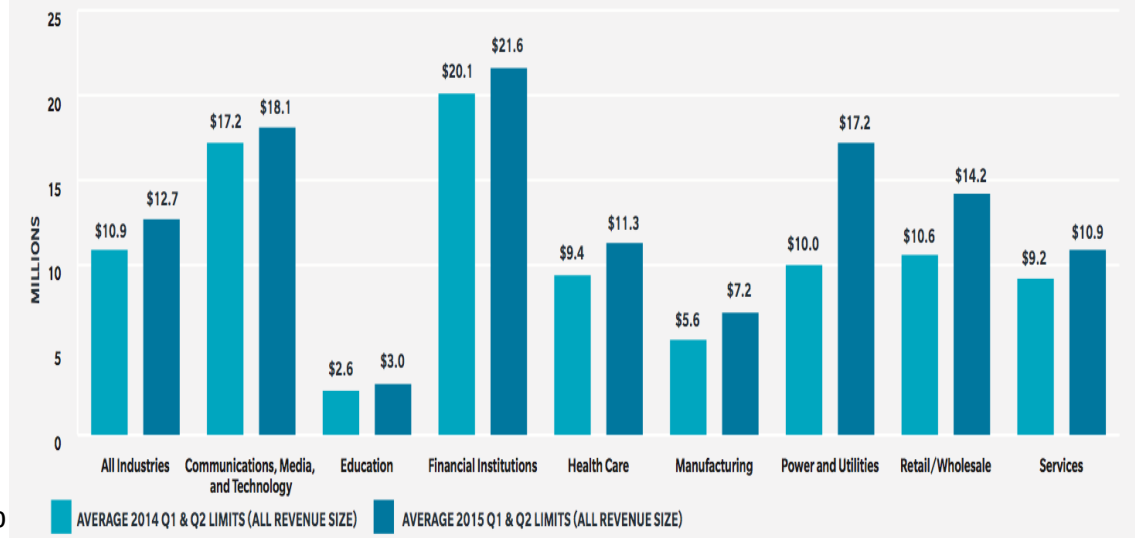


資料來源：Marsh Global Analytics,2016，本研究彙整

- **2015年美國資安保險整體產業需求比例提高**：相較於2014年，整體企業購買資安保險提高了15%，其中以健康照護護比例提升最高(41%)；然在通訊、媒體則呈現小幅提升，約14%(但平均保費為次高)。
- **企業平均網路安全保險限額提高**：相較於2014年，2015年整體企業的平均保險由1,090萬提高至1,270萬美元，其中以金融業平均保費最高達到2,160萬美元。

單位：百萬美元

FIGURE 3: Cyber Liability Total Limits Purchased (All Companies)
Source: Marsh Global Analytics



美國政府機關導入網路資料保險機制

在許多與資訊安全相關法令（例如HIPAA）加重責任主體責任的趨勢下，以及歐巴馬政府對於資通訊關鍵基礎設施的重視，美國將在政府採購程序中，提高對政府承包商的要求

- **要求遵循相關的資訊安全標準**
- **要求應投保相關的資料保險**

April 2015 to April 2016

- Major Government Data Breaches from April 2015 to April 2016

1. state.co.us
2. georgia.gov
3. irs.gov
4. ca.gov
5. opm.gov
6. army.mil
7. nationalguard.com
8. va.gov
9. state.gov
10. illinois.gov
11. mn.gov
12. colorado.gov
13. az.gov
14. amherstohio.org
15. state.md.us
16. whs.mil
17. vermont.gov
18. state.tx.us
19. laems.net
20. flgov.com
21. nyc.gov
22. brunswickme.org
23. floridahealth.gov
24. slco.org
25. myflfamilies.com
26. dentoncounty.com
27. tchhsa.org
28. gsa.gov
29. itsmarta.com
30. ncdhhs.gov
31. fws.gov
32. nasa.gov
33. dhs.gov
34. fbi.gov
35. lacounty.gov

公部門保險解決方案

- Alliant Property Insurance Program (APIP)是一公部門保險解決方案，擁有超過8,000名會員，總總可保價值(total insurable value, TIV)為400億美元。
- APIP網絡責任保險有2500萬美元，而整個APIP計劃屬總額限制，意味著，如果其他APIP計劃成員有重大的網絡責任索賠，可以超過個別責任保險限制，華盛頓州是這個計劃的8000名成員之一。

	2015-2016	2016-2017		
		Primary Layer	Excess Layer	Combined
Insurance Company	APIP Beazley	APIP Beazley	XL Catlin Indian Harbor Ins Co.	
A.M. Best Rating	A (Excellent) XII ($1B to $1.25B)	A (Excellent) XII ($1B to $1.25B)	A (Excellent) XV ($2B+)	
Coverage Form	Primary Cyber Liability	Primary Cyber Liability	Excess Liability Follow Form	
Policy Limits	$2,000,000	$2,000,000	$3,000,000	**$5,000,000**
Privacy Notification Limits				
Beazley Approved Vendors	$1,000,000	$1,000,000	$3,000,000	**$4,000,000**
Non Beazley Approved Vendors	$500,000	$500,000	$3,000,000	**$3,500,000**
Aggregate Limits				
APIP Program	$25,000,000	$25,000,000		
State of Washington	$2,000,000	$2,000,000	$3,000,000	**$5,000,000**
Deductible	$100,000	$100,000	$100,000	**$100,000**

資料來源： Cyber Liability Insurance Overview Policy Year 2016-2017,Washington state,2016

美國-公司治理與資料保險揭露 (1/2)

法源與政策支持

- 公開上市公司必須揭露資安風險、事件，以及因應事項(包含投保相關保險產品)。
- -2011年10月13日美國證券交易委員會(US. Securities and Exchange Commission)發布的企業金融揭露基準議題二:網際安全 (CF Disclosure Guidance : Topic NO.2 Cybersecurity)。
- Consistent with the Regulation S-K Item 503(c) requirements for risk factor disclosures generally, cybersecurity risk disclosure provided must adequately describe the nature of the material risks and specify how each risk affects the registrant. Registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk factor disclosure.[1] Depending on the registrant's particular facts and circumstances, and to the extent material, appropriate disclosures may include:
  - Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
  - To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
  - Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
  - Risks related to cyber incidents that may remain undetected for an extended period;
  - and Description of relevant insurance coverage.

    Relevant insurance coverage. This is a key emerging issue for many clients, who need continuing counsel as threats evolve and as insurance policies adapt to changing conditions.
- [1] Item 503(c) of Regulation S-K instructs registrants to "not present risks that could apply to any issuer or any offering" and further, to "[e]xplain how the risk affects the issuer or the securities being offered." Item 503(c) of Regulation S-K.

資料來源:Division of Corporation Finance Securities and Exchange Commission CF Disclosure Guidance: Topic No. 2 Cybersecurity, October 13, 2011 , *http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm*

美國-公司治理與資料保險揭露 (2/2)

法源與政策支持

- **2014年財政部提交網路安全總統報告(13636號)指出，網路保險機制建立，應參酌類似國家洪水保險計畫，以因應大規模攻擊時，有足夠支援幫助民間部門復原**

Treasury Department Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636, 24 (2014)
To establish a program, akin to the National Flood Insurance Program, to help buttress the private market in the event of catastrophic, wide-spread attacks.(available at http://www.treasury.gov/press-center/Documents/Supporting%20Analysis%20Treasury%20Report%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf.)

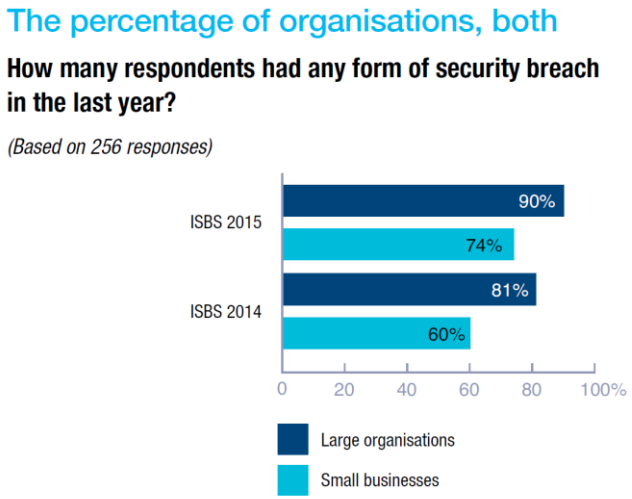
- **2015年 美國證券交易委員會委員新聞稿強調，政府應該提供中小企業相對便宜(簡易版)的資安保險方案**

The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses
Commissioner Luis A. Aguilar U.S. Securities and Exchange Commission* Oct. 19, 2015
Identify Ways of Fostering Economies of Scale for Cybersecurity Solutions: Ultimately, responsibility for cybersecurity lies with the SMBs themselves, not with the government. Even so, to help alleviate the resource constraints faced by SMBs, policymakers could explore ways of encouraging the development of economies of scale for cybersecurity solutions. There are myriad possible avenues in this regard, but one possibility is to develop tax credits for vendors that would encourage them to develop cost-effective cybersecurity solutions tailored to the unique needs of SMBs.Similarly, policymakers could consider measures to help the incipient cyber-insurance market reach a level of maturity that will bring costs down and provide solutions specifically for SMBs.
(available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=cfa8174a-e7f4-434a-9669-09282c0a8f1f.)

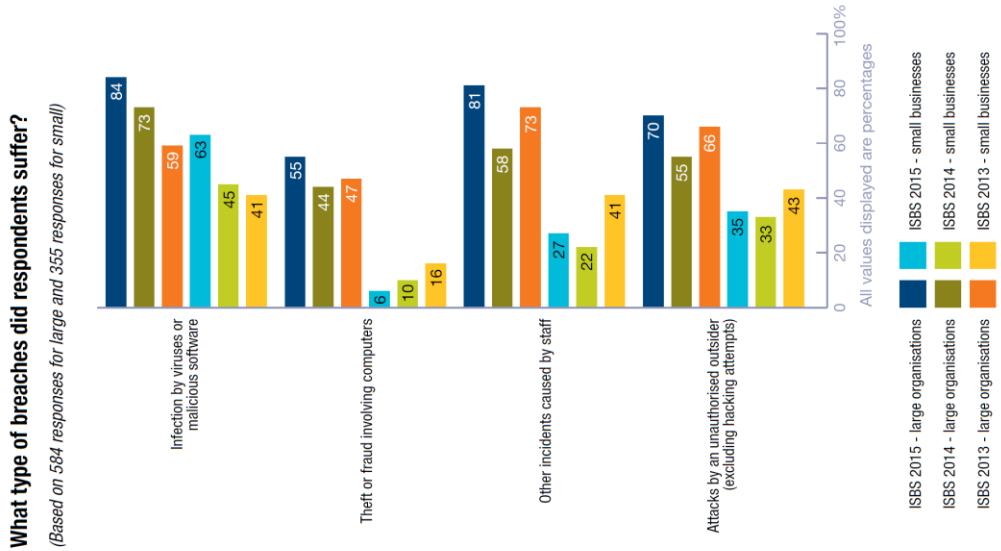
- **2015年 證管會法令遵循檢查及調查室（SEC Office of Compliance Inspections and Examinations, OCIE）於網絡安全審查倡議 （Cybersecurity Examination Initiative），對事件通報強調，應說明是否有投保網路保險，及提供網路安全保險的損賠金額和範圍。**

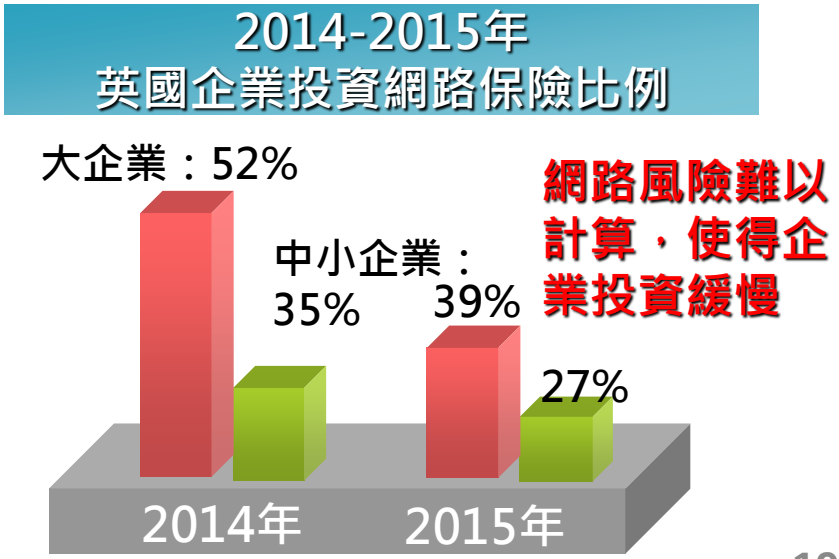
Information regarding the amount of actual customer losses associated with cyber incidents, as well as information on the following:
(1) The amount of customer losses reimbursed by the firm;(2) Whether the firm had cybersecurity insurance coverage, including the types of incidents the insurance covered;(3) Whether any insurance claims related to cyber events were filed; and(4) The amount of cyber-related losses recovered pursuant to the firm’s cybersecurity insurance coverage.
(available at https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf)

英國網路保險市場現況



- 根據英國企業創新與技術部2015年發佈的資訊安全漏洞調查指出，雖然**漏洞事件發生率與平均發生次數較2014年提高**，且**資安漏洞的總成本與單一最嚴重漏洞事件發生的成本，都比2014年還來的更高**。
- 2015年大型企業平均最嚴重的資安漏洞成本約為145.5萬-314萬英鎊(2014年： 60萬-115萬英鎊)
- 2015年中小企業平均最嚴重的資安漏洞成本約為7.52萬-31.1萬英鎊(2014年： 6.5萬-11.5萬英鎊)





資料來源：2014及2015年 Information Security Breaches Survey,UK GOV與本研究彙整

英國產、官合作推動網路保險(1/2)

- **邀集各方專家探討現階段市場概況**：2014年11月，負責英國網路安全策略的英國內閣與英國保險Marsh召開會議，討論**如何促進網路保險產業發展，以保障英國企業的網路安全，提升企業的網路安全風險管理**。
- **企業遭受資料漏洞事件逐年上升**：根據2014年資訊安全漏洞調查指出，81%的大企業與60%的中小企業皆於去年遭受到資料漏洞事件，且較2013年**成長了2倍之多**。

英國內閣 Francis Maude	1. 強化國家網路安全為英國長期經濟政策關鍵之一，打造全球最適合、最安全的經商環境。 2. 藉由與英國保險企業單位合作，促進網路保險市場的成長。 3. 對於企業遭遇資料漏洞事件，網路保險並不會取代網路安全訴訟，而且多了一層更安全的保護。
Marsh UK & Ireland CEO Mark Weil	1. 資料安全事件可能會快速累積花費成本、打擊企業商譽及降低投資者信心。 2. 大量資料漏洞事件恐造成訴訟、產生罰鍰、法律調查。 3. 企業應透過風險管理與保險解決方案以延遲資安事件發生造成的傷害。
Airmic CEO John Hurrell	1. 網路風險橫跨多產業的利害關係人，是一重大的挑戰。 2. 保險產業對於促進企業認知扮演重要的角色。 3. 希望藉由政府與產業的合作，加速與其他重要單位共同合作，包含組織內的IT與風險部門。

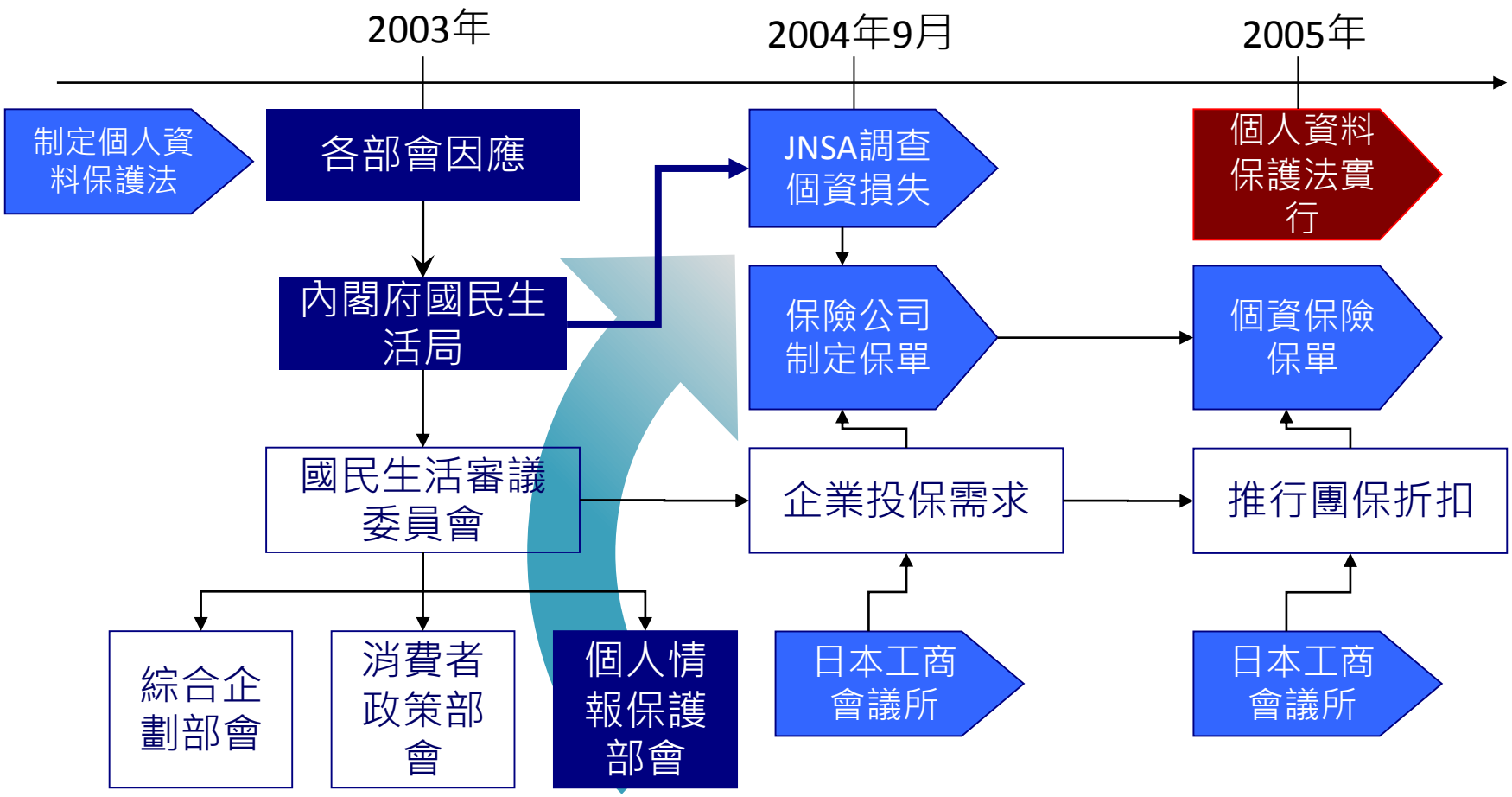
資料來源：https://www.gov.uk/government/news/cyber-security-is-essential-in-todays-marketplace與台經院彙整

英國產、官合作推動網路保險(2/2)

1. 英國政府與MARCH於2015 UK CYBER SECURITY THE ROLE OF INSURANCE IN MANAGING AND MITIGATING THE RISK 報各指出，有2%的大公司具有資安保險涵蓋，對於小公司來說，這個數字接近零。
2. 強調資安事件對英國企業所**帶來的風險**
3. 了解保險業者在促進網路安全風險管理中所能**扮演的重要角色**為何
4. 業界將共同成立一工作團隊與英國政府繼續合作，並致力於以下三點的推動：
   - **利用網路保險強化英國企業的網路安全**，並作為中小企業風險評估的一部份
   - 建立英國企業對於**資安攻擊事件的影響與保險對應的模型**
   - 為降低資安事件對國家基礎設備所帶來的衝擊，**將網路保險作為資安認證的一部分**
4. 倫敦成為網絡風險管理的全球中心。
5. 未來將藉由**政府與業界的合作**，為企業**提出有效的網路保險**

資料來源：https://www.gov.uk/government/news/cyber-security-is-essential-in-todays-marketplace與台經院彙整

日本個資保險推動概要



1.政策諮詢
2.3年政策與法律實行觀察

1.各個公協會參與
2.中小企業最小投保額

資料來源：日本工商會議所、台灣經濟研究院彙整。

日本網路保險市場概況(1/2)

- **日本資安保險需求漸增**：自2013年起，日本對資安保險的需求漸增，市場規模由89億日元成長至2017年的156億日圓。

金額(百萬日圓)/年度	2013	2014	2015	2016	2017	複合成長率
資安產業	776,988	842,842	896,500	932,700	979,600	3.7%
資安產品	414,139	448,941	470,500	487,900	509,900	3.3%
資安服務	362,849	393,901	426,000	444,800	469,700	4.2%
資安保險	8,885	10,479	11,800	13,500	15,600	8.7%
資安保險占整體資安產業比重	1.1%	1.2%	1.3%	1.4%	1.6%	4.8%

日本主要資安保險保單

	AIU	東京海上日動	三井住友海上 あいおいニッセイ同和損保	損保ジャパン日本興亜
商品名	CyberEdge （サイバーエッジ）	サイバーリスク保険	サイバーセキュリティ 総合補償プラン*	サイバー保険
発売時期	2012 年 12 月	2015 年 2 月	2015 年 9 月	2015 年 10 月
補償内容 （主なもの）	損害賠償責任（損害賠償金、争訟費用等） 危機管理対応（事故原因調査・被害拡大防止のための費用、データ復元費用、コンサルティング費用等） 情報漏洩対応（見舞金・見舞品費用、社告のための費用、行政対応費用等） 事業中断対応（事業中断に伴う喪失利益、営業継続費用等）**			
海外訴訟	海外での損害賠償請求訴訟に関する、賠償金・争訟費用も、補償対象			

* 三井住友海上の場合。あいおいニッセイ同和損保では、ｻｲﾊﾞｰｾｷｭﾘﾃｨ保険（IT 業務賠償責任保険［拡張補償プラン］）の商品名で販売。
** 事業中断対応については、オプションでの補償として取り扱われている場合もある
※ 各社の発売時のプレス資料、募集パンフレット等を参考に、筆者作成

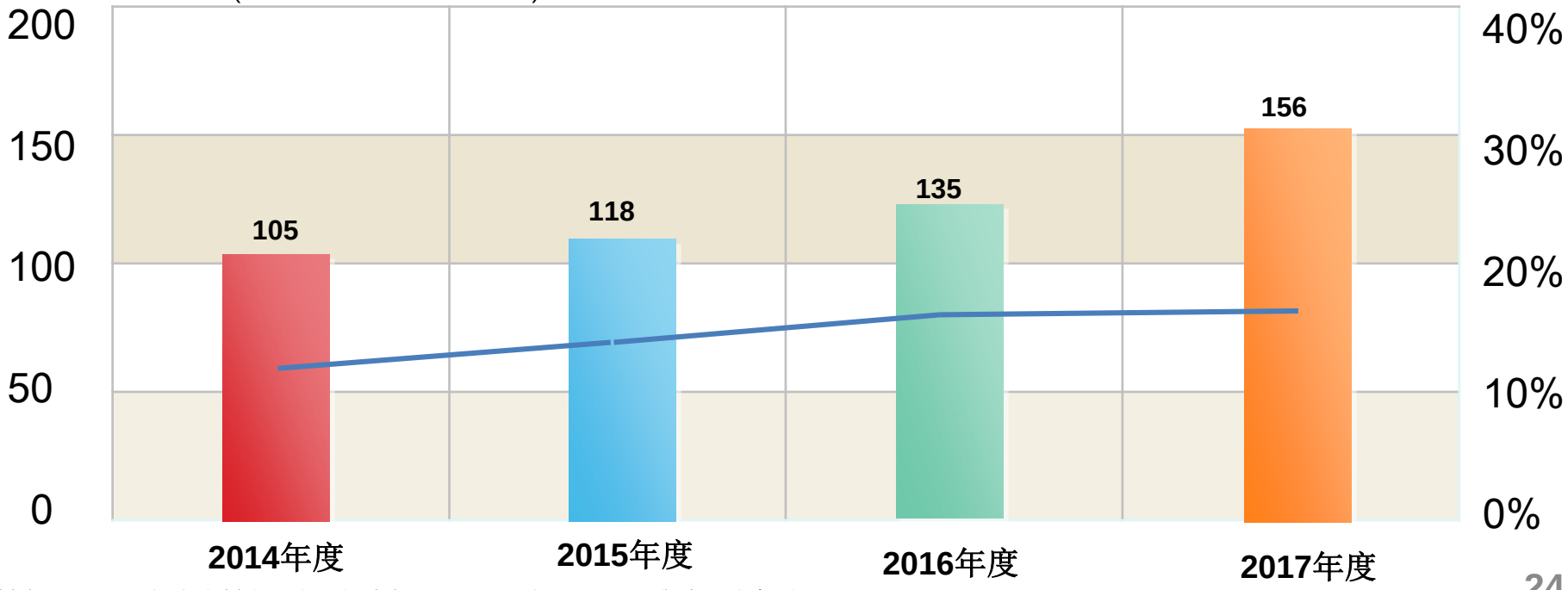
日本網路保險市場概況(2/2)

- **日本資安保險市場緩步成長，年成長率衰退**：自2011年起，日本資安保險市場規模約74.68億日圓，2017年規模則達到156億日圓。2015年起成長力道強勁，是因為多起大型資安事件，造成個資和商資外洩，使大企業增加納保。

年度	2014	2015	2016	2017
相較上年成長率		12.4%	15.0%	15.0%

日本歷年資安保險市場規模

單位：億圓（2011年度為74.68億元）



資料來源：2016年度資料安全市場調查報告書, 2017年9月,JNSA與本研究彙整

資安整體網路保險

美亞CyberEdge天網版保單

2012年，美亞產險AIG推出CyberEdge保險產品，進一步擴大保障範圍，包含個人資料、公司資訊、資料安全；同時亦可附加媒體內容、電腦勒索等條款。

資料責任

- 個人資料責任
- 公司資訊責任
- 委外責任
- 資料安全責任
- 抗辯費用

資料管理

- 資料管理調查
- 資料行政罰鍰

名譽修復

- 公司名譽修復
- 個人名譽修復
- 通知及監控費用
- 電子資料
- 鑑識服務

附加條款：

資料危機管理服務：資料危機事件發生時，可連細資料危機法律顧問或資料危機公關顧問，使用危機管理服務。

媒體內容責任：版權、標題、標語等侵權；構想剽竊、抄襲等；惡意文字敘述、言語等；侵擾、隱私侵犯等。

電腦勒索責任：因安全威脅所致的勒索損失。

網路中斷保險：因安全故障在等待期間後所致的網路損失。

三井住友海上網路保險概要

三井住友海上保險:為協助日本各界因應與日俱增的資安事件以及繁瑣的善後流程，於2013年推出客製化資安保單產品

企業社會責任

企業信用危機

財物損失

資通安全潛在風險

名譽及機密被侵犯

員工惡意行為

個資外洩的事後賠償

資安事件衍生衝擊
(企業流程中斷及軟硬體毀損)

基本賠償

- 法律賠償：因資安事件所造成的法律賠償責任
- 訴訟費用：被保險公司法律訴訟上的支出(包含食宿、交通、加班、文件申請與影印，以及數位鑑識模擬。)
- 鑑識調查費用：包含數位證據保存、資安事件調查費用、其他資安事件衍生費用(交通、食宿、通訊)
- 其他費用：包含仲裁與和解費用。

加保項目

- 企業損失：因資安事件對被保險公司所造成的營運損失(包含企業流程或生產線停擺、MIS癱瘓、伺服器毀損、以及資料毀損等復元費用)
- 其他支援服務：包含法律諮詢費用、廣告活動費用、一般諮詢費用、事故應變費用、賠償金。

雲端服務網路保險

美國雲端保單發展趨勢

Cyber Insurance VS Cloud Insurance

- **雲保險(Cloud insurance)定義:**

  -一種風險管理方法，對於雲端服務商部分特定的潛在故障(potential failures)，提供經濟補償(financial compensation)的承諾。雲保險(Cloud insurance)可能會成為服務等級協議（SLA）的一部分，它可以單獨購買或通過第三方保險公司。(Source : SearchCloudStorage)

- **新型雲端保單**
- **1.管理-雲端暨管理服務險(Cloud and Managed Service Insurance)**

  -2013年4月網路代管業者交易和認證聯盟(MSPAlliance)與保險公司Lockton Affinity合作提出

  -(1) 保險的範圍:網路攻擊、資料滅失、系統故障所需負擔的損害賠償責任、負擔保險給付責任(契約或法律責任)

  -(2) 保額:100萬至1000萬美金

  -(3) 被保險人:不限制於嚴格定義下雲端業者

  -(4) 設定條件(降低風險):被保險人須通過Unified Certification Standard 11項風險控管準則:

  1: Provider Organization, Governance, Planning and Risk Management 2: Documented Policies and Procedures

  3: Service Change Management 4: Event Management

  5: Logical Security 6: Change Management

  7: Data Integrity 8: Physical and Environmental Security

  9: Service Level Agreements 10: Customer Reporting and Billing

  11: Financial Health

2.隱私於責任保險

-2013年2月雲端保險服務平台Cloudinsure宣布與保險經紀公司Lockton合作，擬設計雲端環境的隱私與安全責任保險方案

-(1) 保險的範圍:將網路風險之資料損害所引發之責任範疇納入企業中和責任險的保險範圍

資料來源:UCS Published Standard；http://www.mspalliance.com/ucs-published-standard/與台經院彙整

網路責任保險

- 網絡責任保險降低和保護企業於網絡入侵，丟失的記錄和/或被盜設備（包括筆記本電腦，平板電腦和智能手機）導致資訊洩露，所承擔的風險。客戶或員工數據丟失的責任通常不在企業保險下，額外的網絡責任保險可加以填補，涵蓋範圍包括：
  1.數據洩露/隱私危機管理 (事件管理、調查、補救、事件通知、法律費用、出庭和監管罰款等相關的費用。)
  2.多媒體/媒體責任保險 (第三方損害包括特定網站污損和知識產權侵權。)
  3.勒索責任保險 (因勒索威脅造成的損失)
  4.網絡安全責任 (導致的第三方損害，與第三方資訊供應商所生之相關費用)

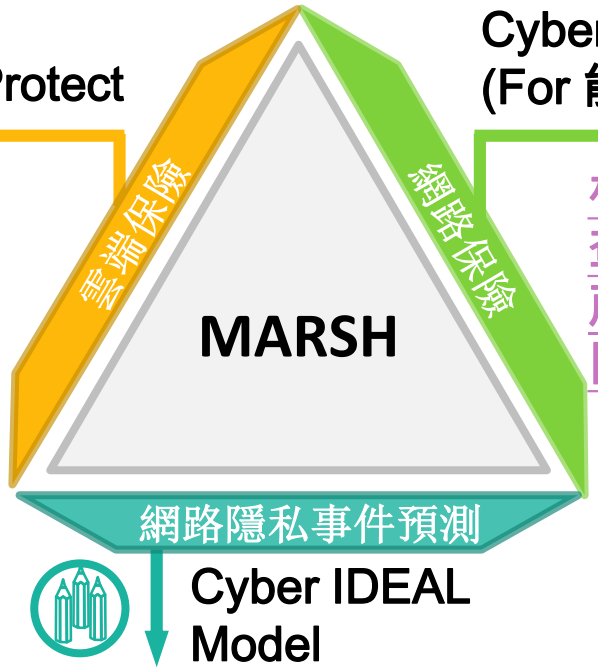
ACUMEN SOLUTIONS GROUP

Cyber Liability Coverage Summary

Who is Covered?	What is Covered?	Policy Triggers	Standard Exclusions
▪ The Named Insured and any subsidiaries ▪ Any director, officer or manager of the Organization (A principal if insured is a sole proprietorship or partner for partnerships) ▪ Employees of the Organization but only while acting within the scope of their employment, Independent Contractors ▪ A lawful spouse or domestic partner under provisions of law	▪ Network Security & Privacy: • Theft, loss or unauthorized disclosure of Personally Identifiable Information or corporate confidential information • Failure to prevent transmission of a Malicious code • Denial of Service attack ▪ Notification costs, Forensics, ID and Credit Monitoring, and legal services, Public Relations expenses ▪ Claims expenses incurred from regulatory proceedings, including fines and penalties where insurable by law ▪ Cyber Extortion costs and expenses ▪ Electronic Business Interruption Costs incurred	▪ Any written demand for money, services, non-monetary relief or injunctive relief received by an Insured, including service of suit or the institution of arbitration proceedings against an Insured, even if the allegations are groundless, false or fraudulent ▪ Regulatory Proceeding against the Insured	▪ Bodily Injury or Property Damage ▪ Breach of Contract ▪ Anti-trust Violations ▪ False, deceptive or unfair trade practices ▪ Unlawful collection of Personally identifiable information ▪ Criminal, dishonest or malicious acts, intentional violation of a privacy policy, or intentional security breach ▪ Patent infringement ▪ Misappropriation of trade secrets

MARSH網路保險概要

- Marsh推出多種相關保險提供更多樣保護：Marsh除提出一般的網路保險外，也提供了雲端保護保險及網路隱私事件預測模型，提供更完整的保險服務。



CloudProtect

Marsh為保護企業因使用雲端服務時發生網路損壞等問題，因而設計CloudProtect保護企業免於金錢上的損失。

產品特色

- 強化公司資安政策，提升整體防護
- 提供企業因雲端服務端所造成的經濟損失與額外花費
- 主要損失涵蓋：經濟損失、轉換新的雲端服務端延伸出的花費

Cyber Gap Insurance (For 能源產業)

根據美國國土安全部相關調查指出，2013年在能源產業所遭受到的資安事件約53%，因而設計網路保險產品。

產品特色

- 進行資安攻擊的防護安全
- 減少資安漏洞
- 延擬更完整的風險延遲與風險計劃
- 由S&D至少A-以上的企業與承保人提供保護安全

Cyber IDEAL Model

產品特色

- 網路策略制定
- 資料洩漏預測
- 產業特定網路資料分析
- 資料裂漏事件的衝擊範圍與成本

CloudInsure&Lockton 雲端保險概要

- 雲端保險平台與保險業者合作：2013年，全家第一家雲端保險平台CloudInsure與全球前十大保險業者Lockton共同合作，推出雲端風險管理解決方案

雲端保險平台

CLOUDINSURE

＋

大型保險業者

LOCKTON®

→

雲端風險管理解決方案

- 全球第一家雲端保險平台
- 聚焦於雲端環境中的隱私與安全
- 與保險人建立關係，提供責任保險

- 全球前十大保險業者
- 運用對市場的了解性與知識，翻轉傳統思維

- 雲端興起，引導企業網雲端發展
- 提供前瞻雲端保險，符合市場需求

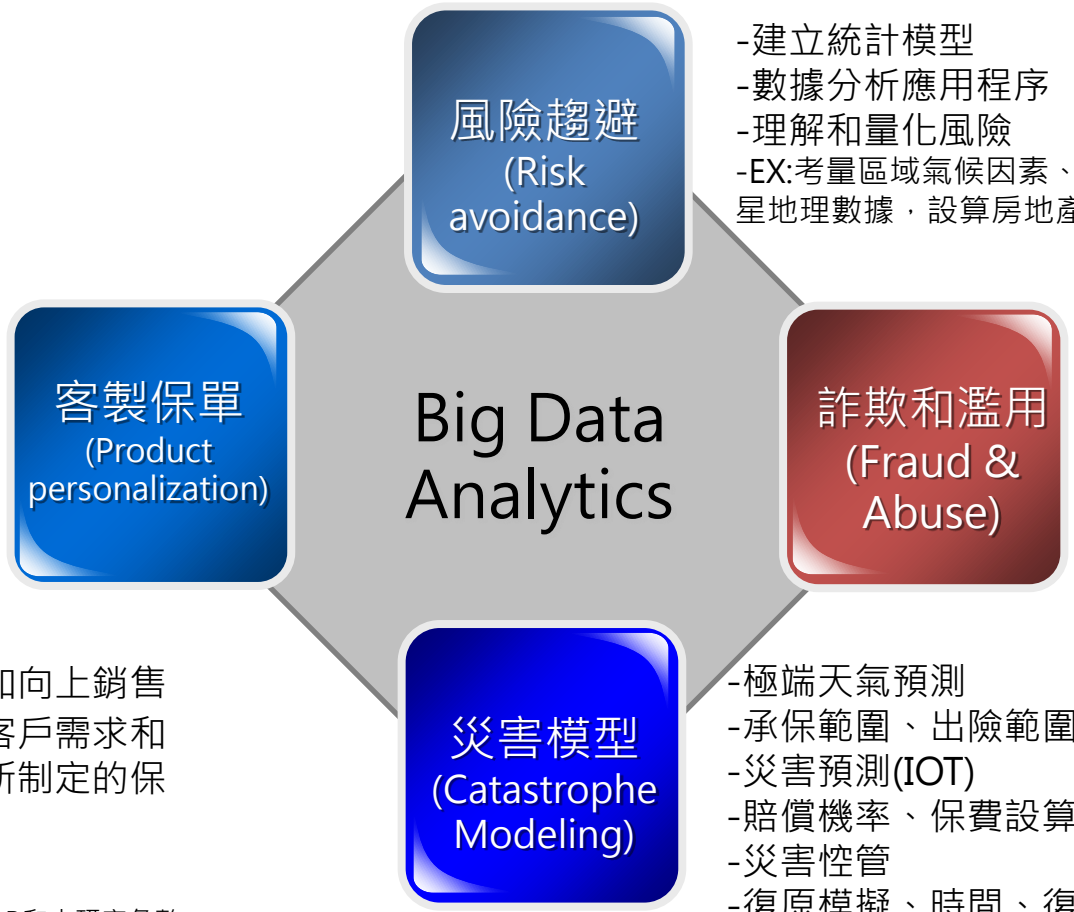
雲端保險方案

市場開拓

巨量資料網路保險

巨量資料網路資料保險

美國保險公司大都會人壽(MetLife)透過Mongo DB 開發創新客戶服務應用程式，以類似Facebook 的使用者介面The Wall ，針對公司客戶提供整合性的檢視，包括政策細節和跨全業務線的交易，因此客服人員能夠在單一介面中，取得所需全部資訊，並以**Big data分析處理4,500 萬個客戶協議，達成風險趨避**。



-建立統計模型
-數據分析應用程序
-理解和量化風險
-EX:考量區域氣候因素、交通、薪資就業、犯罪統計和衛星地理數據，設算房地產相關投保風險(如火災險)

-統計模型
-忠誠管理
-廣告活動
-代理分析
-價值管理
-情感分析
-帳戶資訊
-駕駛記錄
-健康資訊
-社群資訊
-交叉銷售和向上銷售
-達成根據客戶需求和風險因素所制定的保單和保費

-社群分析
-社會網絡
-交叉比對
-自動分析

-極端天氣預測
-承保範圍、出險範圍模擬
-災害預測(IOT)
-賠償機率、保費設算
-災害控管
-復原模擬、時間、復原成本

Source:MetLife、Mongo DB和本研究彙整

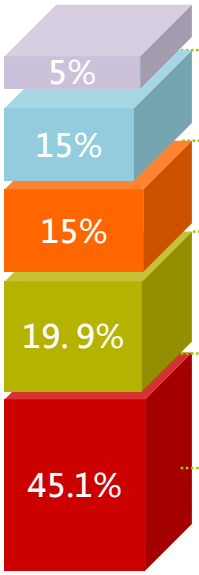
新興網路保險

中國人保財險-虛擬財產保險

發展趨勢快過台灣

眾安線上財產保險公司	中國人保財險

註冊資本10億人民幣
股權結構



- 5%：攜程網
- 15%：中國平安保險股份有限公司
- 15%：騰訊
- 19. 9%：阿里巴巴
- 45.1%：網路科技公司和投資公司
  包括優孚控股、日訊網路科技、日訊互聯網、加德信投資、遠強投資等

經營特性

1.業務範圍限於互聯網相關的財產保險業務

2.不設分支機構

3.自2013年02月18日收到批准籌建通知之日起 1 年內完成籌建工作

4.籌建期間不得從事保險經營活動

5.未經批准不得變更主要投資人

6.針對網路交易安全、網路服務等方面進行產品創新，為互聯網用戶提供解決方案

虛擬財產保險

1.2012年9月，中國人保財險與國內最大的網絡遊戲交易平臺5173網絡遊戲服務網開展業務合作，雙方共同設計開發保險產品，共同推廣網絡遊戲虛擬財產損失保險。

2.該保險主要保障遊戲買家在網上進行遊戲裝備、遊戲幣、遊戲賬號等交易時，由於賣家的惡意行為致使保險標的被盜、被遊戲運營商收回，或被遊戲官方封號時導致的買家直接經濟損失。(事件發生➔保險啟動➔復原與填補損失機制)

3.2013年5月初簽發第一張網絡遊戲虛擬財產保險保單以來，開辦首月已為10萬多人次的網絡玩家提供了虛擬財產安全保障服務

資料來源:眾安線上財產保險公司2013年07月09日，人保財險首款虛擬財產保險首月投保破10萬人次，新華財經網，http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/fortune/2013-07/09/c_124981844.htm、本研究彙整

大 綱

- 科技創新所造成的資安風險
- 網路資料保險之需求與發展
- 全球網路資料保險概況
- 我國資料保險制度未來發展之建議

我國資安保險保單銷售概況

1.2017年臺灣資安保費總銷售約為5,606萬元，其中一半保費收入為資訊及網路錯誤或疏漏之責任保險。
2.2017年AIG所提供的資料保護保險平均一年保費約為15.1萬至18.2萬間，承保客戶約有30家。
3.怡安風險集團2017年調查全球企業，資訊安全被列入企業營運的前5大風險，因此，國外企業相當重視資安，也投入相當多的資源在作資安維護及防禦；至於資安雖也被國內企業列入第11大風險，但是國內大部份企業對於買資安險不感興趣，前3季比去年同期多賣了16張。

文/ 黃泓瑜 | 2017-09-13 發表

臺灣資安險主要險種

保險名稱	對象	定義	投保範圍
資料保護保險	不限	發生違反資料保護或違反資料安全之情事，致第三人受有損害。	企業如果發生個資外洩，能夠提供第三責任賠償，包含和解金、訴訟費、判決金和抗議費，包括外包廠商將客戶資料流失。
資料及網路錯誤或疏漏責任保險	不限	因勒索或犯罪行為或內部管理疏失等造成相關損失。	承保網路中斷保險、電腦勒索保險、媒體內容責任及其他費用、營業中斷損失、電子資料修復、重置系統費用、鑑識服務、名譽修復。
資料系統不法行為保險	金融機構，如銀行業、證券業	電腦系統入侵而遭到資金或財產損失，保險公司能夠轉嫁。	資訊輸入竄改或銷毀、電腦指令之偽造或變造、電子資訊及媒體之毀損滅失、電子訊息之誤傳或竄改、資訊系統服務之失誤、電子傳送之導誤，電腦病毒侵害。

資料來源：AIG、臺產、iThome整理製表，2017年9月

資安險保單 前3季年增16張

去年及今年前三季資安險投保狀況

商品名稱(保發)	2017年 簽單筆數	2017年 簽批保費總計	2016年 簽單筆數	2016年 簽批保費總計
資料保護保險	32	14,379,841	26	10,262,935
資訊及網路錯誤或疏漏責任保險	32	28,620,982	25	22,237,874
資訊系統不法行為保險	4	7,584,029	0	0
資訊服務業專業責任保險	156	5,471,713	40	3,416,585
總計	224	56,056,565	91	35,917,394

資料來源：保發中心　註：資料保護險和資訊系統不法行為險為一般企業投保

去年及今年前三季資安險投保狀況

工商時報　A A A 友善列印

資料來源：ITHOME與http://www.chinatimes.com/newspapers/20171123000311-260208

國內推動Cyber Insurance推動困境

- 1.台灣無個人資料保護委員會(美、日等國均有)，難以落實個資保護，使的企業資料外洩有恃無恐，而無保險需求。
- 2.無類似美國法律明文規定，將資料保險納為公司治理之一環。
- 3.保費估計困難(台灣目前無樣本調查)，使投保成本較高，致投保比例較少。
- 4.因法律的不確定性及政府解釋的不清楚，致保險業目前不敢冒然提賣保單。
- 5.投保風險過高商品選擇較少，使投保成本較高。

網路保險投保發展建議(1/2)

遭遇困難	政策建議
1.無類似美國法律明文規定，將資料保險納為公司治理之一環	1.短期將標章認證機制配套跟政府認定機制能互相配合，將資料保險機制納入。 2.中長期促成證交會將資安、資料保險納入公司治理揭露的一環，強化市場和投資人保護。
2.保費估計困難(台灣目前無樣本調查)，使投保成本較高，致投保比例較少	仿效日本由政府委託民間機構針對資安事件統計數據調查，了解求償原因、求償人數、求償件數、求償金額等統計，提高保險業界堆資安風險估計可能性。
3.因法律的不確定性及政府解釋的不清楚，致保險業目前不敢冒然提賣保單。	1.責成法務部函釋個資法損賠要件，是否先有損害，才有所謂的賠償金。 2.保險的範圍目前是用個資的損害賠償來界定，如果涉及雲端應重新界定損賠要件。
4.投保風險過高商品選擇較少，使投保成本較高	1.費率參考日本、自付額限制，保單保額上的限制。 2.以政策促成保險業者多方引進雲端或資料保險等創新商品，以強化雲端安全環境。

網路保險投保發展建議(2/2)

賠償範圍界定

- 資料洩漏屬連續性，因此需給予一次或多次的賠損定義，否則將造成保險公司過高賠償。

導入網路保險評鑑機制

- 美國證交會資安揭露準則形成模範規定，使公司訂定內部治理準則；國內則以中華公司治理協會於公司評鑑時加入網路保險評鑑，以引導公司導入。

責任範圍

- 資料保險責任範圍界定，須思考範圍，以免發生爭議。

訂定附加條款

- 使用Big data或Open data時，可以給定附加條款。

網路保險所建構的Ecosystem

網路保險

保單規劃

保費核保

事件處理

風險降低

資安健檢

資安產品	顧問業	資安稽核
資安服務	資安認證	資安稽核
SOC	資安代管	雲端虛擬
數位鑑識	顧問業	律師業
教育訓練	安全系統	委外服務

- 提升國內資安產業發展
- 強化雲端應用環境(從雲端應用走向終端安全)

報告完畢

敬請指教

附件

歐盟網路發展與契機

網路保險 需求

風險與需求

1. 大數量相似的裝置設備（如大多數人使用相同的作業系統、軟體）
2. 潛在的意外損失
3. 可負擔的保費
4. 可計算的損失
5. 可確認損失發生的時間
6. Cyber-insurance涵蓋的風險項目與現有保險的差異

未來

1. 加強企業之資安體制，以降低保險保費
2. 完善整體資安規範
3. 歐盟亦建議修改資訊保護的框架，包括對違規公司的最高刑罰增至企業整年**全球營業額的2%**。

政策

1. 洩漏通報制度（Breach Notification)
2. 利用調查蒐集cyber-insurance相關實證資料（風險型態、損失型態、保費、侵權責任等），並由保險公司、消費者及主管機關共同努力將資訊彙整，作為參考建議文件
3. 更新歐洲消費者權利法
4. 利用制訂架構以幫助消費者了解並評價其資訊的價值
5. 考慮由政府擔任再保險者

網路保險 供給

市場阻礙

1. 對新型態的風險熟悉程度低
2. 缺乏保險精算的資料
3. **相關性風險**（保險公司會擔心本身因同時發生索賠而遭受重大的損失）
4. **資訊不對稱**（保險公司可能因為缺乏充足風險資訊，造成逆選擇；而被保險人則可能因投保有道德風險問題產生。
5. 缺乏再保險業者

未來

1. 發展**資安顧問服務**市場
2. 配合科技快速發展下，帶來之新風險、新威脅而規劃保險配套
3. 促進IT安全產品與服務的認證，且保險市場可成為良好（best practice）資安推廣實施的平台或機制

資料來源:王仁甫、周蓉慧，2012年，資安融合ICT產業研究，台灣經濟研究院執行，資策會，行政院科技會報指導

德國安聯人壽網路保險概要

Allianz Cyber Protect ：IT已成為全球企業營運的必要工具，隨著姿通訊技術發展，駭客攻擊手法趨於多元迅速，為協助全球企業因應資訊安全潛在風險，安聯資安專案結合專業資安健檢服務，提供客製化彈性的資安保險項目。

Allianz Cyber Protect

- 資料外洩保障：包含對企業與客戶資料之外洩損失理賠。
- 資安事件處理及連帶損失：包含企業營運中斷與違約損失、資安事件應變、網路犯罪與詐騙、商譽損失。
- 法律程序費用：包含數位鑑識與調查

Allianz Cyber Protect Premium

- 根據客戶營業項目進行風險分析，擴大因資安事件所引起的損失理賠範疇。

Allianz Cyber Protect Premium Plus

- 根據顧客資安需求進行保單內容調整
- 為顧客資訊系統提供安全評估
- 檢視顧客資安風險與保單內容差距

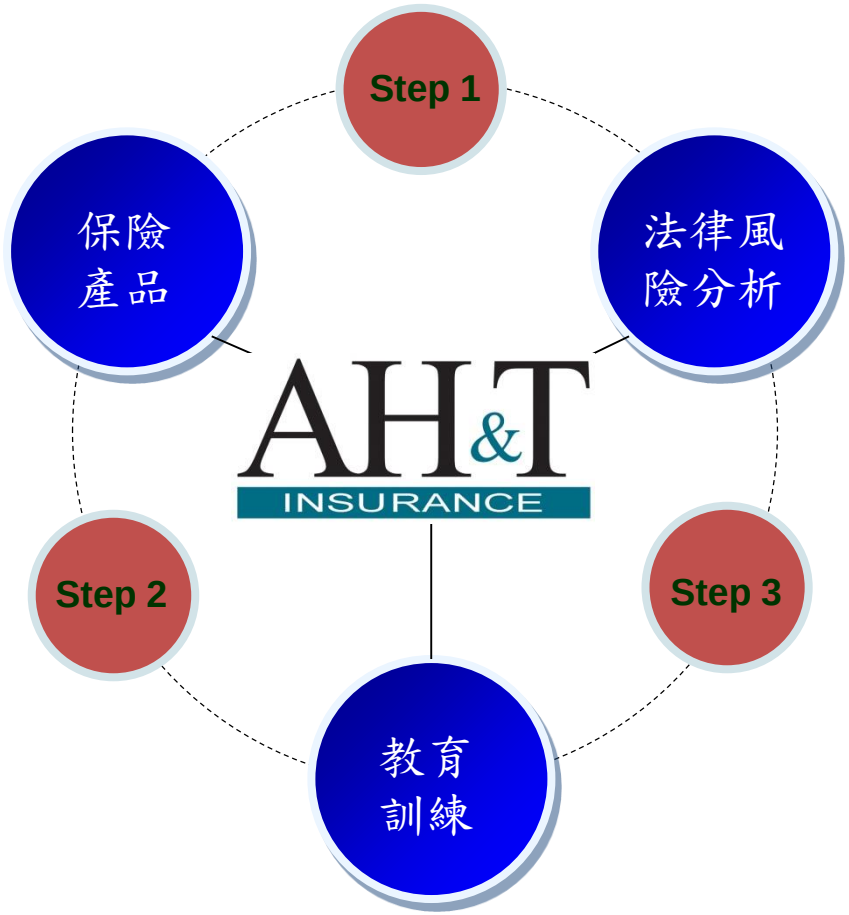
美國-國家國土安全部

- **網路安全保險定義**：為減緩各種資安事件的發生所帶來的損失所設計的保險。
- **邀集各方專家探討國內網路安全保險市場**：近年來，國土安全部(DHS)的國家保護與計劃局(NPPD)整合公與私部門的利益相關者(包含保險公司、風險管理、IT/網路專家、基礎設備擁有者與社會科學家)，檢討現階段的網路保險市場並探討如何有效強化其網路風險管理。

會議日期	會議目的
2012/10	該次會議重點為「第一方」市場企業受到資安事件攻擊的直接損失增加，包含網路相關的重大基礎設施損失。其中，與會者指出**缺乏精確數據與結果導項分析為市場成長的障礙**；同時，指出應以建立有效的網路風險文化為前提以擴大覆蓋範圍。
2013/05	**探討有效網路風險文化當中的「四大標的」：行政領導、目標性的網路風險教育與認知、有效成本技術的投資、相關資訊分享。**其中，與會者提出該四大標的應在企業、企業與會者及國內實施。
2013/11	探討**如何告知企業其重大網路風險與適當的風險管理投資？**其中以健康照護機構提出資安事件為例，該機構如何解決該事件、該事件如何受到影響、促進病人安全的投資(包含網路安全保險)。
2014/04	匯集過去會議資料，於2014年4月提出保險產業工作會議：**創造匿名網路事件資料庫、強化網路事件回應分析、推廣企業風險管理**

資料來源：https://www.gov.uk/government/news/cyber-security-is-essential-in-todays-marketplace與台經院彙整

美廠商執行政府專案投保資料保險



量身定作

1.法律風險分析 Step1

專精於分析廠商執行政府專案可能遭遇的法律風險

2.保險產品規劃 Step2

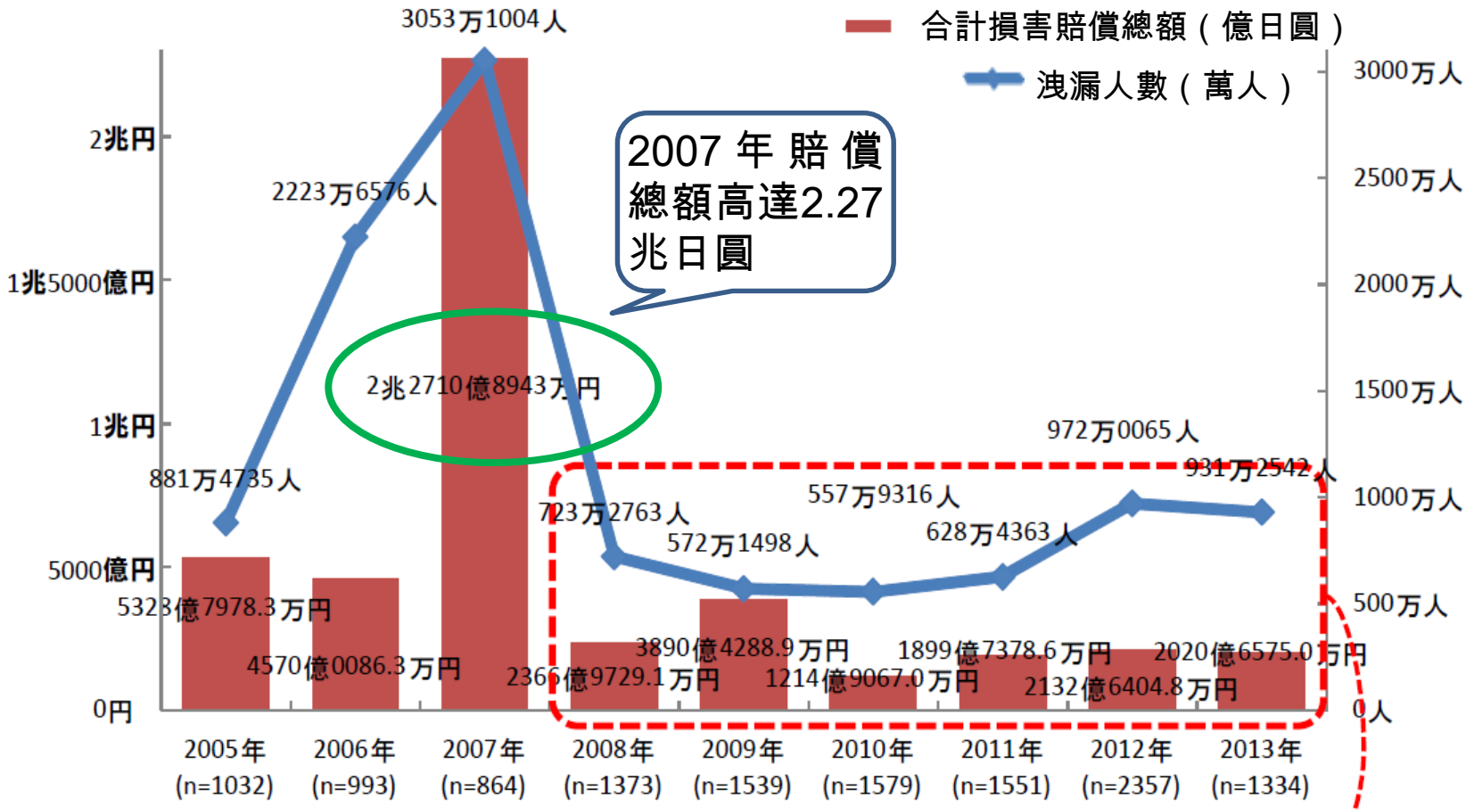
提供各種適用於執行政府專案的保險產品。包括資料責任保險（Cyber liability）

3.教育訓練降低風險 Step3

兼提供教育訓練以供各承保商瞭解相關的風險管理、法規環境與損害控制措施

資料來源：資策會科技法律研究所與台經院彙整

日本2005年～2013年估計賠償總額統計



2007 年 賠 償 總額高達2.27兆日圓

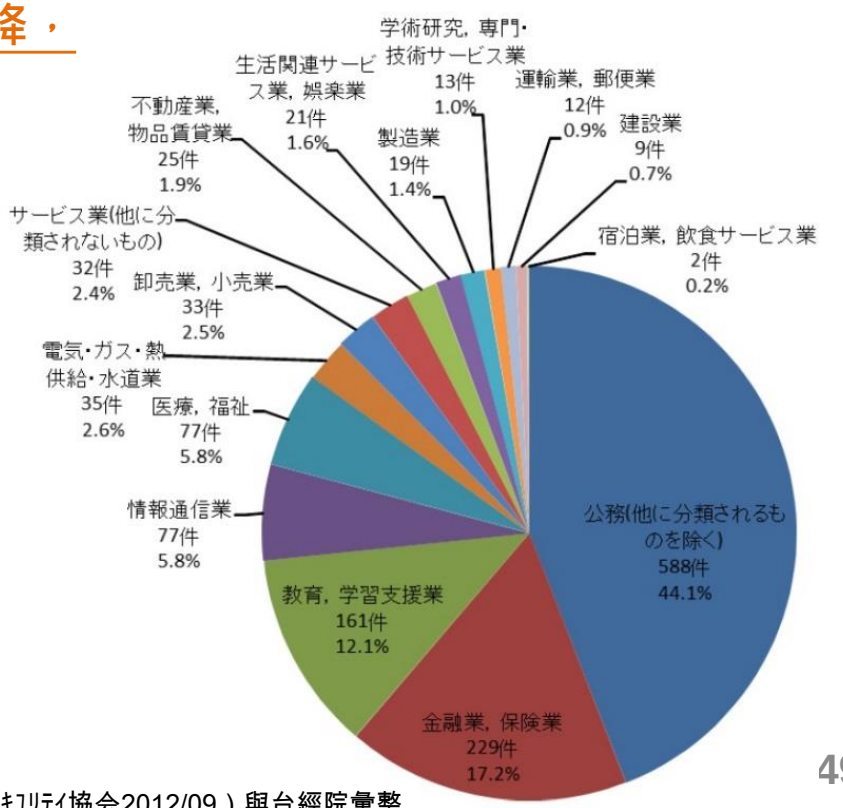
自2010年以來，資料洩漏人數與損害賠償總額呈現微幅增加態勢

資料來源：2013年情報セキュリティインシデントに関する調査報告書（日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会2012/09）與台經院彙整

資安事件發生狀況

- **日本資料洩漏人數與事件數減少**：相較於2012年，2013年發生資料事件洩漏人數下降了40萬7,522人；而發生事件數也減少了約一千件。
- **雖估計總賠償額下降，但平均事件洩漏資料及侵害賠償額卻呈現增加之態勢**：2013年，平均每一事件洩漏資料人數較2012年增加了3,140人；此外，雖該年的總賠償額較2012年減少了約112億日圓，但平均每件侵害的賠償額卻較2012年增加了約6,000萬日圓。
- **雖日本資料洩漏人數、事件數與總賠償額下降，但平均每一事件皆較2012年來得更重大。**

項目	2013年	2012年(比較)
資料洩漏(人數)	931萬2,543人	-40萬 7,522 人
事件數	1,333件	-1,024件
估計總賠償額	2,020億6,575萬	-111億9,830萬
平均每一事件洩漏資料(人數)	7,385人	+3,140人
估計每件侵害賠償額	1億6,024萬	+6,411萬
人均損失承擔	4萬4,628	-1萬6,953

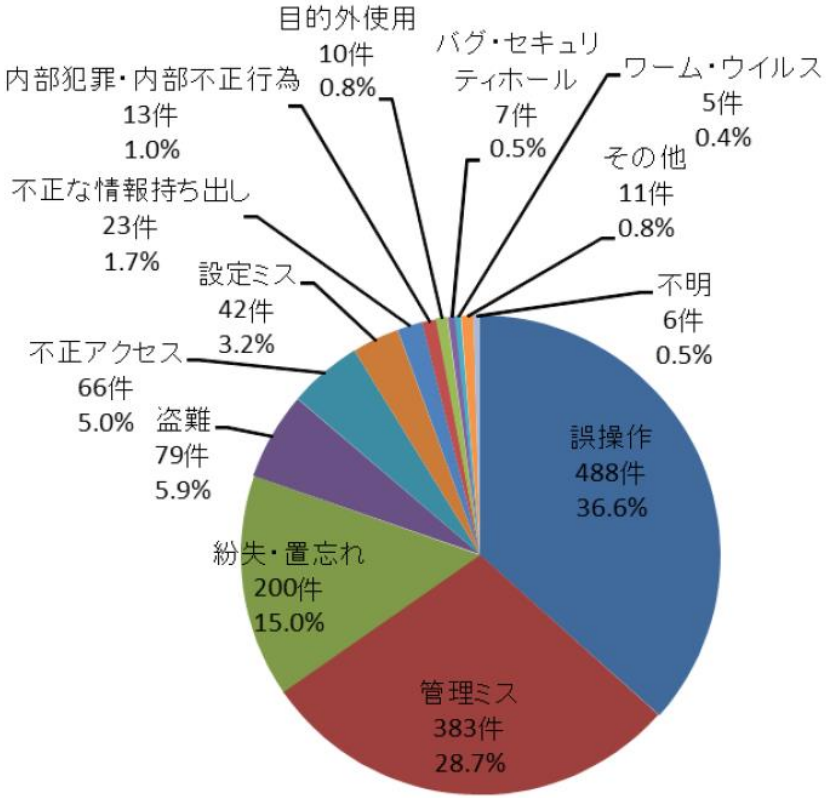


資料來源：2013年情報セキュリティインシデントに関する調査報告書（日本ネットワークセキュリティ協会2012/09）與台經院彙整

資安事件發生狀況

- **日本個資洩漏事件人數以資訊通訊業最多**：2013年發生洩漏事件人數最多的為資訊通訊業，洩漏人數達400萬人；此外，在前十項排名當中，資訊通訊業就占了六位。
- **資料洩漏主因不正確的操作比例最高，達36.6%**：整體資料洩漏事件以不正確操作所導致之比例最高；其次為管理不善，達28.7%。然而在前十項排名當中，則是以錯誤存取為主因所占比例最高。

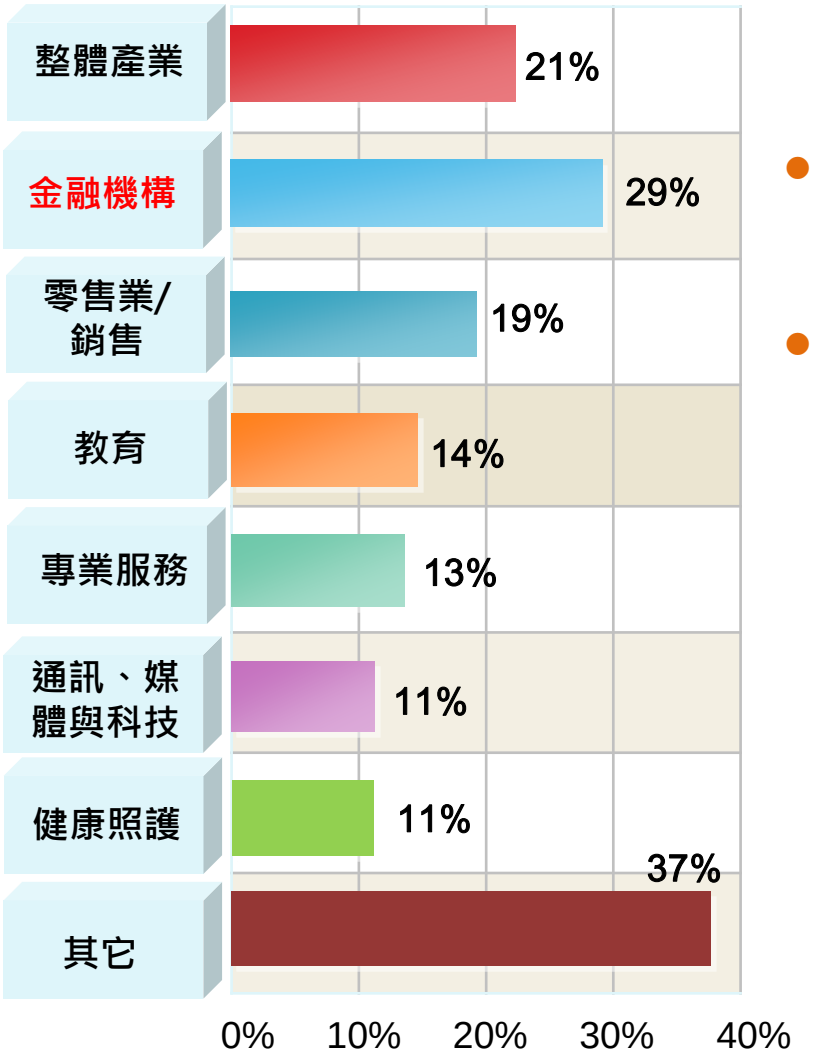
2013年個人資料洩漏事件			
No.	洩漏人數	業種	原因
1	400萬人	資訊通訊業	錯誤存取
2	169萬2,496人	資訊通訊業	錯誤存取
3	47萬人	批發、零售業	錯誤存取
4	42萬人6,000人	公務	遺失、置忘
5	24萬3,266人	資訊通訊業	錯誤存取
6	17萬5,297人	資訊通訊業	設定錯誤
7	15萬165人	批發、零售業	錯誤存取
8	12萬616人	金融業、保險業	管理不善
9	10萬9,112人	資訊通訊業	錯誤存取
10	9萬7,438人	資訊通訊業	錯誤存取



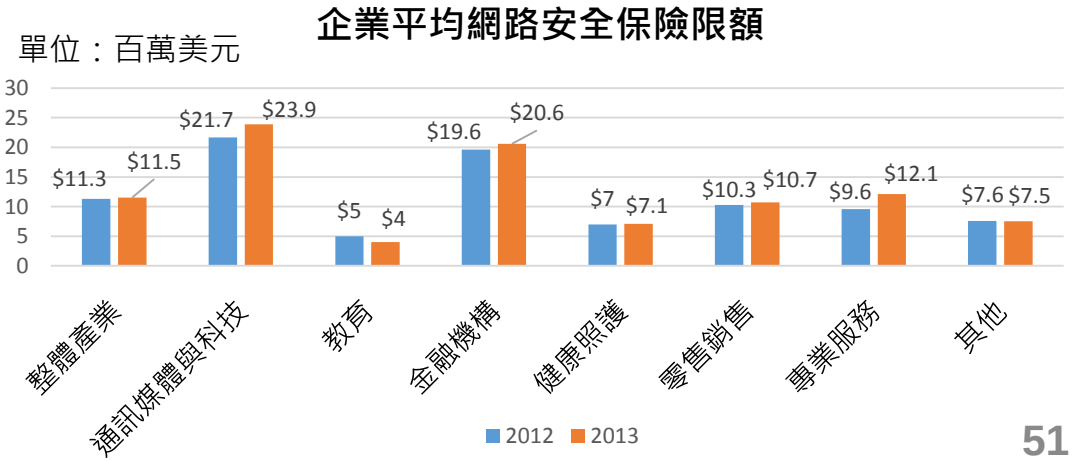
資料來源：2013年情報セキュリティインシデントに関する調査報告書（日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会2012/09）與台經院彙整

美國網路保險市場概況

2013年購買資安保險增加比例



- **2013年美國資安保險整體產業需求比例提高**：相較於2012年，整體企業購買資安保險提高了21%，其中以金融機構比例提升最高(29%)；然在通訊、媒體與科技及健康照護上則呈現小幅提升，約11%。
- **企業平均網路安全保險限額提高**：相較於2012年，2013年整體企業的平均保險由1,130萬提高至1,150萬美元，其中僅在教育與其他產業部份呈現下降之態勢。
- **美國網路安全保險市場成長較歐洲快速**：依據Marsh & McLennan調查報告指出，2013年美國市場已達到7.3億美元，並且估計2014年將高達14億美元。然在歐洲市場概況，其產值僅占美國市場的一部份，約1.5億美元，預計於2018年前將成長至約10億美元。



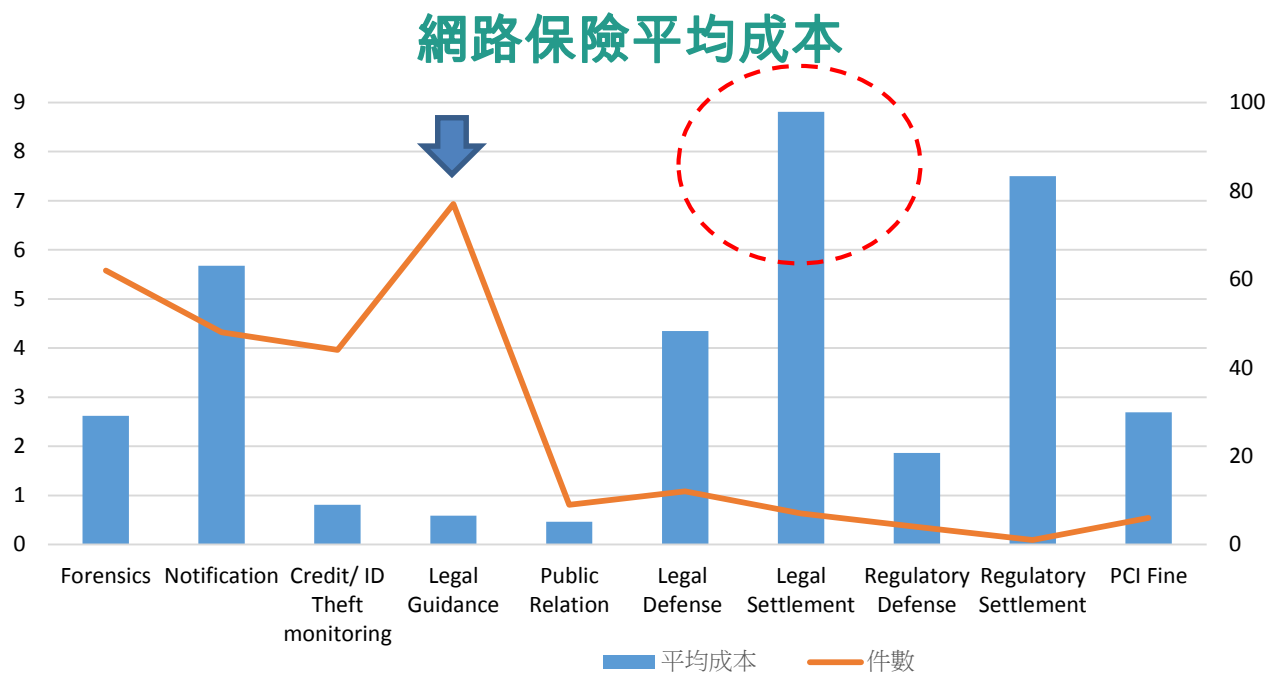
資料來源：Cyber Risks: the Growing Threat, June 2014, Insurance Information Institute與台經院彙整

網路保險平均成本與案例

2015年網路保險以犯罪服務比例最高：2015年網路平均成本一共約673,767美元(相較去年下降8%)，以犯罪服務比例最高，達78%，其次庭外和解與法律辯護則分別占9%與8%。

2021年全球網路犯罪成本將高達六兆美元：

Herjavec 集團（Cyber Venture）委託的研究報告中，預測2021年全球網路犯罪成本將高達六兆美元。



不購買網路保險的原因：

1. 經銷商、保險公司與被保險人間溝通問題
2. 投資在預防措施而非購買保險
3. 保險範圍太多限制也不夠清楚
4. 資訊不足無法做決策
5. 保費過高
6. 申請程序過於複雜
7. 保險承保範圍外之費用過高
8. 損失難以量化

資料來源：Cyber Liability and Data Breach Insurance Claims: a Study of Actual Pay-outs (2013)與台經院彙整