KPMG

2022 臺灣企業資安曝險大調查

台灣企業資安曝險大調查

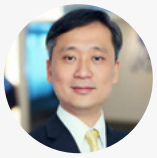
前言

2022 年 9 月臺灣面臨地震高活躍期的風險，而平時不顯露於地表的盲斷層又開始被民眾廣為討論。依據網路維基百科所述：盲斷層是指沒有破裂到地表，因此從地表看來沒有任何異狀的斷層類型，大部分在地圖上也沒有繪製出盲斷層的實際位置，只有當發生突如其來的地震時才可能被人們所發現。而臺灣企業所面臨的資安風險，也有著相似的「盲斷層」現象。

KPMG 安侯建業透過 CEO 2022 outlook 觀察到，臺灣企業 CEO 普遍對組織的資安有著高於全球平均的信心，為了免企業「自我感覺良好」，協助臺灣企業找尋「盲斷層」突破盲點，KPMG 彙集資安各領域專家，發表 2022 年臺灣企業資安曝險調查報告，KPMG 資安曝險大調查針對六大產業，包括金融、半導體、電腦及周邊製造、電子商務、供應鏈核心及新創。透由報告發現台灣本土企業潛在資安風險。報告經抽樣調查 60 家臺灣企業的平均曝險僅為 C 級（70 ～ 80 分），通常具備一般技術的駭客就能入侵。

報告內更進一步揭露許多資訊，如金融業能否延續優異的表現，持續成為臺灣資安領頭羊？新受調產業 (如：新創、電子商務等) 的表現如何？我國總統蔡英文出席 HITCON PEACE 2022 開幕式時表示，提升台灣資安防禦及應變的能力是首要任務。臺灣地處高度敏感地緣政治區域，依據資安廠商調查我國遭受網路攻擊的頻率，已多年為全球之最。KPMG 希望透過這次資安曝險調查，讓臺灣各產業能夠透過駭客的視角，全面性審視企業目前網路防禦現況是否充足、應變人力是否齊備。本次資安曝險報告產業涵蓋範圍較過去擴大許多，也針對產業有更深入地剖析。希望透過這次的曝險調查報告，讓讀者能夠全觀的了解，目前臺灣所面臨的資安挑戰有多麼嚴峻。

針對相關章節內容，如有任何疑問或意見，歡迎您進一步與本調查最後所列聯絡人聯繫。



陳俊光 Jeff Chen
主席 Chairman
KPMG in Taiwan

吳麟 Lin Wu
執行長 CEO
KPMG in Taiwan

目錄

關於本調查

調查作業核心目標

近年來，NFT（Non-fungible token）、De-Fi 乃至加密貨幣等新興科技，顛覆全球對金錢與投資的想像。然而，國際間對創新應用的不熟悉，成為駭客能趁虛而入的途徑，導致業界之資安事件頻傳。無獨有偶，我國更因台海局勢升溫，資安事件層出不窮。為了進一步剖析與瞭解臺灣企業目前的數位曝險狀態，KPMG 著手蒐集有關臺灣指標企業針對網路安全環境的資料，包含 2022 年重點產業及組織網路曝險的現況與趨勢，彙整並製作成此份調查。讀者閱讀本調查後，我們期盼能帶來以下效益：

1. 量測全面網路風險

不同於市面上一般的技術性量測工具，本調查增加資安 13 項技術檢測，除了資訊安全的技術分析外，也量化資安人員配置，讓企業了解其有形及無形的風險。

3. 配置合理資安預算

了解指標產業平均的資安風險，讓讀者能有依據地在其組織做網路風險評鑑，並在人力、預算許可的範圍內，訂定合理的可接受風險值，有助於替潛在的風險訂定改善計畫，並在考量所需預算、優先順序、時程與負責人後，以最少的資源處理與改善這些風險。

2. 比較產業資安現況

依據企業營運特性，將檢測的 60 家企業分成六大產業，可以結合產業趨勢做更精準的分析，真實地掌握同產業、委外 / 合作廠商所屬產業，了解各產業曝險控管情形。

4. 部署資安防禦策略

呈現內、外部各面向的檢測結果，再針對普遍有待加強的項目給予深入剖析與建議，輔助讀者制定內部網路管理的策略。

調查報告核心效益

對於相關企業管理者與專業 IT 人員，透過本調查我們期待可以分別帶來以下收穫：

1. 董事會 / 執行長 CEO/ 經營管理高層：

企業管理高層可透過本調查，了解同產業的網路曝險程度及管理現況，以制定相關政策與編列經費、建立「最高層級定調(Tone at the Top)」的資安承諾，創造具資安觀念的文化並貫徹於全組織。

2. 營運長 COO/ 風控長 CRO / 數位長 CDO/ 資安長 CISO：

根據《2021 台灣 CEO 前瞻大調查》，在 COVID-19 下，企業仍持續對數位科技進行資源投入，受訪 CEO 票選最重要的投資項目即為「數位網路安全風險」。企業資訊與風險管理高層，可透過本調查了解企業常見的安全、隱私漏洞，並研發或部署最新科技與技術，對症下藥進行資安防護。此外，管理者將可以呈現量化的資安風險，與整體員工、廠商、客戶教育與溝通，有效提升整體公司的資安知識與意識。

3. 財務長 CFO：

資安事件可能造成營運延宕與法遵罰款等巨額財損，而事件揭露於媒體與財報，將嚴重損害組織聲譽與利害關係人之信任。本調查全面量化企業於網際網路的數位資安風險，讓 CFO 能依此量化數據，衡量組織的資安策略與相關投資，有效規劃未來的預算，以降低直接與間接的數位風險。

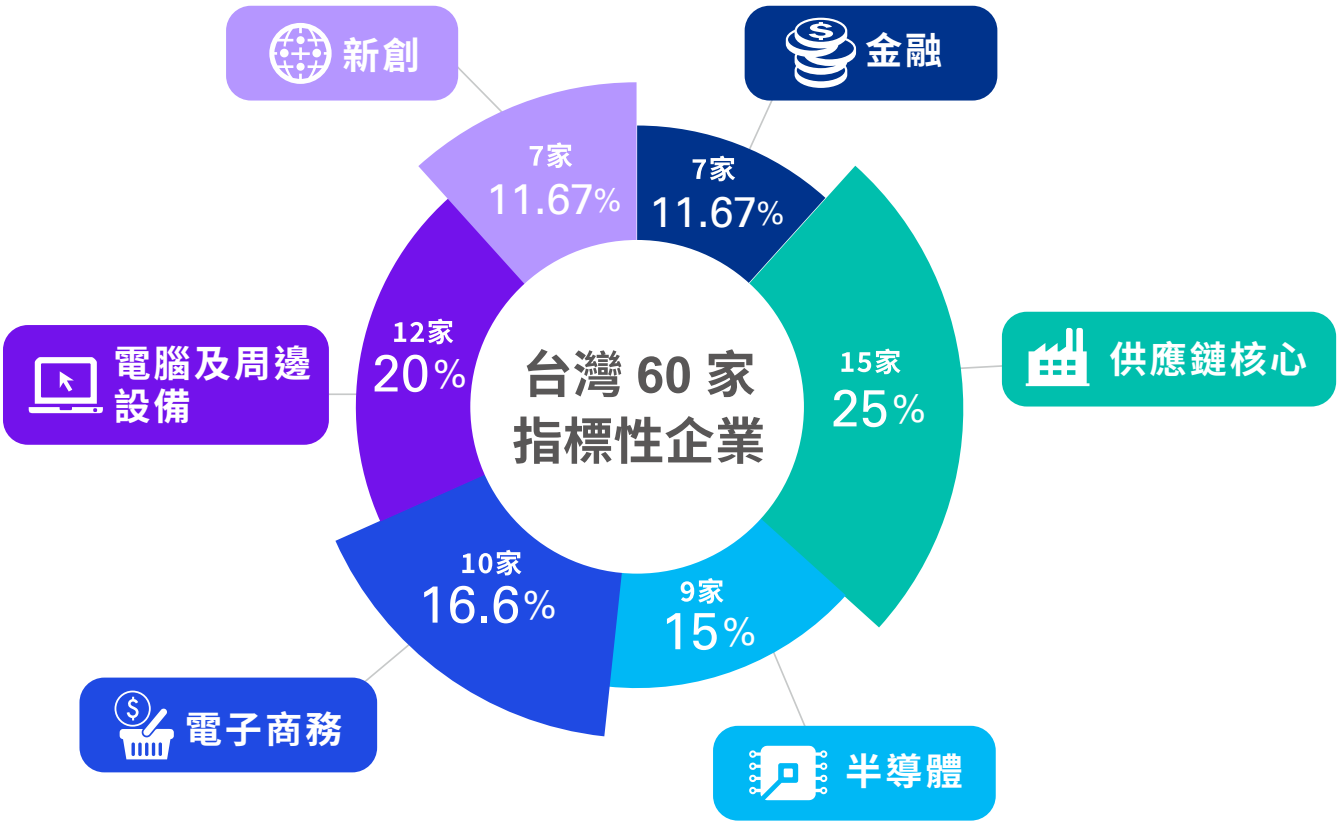
4. 資訊管理、資安及數位應用技術相關人員

透過本調查，資訊管理、資安與數位應用相關技術專員可以將整體環境、所處產業分別做為基準，與自己組織內的資安狀況進行觀察與比較，以採用合適的技術維護組織的資安環境。

企業調查範圍

KPMG 以富比士、證交所及臺灣近年新創競賽所列企業為母體，結合 KPMG 豐富的風險評估經驗，依據本次調查範圍之六大產業 (電腦及周邊設備、半導體、電子商務、新創、供應鏈核心與金融) 進行分層隨機抽樣。

KPMG 參考近年來國外與國內所發生的產業重大資安事件為借鏡，我們觀察到某些特定產業於發生資安事件後，會對其他相關產業發生全面且深度的影響。而其中原物料與運輸產業更是扮演起串連整體產業的重要角色。所以 KPMG 於本次曝險報告中特別針對原物料及運輸業所組成的「供應鏈核心產業」進行資安曝險調查，期待能夠透過挖掘目前曝險狀態，提供「供應鏈核心產業」強化與固守方向。



資安曝險評估方式

本調查廣泛、充分蒐集網際網路上資安風險情資，評估台灣企業的真實曝險程度。有別於傳統企業內部執行的資安風險評鑑、弱點掃描或滲透測試演練等活動，以及其他問卷調查，本調查的特點為：

- 以外部多元大數據情資蒐集為客觀調查依據
- 揭露更廣泛、具體的臺灣關鍵產業網路曝險實況，並以整體供應鏈或產業視角進行深入分析。
- 以非入侵式、自動化的智慧型工具執行，兼顧調查的有效性與可信度。
- 曝險評估同時考量資安技術、企業內部人力資源風險向及企業於暗網之名聲。
- 因應法規設立資安長及專責資安人員之趨勢，同時以近期資安事件進行說明。
- 探討企業是否取得國際資安標準認證對於實際資安防護能力之效益。

	本資安曝險調查	弱點掃描	滲透測試
侵入式檢測	否	視情況而定	視情況而定
資料提供	**網域名稱**	URLs、IP (視情況增加測試用帳密)	URLs、IP (視情況增加測試用帳密)
檢測手法	**自動化工具檢測**	自動化工具檢測	手動組合式攻擊
檢測範圍	**外部的網際網路風險**	內部的資安漏洞	內部外部潛在的資安漏洞
評估面向	從網路多面向進行分析 例如 **應用安全性、人力資源風險等**	大範圍偵測主機設備漏洞 例如 Injection、XSS、Security Misconfiguration	透過組合技驗證商業邏輯漏洞 例如 權限跳脫、目錄瀏覽、URL 重新導向等漏洞

技術檢測項目及分數含意

將技術檢測得出的網路防護分數，以每十分為一級距，分為 A、B、C、D、F 五個等級，提供讀者一個更直觀、易懂的衡量標準。

等第	分數範圍	說明	資安定義
A	90 以上	卓越	需要世界一流駭客才能侵害
B	80~90	良好	要豐富經驗的駭客才能侵害
C	70~80	普通	一般的專業駭客就可侵害
D	60~70	需改善	入門駭客即有機會侵害成功
F	60 以下	亟待改進	會寫基本網路程式的初學者就可能侵害

本調查所評估的 3 大面向與 14 項檢測項目

應用面安全
Application

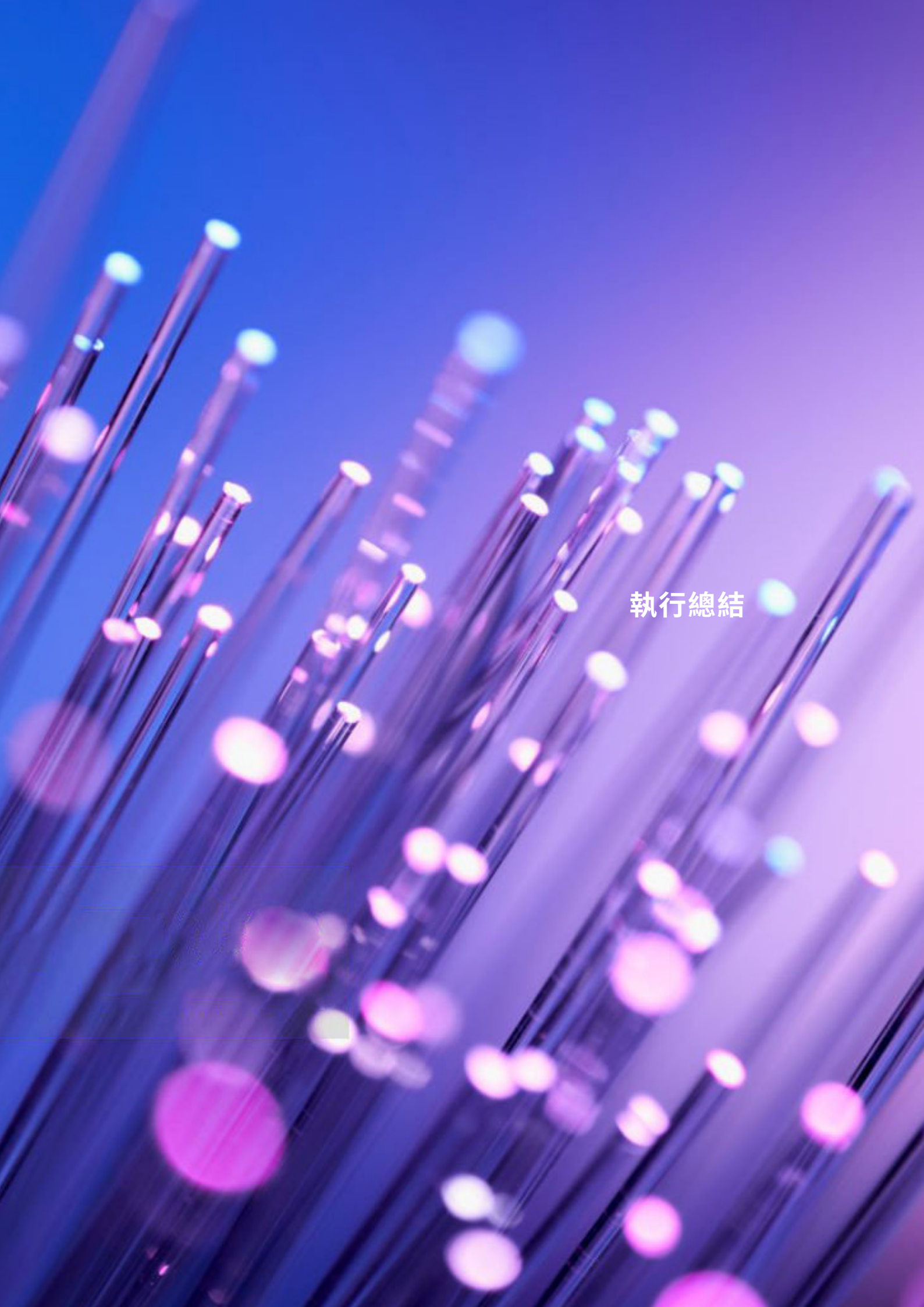
- **應用程式風險**
  Application Security
- **網域安全**
  Domain Attacks
- **服務暴露風險**
  Exposed Services
- **技術風險**
  Technologies

人力資源風險
Human

- **資安事件回應力**
  Responsiveness
- **網攻承受力**
  Employee Attack Surface
- **資安團隊戰力**
  Security Team
- **社群媒體風險**
  Social Posture

網路與科技風險
Network and IT

- **資產聲譽評量**
  Asset Reputation
- **雲端服務風險**
  Cloud
- **域名解析風險**
  DNS
- **電子郵件與網路加密風險**
  TLS、Mail Server
- **網頁系統風險**
  Web Server



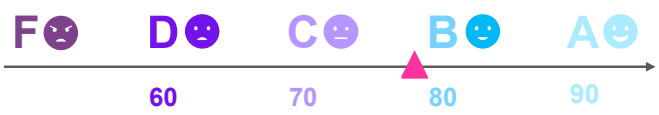
執行總結

調查結果縱覽

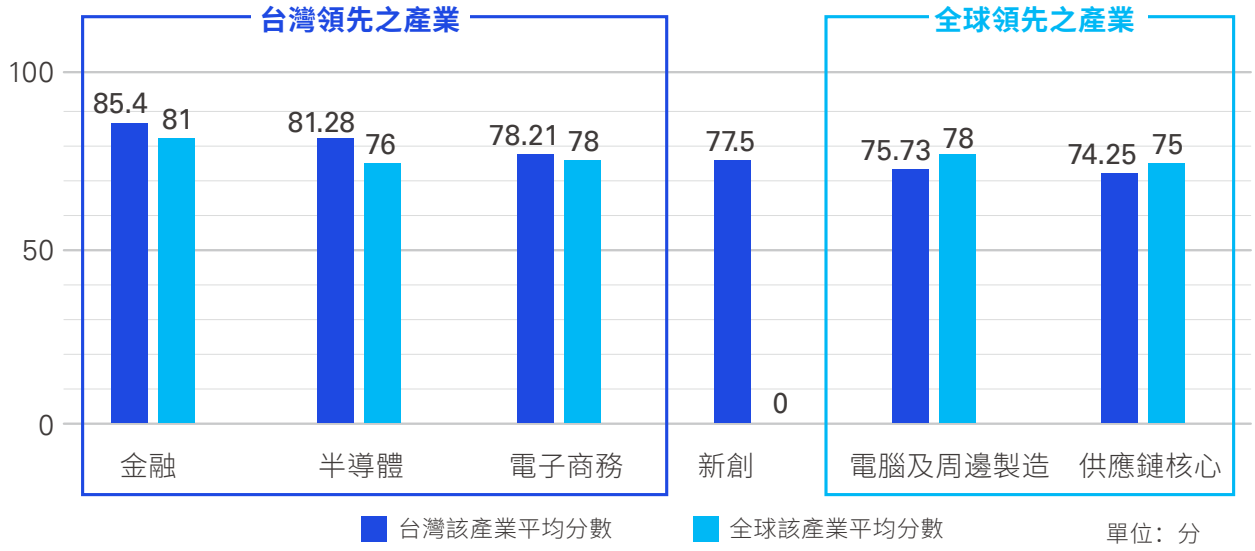
分數 低 高

資安曝險評估項目	評估說明	臺灣60家受調企業
應用面安全	應用程式風險	
	網域安全	
	服務暴露風險	
	技術風險	
人力資源風險	資安事件回應力	
	網攻承受力	
	資安團隊戰力	
	社群媒體風險	
網路與科技風險	資產聲譽評量	
	雲端風險	
	域名解析風險	
	電子郵件風險	
	網路加密風險	
	網頁系統風險	

平均網路防護分數 C (78.72)



臺灣受調企業平均繳出 C 級的防護成績單，持續面臨高度網路風險，亟需改善內部的資安現況。



註：由於新創產業組成繁多，於調查中尚無法顯示全球平均分數。

調查主要發現

1

❶ 多數企業輕忽社群媒體所衍生的網路攻擊

大部分企業都擁有社群媒體的專頁，且員工也非常容易於社群媒體上暴露自己的公司聯絡資訊，導致駭客發動魚叉式精準社交工程時，成功得手機率大增。

2

❷ 臺灣各產業資安人員能量均嚴重不足，企業資安人力亮警訊

臺灣企業在人力資源風險 (Human) 中，於「資安團隊戰力」相關成績顯示，資安人力缺口十分明顯。60 家受調企業中，經外部情資分析顯示，就可能有高達一半以上企業未配置 CISO 或資安人員。

3

❸ 供應鏈核心產業亟需加強網路防護

原物料、運輸等供應鏈核心產業，不僅在平均網路防護分數墊底，該產業更有高達近 50% 的企業落在整體排名的倒數 15 名，網路防護亟待加強。

4

❹ 金融業網路防護表現仍最佳，但面臨高度挑戰

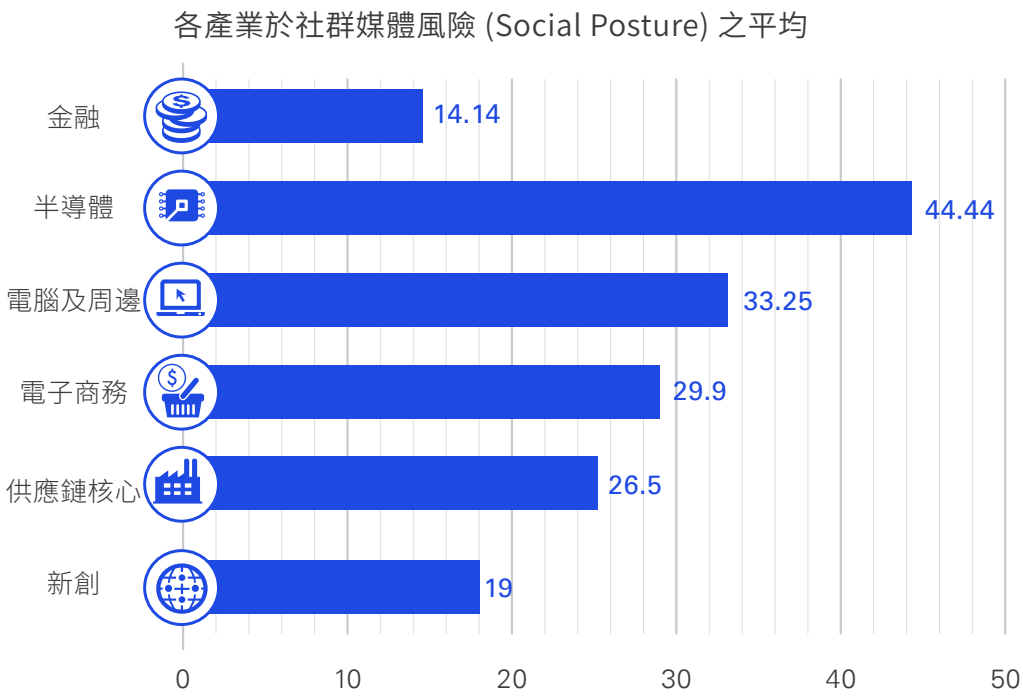
金融業於各面向（應用程式、人員、網路與科技）的平均分數皆取得優異的成績。但因金融網路犯罪利益巨大，讓金融業今日仍飽受內外部威脅與挑戰。

5

❺ 導入並驗證資安國際標準，將顯著降低資安曝險

本調查發現取得國際資訊安全認證能顯著的提升資安能力，根據分析調查結果發現，在 60 家台灣企業中，其中有 21 家企業有取得國際資安管理標準認證。對比曝險分數可以發現，成績越高的群組，導入並驗證國際資安標準的比例越高。

❶ 多數企業輕忽社群媒體所衍生的網路攻擊



本調查發現於受調企業中，不論是哪個產業都深陷行銷管道所帶來的數位曝險，其主要的曝險因子來自於社群媒體的控管。我們在社群媒體風險 (Social Posture) 檢測中，所有產業都繳出了不及格的成績單 (平均：29 分，F 等級)。

主要原因是目前多數企業大量運用社群媒體 (如 Facebook, Twitter, LinkedIn 等) 觸及受眾，而有意或無意地留下公務聯絡訊息 (如電子郵件、電話等)。另一原因是員工於註冊社群媒體時，時常將目前服務之企業名稱、公司電子郵件等資訊，提交於社群網站的個人資料上。此類行為，讓員工相關資訊十分容易取得，使駭客能輕易發動魚叉式社交攻擊，且可透過社群媒體推論企業電子郵件帳號之命名規則，不可不慎。

另外，本調查意外地發現六大產業中平均分數最低之產業屬金融業，平均僅得 14.14 分。由於金融業大量透過社交媒體來發布其最新資訊，像是新興金融服務、最新理財商品、更新的金融相關政策與徵才資訊等等，而上述這些公告資訊皆需留下公務聯絡訊息。因此，金融業須特別謹慎運用社群媒體，並提供員工相對應的資訊安全教育訓練，以提升員工資安意識，改善媒體曝險情形。

KPMG 建議

1. 建議組織對於社群媒體控管應制定社群媒體管理政策，且至少每年檢視一次，此外應制定社群媒體使用守則，明確列出可接受使用的社群媒體、功能及使用規則，且同時規範在社群媒體上言論發表。

2. 組織應針對社群媒體運用制定妥適管理規範，並透過資安縱深防禦策略、Anti-spam 等機制，於有效的控管社群平台上之資訊前提下，行銷與推廣相關數位服務，並防護企業員工之電子郵件帳號安全，避免員工個人登入資訊 (Credential) 遭到竊取，引發後續更嚴重之後果。

❷ 臺灣各產業資安人員能量均嚴重不足，企業資安人力亮警訊

臺灣企業在「人力資源 (Human Resource) 風險」評比大項中，於「資安團隊 (Security Team)」相關成績顯示，臺灣各產業資安人力缺口十分明顯。

資安曝險分數三大面向

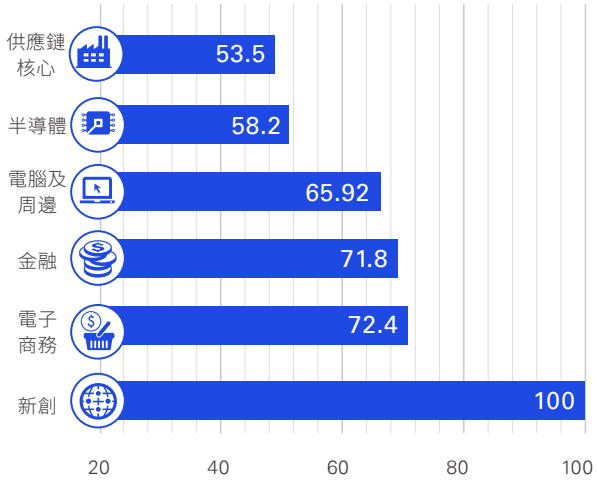
應用面安全
Application **84.5**

網路與科技風險
Network and IT **81.5**

人力資源風險
Human Resource **62.5**

人力資源風險：包含資安事件回應力、網攻承受力、資安團隊戰力及社群媒體風險等評估項目

各產業於資安團隊 (Security Team) 之平均



* 新創產業因受調企業僅有原配置，其餘企業均為 N/A 之數值故分數較高。

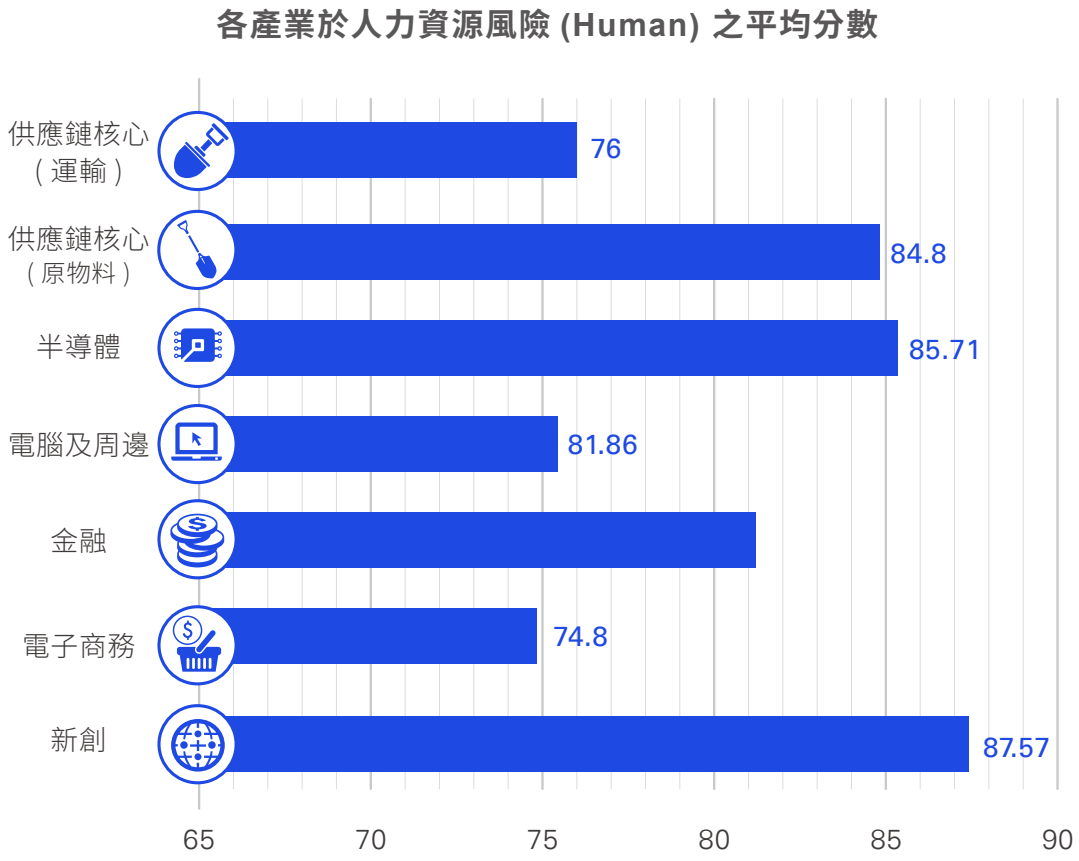
本調查從公開資訊中蒐集並分析相關資料發現，受調產業中僅有金融業與電子商務兩大產業的資安團隊達 70 分以上（等級：C 級），其餘產業分數皆較為落後。

再深入探究表現較好的兩產業，相較於金融業，電子商務雖於此項目取得較優異的分數，然而在此產業的受調企業中，有超過一半的企業缺乏成績 (Not Applicable)，探究原因為其網際網路的公開資料有限。反觀金融業，自 2021 年 9 月金管會修法，明文要求符合條件之金融業者配置資安人員。在主管機關的強力要求下，金融業於資安團隊實力可說是脫穎而出，成為其他產業學習之標竿。

分析近年金融業主管機關針對資安長的設立標準，除了銀行業者外，達到一定條件與規模的保險公司、證券商、期貨商與投顧業，以及大型或從事電子商務之上市櫃公司也都必須設立資安長及配置適當數量之資訊安全員及設備，並明定將資安管理、事件影響與因應納入公司年度報告。

資安長成立的趨勢，體現今日企業對於資安態度的轉變，從過去遭遇資安攻擊事件後才有所改善的被動應付，轉為現在的主動正視、防患未然的態度。資安長職責包括下列事項：

一、對外掌握目前的資安威脅最新動態，對內控管其系統與組織人員，確保企業內部資料的存取管理控制與漏失預防，達到有效的資安治理。
二、協助 CEO 和董事會了解企業營運的潛在資安威脅，以協助推動企業內部資安策略，並提升內部人員資安意識。
三、資安長能夠協助組織在面對資安攻擊時即時回應威脅，並針對事後進行內部檢討與弱點改善。



本調查在人力資源風險分析項目中，亦將企業登入資訊洩露 (Compromised Credential) 的威脅納入評比，其主因為駭客透過自動化攻擊，可能掌握大量的使用者登入資訊，透過這些登入資訊去猜測企業中可能的既有使用者是否存在，造成使用者資訊遭受未經授權的存取。此一行為在資安產業中稱之為「撞庫」。

以 2021 年 11 月發生的證券業遭受駭客「撞庫攻擊」事件為例，所謂「撞庫攻擊」(credential stuffing attacks) 指的就是駭客將其他已得手的使用者登入資訊，去嘗試登入其他產業的線上服務平台，包含安全保護層級較高的銀行業、證券業，若撞庫後導致該使用者資訊登入成功，等於讓駭客掌握萬用鑰匙，廠商或使用者亦較難察覺異狀。

由此可見，今日企業資安問題已無法自掃門前雪，一家企業的資安漏洞可能危及整個產業。

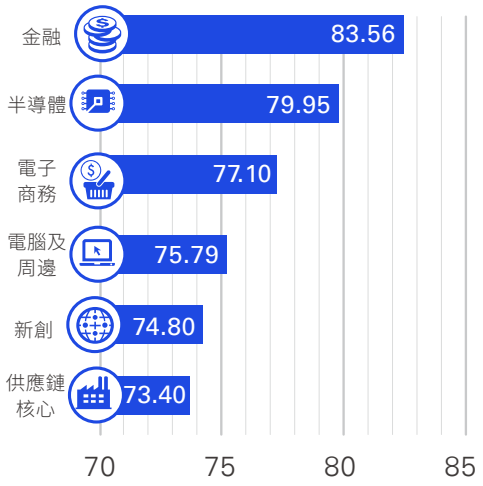
因此，呼籲企業皆應設立資安長與資安團隊，落實企業整體的風險控制，正視目前組織的資安威脅，讓產業生態圈資安防護更加完善。

KPMG 建議

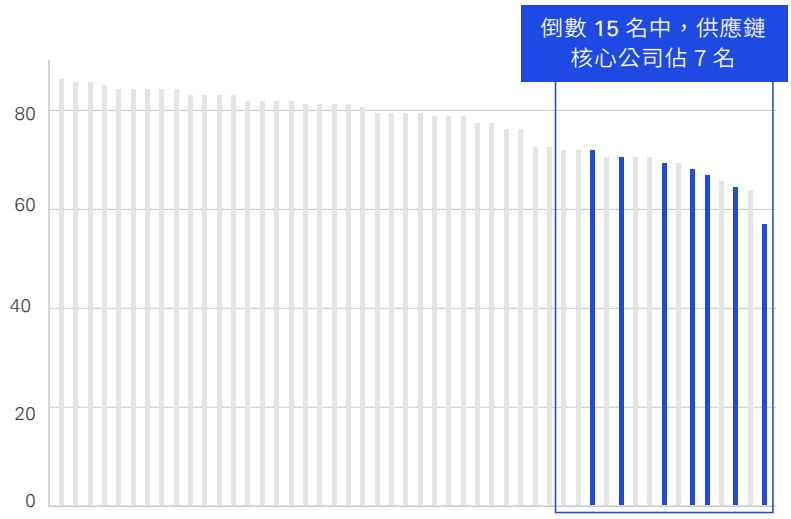
1. 不論所屬產業，都應評估自身規模與資源後，設立資安長與資安專責人員，並明確定義其職責。
2. 企業應設立之職直接回報與對應企業內部高層，如董事會等，以利高層能全面掌握整體企業資訊資產相關疑慮、強化措施與危機應變等。
3. 企業應提供內部員工適當的資安教育訓練，藉以加強員工資安意識，並定期辦理如攻防演練等測試，增強第一線資安事件通報與危機處理人員的能力。

❸ 供應鏈核心產業亟需加強網路防護

網路防護分數（依產業區分）



供應鏈核心產業之分數分布圖



本調查發現原物料、運輸等這類供應鏈核心產業資安實力參差不齊、落差極大，且超過 60% 的受調企業分數位居 C 級以下，雖然少數公司 (2 家位於前五分之一) 表現出眾，但多數企業之資安防護能力卻有待加強。

推測其可能原因，為上述產業因近年開始導入大數據與人工智慧等新興科技，智慧應用大幅增加，網路架構更為複雜、系統軟體未能即時更新與升級等情況下，導致駭客有機可乘。KPMG 也因此建議原物料、運輸業等供應鏈核心產業，在享受數位化的美好果實時，更應努力提升其網路防護作為。

本報告發現此產業內的企業，與其它產業相比，於「人力資源風險」檢測項目中能力相當，但在「應用面」和「網路與科技風險」兩大項目中，供應鏈核心受調企業卻有相當大的等級差距。

經本調查逐一探究兩大項目，在「網路與科技風險」中 域名解析風險 (Domain Name System, DNS)、網路加密風險 (TLS) 與電子郵件風險 (Mail Server) 三大檢測項目 ，總分位於前段企業與後段企業相差甚大，皆有將近 2-3 個等級 (20-30 分) 之差距；而在「應用面安全」中則是技術風險 (Technologies) 的漏洞檢測，其詳細檢測內容會於後面章節提及，總分位於後段企業多半為未定期落實軟體版本之更新、關注最新且積極修補漏洞、未使用密文傳輸可能敏感之資訊（如：未使用 HTTPS）等弱點漏洞，甚至未確實驗證身份，以及準確落實權限控管，導致其易成為攻擊或釣魚網站之中繼站。

除了上述檢測項目以外，本調查探究此產業內部企業之資安實力，發現總分位於前半企業幾乎皆取得 IS0 27001 國際認證資安標準，並成立資安小組負責定期向董事會報告公司資安事務。

透過公開資料分析，後半企業對於上述項目皆無在年報內明確表示。此外，前半企業皆於公司年報中詳述資安管理內容，可見資安防護能力的推動若能被企業高層重視且以國際標準為基準發展與加強，能更有效率且有效的提升實際資安防護能力。

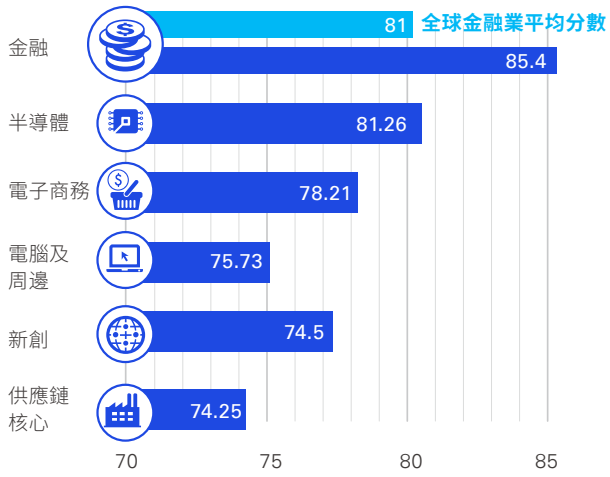
KPMG 建議

1. 供應鏈核心產業中的企業通常歷史較為悠久，在傳統觀念的長期洗禮下，也較難接受流程大規模改動與快速深植資安意識。

   因此本調查建議可採取補償性控制措施，針對資訊資產的不足或缺陷，額外補充安全控制措施或強化安全控制措施，像是為資訊系統及系統所處理、儲存或傳輸之資訊，提供較安全的加密演算法，防止機敏資料外洩，以利降低資安曝險因子。

2. 組織應透過適當縱深防禦架構，保護重要資訊資產，像是透過建立定期清查帳戶權限、軟體清查與更新的流程做好內部存取控制；抑或是企業採取零信任架構，兼併多因子驗證等方式，建立完善的資料防護機制，避免資料外洩或遭竊取，藉此顯著提升資安防護。

❹ 金融業網路防護表現仍最佳，但面臨高度挑戰

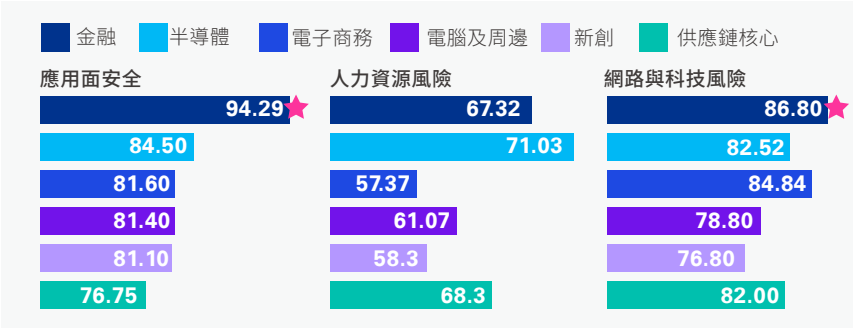


金融業在網路防護分數的三大面向中，不論何種評估面向均取得了相較全產業表現優異的成績。其中臺灣產業表現有待加強的「網路與科技風險」，金融業仍維持超過 86 分的高水準，更高於全球金融業平均分數 (81 分)。

分析國內金融業普遍成為「績優生」，是因為主管機關的高度監理及產業的自律性。在違反金融法規時，除了將遭重罰，信譽下降、創新服務無法順利上線等因素都將造成重大營收損失，因此讓金融業成為遵守資安秩序的模範生。

金融業三大檢測面之平均分數

應用面安全 Application	94.29
網路與科技風險 Network and IT	86.8
人力資源風險 Human	67.32



雖然金融業資安能力普遍高於其他產業，然而金融業擁有含金量極高的資訊與資產，近年又廣泛使用金融科技、開放金融資料並與多元的第三方合作而擴大曝險層面，因此至今仍為駭客集中精力攻擊之標的。國際機構研究報告即指出，金融業受到網路攻擊的可能性為其他業的 300 倍，且每年攻擊數都在攀升，而全球金融企業每年平均承擔網路犯罪的成本更是高達 5.28 億新台幣。

經本調查分析，金融業在各面向的成績表現都最好，在「網路與科技風險」檢測項目中，包含網路加密風險中的憑證安全、一般性技術風險，以及網頁伺服器檢測項目裡的安全設定（Content-Security Policy, CSP） 與跨網站指令碼 (Cross-Site Script, XSS) 的高風險漏洞，平均有近 20 個風險注入點可供駭客所利用，即便金融業普遍為「模範生」，對於上述的技術漏洞仍需修補或加強控管。

在主管機關的高度監理下，金融業更應審慎的面對與處理其資訊系統，更需持續強化相關資安政策、資通安全事件回應計畫與主管機關通報規範等，在發生資安事件時，依據相關程序進行通報，避免遭受重罰、信譽下降、創新服務無法順利上線等狀況。

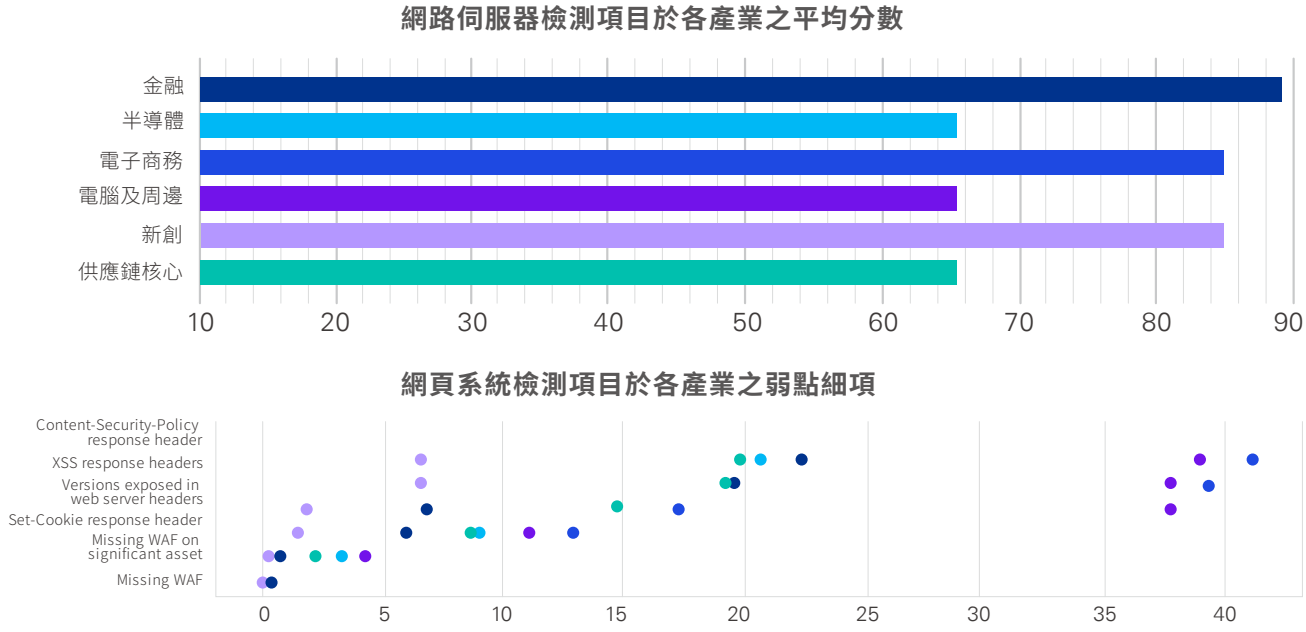
KPMG 建議

金融業應更加重視域名解析伺服器與郵件伺服器的安全管控，管控良好則可透過資料比對、安全認證等步驟，避免客戶連結到詐騙網站、過濾惡意連結，並確保重要客戶與機敏資料安全無虞。

資安風險趨勢

技術弱點與精進方向

❶ 網頁系統風險



檢測說明

檢測企業網頁伺服器(Web Server)是否建立CSP(Content-Security-Policy)、XSS(Cross-Site-Scripting)和Cookies的Response Headers與揭露其版本配置之風險，以及利用工具檢測其應用程式防火牆(Web Application Firewall, WAF)設置。

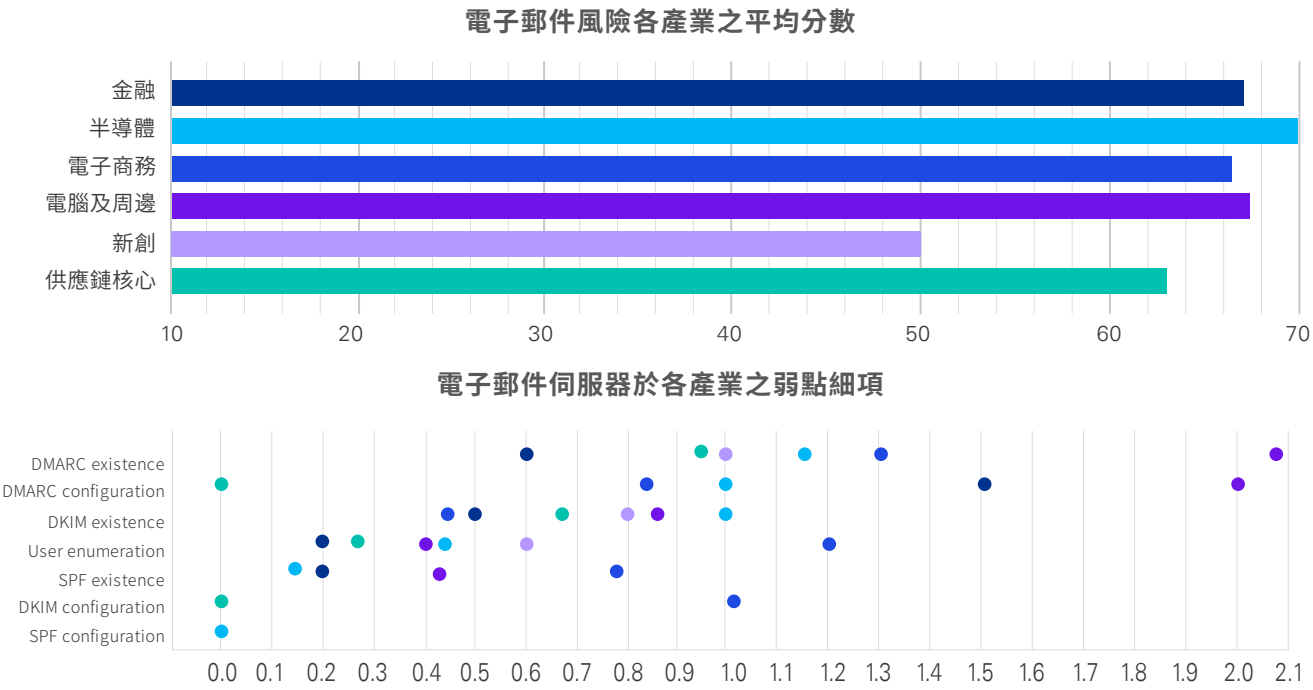
企業現況

企業的網路伺服器皆有支援內容政策(Content-Security-Policy,CSP)，以此告知瀏覽器的請求位置是否值得信任，並加載瀏覽器信任的來源，有效阻擋不明的對外連線；而跨站腳本(Cross-Site-Scripting,XSS)Response Headers設置當偵測到XSS攻擊時可停止載入。根據本調查報告發現，大多數企業皆缺乏設置網站的CSP與XSS的Response Header，甚至不經意揭露其版本配置，如此一來便會增加駭客對於企業網站攻擊的可能性，導致資安曝險程度提升。除了金融業以外，此風險平均分散在每個產業中，而這些高風險的漏洞，企業都應需特別關注。

KPMG 建議

1. 企業於開發網站系統時應於開發階段，即考慮相關資訊安全設置是否影響網站系統運行，以透過設定建立有效的CSP與XSS Response Headers，阻擋惡意人士所設立之不明網站連線。
2. 透過企業既有之資訊安全防禦縱深及妥善的布建網頁防火牆(WAF)，藉此降低駭客入侵之風險與資訊安全的曝險程度，防範一般駭客的工具腳本攻擊。

❷ 電子郵件風險



檢測說明

經由全網域掃描器蒐集檢測受測標的企業之電子郵件伺服器是否實施 SPF(Senders Policy Framework)，DKIM(DomainKey Identified Mail) 與 DMARC (Domain-based Message Authentication, Reporting, and Conformance) 的設定與配置。

企業現況

郵件往來是駭客最容易攻擊的目標，商業郵件攻擊已經成為駭客常用的手段之一，透過寄送釣魚信件來間接取得使用者的帳號與密碼，進而駭入企業的系統，導致個資外洩，或是企業需支付相對應贖金贖回加密檔案等重大資安災情，造成企業財務上與名聲的損失。

因此郵件伺服器中的 SPF、DKIM 與 DMARC 的認證及配置皆是非常關鍵。根據本調查發現，相比去年資安曝險報告，郵件伺服器於今年的調查屬於 14 項技術檢測中配置與設定較不健全的項目之一，容易導致資安曝險程度提高；本報告調查的六個產業中，屬新創與供應鏈核心兩大產業面臨此一風險最為嚴峻。

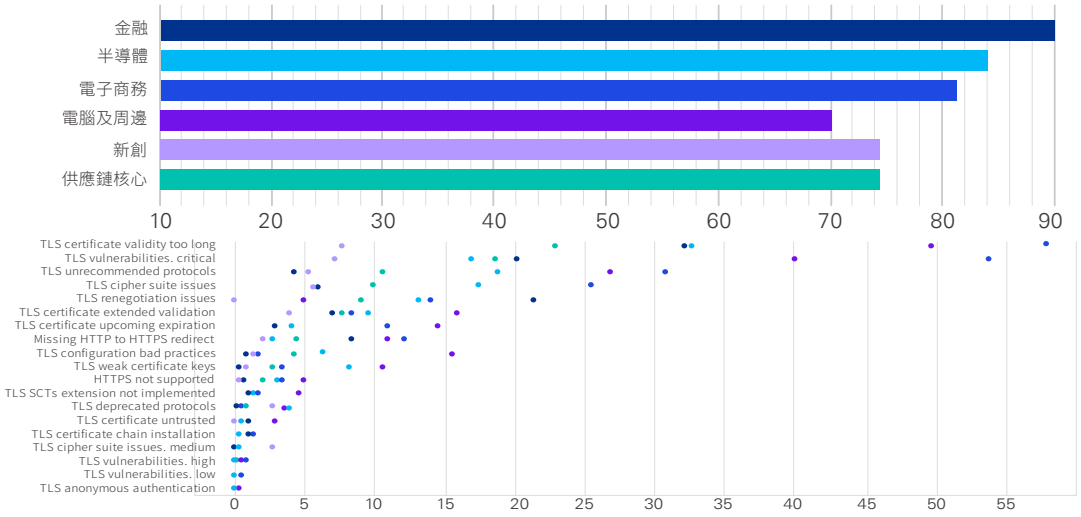
倘若未實施郵件伺服器中的設定與配置，駭客便能假冒企業網域名發出郵件，以此進行電子郵件詐騙或是發送網路釣魚郵件等。其中供應鏈核心除少數企業外，多數較不重視電子郵件伺服器安全，導致整個產業平均分數低下。

根據本調查發現，電子郵件風險主要問題為DMARC 的配置。除了郵件伺服器中最基本的 SPF 與 DKIM 的配置以外，DMARC 為防止勒索病毒第一道防線，實施 DMARC 能有效檢測收到的訊息是否來自認證過的一方以及其簽名認證，並有效攔截釣魚信件或是詐騙郵件，以此對郵件進行監控與管理。假若未通過驗證時將會觸發 DMARC，針對未通過驗證的郵件傳送完整的報告，以利改善與監控域之保護，切勿成為電子郵件詐騙的幫兇。

KPMG 建議

1. 搭配完善的郵件認證機制，為了獲得更安全的防護，應實施認證與配置 SPF、DKIM 與 DMARC，強化其郵件伺服器防禦能力，且更能有效的監控與管理，確保電子郵件傳送能力。
2. 倘若企業缺乏 DMARC 的認證與配置，使用者亦會接受沒有標記且未回報的可疑郵件，甚至無法接受針對可疑信件進行有效控管。
3. 持續維持 A 相關 DNS MX 紀錄之完整，降低攻擊風險。

❸ 網路加密風險



檢測說明

由多個來源 (如 : Qualys SSL Labs scanner, HTBridge, Mozilla Website Observatory) 檢測 SSL/ TLS 的安全性，識別其加密套件、協定細節、HSTS、PFS。

企業現況

SSL/TLS 為網際網路通訊提供安全及資料完整性保障，保障瀏覽器與網站伺服器之間傳輸內容較不易受他人輕易竄改、攔截與窺視等。當加密流量成為主流，日新月異的密碼學以及 ECC 等新興加密協定會大幅增加處理 SSL/TLS 流量時所需的效能。如此可能會導致現有的設備無法負荷，抑或是允許未經檢查的流量進入內部網路。

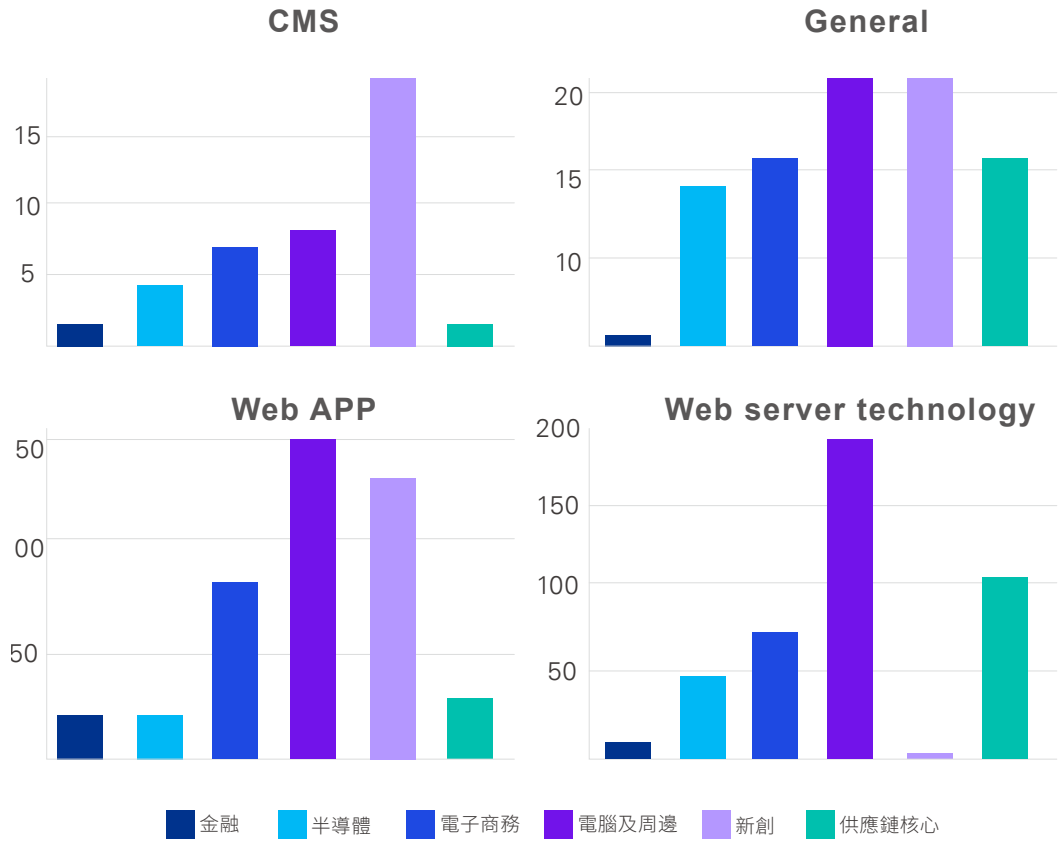
根據本調查發現受調之六大產業對於 SSL/ TLS 強度設定皆仍有待加強，其中包含 TLS 認證是否符合擴充性驗證 (Extended Validation) 與未被信任的第三方驗證端認證；或是 TLS 使用的加密套件 (Cipher Suites) 之安全性是否存有漏洞，給予駭客進行 BEAST(Browser Exploit Against SSL/TLS) 攻擊的機會；抑或是使用較弱且不安全的 SSL/ TLS，駭客可透過舊版的通訊協定漏洞發動攻擊或是攔截資料等。更引人擔憂的是，在駭客入侵事件頻傳的現在，透過與先前的分析結果比較，仍以電腦及周邊產業的 SSL/ TLS 強度最令人擔憂，須改善且加強其加密套件的應用與擴充性驗證；其次，供應鏈核心產業有極大的 M 型化趨勢，該產業內的受調企業在此項目檢測上有著極端的表現，導致其平均分數較低，而根據本調查結果，在此產業中規模較大的企業，對於 SSL/TLS 擴充性驗證，加密套件的安全性與其弱點暴露程度皆有待強化。

因此企業對於網路加密通訊安全設置上應更加關注產業趨勢且定期更新，才能有效的提升網路訊息傳輸安全，降低資安曝險程度。

KPMG 建議

1. 審慎使用如 Wildcard 萬用憑證與多網域 / 多域名 (SAN) 憑證。
2. 注意最新憑證使用限制。(如 2020 年起，憑證最長效期縮短至 397 天)
3. 對外網站之 TLS/SSL 憑證更新應考量使用自動化更新機制。
4. 使用合宜強度加密演算法

❹ 一般技術風險



檢測說明

檢測企業的網站應用程式 (Web Application)、網站伺服器 (Web Server)、內容管理系統 (CMS) 與常見資訊系統 (Gerneral) 四大面項的弱點風險值。

企業現況

根據本調查結果，一般技術風險有以下發現：

1. 六大產業中金融業在此曝險評分項目中表現最佳，且主要皆屬低風險值弱點，且集中網站應用程式系統中。
2. 半導體產業為一般系統 (General) 與網站伺服器 (Web Server) 暴露較多弱點，且多數被發掘的弱點分布於中低風險。
3. 電腦與周邊產業中包含網站伺服器、一般系統與網站應用程式三大類別存有最多弱點漏洞，也造就此產業時常為駭客主要攻擊對象之一。且所發掘之弱點大多屬高、中風險值。以此產業特性與綜觀目前資安威脅態勢，絕對需要特別關注此項目之曝險狀況。
4. 供應鏈核心產業在網站伺服器與應用程式的建置上存有較多的漏洞，且分布於緊急與高風險之弱點居多，針對此一高曝險的情況，應儘速著手進行漏洞修補。
5. 依據本曝險項目系統類別分析，內容管理系統 (CMS) 的弱點暴露最多之產業為新創產業，其主因有可能為內容管理系統做為版本控制與系統整合之工具，但由於新創產業的發展所屬起步階段，因此對於管理工作流程系統的實施與設置較不成熟。

KPMG 建議

1. 建置由內到外之資訊安全防禦縱深，及針對網際網路服務建置資安解決方案 (如 WAF)
2. 企業應針對資訊系統定期進行弱點掃描與滲透測試，從中了解其內部資訊系統之弱點漏洞，應盡快修補之，降低駭客攻擊的可能性，以防止重大的資安漏洞，造成其商譽與財務上的損失。
3. 根據掃描檢測結果，企業應針對資訊系統有存在弱點之版本，將其更新至較新或最新版本，防止駭客利用該弱點針對系統進行攻擊；倘若無法修補弱點之資訊系統，則採取補償性控制措施，降低弱點被利用的可能性。

結論

本調查針對上述的調查發現與今日產業的資安挑戰，統整以下六點結論：

- 金融產業雖然為各大產業中的翹楚， 但其位於人力資源風險的社群媒體風險 (SocialPosture) 檢測項目中，卻是最後一名，代表金融業對於社群媒體的控管應審慎因應。
- 近年來電子商務產業頻頻出現資料外洩等資安事件，伴隨著業者對上市櫃公司，都有強烈要求設置資安長與專責資安人員，因此相關資安從業人員的稀缺性與配置應持續受到重視。
- 供應鏈核心產業中的受調企業資安分數普遍欠佳，尤其此產業大多設立已久，對於使用新興科技、網路與數位應用等風險觀念也較為缺乏，造成曝險因子提高。
- 電腦與周邊產業一直是駭客眼中的肥羊，此產業網路與科技風險中的檢測項目都較為落後，尤其是網頁系統檢測項目皆為倒數，而網頁伺服器又很常是駭客入侵時，時常覬覦的攻擊目標之一。
- 近幾年隨著資安的重要性遽增，企業對於取得國際標準認證（如：ISO 27001）也越來越重視，然而經本調查發現，許多企業於年報中提及「符合」國際資安標準相關要求，但卻未實際通過獨立第三方之驗證，對於企業十分容易造成自我感覺良好的負面效果，無法實質提升其資安防護實力。
- 本調查認為傳統資安防護能力與 "ZeroTrust" 設計，以及加強終端裝置訊息蒐集控管之結合始能為企業穿上一套基本防護衣，" N everTrust, Always Verify" 亦指零信任此時成為新一道資安防護防線。

調查方法

調查方法

國際資安認證資訊來源

本調查中的國際資安認證資訊是依據企業提供之年報，從中檢閱其內文是否提及通過相關國際資安認證標準，亦或將國際資安標準之架構部署於企業內部資訊安全系統中，以及對於資訊系統內部控管規劃與訂定資訊安全政策之規範等。

1

情境分析

不考慮產業別，以資安國際標準通過與否評估資安防護能力。

✓ 通過資安國際標準能明顯提升企業資安防護力

2

情境分析

不考慮是否通過標準的情況下，與金融業進行防護能力比較。

✓ 金融業平均資安防護能力最佳
✓ 電腦及周邊設備、電子商務、半導體、基礎建設等產業平均資安防護能力明顯較差

3

情境分析

不考慮其他因素，僅以產業類別探討資安防護能力。

✓ 通過資安標準平均可提升資安防護能力

屏除新創產業並以企業資安防護能力為依變數之迴歸結果表

變 數	資安防護分數		
	以資安國際標準為基準 估計量	以金融業為基準 估計量	以產業別探討 估計量
截距	74.30 ***	87.43 ***	81.08 ***
通過資安國際標準 "Y"	7.22 **		6.35 **
產業 電腦及周邊設備		-13.36 ***	-10.18 **
產業 電子商務		-9.05 *	-3.5
產業 半導體		-7.71	-2.27
產業 供應鏈核心		-13.63 ***	-9.39 *
Observations	51	51	51
R^2 / R^2 adjusted	0.180 / 0.163	0.307 / 0.247	0.403 / 0.337
* p<0.05 ** p<0.01 *** p<0.001			

根據本調查 (如上表) ，Model 1 指出「通過資安國際標準」能非常顯著地提升企業資安防護能力（β=7.22, p-value<0.05），Model 2 以金融業當作參照組進行迴歸，結果顯示電腦及周邊設備產業、供應鏈核心

結果顯示供應鏈核心產業 (β=- 13.36, p-value<0.001) 與電子商務產業 (β=-13.63, p-value<0.001) 在資安防護能力上與金融業有極其明顯的負向差距，平均資安總分低於金融業 13 分以上。Model 3 以產業類別當作控制變數，結果顯示在去除產業資安能力差距的情況下，「通過資安國際標準」始終非常顯著地提升企業資安防護能力（β=6.35, p-value<0.05）。

樣本選取的方法

本調查蒐集台灣前 100 大企業，依據各大企業進行產業分類，最後按照產業比例進行分層抽樣 (Stratified Sampling)，選取 50 家企業，並增加新創與電子商務兩大產業。

技術面向：評估架構與流程

本調查透過輸入企業之主網域名稱，同時從各大搜尋引擎與網路掃描器蒐集的資料進行比對，推斷企業的資產範圍，並預測企業極可能產生之資訊安全風險與其曝險程度。

透過整合上百種搜集器與資料檢測來建立本調查之資料庫，並基於三大面向，包含「應用面安全」、「網路與科技風險」與「人力資源風險」評比企業之資產與其資訊風險之高低，最後再依據其檢測結果進行評分，並探討六大產業共同面臨的資安議題及曝險程度之高低與其影響。

技術面向：檢測項目及說明

❶ 應用面安全 (Application)

- 應用程式風險 (Application Security)- 檢測企業網頁 APP 端是否存有的潛在安全問題，如 XSS、暴露的使用者訊息，以及容易淪為攻擊者目標的重要內容 (如：攻擊者藉由暴露資訊以 Brute-force 攻擊破解管理員密碼)。
- 網域安全 (Domain Attacks)- 相似的網域名稱能被攻擊者購買以進行網路釣魚和域名仿冒的相關活動，本項目檢測企業之網域名稱是否遭受劫持攻擊或使用者誤植導致的風險。
- 服務暴露風險 (Exposed Services)- 包含未使用密文傳輸敏感資訊、未限制最高權限埠口的控管等應用端設計缺陷，檢測企業系統之對外服務配置是否完善與是否存有漏洞。
- 技術風險 (Technologies)- 檢測企業的網站應用程式 (Web Application)、網站伺服器 (Web Server)、內容管理系統 (CMS) 與常見資訊系統 (Gerneral) 四大面項的弱點風險值。

❷ 網路與科技風險 (Network & IT)

- 資產聲譽評量 (Asset Reputation)- 資產聲譽分數源於評估企業各項資產在資安層面之名譽。
- 雲端服務風險 (Cloud)- 本項目針對企業使用雲端之私人雲端服務之連線與公共雲端容器存取設定等配置作為檢測評分之依據。
- 域名解析風險 (DNS)- 檢測企業 DNS 在區域傳輸與開放解析器，以及 DNSSEC 的配置是否完善。
- 電子郵件與網路加密風險 (TLS, Mail Server) - 檢測企業郵件伺服器是否實施 SPF(Senders Policy Framework)，DKIM(DomainKey Identified Mail) 與 DMARC (Domain-based Message Authentication, Reporting, and Conformance) 的設定與配；多項來源針對企業 SSL/TLS 強度進行安全檢測、加密套件安全性、協定的擴充性驗證與可用性版本與認證來源的可信度等。
- 網頁系統風險 (Web Server)- 檢測企業網路伺服器 (Web Server) 是否建立 CSP(Content-Security-Policy) 、XSS(Cross-Site-Scripting) 和 Cookies 的 Response Headers 與揭露其版本配置之風險，以及利用工具檢測其應用程式防火牆 (WAF) 設置。

❸ 人力資源風險 (Human)

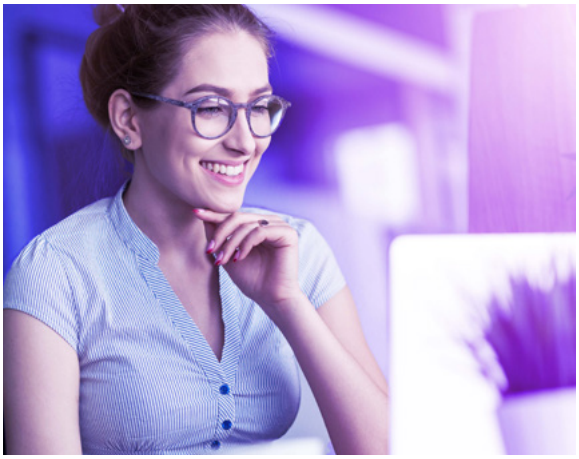
- 資安事件反應力 (Responsiveness)- 企業對於已知系統漏洞的修補速度以及危機處理與反應能力。
- 資安團隊戰力 (Security Team)- 從公共平台中檢測企業是否有設立資安小組與資安長之職。
- 域名解析風險 (DNS)- 檢測企業 DNS 在區域傳輸與開放解析器，以及 DNSSEC 的配置是否完善。
- 網攻承受力 (Employee Attack Surface) - 駭客可利用社交工程寄送網路釣魚信件給企業內部員工，從中入侵企業內部系統，此項目為檢測企業內部員工之資安意識程度、員工公共數位足跡與員工遭攻擊之可能性。
- 社群媒體風險 (Social Posture)- 此項目為檢測企業是否對於社群平台之其企業資訊做防偽措施與管理。

調查限制

方法之限制

本檢測工具為調查期間 (2021/12-2022/01)，透過大量的情資搜集器，與相關大數據技術分析等客觀調查依據。

此資安曝顯報告僅能作為產業資安概況之參考指標，倘若企業需加強其資訊安全防護能力，仍需搭配專業顧問之協助，以及弱點掃描與滲透測試等檢測工具之輔助。



樣本之限制

抽樣方法：KPMG 以富比士、證交所及台灣新創競賽所列企業為母體，結合風險評估之經驗，依據六大產業 (電腦與周邊、半導體、電商、新創、供應鏈核心與金融) 進行分層隨機抽樣。

另外，與往年不同之處在於本調查報告新增電商、新創與基礎建設三大產業，並隨機抽樣產業內供應鏈核心企業為樣本。本調查中的六大產業是依據集團之主網域公司的主營業項目的性質為產業區分，倘若集團跨足不同產業，其主營業項目之產業與子公司分別實際所屬之產業將有所不同。

此外，本調查範圍主要以台灣上市櫃與新創競賽企業為主，雖無法代表台灣整體企業的資安曝顯狀況，但挑選企業皆為各產業代表，因此仍足夠具有代表性與參考價值。

聯絡我們

Contact us

謝昀澤 Jason Hsieh

KPMG 安侯數位智能風險顧問股份有限公司

董事總經理

T +886 2 8101 6666 #07989

E jasonhsieh@kpmg.com.tw

邱述琛 David Hsiu

KPMG 安侯數位智能風險顧問股份有限公司

執行副總經理

T +886 2 8101 6666 #11900

E dhsiu@kpmg.com.tw

林大馗 Toni Lin

KPMG 安侯數位智能風險顧問股份有限公司

副總經理

T +886 2 8101 6666 #15320

E tonilin@kpmg.com.tw

kpmg.com/tw