KPMG

臺灣企業資安曝險大調查

January 2021

安侯數位智能風險顧問股份有限公司

臺灣企業資安曝險大調查

Investigation Report: Cyber Risk Exposure in Taiwan

關於 KPMG Cybersecurity Co.

KPMG 安侯數位智能風險顧問股份有限公司 (KPMG Cybersecurity Co.) 致力提供最可信賴、最具權威的數位風險顧問諮詢，包含資訊治理政策與制度規劃、各產業數位法遵、網路安全技術防禦、數位轉型風險控制、資安事故處理與回應、個資與隱私保護工程等多元服務，協助企業從作業流程、法律、資安技術，與風險管理等不同層面，全面預防與降低數位應用所產生的營運衝擊。

藉由與全球 KPMG 資安專家緊密結合的知識網路，以及專注、熱情與創新的服務精神，我們有信心可以協助企業在 5G 時代中，與時俱進地結合資訊安全防護，建構一個最可靠、安全的智慧聯網商業模式與營運管理制度，以跟上數位轉型的潮流，共享人工智慧、雲端、物聯網及大數據等新興科技所創造的美好未來。

前言

KPMG 安侯建業很高興能在 2021 年初發表第一版針對臺灣本土企業的資安曝險大調查。近年來，KPMG 推出區域性的專題報告，即是運用在地化的專業知識，更貼近地診斷客戶正面臨的挑戰，貫徹「以客戶為中心 (Client-centric)、客製化」的全球資訊安全服務宗旨。

臺灣長期受地緣政治影響，駭客威脅一直高度存在，網路安全的不確定性不斷提升。加上在 2020 年新冠疫情 (COVID-19) 肆虐下，國內企業更廣泛地應用雲服務、物聯網等新興科技，遠端工作、智慧生產及網路購買行為也達歷史性的巔峰，這些都使臺灣資安問題，成為所有企業與民眾關注的焦點風險。我國副總統賴清德於 2020 年出席「臺灣駭客年會 HITCON」時即指出，臺灣每月平均遭受高達三億次的駭客掃描、三千萬次的攻擊，更凸顯今日網路管理與防護為臺灣刻不容緩的議題。

在新現實 (New Reality) 中，疫情促成的遠距工作、改變的營運與消費模式，讓科技應用「大躍進」，正是企業進行數位優化或轉型的好機會，卻也擴大網路曝險的範圍。KPMG 因此集合數位風險領域人才的專業與服務經驗，於本調查向讀者說明國內大型企業的數位風險情勢，並提出我們的觀點與建議，俾協助企業更密切關注組織內部的風險管理政策，同時制定因應策略。在數位發展多變的世界中，我們期盼給予企業協助，一起更有自信且可靠地應用各種智慧科技、降低科技風險、保護企業資產，提升企業整體的競爭優勢。

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。

KPMG 安侯建業
執行長

目錄

關於本調查

調查作業核心目標

KPMG 著手蒐集有關臺灣指標企業有關網路安全環境的資料，包含 2020 年重點產業的趨勢、組織網路曝險的現況等，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，本調查除了資訊安全的檢測外也包含了可量化的財務評估，讓企業了解其有形及無形的風險。

2. 比較產業資安現況

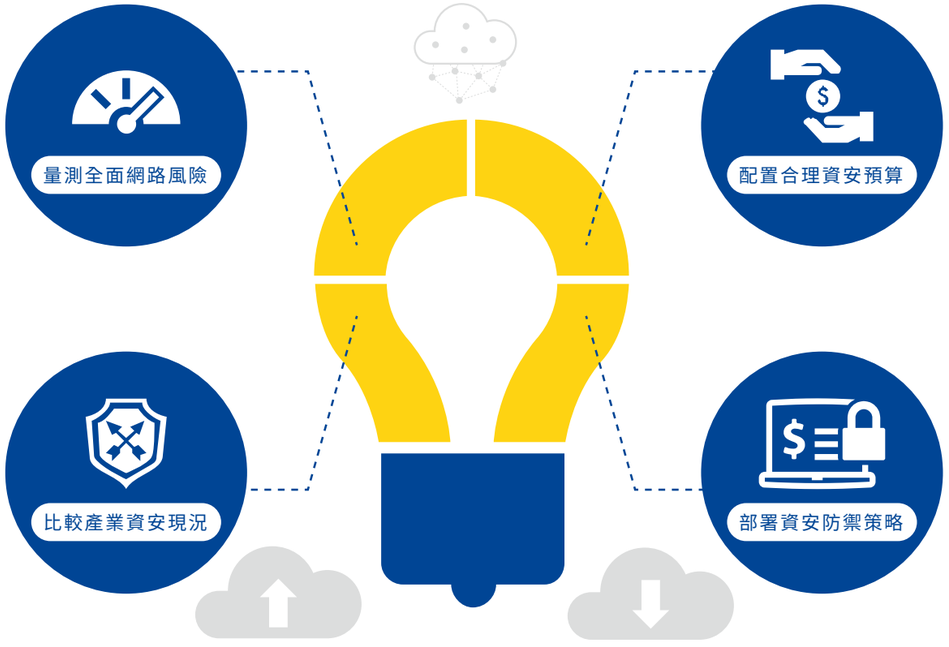
依據企業營運特性，將檢測的 50 家大型企業分成五大類，可以結合產業趨勢做更精準的分析，真實地比較同產業、委外 / 合作廠商所屬產業，了解各自曝險控管的優劣。

3. 配置合理資安預算

了解指標產業下一年度若發生資安事件的平均財務損失風險，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，以最少的資源降低、轉移或接受這些風險。

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進行深入剖析與提供建議，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，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. 資訊長 CIO、數位長 CDO、資安長 CISO、風控長 CRO：

根據《2020 KPMG 全球 CIO 調查報告》，在 COVID-19 下，企業仍持續對數位科技進行資源投入，受訪 CIO 票選最重要的投資項目即為「安全與隱私」。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。本調查以網路事件資料庫中的「發生頻率」與「損失金額」來推估下一年度資安財損風險，讓 CFO 能依此量化數據，衡量組織的資安策略與相關投資，有效規劃下年度的預算來降低直接與間接數位風險成本。

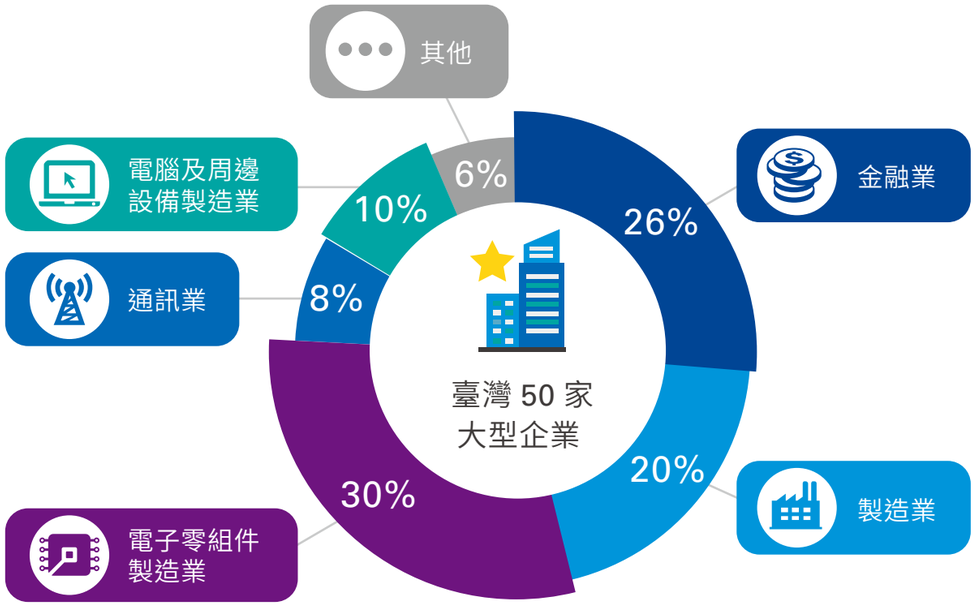
4. 資訊管理、資安與數位應用相關技術專員：

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。

我們希望能透過本報告，讓企業領導者、供應商與 IT 人員能更有效率地討論其科技策略，同時提供網路控管知識給資安領域的讀者。

企業調查範圍

KPMG 參考富比世、天下、CRIF 中華徵信所的統計資料，並結合風險評估的經驗隨機挑選 50 家大型企業，進一步依臺灣近年的發展趨勢分為五大產業，進行本次調查。



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，評估臺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
- 以非入侵式智慧型工具自動執行，提高調查的有效性
- 曝險評估同時考量技術與財務面向
- 以資安事件估計造成的損失金額，將資訊安全風險進行量化

	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 （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 如：隱私性、韌性、聲譽、安全性	大範圍偵測主機設備漏洞 如：Injection、XSS、Security Misconfiguration	透過組合技驗證商業邏輯漏洞 如：權限跳脫、目錄瀏覽、URL 重新導向等漏洞

© 2021 KPMG Cybersecurity Co., a Taiwan company limited by shares and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

臺灣企業資安曝險大調查 關於本調查

技術檢測項目及分數含意

隱私性 Privacy

- SSL/TLS Strength　SSL/TLS 強度
- Leaked Credential　機密洩漏
- Hacktivist Shares　暗網分享
- Social Network　社群網路
- Information Disclosure　資訊揭露

韌性 Resiliency

- Attack Surface　攻擊面
- DNS Health　DNS 健康度
- Email Security　Email 安全性
- DDoS Resiliency　DDoS 承受度
- Network Security　網路安全性

聲譽 Reputation

- Brand Monitoring　品牌監控
- IP Reputation　IP 聲譽
- Fraudulent Apps　欺詐應用程式
- Fraudulent Domains　欺詐網域
- Web Ranking　網頁排名

安全性 Safeguard

- Digital Footprint　數位足跡
- Patch Management　漏洞修補管理
- Application Security　應用程式安全性
- CDN Security　CDN 安全性
- Website Security　網頁安全性

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 五個等第，提供讀者一個更直觀、易懂的衡量標準。

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

© 2021 KPMG Cybersecurity Co., a Taiwan company limited by shares and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

執行總結

© 2021 KPMG Cybersecurity Co., a Taiwan company limited by shares and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

調查結果總覽

平均網路防護分數

C 78.68

平均財務損失風險

2000 萬台幣

分數 低 高

資安曝險評估項目	評估說明	臺灣 50 家大型企業
隱私 Privacy	憑證管理	
	暗網分享	
	資訊揭露	
	社群網路	
	SSL/TLS 強度	
聲譽 Reputation	品牌監控	
	欺詐應用程式	
	欺詐網域	
	IP 聲譽	
	網頁排名	
韌性 Resiliency	攻擊面	
	DDoS 承受度	
	DNS 健康度	
	Email 安全性	
	網路安全性	
安全 Safeguard	應用程式安全性	
	CDN 安全性	
	漏洞修補管理	
	網頁安全性	
	數位足跡	

初步的資安曝險評估。透過網域名稱掃出在各數位資料來源中有多少**足跡量**，而**非進行評分**

調查主要發現

1

數位足跡數越多，越可能被駭客盯上

企業於網路上的數位足跡越廣，代表在網路上的行蹤較容易被駭客追蹤，因此往往有越低的網路防護分數。

2

臺灣四大產業網路安全性防護等級平均在 C 級以下，資安亮警訊

臺灣企業在網路防護分數四大面向中，於「安全性」成績明顯落後。臺灣 50 家大型企業中，就有高達 11 家企業安全性分數不及格，而若依產業別，除金融業之外的四大產業皆低於 75 分。

3

電腦及週邊設備製造業，最需加強網路防護

本產業不僅在平均網路防護分數墊底，更有高達 80% 屬於該產業的企業落在整體排名的最後 15 名，網路防護亟待加強。

4

金融業網路防護表現最佳，但仍面臨高度挑戰

金融業於各面向 (隱私性、安全性、韌性、聲譽) 的平均分數皆表現最優異，也是資訊防護領域扎根最久之產業。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，資安防護也因此需與時俱進，不可掉以輕心。

5

提升網路安全將顯著降低財損風險

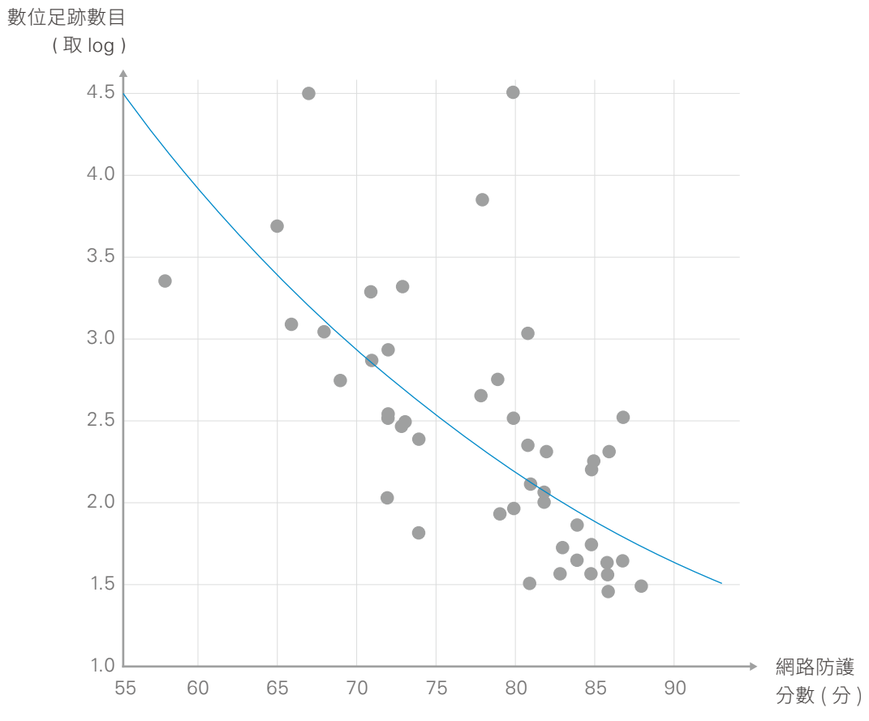
企業的財損風險與網路防護具高度的負相關性。以 5 分為級距時，分數每提升一個級距，財損風險減少超過 60%。這表示若能做好網路防護，將能有效降低資安事件發生的財務損失。

1
數位足跡數越多，越可能被駭客盯上

由調查結果得知，數位足跡數目與網路防護分數具有高度負相關。本調查的第一步，即透過每個網域名稱，進行快速偵測並呈現企業的數位足跡數。這個方法與駭客入侵所慣用的狙殺鍊架構 (Kill Chain Framework) 的情資蒐集程序相似，兩者皆針對開放性資訊與情報來源進行挖掘與分析。而數位足跡越多時，往往代表在網路上的行蹤較易被追蹤，駭客攻擊的機會也因此較大。

此外，本次調查方法蒐集網路之大數據情資，來源包含駭客網站 / 論壇、弱點資料庫等。由於這些網頁多半呈現企業有關資安的負面訊息 (試想：駭客為何會討論一企業？、弱點資料庫為何會有一企業的資料？)，故數位足跡數目越多時，通常也表示網路的曝險控管較差。

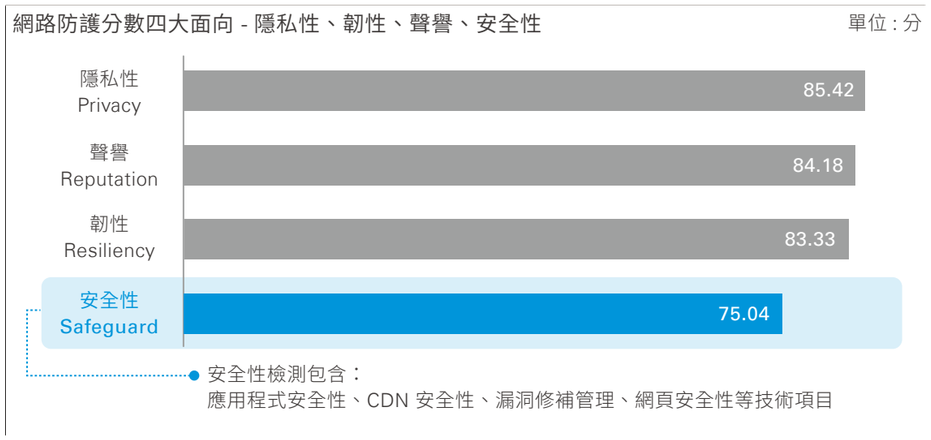
因此 KPMG 建議組織應透過適當網路縱深架構，保護重要數位資產，並透過內部存取控制、資料盜失防護等機制，如採取多因子驗證等方式，妥善管理重要數位足跡。

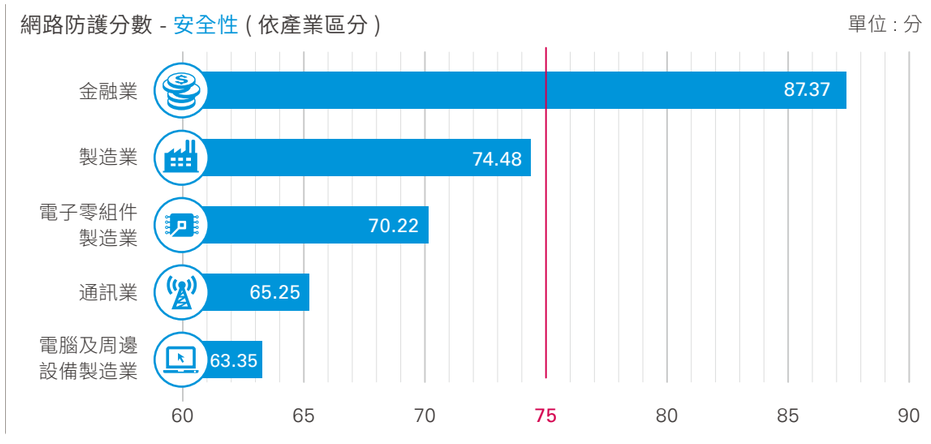


2
臺灣四大產業網路安全性防護等級平均在 C 級以下，資安亮警訊

臺灣企業在網路防護分數四大面向 - 隱私性、韌性、聲譽、安全性中，於「安全性」成績明顯落後其他三者。50 家大型企業中，在此面向有高達 11 家企業分數不及格。

若依產業別，除金融業的平均 87 分、其中超過半數企業有 A 級的優異表現之外，其餘四大產業 (電子零組件製造業、製造業、電腦及設備製造業、通訊業) 安全性的平均成績皆低於 75 分。此外，調查結果顯示不同產業間的全距達 24 分，表示臺灣各產業的安全性防護的強弱有很大的落差。





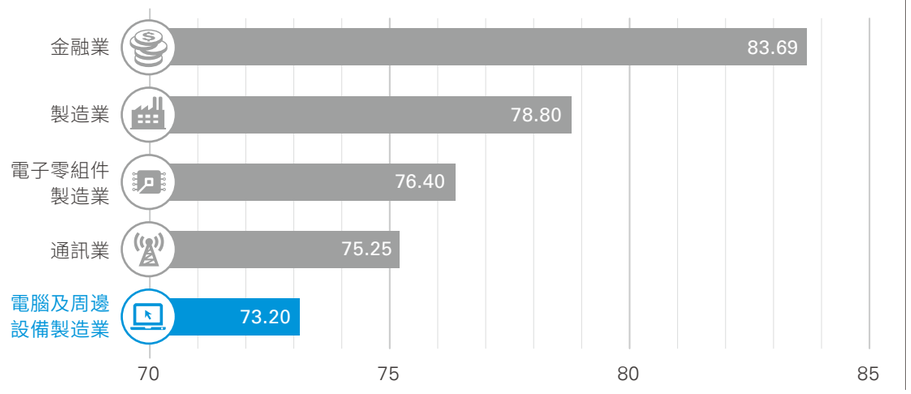
3

電腦及週邊設備製造業，最需加強網路防護

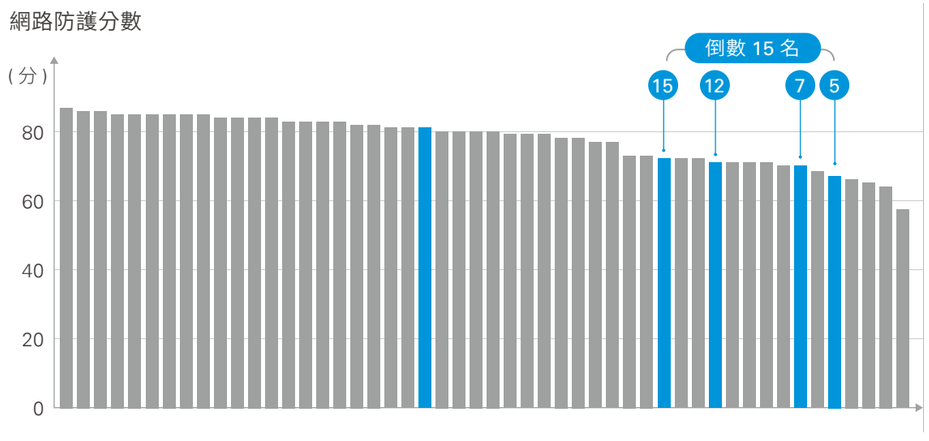
電腦及週邊設備製造業在本次調查中平均網路防護分數墊底。該產業的企業中，只有一家勉強進入前段班 (第 22 名)，其餘皆落在整體排名的最後 15 名。對此，KPMG 分析是國內企業近年快速推演智慧製造，網路架構複雜程度的增加、軟體未能即時更新與升級等，都使駭客有機可乘。KPMG 也因此建議電腦及周邊設備製造業，在享受數位化的美好果實時，更應努力提升其網路防護分數。

網路防護分數 (依產業區分)

單位 : 分



網路防護分數



4

金融業網路防護表現最佳，但仍面臨高度挑戰

金融業在網路防護分數的四大面向中，不論是隱私性、安全性、韌性、聲譽皆為全產業表現最優異，且平均成績都接近 A 級。其中臺灣產業表現有待加強的「安全性」，金融業仍維持 87 分的高水準。分析國內金融業普遍為「資優生」，是因為主管機關的高度監理。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，因此讓金融業成為台灣企業的資安標竿。

乍看之下金融業似乎不用擔心網路攻擊，然而該產業擁有豐富且價值高的資訊與資產，近年又廣泛使用雲端儲存、資料分析工具並與多元的第三方合作而擴大曝險面積，因此至今仍為駭客集中精力攻擊之標的。國際研究機構的報告即指出，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。

KPMG 也針對此次調查，給予金融業三點對未來「數位風險」的提醒事項：

1. 臺灣金融業兩大數位現象需要留意

   金融業雖然在網路防護中四大面向的平均分數皆領先其他產業，但在「聲譽」面向的「品牌監控」和「網頁排名」兩項檢測卻落於最後一名。

2. 臺灣金融業資安落隊者，易成駭客之眾矢之的

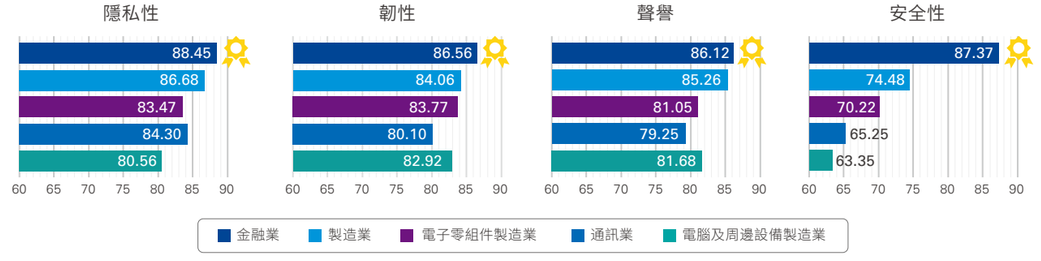
   13 家金融業中，高達 11 家的網路防護分數名列本次調查的前 20 名，但剩下 2 家卻落於 30 名之後。檢測項目中，又以「漏洞修補管理」、「欺詐應用程式」的分數差異最明顯：其餘金融企業在前項檢測平均能有 91.5 分、後項皆為 100 分，但該兩間在前項卻僅分別獲得 45 和 20 分、後項則分別為 89 和 75 分，明顯未能跟上整體水平。

3. 臺灣金融業控管網域名稱系統的能力較差

   雖然金融業在韌性面向的成績最好，但在韌性面向中的「網域名稱系統 (Domain Name System, DNS) 健康度」，分數僅有 76.46 分，大幅拉低韌性面向的平均 (86.56)，且在五個產業中排名倒數第二。DNS 若控管良好，則可以透過資料比對、安全認證等步驟，來避免連結到詐騙網站、過濾惡意連結，反之亦然，因此提醒金融業需再加強 DNS 的控管。

網路防護分數 - 四大面向 (依產業區分)

單位 : 分

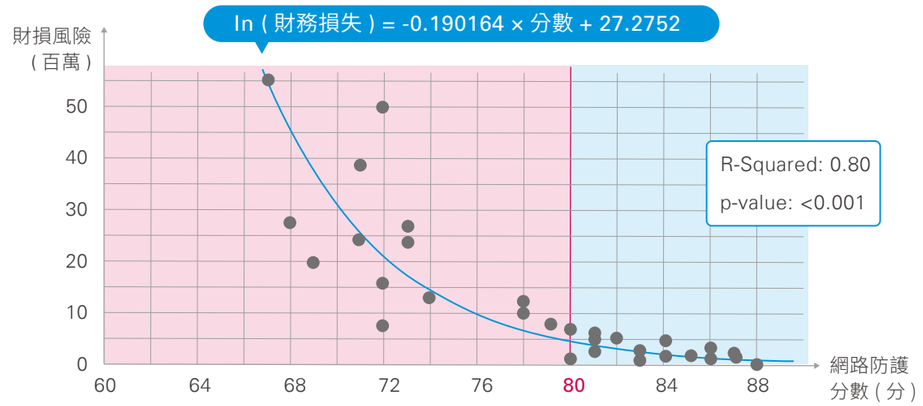


5

提升網路防護將顯著降低財損風險

經本調查分析可得知，企業的財務損失風險與網路防護強度具高度的負相關性。財務損失風險隨著網路防護分數的下降呈現指數性的增長，尤其在分數低於 80 分的群組格外明顯。

以 5 分為一級距時，分數每提升一個級距，財損風險將能有效地減少 60% 以上。而臺灣目前重點產業的平均網路防護分數只有 78.68 分，未達 80 分的關鍵分水嶺。由此可見，國內產業非常有可能成為駭客鎖定攻擊、勒索的重點對象，正面臨高財務損失的風險。



每上升一級減少 60% 財損風險

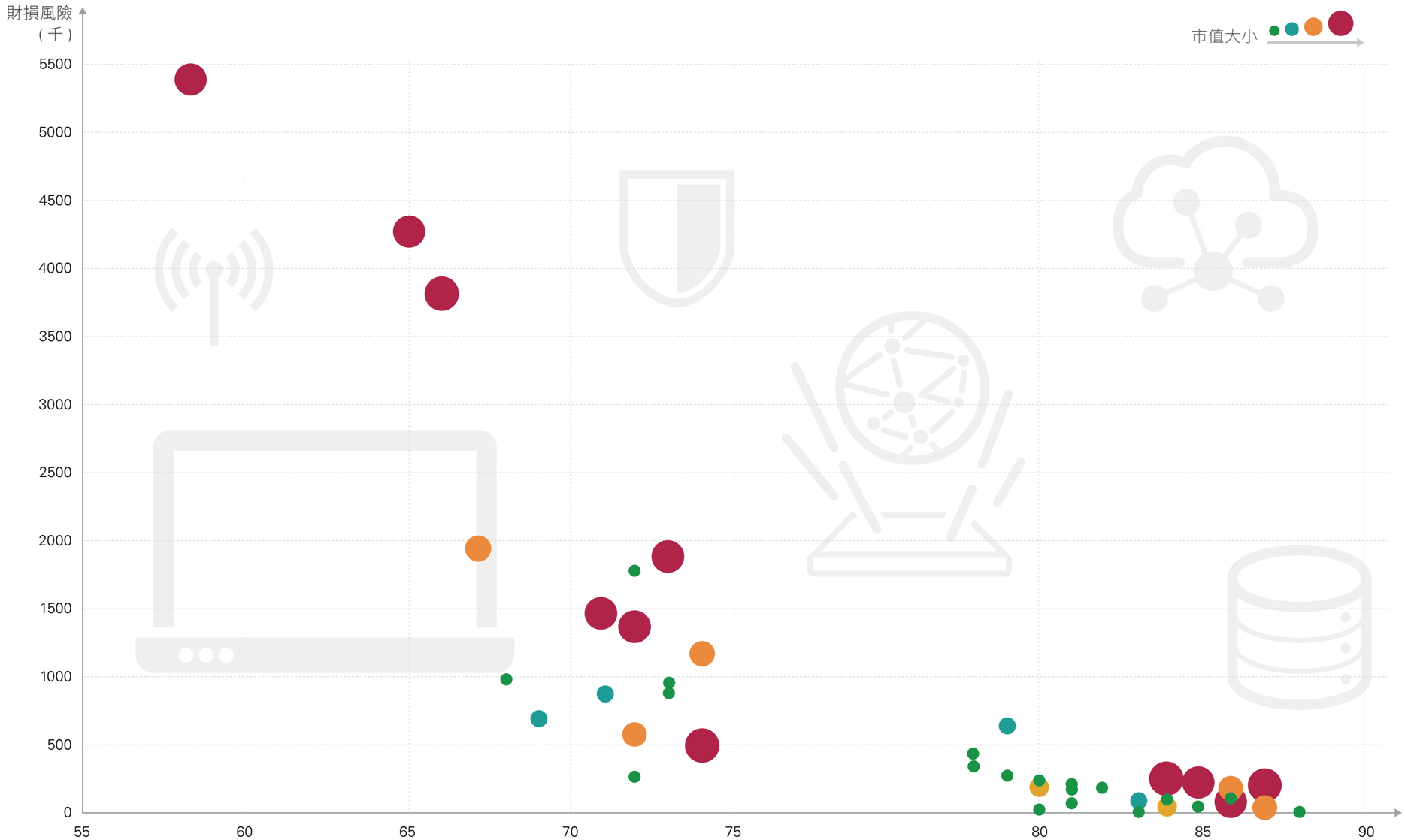
分數	財損風險	企業數	平均財損
85 以上	200 萬	13	330 萬
80~84	500 萬	16	
75~79	1300 萬	4	4300 萬
70~74	3400 萬	11	
未滿 70	8800 萬	6	

獨特議題探討

臺灣企業資安曝險大調查 獨特議題探討

規模大是網路防護佳、低財損風險的保證？

市值規模、網路防護、財務風險關聯性



一般認知規模較大的企業擁有較多財力可以聘請更多資安專家、添購更完善的網路基礎設備以做更好網路防護，因此普遍的網路防護分數較高。然而調查統計資料顯示，市值大小和網路防護分數相關性低。

大眾往往也認為較大的企業為了要保護其雄厚的資產，而訂定比小企業還低的可接受風險值，努力減少資安事件的風險、降低企業潛在的財務損失。但是本調查指出，市值與財務損失風險並無明顯關聯。

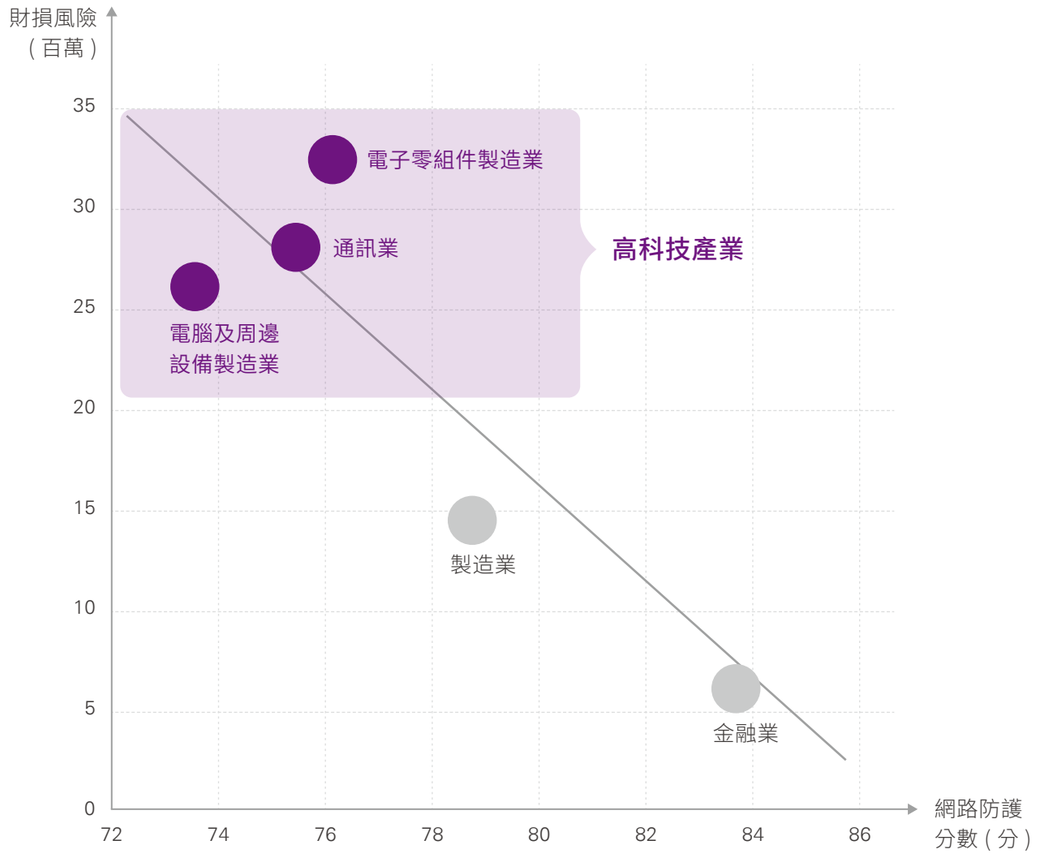
由左方氣泡圖可得，市值規模（氣泡大小）不論與網路防護（X 軸）或與財損風險（Y 軸），都不具顯著關聯。KPMG 分析，這是因為規模越大的企業必須投入越多網路防護資源，才有辦法維持同等金額的財損風險，然而國內當今的大企業尚未找到增加防護支出與降低風險的平衡點，才會反映出此現象。建議未來企業進行風險評鑑時，應審慎考量資安預算、支出。

© 2021 KPMG Cybersecurity Co., a Taiwan company limited by shares and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

誰是駭客眼中的肥羊？

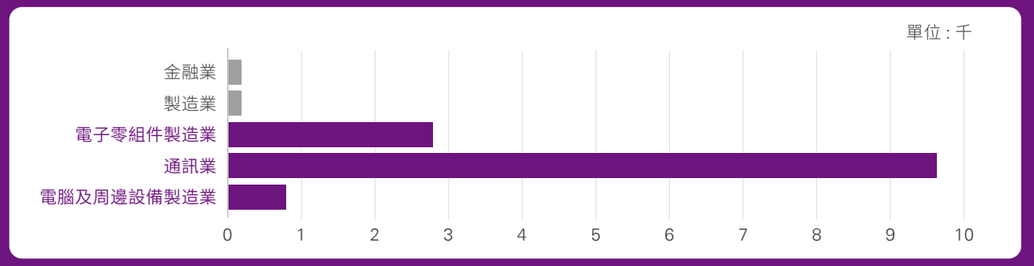
由下圖得知，電子零組件製造業、通訊業與電腦及周邊設備製造業，亦即傳統所稱「高科技產業」，是估計於發生資安事件後潛在財務損失風險最高的產業群，每家公司平均財損風險超過 3 千萬台幣。臺灣大型高科技產業在全球產業供應鏈中，往往扮演關鍵角色。然而，高科技產業的網路防護成績不僅在所有產業中墊底，其中的電子零組件製造業與電腦及周邊設備製造業與全球平均相比時，表現更是明顯落後。

分析駭客對臺灣高科技產業的攻擊事件，過去多為關鍵資訊系統的破壞、重要營業秘密的竊取，近年來卻轉為更明目張膽地進行系統綁架與財務勒索、商業郵件詐騙、持續性攻擊等，由此可一窺端倪，未來資安挑戰必然更加嚴峻，KPMG 因此提醒高科技產業要更努力守護資訊安全，才不會淪為全球駭客眼中的「肥羊」。

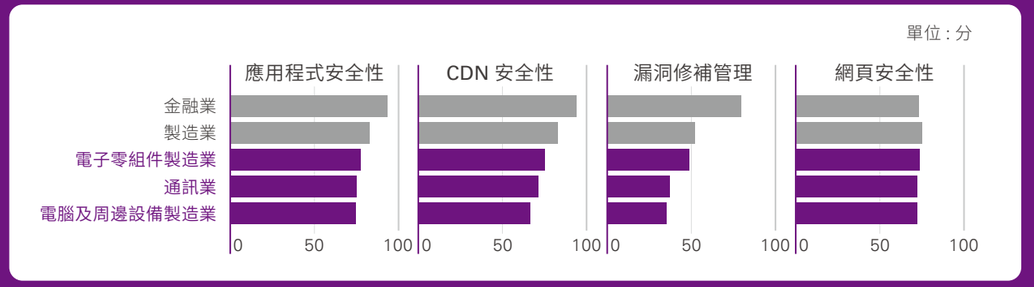


KPMG 針對高科技產業整理了三個重點議題：

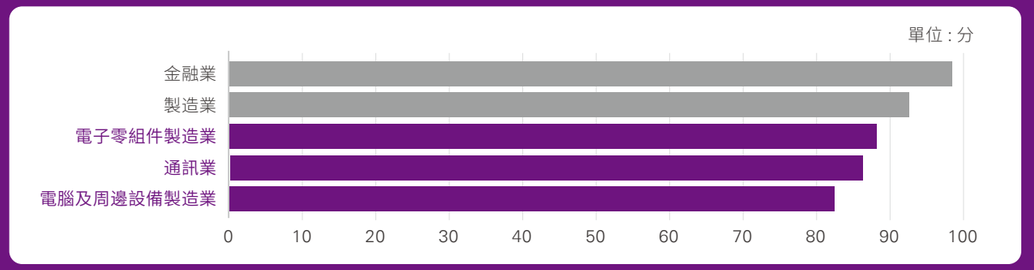
1. 臺灣高科技產業網路數位足跡廣泛
   本調查蒐集之情資來源涵蓋常見資安負面訊息的網站 (詳見執行總結 1)，因此檢測出越多數位足跡時，往往代表駭客越有可能追蹤、預測企業在網路的行為並進行攻擊。而本次調查中通訊業的數位足跡控管最差，其數目將近是金融業、製造業的 60 倍之多。電子零組件製造業、電腦及周邊設備製造業的數位足數亦分別為金融業、製造業的 20 倍、5 倍，宜再加強管理。



2. 臺灣高科技產業安全性的各項檢測排名皆為產業之末，亟需加強
   網路防護的四大面向中，安全性已經為整體產業平均最低的一個面向，而高科技產業安全性涵蓋的五項檢測：應用程式安全性、CDN 安全性、漏洞修補管理、網頁安全性、數位足跡的表現又全數落後金融業和製造業，由此可見，臺灣高科技產業的網路安全亟需著手防護。



3. 臺灣高科技產業產能旺季成了駭客收割季
   在「攻擊面」的檢測中，針對開放埠、過時服務、應用程式弱點及錯誤配置進行技術分析，而高科技產業的成績明顯落後。在傳統高科技產業的旺季，將可能因曝險面積擴大而面臨更多的勒索軟體攻擊，提醒高科技業要趕緊加強其資安控管和自身防護能力，避免造成巨額損失。

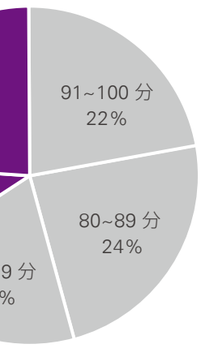


1/4 企業 0 分的漏洞是？

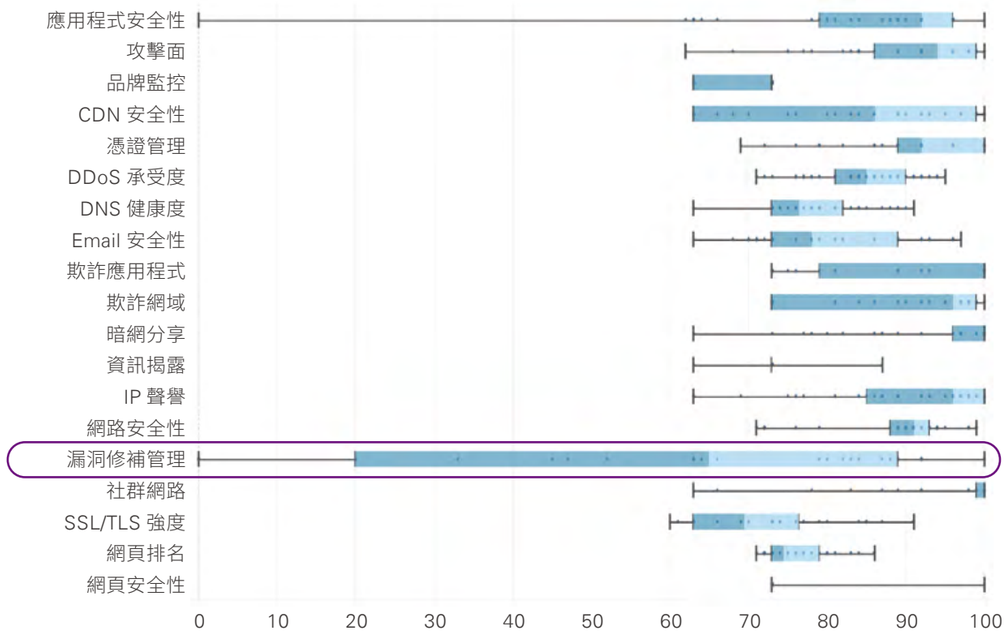
漏洞修補管理 (Patch Management) 在整體表現最差，整體平均分數未達 60 分，其中 24% 的企業甚至「抱鴨蛋」，面臨各項利用弱點的網路攻擊手法，亟需補強。雖然不少企業 0 分，卻仍有 4 家企業得到滿分，顯示漏洞修補管理這項指標，只要有具體投入，必能控制風險。

有將近 35% 企業不合格

50 家大型企業 - 漏洞修補管理分數

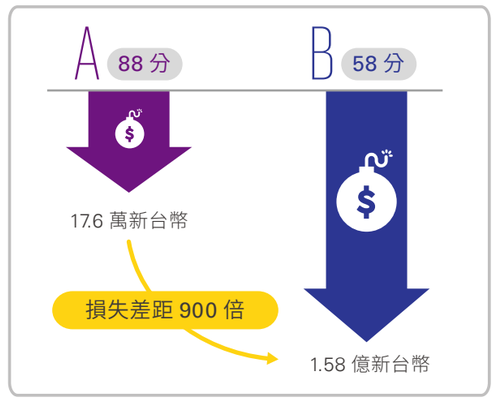


單位：分



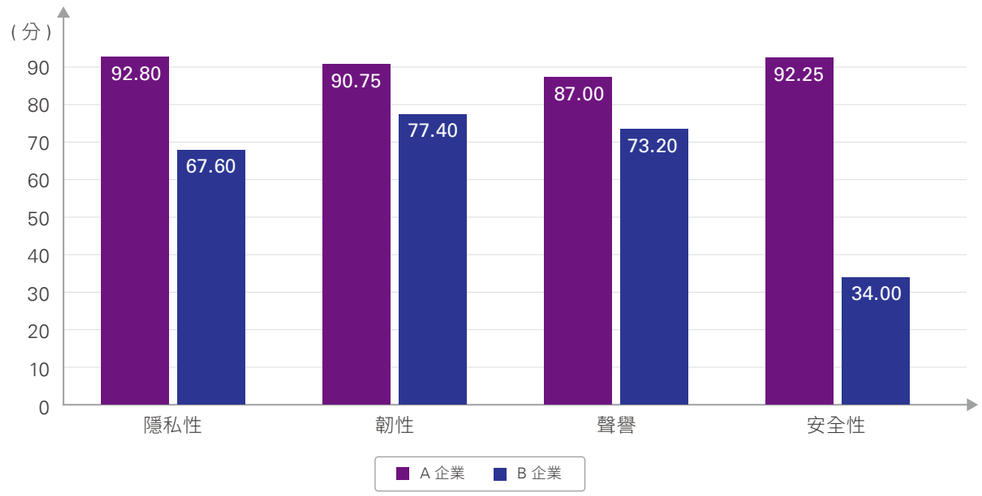
同為大型企業，但存在兩極差異？

本次挑選的 50 家大型企業中，發現不論在技術面、財務面的表現皆一致。表現冠軍的 A 企業，網路防護分數 88 分、財務損失風險僅 17.6 萬新台幣，反觀墊底的 B 企業為 58 分與 1.58 億新台幣。這兩家在網路防護分數差距高達 30 分，財務損失風險差距更高達 900 倍。



若進一步剖析四大面向的檢測，可以觀察到成績最差的 B 企業均明顯落後於成績最佳的 A 企業，其中在安全性層面平均分數更是落後將近 60 分。由此證明雖同為大企業，但在網路曝險管理的整體表現仍有極大的差異。

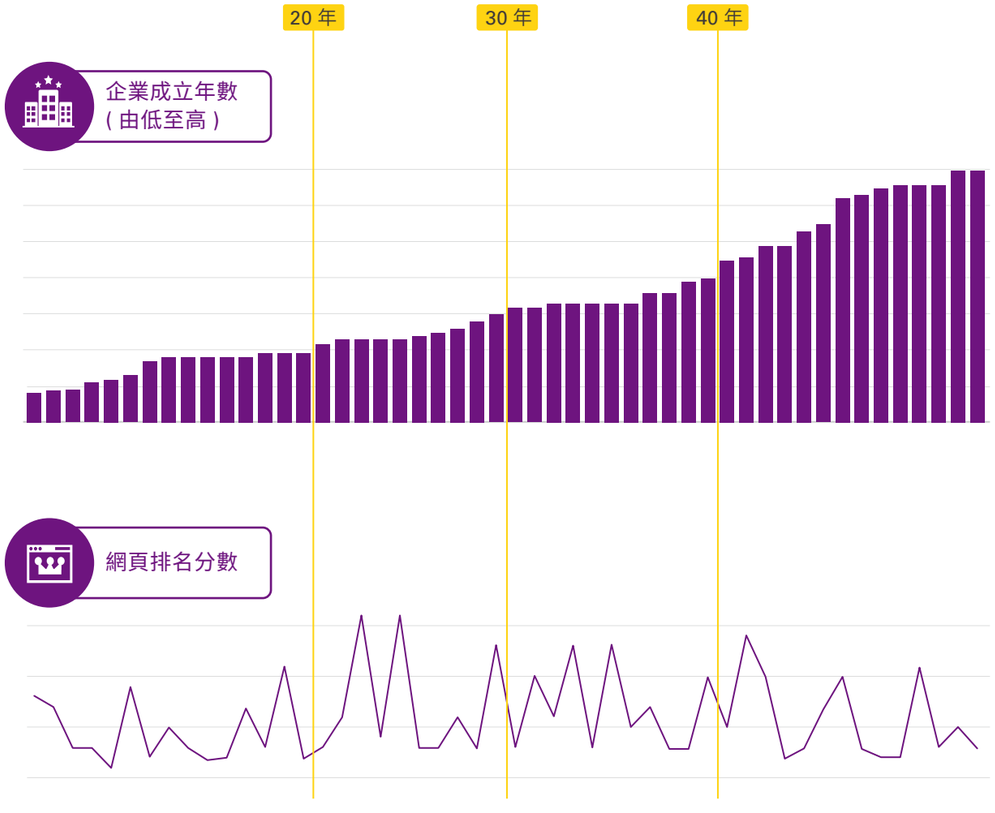
兩網路防護分數極端企業比較



企業歷史越悠久越知名？

在傳統的傳播世代中，成立越久的企業，透過民眾口耳相傳、電視媒體的報導累積聲量，普遍就能有更好的品牌曝光度。然而本次調查顯示，企業的網頁排名並未隨著成立年數的增長而有一定的成長。說明了在數位時代下，時間並不能換取知名度，網路經營方法與工具才是賺取流量紅利的可行方式。

企業成立年數與網頁排名分數相關性



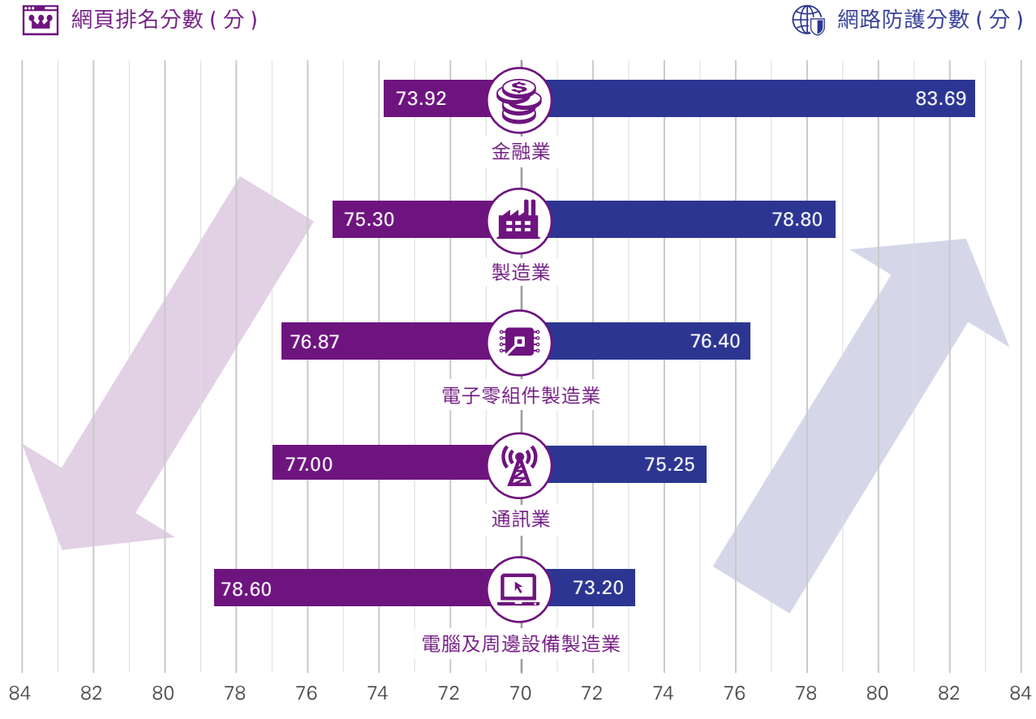
網路知名度與風險的平衡點在哪？

本調查發現，網路知名度與整體網路防護分數呈現反向的樣態。例如金融業雖然在整體網路防護分數領先群雄，但在網頁排名的表現卻顯失色，落後於整體水平。

在數位化的時代下網頁排名固然重要，各企業皆努力透過品牌行銷及搜尋引擎最佳化 (Search Engine Optimization, SEO) 來提升網頁的能見度，但可能也因此引來更多的網路風險。

然而，企業也不能為了迴避風險而放棄數位化的推廣。例如金融業雖有做好網路防護，但卻可能因數位品牌形象不夠鮮明，影響了金融機構數位金融 (FinTech) 的發展，在純網銀與開放銀行的加入下更面臨客戶流失的風險。

因此，在提升網路知名度和守護資訊安全中找到平衡點是這個時代下企業需要去思考的問題。



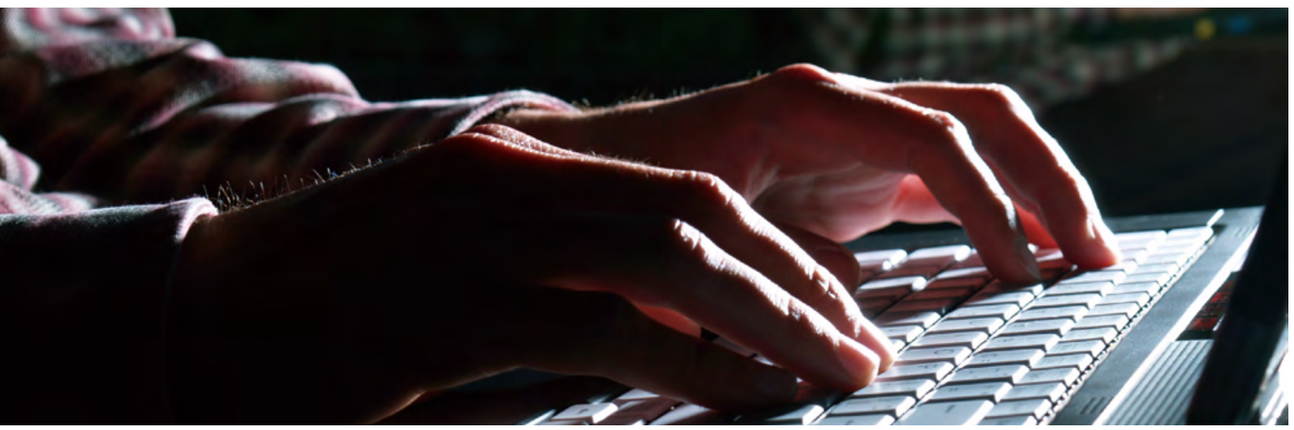
新現實下的資安挑戰

洞悉疫情催化的資安危機

2020 年底國際最受矚目的資安事件，當屬美國網路安全與基礎設施安全局 (CISA)，其緊急通報管理軟體 SolarWinds 於特定 Orion 版本遭植入 SUNBURST 與 SUPERNOVA 惡意程式，影響包含微軟、思科等科技巨擘甚鉅。CISA 進一步要求所有政府機構須立即回報目前狀態，從緊急通報內文描述、影響範圍、乃至美國政府機構要求之回應時間，都顯示此一事件非同小可。無獨有偶，越南國家政府憑證中心網站上的下載程式，也遭駭客透過該中心系統的弱點，置換為含木馬病毒之下載程式。近期臺灣民間產業中，勒索軟體與商業郵件攻擊 (Business Email Compromise, BEC) 於各產業中肆虐，屢次爆發重大資安災情，造成企業財務損失，企業營運之效率亦嚴重下降。

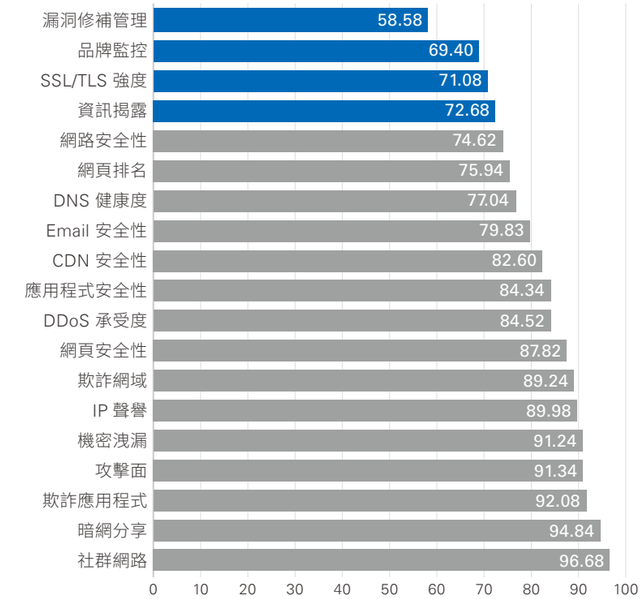
參照上述等重大資訊安全事件情境，雖然資安事件的成因眾多，但不脫組織資訊系統未及時修補的弱點與過多暴露在外的數位足跡遭利用，而提供惡意人士可乘之機。組織於網際網路上留存的數位足跡，若包含內部員工有心 / 無心的資訊洩漏 (Information Disclosure)、企業的雲端協作平台 (如 Github) 組態設定錯誤等高風險因子，則組織的數位空間 (Cyber Space) 將高度曝險。

我們期望打破企業於數位曝險之迷思：過去企業在網際網路門口砸下重本部署入侵偵測、防火牆、乃至網頁應用程式防火牆 (WAF) 等防堵來自網際網路的攻擊，但往往疏於處理過多流落在外的數位足跡、監控軟體失能等導致內部網路資訊外洩的問題。因此，本調查針對由外至內攻擊的防禦、由內至外機密資訊外洩的可能性，進行 20 項全面的技術檢測，深入剖析企業最需關注的風險熱區。



整體檢測分數

20 項技術檢測分數　　單位 : 分



左圖呈現 50 家大型企業在每個檢測項目的平均成績。在下四頁中，我們將取平均分數最低的四項檢測項目，結合現況進行分析，並給予因應之方法。

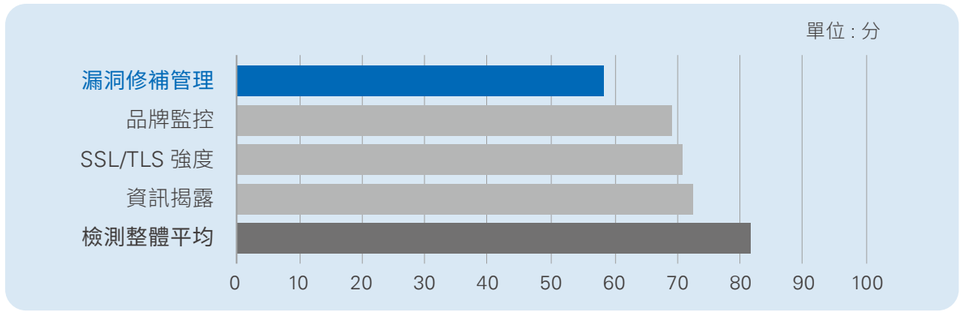
分數 低 高

資安曝險評估項目	評估說明	臺灣 50 家大型企業
隱私 Privacy	憑證管理	
	暗網分享	
	資訊揭露	
	社群網路	
	SSL/TLS 強度	
聲譽 Reputation	品牌監控	
	欺詐應用程式	
	欺詐網域	
	IP 聲譽	
	網頁排名	
韌性 Resiliency	攻擊面	
	DDoS 承受度	
	DNS 健康度	
	Email 安全性	
	網路安全性	
安全 Safeguard	應用程式安全性	
	CDN 安全性	
	漏洞修補管理	
	網頁安全性	
	數位足跡	

初步的資安曝險評估，透過網域名稱開出在各數位資料來源中有多少足跡量，而非進行評分

檢測分數

■ 漏洞修補管理



檢測說明

經由全網域掃描器 (如：Censys, Shodan, Zoomeye) 蒐集網路企業資產系統版本，版本號碼經轉換為相對的 CPE-ID 並與 NIST NVD 和 MITRE CVSS databases 進行關聯分析以偵測並估計未改善的弱點。

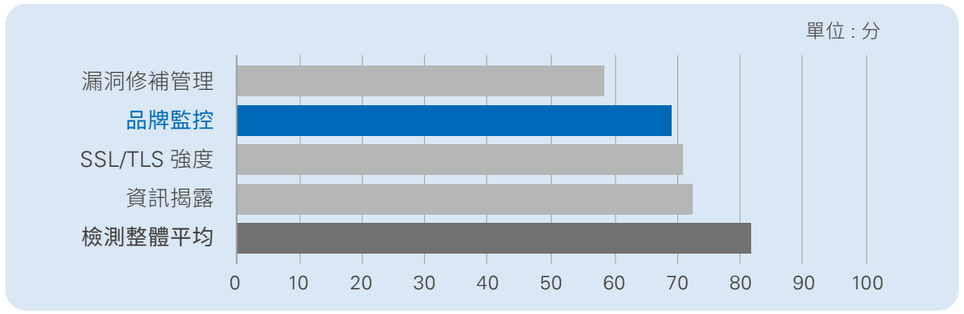
企業遭遇的現況

- 依據 Security Boulevard 調查，有 60% 的弱點攻擊事件，已存在可用之弱點修補程式而未套用
- 在 Dell 調查中，有 63% 的公司認為他們的資料，可能在 1 年內因硬體或晶片的安全漏洞遭到感染

KPMG 建議

- 重視完整的系統弱點管理程序，包含主動資產搜尋、持續監控、緩和風險、修復和防禦步驟
- 廣泛蒐集多元弱點情資，包含情資來源多樣性，與弱點範圍涵蓋性 (如物聯網、雲端、營運科技等)
- 加速修補弱點過程，降低漏洞攻擊風險
- 提升弱點資料庫與現有資訊資產比對之有效性

■ 品牌監控



檢測說明

品牌監控為一項商業分析流程，監控網頁上或透過多種媒體管道以取得企業、品牌、其他與企業外部連結事項的相關資訊。

企業遭遇的現況

企業於網路上的品牌風險如下：

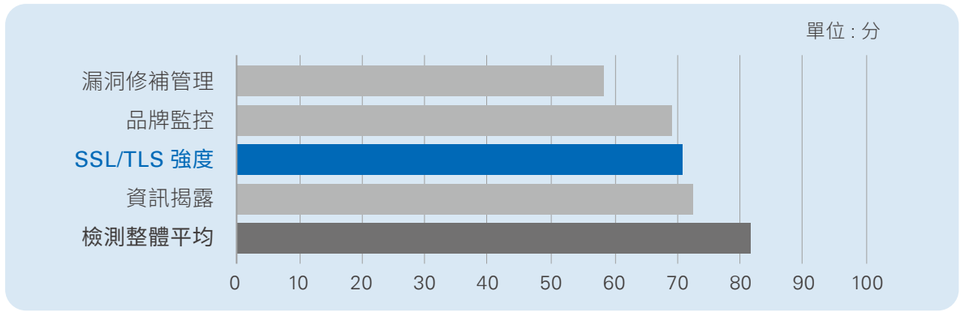
- 因企業域名遭搶註而被劫持 (Typosquatting)
- 商標濫用 / 誤用
- 未經授權的社群媒體帳戶
- 惡意或未授權的應用程式
- 錯誤 / 有問題的機密聲明關係
- 工作場所的負面評論
- 員工的不當行為
- 公司郵件帳戶的可疑使用

KPMG 建議

- 注重社群評論 (如 Google、社群媒體等)
- 監控目前與自身相關之商標、網域名稱 (Domain Name) 或行動 APP 等數位科技運用狀況
- 部署完整的網域保護方案

檢測分數

■ SSL/TLS 強度



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。

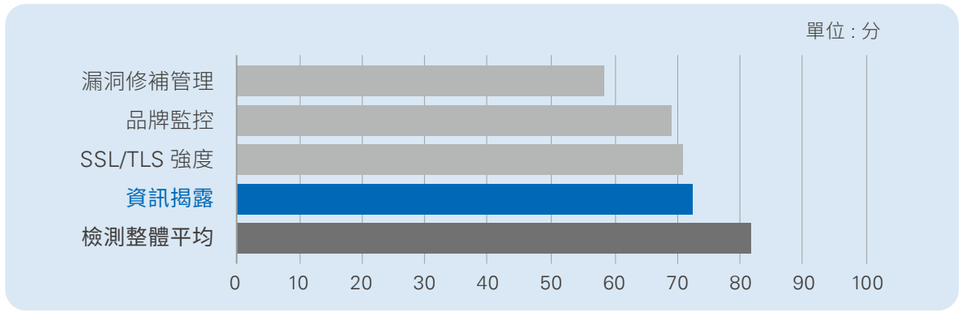
企業遭遇的現況

- 當加密流量成為主流，日新月異的密碼學以及橢圓曲線密碼學 (Elliptic Curve Cryptography, 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

KPMG 建議

- 應審慎使用多網域 / 多域名 (SAN) 憑證
- 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)
- 對外網站之 TLS/SSL 憑證更新應考量使用自動化更新機制
- 使用合宜強度加密演算法

■ 資訊揭露



檢測說明

檢查是否有錯誤的配置或是公開的資產會揭露企業的 IP 位址、email、版本號以及 WHOIS 的紀錄等敏感資訊存在於網路。

企業遭遇的現況

造成資訊揭露的可能性很多，但可以主要區分為三類：

1. 在公開的內容中透漏內部資訊：
   ex. 用戶偶能在開發環境中看到開發人員的註解
2. 不安全的網站配置：
   ex. 沒關掉除錯及偵錯功能，可能讓惡意人士得以用工具獲得敏感資訊
3. 應用程式的設計缺陷：
   ex. 如果網頁會針對錯誤送出明確的錯誤狀態訊息，惡意人士能透過列舉法取得敏感資料

KPMG 建議

- 確保每個網站開發者都充分了解何謂敏感資料，有些看似無害的訊息對攻擊者可能比我們想像中有用
- 盡可能地使用一般錯誤訊息，不向攻擊者透漏多餘線索
- 使用開放或雲端開發環境，應限制除錯、診斷功能，或避免使用真實環境之組態進行測試

後疫情時代的
資安藍圖

2020 年被喻為「5G 元年」，宣告高頻寬、多連結、低延遲的智慧生活即將來臨，而 COVID-19 進一步催化新興科技的腳步，導致要如何應變數位化的挑戰與驟增的資安事件，成為當今全球管理階層最頭疼的問題。KPMG 鑑於臺灣缺乏相關的統計數據和經驗，首次從多個角度檢測臺灣指標企業的網路風險，並依專業提供洞悉與建議。我們將持續留意疫情的趨勢，在不久的未來向各位報告臺灣資安曝險控管的最新情況。最後，在後續的版本中，期許能將數量更多的大小企業、更多元的產業彙整於調查報告，並融合每一次調查的資料進行深入比對與剖析，提供完整的解決方案。

謝昀澤
董事總經理
安侯數位智能風險顧問 (股) 公司

Anticipate tomorrow, deliver today.

期盼本次資安曝險調查調查能成為企業在進行網路防護時的參考依據，透過了解臺灣代表企業普遍的問題、產業的資安曝險概況以及可能造成的財務損失，分析企業須優先改善的項目以及投資的效益。也期待臺灣企業能持續進行內外部各項技術、管理與財務面改善，降低外部威脅提高防護力，往可靠的智能企業邁進。迎接未來數位轉型的榮景，由今日的資安投入做起！

邱述琛
副總經理
安侯數位智能風險顧問 (股) 公司

To make cyber security a business enabler.

本調查能在企業積極擁抱 AI、IoT、雲端及大數據等新興科技的大 5G 新時代，協助了解外部存在的實際威脅。KPMG 正不斷提供引領尖端的優勢服務，由可信賴且具備專業知識及技術的傑出人才，從多元面向預估未來的風險，並協助客戶於現在開始管控。同時我們必須保持冷靜、尋找有彈性、且可信賴的方法來平衡資安威脅與數位應用機會，使網路安全成為業務機會的推動者。

林大馗
副總經理
安侯數位智能風險顧問 (股) 公司

Protect your cybersecurity in the new reality.

疫後全球企業正在面對不尋常的挑戰，經由本調查企業更可了解，臺灣所面臨的數位安全挑戰，比以往任何時候都顯得更為嚴峻，且存在未來的新日常中。為了保護未來的數位發展，KPMG 將尋求一切可能性，協助我們的客戶，能為未來的風險超前佈署，化危機為轉機。

調查方法

© 2021 KPMG Cybersecurity Co., a Taiwan company limited by shares and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

臺灣企業資安曝險大調查　調查方法

財務面向：評估架構與流程

本調查的財務損失風險是依據資訊風險因素分析(Factor Analysis of Information Risk, FAIR)模型，利用發生頻率、比率、數值化無形資產損失等進行計算，將資訊安全的風險量化。本模型將由曝光度、威脅機率、應變能力等算出明年可能會發生多少次損失事件(損失事件發生的頻率)，並由每次資安事件所估計造成的直接與間接損失算出將對企業造成多少損失(損失規模)。最後，將損失事件發生的頻率與造成損失相乘，計算下一年度財務損失風險最大最小金額的可能區間，以得出下一年度的財務損失風險。

下一年度
財務損失風險

- 損失事件發生的頻率 (Loss Event Frequency)
  - 組織將面臨多少次威脅
    - 威脅者可能接觸組織的次數(與曝光度有關)
    - 接觸中有多少比例將造成威脅
  - 威脅有多少比例會導致損失
    - 威脅社群成功造成損失事件的能力
    - 控制元件的抵抗能力
- 損失規模 (Loss Magnitude)
  - 每次事件將損失多少錢
    - 組織面臨資料外洩事件的平均規模
    - 其他要素，如：事件應對能力、員工訓練、保險
  - 連帶利害關係人的損失影響

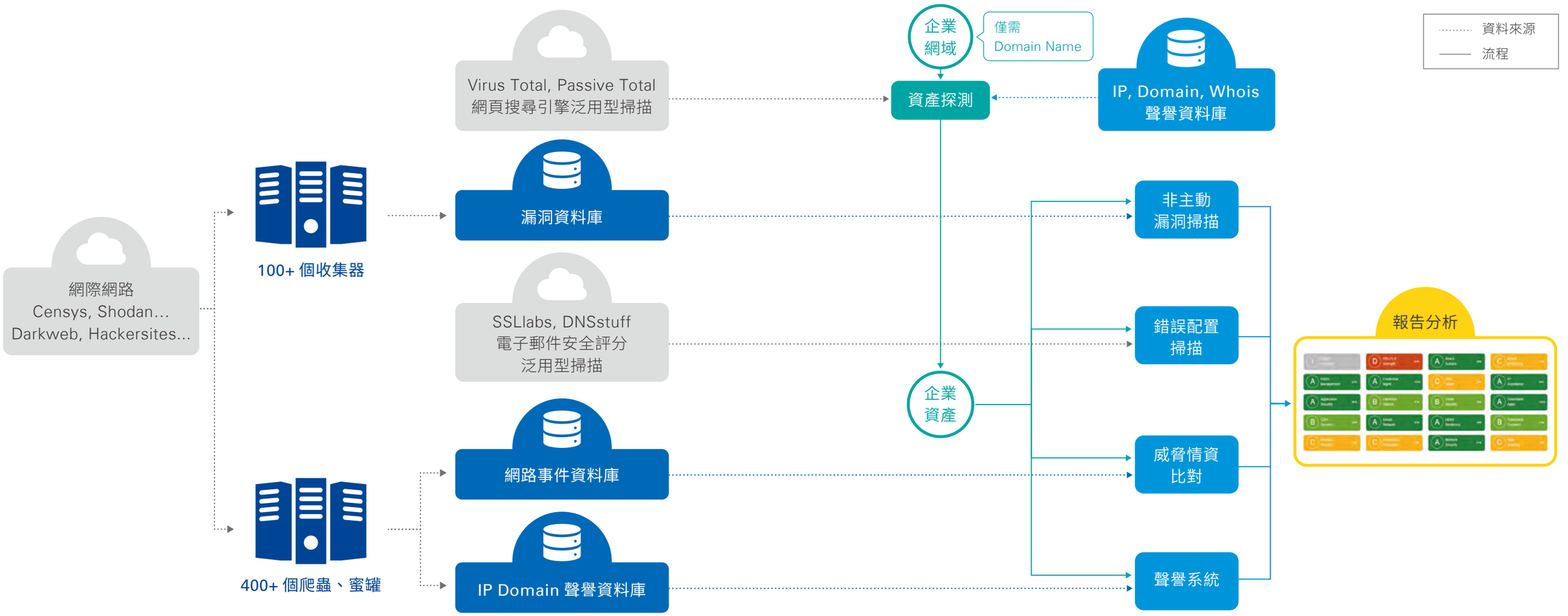
© 2021 KPMG Cybersecurity Co., a Taiwan company limited by shares and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

臺灣企業資安曝險大調查　調查方法

技術面向：評估架構與流程

本調查透過輸入企業的主網域名稱，並與從 VirusTotal、PassiveTotal、網頁蒐集引擎和網路掃描器等蒐集來的資料進行比對，推斷企業的資產範圍。

另外也透過上百個收集器、網路爬蟲等來進行資料庫的建立，並依四大面向進行分類，最後將企業資產與情資進行比對，將檢測結果進行評分。



© 2021 KPMG Cybersecurity Co., a Taiwan company limited by shares and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

臺灣企業資安曝險大調查　調查方法

技術面向：檢測項目及說明

隱私性 Privacy

- **SSL/TLS 強度**
  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
- **機密洩漏**
  檢測及比對網路、地下論壇的五十多億筆遭駭的電子郵件和密碼
- **暗網分享**
  駭客在地下論壇或暗網中公開他們的攻擊目標，檢測將從上百個暗網論壇、犯罪網站蒐集資訊，並篩選出屬於企業的資訊結果
- **社群網路**
  駭客常在社群網站公開其攻擊目標，並鼓舞其他駭客一同對該目標進行攻擊。此項檢測為篩選數十億筆社群網站內容的結果
- **資訊揭露**
  檢查是否有錯誤的配置或是公開的資產會揭露企業的 IP 位址、email、版本號以及 WHOIS 的紀錄等敏感資訊存在於網路

聲譽 Reputation

- **品牌監控**
  品牌監控為一個商業角度的分析，關注網路、其他媒體等多種管道以取得企業、品牌、其他與企業外部連結的事項的相關資訊
- **IP 聲譽**
  資產聲譽分數為根據被列入黑名單或用作複雜的進階持續性滲透攻擊 (APT) 攻擊的 IP 或網域數量計算而成，聲譽資料藉由 VirusTotal, Cymon, Firehol, BlackList DNS servers 等蒐集
- **欺詐網域**
  詐騙的網域和子網域經網域登記資料庫取得，登記的網域資料庫有超過 3 億筆紀錄
- **欺詐應用程式**
  偵測可能被用來駭入或釣取員工或客戶的資料詐騙或私人行動裝置或桌面應用程式 (如 Google Play、App Store 和其他私有應用程式商店裡的應用程式)
- **網頁排名**
  Cisco、Alexa、Majestic 追蹤網頁並根據受歡迎度、反向連結、參考資料等排名網頁，這個項目展現 Alexa 和 Majestic 的結果、Google Page insight 速度檢測成果及網頁內容可及性指引 (WCAG) 2.0 解析的合規結果

韌性 Resiliency

- **攻擊面**
  攻擊面是對企業公開的重要埠、過時服務、應用程式弱點、SSL/TLS 強度、任何配置錯誤進行的技術分析
- **DNS 健康度**
  DNS 健康度報告經由 40 多個控制項目產生，經由線上服務 (IntoDNS, Robtex, Netcraft and HackerTarget) 蒐集
- **Email 安全性**
  經線上服務 (如 : MxToolbox and eMail Security Grader) 蒐集潛在的電郵伺服器和 SMTP 錯誤配置
- **DDoS 承受度**
  此項目進行了 15 項 DDoS 的檢測，並偵測是否有被進行放大攻擊的可能。該資料是經由非侵入式的掃描器及其他全網掃描器蒐集
- **網路安全性**
  分析網路層問題和偵查任何開放的重要的埠、未受保護的網路裝置、防火牆的錯誤配置

安全性 Safeguard

- **數位足跡**
  範圍涵蓋 open ports、services、application banner
- **漏洞修補管理**
  經由全網路掃描器 (如：Censys, Shodan, Zoomeye) 蒐集網路企業資產系統版本，這些版本號碼經轉換為相對的 CPE-ID，並與 NIST NVD 和 MITRE CVSS databases 進行關聯分析以偵測任何未進行改善的已知弱點
- **CDN 安全性**
  分析 CDN 的傳輸內容以偵測淺在的弱點
- **應用程式安全性**
  從多個網路掃描器蒐集網頁應用程式的內容並分析應用層弱點 (如：Cross-site request forgery、Cross Content Mixing、敏感資訊的純文本傳輸)。結果再與 MITRE CWE 資料庫進行關聯分析以偵測發現事項的嚴重層級
- **網頁安全性**
  檢測企業主網頁的 SSL/TLS 、漏洞修補管理、應用程式安全性、網頁排名及品牌監控

調查限制

方法之限制

本檢測工具為調查期間 (2020/8 - 2020/10) 透過收集器、爬蟲技術取得外部多元大數據「情資」等客觀調查依據，此資安曝險僅能作為資安概況的其中一項參考指標。

企業仍需搭配弱點掃描、滲透測試等深入的檢測來做資訊安全的防護。

樣本之限制

本次調查範圍鎖定臺灣 50 家大型企業，雖不能完全代表臺灣整體企業的資安曝險狀況，但因為皆為各產業代表企業，仍具足夠參考性。

另外，調查中 5 大產業是依集團之主網域公司的主要業務性質做大致區分。如集團橫跨不同產業，其產業分類將與子公司分別實際所屬的產業有所差異。

推論之限制

財務損失風險的預測，是經自動化智慧型工具計算產出，頻率及規模皆為估值，其風險結果為一區段，將產生某些程度的偏差。

網路防護分數則是由不同權重的各檢測項目加權平均計算得出，因此總分反映的是組織的網路防護概況，並不完全代表資安曝險個別項目的水準。

Contacts

數位智能風險顧問服務團隊

Team Leaders

張允洸 Stanley Chang
執行副總 Partner
安侯企業管理股份有限公司
T +886 2 8101 6666 #07070
E schang@kpmg.com.tw

謝昀澤 Jason Hsieh
董事總經理 Partner
安侯數位智能風險顧問股份有限公司
T +886 2 8101 6666 #07989
E jasonhsieh@kpmg.com.tw

邱述琛 David Hsiu
副總經理 Director
安侯數位智能風險顧問股份有限公司
T +886 2 8101 6666 #11900
E dhsiu@kpmg.com.tw

林大馗 Toni Lin
副總經理 Director
安侯數位智能風險顧問股份有限公司
T +886 2 8101 6666 #15320
E tonilin@kpmg.com.tw

Contributors

蕭子勤 Sherry Hsiao
研究員 Researcher

黃國禎 Charlie Huang
研究員 Researcher