Dec. 2021

OneDegree
臺灣保險業
資安曝險調查報告

IXT | Cymetrics

關於 OneDegree

OneDegree 成立於 2016 年，為跨國保險科技新創，致力透過數位科技與創新服務來實踐保險的初衷，將保險流程簡單化及透明化，協助企業發展多元的商品和服務。OneDegree團隊由來自海內外頂尖的金融保險、雲端技術與資訊安全領域專家所組成，已獲世界級企業投資，並與多間國際級保險公司合作。

OneDegree 以旗下 IXT 保險科技解決方案，賦能保險業者快速推展銷售創新商品，提升營運效率，其開放式架構可無縫與外部通路平台整合，透過異業合作建構保險生態圈，豐富業務場景、實現營收增長，並藉由數據驅動的技術應用導入，協助業者打造全新保險體驗，創造顧客價值。同時OneDegree擁有 ISO27001 與 ISO27017 雙重認證，搭配內部資安團隊 Cymetrics 提供的資安檢測與顧問服務，以最高規格提供企業嚴密的資安防護與隱私管理。

前言

金融業是資訊防護領域扎根最深的產業，因金融網路犯罪利益驚人，且其管理的數據資料在資訊時代是高價值的無形資產。然而，駭客攻擊標的正逐漸由銀行業轉向保險業，主要因保險業擁有不遜於銀行業的龐大數據資料，資安成熟度卻普遍不及後者，駭客因此能以較低成本獲取更高報酬。

2021 iThome 的資安大調查結果顯示，金融保險業面臨的資安風險以駭客與資安漏洞為主。OneDegree 長期密切關注產業資安動向，亦觀察到業界從 2021 年初以來發生了多起大型資安事件實例，包含三月份美國第六大保險公司 CNA 遭到勒索軟體攻擊，導致保險業務的承保和索賠方系統因破壞而被中斷，迫使其支付 4 千萬美金。五月份開始，保險業更是面臨一連串資安攻擊，保險巨頭 AXA 安盛遭到雙重勒索軟體攻擊，駭客盜竊包括身份資料、銀行文件、醫療及索償記錄等約 3TB 規模之數據。加拿大學生健康險提供公司 Guard.me 偵測到駭客入侵，外洩之資料包含客戶生日、電話號碼、電子郵件及加密後的密碼。英國 One Call Insurance 主動揭露其遭遇勒索軟體攻擊致使保險服務停擺。八月份則是新加坡 Tokio Marine Insurance Singapore 於聲明稿中揭露遭遇勒索軟體攻擊，幸而已採取必要措施，並沒有造成損害。

該份 iThome 調查也顯示，在資安投資金額上，整體企業資安預算編列約新台幣 772 萬。即便如此，資訊長普遍認為資安預算需再增加四成，方能因應頻繁發生的資安威脅。然而資安攻防是一場不對稱的戰爭，防守方即使投入了不成比例的資安預算，仍可能因一個微小的防禦缺口，導致全盤潰敗。資安理論上常引用的短板理論亦呼應此點——企業資安防禦的能量，並非取決於木桶的平均高度，而是取決於最短的那根木板。為了跟上駭客腳步，現代化的資訊安全策略應從傳統的「合規導向」，演進成「駭客視角的風險導向」。重點不在於投入高額預算，而是從持續性的資安檢測開始，早駭客一步改善可能被突破的缺口，化風險為企業競爭優勢。

此資安曝險調查報告，為 OneDegree 使用內部資安團隊 Cymetrics 研發的專業 SaaS 資訊安全評估平台，透過其所提供的曝險評估即服務 EAS (Exposure Assessment as a Service)，結合法遵技術面之合規評估，針對臺灣 30 家壽險及產險業者的外在資安曝險情形進行評級與分析，望力助在地保險業者洞悉其可能存在之外在資安曝險，著手優化治理流程，提升風險管理效益。

目錄

關於本調查 1

調查主要發現 5

改善建議 9

總結 11

關於本調查

調查範圍

為協助臺灣保險業者了解其可能存在之外在資安曝險，OneDegree 透過 Cymetrics EAS（資安曝險評估即服務；Exposure Assessment as a Service），並綜合比對相關法遵技術，在不影響受測業者提供服務的前提下，針對臺灣 30 家壽險及產險業者的外在資安曝險情形進行評級與分析。

檢測項目

本調查所使用之EAS 資安曝險評估即服務，主要針對下述五大常見的外部曝險面向進行檢測評估：

網路服務 (External Service)	網站 (Website)	電子郵件 (Email)	帳號密碼 (Credential)	雲端安全 (Cloud Security)
• 遠端控制 • 資料庫 • 應用服務 • 黑名單	• 網頁伺服器 • 網頁應用 • 憑證 • 網域	• 公開的對外郵件服務 • SPF • DMARC	• 帳密外洩 • 外部服務帳號 • 暗網情資比對	• 公開的雲端儲存 • 公開的公共程式庫

網路服務（External Service）

此項為企業依據業務型態提供公開對外的網路服務，例如藉由開放對外資料傳輸介面來滿足供應商的資料交換需求，或是開放遠端連線介面以滿足員工在家工作需求。若沒有妥善管理這些網路服務介面，其往往會成為常見的駭客入侵管道。本項測試主要蒐集下列資訊進行風險評估：

- 遠端控制：確認是否有公開對外的遠端控制服務，以及該服務是否有被入侵之可能性。
- 資料庫：確認是否有公開對外的資料庫服務，以及該資料庫是否有已知漏洞。
- 應用服務：枚舉企業對外的應用服務，並確認其攻擊表面所存在之弱點。
- 黑名單：檢視暗網情資，了解業者是否因防護疏失，而被列為惡意攻擊跳板黑名單。

網站(Website)

幾乎每家企業都有一個以上的對外網站服務,而無論其目的是提供客戶完成交易、協助員工執行例行工作,或開放大眾取得公司簡介,網站常是駭客首先用以檢視該企業資安狀態的重要標的。若網站呈現鬆散的資安控管,駭客便會認為其入侵成本低,也因此提升後續研究入侵管道的誘因。本項測試主要蒐集下列資訊進行風險評估:

- 網頁伺服器:確認網頁伺服器所有未設置或安全等級不足的安全性設置,並檢視該伺服器版本是否存在已知漏洞。
- 網頁應用:檢測不安全的標頭設定,降低用戶在與網站互動過程中洩漏敏感資訊及被偽冒請求的風險。
- 憑證:檢測憑證加密套件的安全性強度,確認網站是否使用有漏洞之加密套件。
- 網域:列舉與該企業相關的網域,了解是否存在會對其造成影響的惡意網域。

電子郵件(Email)

每個員工每天幾乎都需要透過電子郵件服務與外界互動,然而再嚴密的資安防護,也很難確保員工擁有完善的資安意識。根據統計,八成以上之資安事件主要是以電子郵件為起點,因此管理好企業的郵件曝險,可有效事先降低駭客事件發生。本項測試主要蒐集下列資訊進行風險評估:

- 公開的對外郵件服務:檢測企業是否有對外公開之郵件伺服器,避免該伺服因安全設置不完善而成為資安破口。
- SPF:檢測企業網域之 SPF 設定是否完善。SPF 設定主要確認郵件是否確實由該企業所授權的伺服器發送,避免駭客假冒企業內部網域發釣魚信件至員工或客戶。
- DMARC:檢測企業網域之 DMARC 設定是否完善。SPF 若搭配 DMARC 設置,則能進一步強化收信方於電子郵件閘道中處理假冒電子郵件之能力,DMARC 也為 Gartner 2021 資安防禦十大重點之一。

帳號密碼 (Credential)

由於社群網站及雲端軟體即服務盛行,越來越多的員工會將企業內部帳號密碼使用於外部服務中。若該服務廠商資料外洩,駭客也往往得以輕易取得內部員工之帳號密碼而進行滲透,或是使用該等資訊對企業高層、員工或客戶進行社交工程。本項測試主要蒐集下列資訊進行風險評估:

- 帳密外洩:將企業內部帳號與知名資料庫進行比對。
- 外部服務帳號:檢測企業網域是否已註冊於常用之外部服務;駭客可能先使用企業內部網域註冊該等外部服務,作為社交工程之攻擊準備。
- 暗網情資比對:檢測企業網域是否於暗網中被提及;駭客可能於暗網中分享該企業已被開採之漏洞或機敏資料。

雲端安全 (Cloud Security)

越來越多企業因考量成本效益而採用雲端解決方案，然而由於雲端架構打破傳統疆界之防護概念，加上雲端安全性設定複雜度高，企業容易因不經意的小失誤而引發嚴重的資安事件。本項測試主要蒐集下列資訊進行風險評估：

- 公開的雲端儲存：檢測企業是否有公開對外的雲端儲存體；目前排名前幾名的資料外洩事件，多數是由公開的雲端儲存體外洩，因此如何妥善管理好雲端儲存體，避免其成為機密資訊外洩的管道，為雲端資安管理的重要課題。
- 公開的公共程式庫：檢測企業是否有公開對外的公共程式庫；公共程式庫中可能存在組織內重要服務之程式碼、帳號密碼與歷史編輯紀錄，這些資訊都有機會被駭客進一步用以尋找漏洞並伺機攻擊該企業。

評級說明

本調查之資安評級方式為系統性地歸納由 MITRE 提出的 ATT&CK 資安框架，以及美國國家基礎建設諮詢委員會 (National Infrastructure Advisory Council；NIAC) 公開的通用漏洞評分系統 (Common Vulnerability Scoring System；CVSS)，並根據即時風險情資調整評級權重。評級越高代表企業曝險及弱點越少，亦即企業資訊安全的防禦越完整及穩固，反之，評級越低代表駭客可利用資訊及完整執行攻擊鏈的可能性越高。此資安評級由高至低依序分為 A、B、C、D、F 五大評級，各評級代表之意義如下表：

評級 / 項目	A	B	C	D	F
可被用於攻擊的對外資訊量	極度有限	少量	有一定數量	大量	極大量
是否引發駭客攻擊動機	極難引發	低機率	有可能	高機率	極高機率
攻擊成功機率	極難成功	低機率	有可能	高機率	極高機率

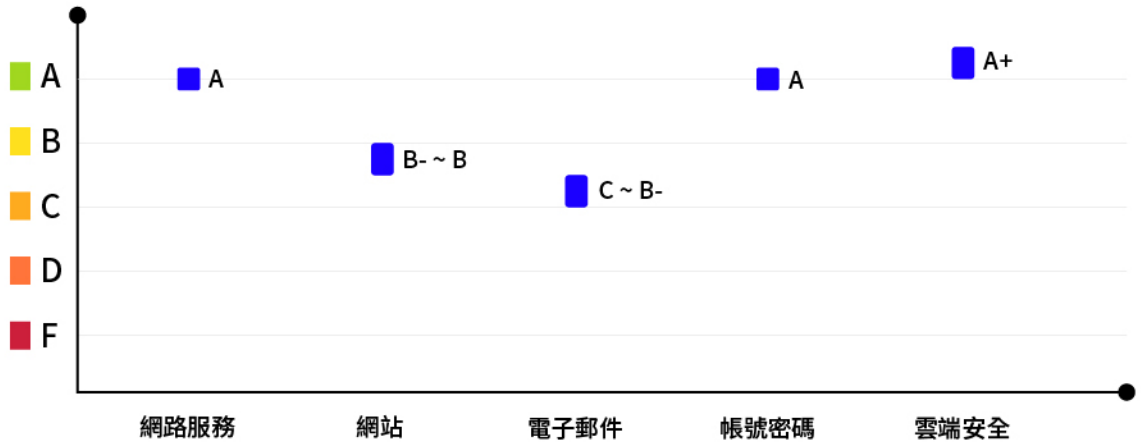
法遵技術面評估

除了藉由上述五大外部曝險面的安全評估檢視，OneDegree 亦針對產業法遵技術面進行合規評級。合規評級主要有兩大來源，一部分為企業自身產業或客戶要求所需遵循的合規標準，如 ISO27001 資訊安全管理及 PCI DSS 支付卡產業資料安全標準，另一部份則為政府所制訂的資訊安全規範，如歐盟為保護個人資料所制定的 GDPR 一般資料保護規範，而在臺灣則是有個人資料保護法跟資通安全法。

本調查所評估的法遵技術面向包含 ISO27001、PCIDSS、GDPR 之三大產業常見遵循法規，可協助企業從合規面向檢視資安曝險。相較於傳統內控面的合規狀況，由於技術面合規更直接關聯到企業防禦工事的完善程度，因此藉由技術面合規評比，企業能夠更透明地從法規面向之短板開始，逐步改善資訊安全，同時也能避免因未做好合規管理而遭主管機關裁罰，導致直接或間接影響業務營運。

調查主要發現

本次針對臺灣保險業者之五大外部曝險面調查結果概覽如下：



網路服務 (External Service)

在網路服務中臺灣保險業者的表現良好，95% 以上的保險業者皆有控管對外服務，資安評級平均落在 A 的等級，即從外部的角度蒐集不到資料，很難針對業者的對外服務進行資料蒐集及攻擊嘗試。

網站 (Website)

在網站應用的部分，臺灣保險業者資安評級平均落在 B- ~ B，也就是有外部曝險面上的短板產生，可能因此成為攻擊者攻擊鏈的一環，而評級降低的原因主要在於業者網站的防禦設定上有五項安全設置錯誤比例偏高，推測因其大多為預設的配置，導致容易被忽略。以下針對五點導致評級降低的錯誤設置進行說明：

1. Cookie 的三項基本安全設定 Secure、HttpOnly 及 SameSite 未完整設置

針對 Cookie 的三項基本設定項目 (含「能夠預防跨腳本攻擊的 HttpOnly」、「強化 Https 機制的 Secure」、「預防跨站請求偽冒的 SameSite」)，有 60% 的業者設置不全，其中 38% 業者三項皆無進行防護設置。由於三項安全設定皆為網站公開資訊，在相關資訊容易取得的情況下，此項目成為目前攻擊者篩選攻擊標的第一層過濾，故設置不全以及未設置的業者，很容易被納入攻擊者的標的清單。

2. 內容安全性原則 (Content Security Policy, CSP) 未完整設置

針對跨腳本攻擊的強化防護設置CSP（內容安全性原則）項目，業者未設置或設置錯誤的比例高達86%。經過檢視，其中多數的設置錯誤都是考量網站建置的方便性，讓第三方套件能更順利地應用在網站中，而採用不安全的內容安全性原則如 unsafe-inline 或 unsafe-eval，使內容安全性原則出現漏洞。攻擊者便可以利用配置錯誤的內容安全性原則，設計針對性的攻擊鏈。

3. X-Frame-Options 未設置

針對點擊劫持攻擊進行防禦的 X-Frame-Options 設置項目，有 60% 的業者無進行此項設置或安全等級不足，代表網站可能有遭「點擊劫持攻擊」的風險。「點擊劫持攻擊」是攻擊者在網站上通過 iframe 隱藏目標網頁，欺騙用戶點擊隱藏惡意連結，例如覆蓋於購物網頁的購物車上之隱藏超連結。使用者點擊後，便會自動下載惡意軟體或造訪惡意網頁，導致機密資訊外洩。而此類資安事件發生，極有可能致使業者商譽受損。

4.未實作 CSRF Token

預防跨站請求偽冒的強化 CSRF Token，是在網站防護上為了防止用戶身份被竊取盜用而衍生出的網站進階防護。由於此項設置需建置額外的套件或框架，在資安資源有限時，業者大多會將其建置次序向後遞延。或許也因此於此次資安評估中有 56% 的業者並未建置 CSRF Token 功能。

5.網站憑證授權機關資源記錄檢查未設置完整及加密等級不足

在網站憑證的資安評級中，有 90% 的業者憑證完整性不足，例如憑證撤銷機制未設定完整。在沒有這些設定的情況下，業者難以防堵任意數位憑證認證機構擅自簽署網域憑證，而憑證完整性不足的業者中還包含 30% 使用不安全的加密及 20% 的過期憑證與過舊的 SSL/TLS 協議；以上情況皆增加業者在憑證層面發生資安事件的風險機率。

電子郵件（Email）

在電子郵件部分，臺灣保險業者資安評級平均落在 C ~ B-，也就是從攻擊者的角度而言，有明顯的資安短板產生，若被攻擊者發現則很有可能成為攻擊鏈上的一環。而評級降低的原因主要在於業者大多忽略 DMARC 以及 SPF 設置，導致郵件系統安全出現短板，使業者容易成為攻擊者鎖定執行社交工程攻擊的標的。以下針對 DMARC 以及 SPF 配置狀況進行說明：

1. DMARC 設置不全或無設置

DMARC 可以拒絕惡意電子郵件訊息並隔離其他電子郵件訊息，強化收件者對未授權郵件的識別，藉此降低社交工程發生的可能性。DMARC是業者在進行社交工程演練以及強化員工資安意識之外的建議防護手段，但在此次的資安評估中，73% 業者的 DMARC 設置不全或無設置，其中無設置的比例更高達86%，意味著目前多數的業者仍是依靠社交工程演練以及資安訓練作為防範社交工程的手法。但也如前所述，「勒索軟體即服務」的誕生導致攻擊頻率增加，社交工程防不勝防，僅靠傳統的方式並不能確保業者不受社交工程的影響。

2. SPF 配置錯誤或無配置

SPF 能夠防範網域遭到假冒，讓收件伺服器在收到看似來自業者網域的郵件時，藉由 SPF 驗證該郵件是否確實由授權的伺服器傳送，避免業者成為攻擊者偽冒寄件的目標。在此次資安評估中，有 36% 的業者 SPF 配置錯誤或無設置 SPF，其中無設置 SPF 高達 60%，代表這些業者很有可能因此成為攻擊者偽冒寄件的目標，嚴重則可能導致商譽受損的資安事件發生。

帳號密碼 (Credential)

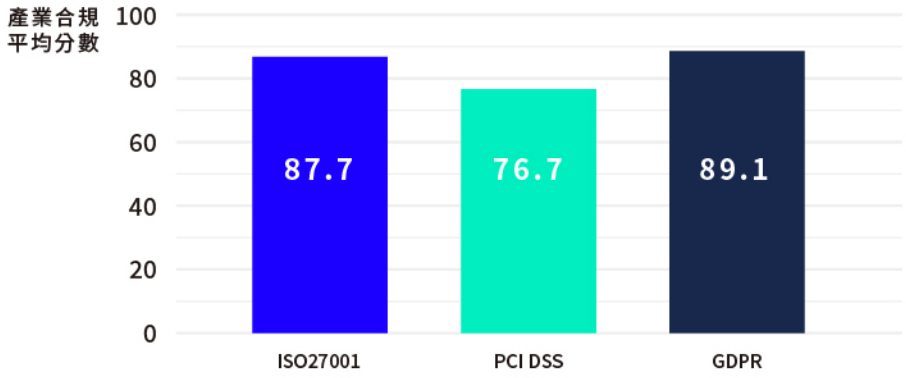
在帳號密碼項目中，臺灣保險業者資安評級平均落在 A，然而需要注意的是有 20% 的業者在暗網被揭露相關帳號密碼等情資，產生極大的資安曝險，故此項目評級特別拆開為 80% 業者為 A+，而 20% 業者為 C+。

雲端安全 (Cloud Security)

在雲端安全項目中，臺灣保險業者評級分數都在 A+ 以上。本調查並未發現保險業者在該網域名稱下有任何對外公開之雲端儲存體或公共程式庫，然而 OneDegree 預期在數位轉型驅動下，將有越來越多企業會逐步採納公有雲服務，OneDegree 亦將持續關注並擴充雲端安全的曝險測試項目。

法遵技術面評估

以下針對三大產業法遵技術依產業平均分數做合規分析，提供業者檢視問題與研擬改善方向，然本調查只針對技術層面可能違反法規之項目進行比對，並不包含政策執行面。



ISO27001

產業合規平均分數 87.7 分，主要因證撤銷機制未設定完整、不安全加密套件及憑證過期，使業者在「Cryptographic Controls」此項目被扣分。

PCI DSS

產業合規平均分數 76.7 分，主要有兩大項扣分項目。第一大項為網站應用上的 CSP（內容安全性原則）未配置或配置錯誤、X-Frame-Options 未設置或安全等級不足及缺少 CSRF Token 及 Cookie 的三項基本設定未設置或配置錯誤，導致在 PCI DSS 的「Develop and maintain secure systems and applications」規範中被扣分。

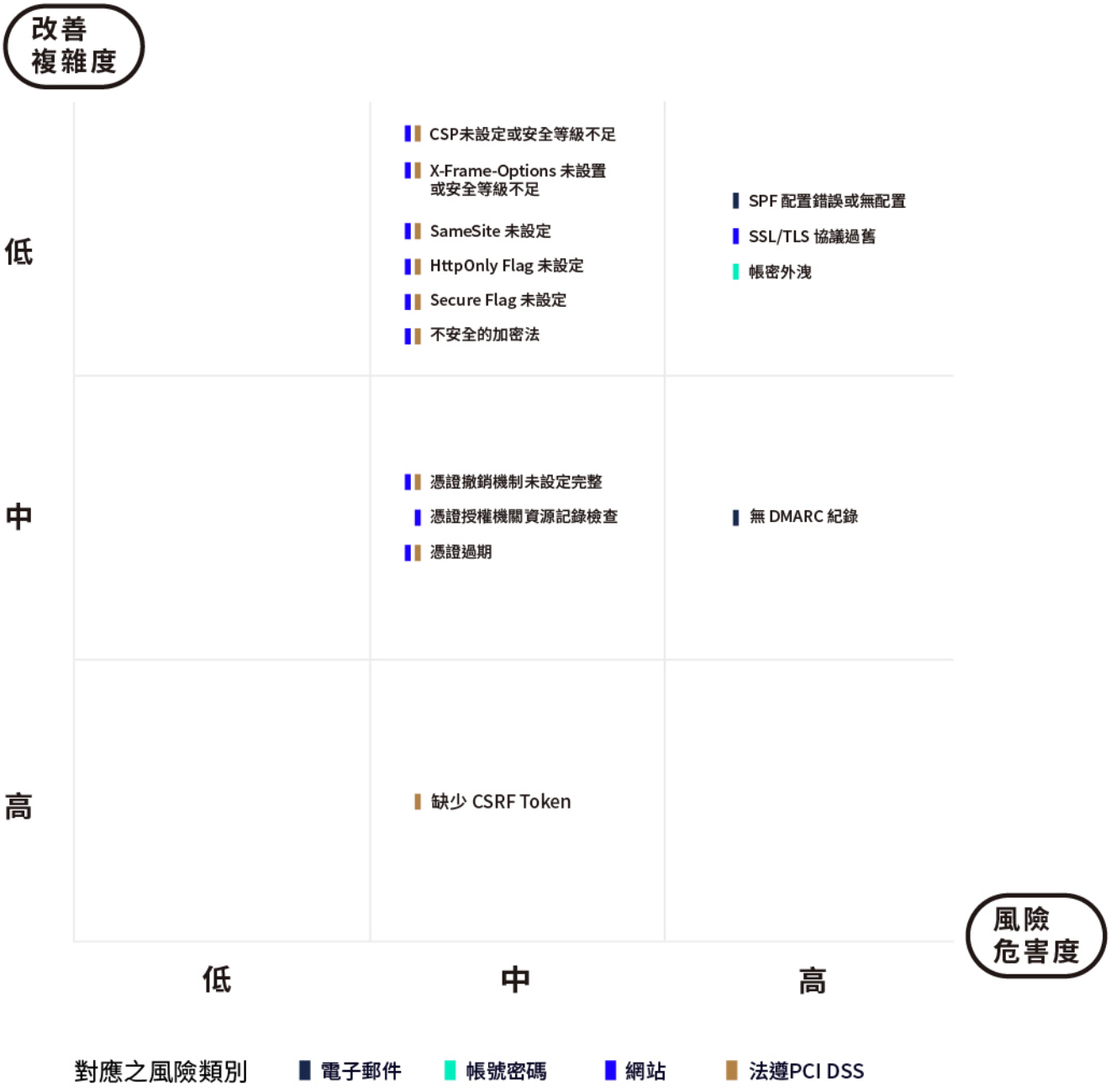
第二大項則是因憑證撤銷機制未設定完整、不安全加密套件及憑證過期，使業者在「Encrypt transmission of cardholder data across open, public networks」以及「Develop and maintain secure systems and applications」此兩項規範中被扣分。

GDPR

產業合規平均分數 89.1 分，主要因證撤銷機制未設定完整、不安全加密套件及憑證過期，使業者在「Responsibility of the controller」、「Data protection by design and by default」、「Security of processing」此項目被扣分。

改善建議

OneDegree 統合上述臺灣保險業者之總體風險及曝險狀況，依據風險危害程度與改善之複雜度進行衡量，以矩陣方式視覺化改善建議項目，提供業者權衡自身內部資源，評估改善之優先順序。



風險危害程度高、改善複雜度低

- SPF 配置錯誤或無配置：依產業最佳實踐為網域設定 SPF 紀錄
- SSL/TLS 協議過舊：停用如 TLS 1.1 等之過舊協議
- 帳密外洩：更換並使用高強度的密碼，且新密碼不應重複使用於其他服務，不應使用生日、姓名等容易取得之個資

風險危害程度高、改善複雜度中

- 無 DMARC 紀錄：依產業最佳實踐為網域設定DMARC 紀錄（必須先設置 SPF 與 DKIM）

風險危害程度中、改善複雜度低

- CSP 未設定或安全等級不足：可於 HTTP Headers 設置 Content-Security-Policy 以避免此風險
- X-Frame-Options 未設置或安全等級不足：為避免此風險，需確保只有可信任來源才能嵌入
- SameSite 未設定：依據網站需求選用 Strict 或 Lax 進行設定
- HttpOnly Flag 未設定：設置開啟 HttpOnly
- Secure Flag 未設定：設置開啟 Secure
- 不安全的加密：在伺服器設定中停用已遭破解之加密套件

風險危害程度中、改善複雜度中

- 憑證撤銷機制未設定完整：依據不同伺服器在設定中使用加密套件完整此功能
- 憑證授權機關資源記錄檢查：為網域設定憑證授權機關資源記錄檢查（CAA RR）
- 憑證過期：聯繫 CA 更新憑證

風險危害程度中、改善複雜度高

- 缺少 CSRF Token：使用經過審查的套件或框架建置 CSFR Token

結論

平衡數位轉型之風險與效益，化資安危機為創新轉機

隨著保險模式快速推陳出新，如今業者不僅可在官網上銷售產品，跨界電商合作和其他多元異業結盟的趨勢也不容小覷，加上大數據、物聯網與新興保險科技等發展，使得系統結構日趨複雜，也意味駭客能藉由更多資安漏洞伺機而起。然而企業在推進創新服務與數位轉型的過程中，往往難以掌握每一個環節的安全性，因資安建置為一漫長且需持續投資的活動，建議企業優先掌握及改善自身資安短板，兼顧業務推展與資訊安全，企業便更有機會顛覆既有模式，成功轉型創新。

掌握企業資安風險，提升品牌信譽與價值

在資安高風險時代，要與時俱進地掌握企業資安風險並非易事，OneDegree 鑑於臺灣保險產業的資安狀況缺乏相關數據，使用內部團隊開發的資安評估平台 Cymetrics 進行多維度的檢核調查，並提供可直接採納的建議。此外，OneDegree 亦整合了 Cymetrics 平台至 IXT 保險科技解決方案中，協助業者持續性地掌握自身企業的網路曝險和系統弱點，提高資安風險管理能力，在提供給客戶更好的服務體驗時，也能同時保護品牌信譽，提升品牌價值。

OneDegree

更多資訊 請聯繫

grow@theixt.com | ask@cymetrics.io