

網路安全的職責

CISO 和 CIO 應如何共享 網路安全所有權

權衡網路安全的職責，會隨著商業環境與威脅版圖的改變演進。

文／Michael Hill 譯／Nica

在多數企業組織中，資安長（CISO）與資訊長（CIO）對網路安全皆負有責任是相當常見的，這是現代企業有效運作越來越重要的關鍵。顯然，明確的網路安全主控權已證實是企業組織安全性定位成功不可或缺的一部份。

近期一份 ISACA 對 3,700 名左右全球網路安全專家的調查中發現，雖然近半數（48%）網路安全團隊直接向資安長報告，但也有四分之一是向資訊長報告。但僅管報告的系統不同，調查報告發現，就資安長與資訊長間安全性職能主控權方面；在網路攻擊的增減、偵測與反應網路威脅的能力，以及網路犯罪報告，並沒有明顯差異。

不過，這份報告發現了網路風險評估的管理階層評價、董事會看待網路安全優先權的方式，與策略一致性相關的差異。甚至，這份報告還指出越來越多業界的做法是資安長向除了資訊長以外的任何人報告，尤其是資安長權責範圍內容包含管理、風險與合規性、營運永續性/災難復原、詐欺、信任與安全性或危機關理的情況下。

網路安全事務的權責在資訊長與資安長間不盡相同，理由無非是企業組織規模大小、領域與合規性要求的不同。儘管如此，隨著網路安全與更廣泛的營運元素變得密不可分，由誰肩負哪種型態網路安全主控權職責，以及為何這麼做，變得越來越重要。

網路安全職責：資安長 vs. 資訊長

Lightico 的資訊長 Omri Braun 用如此總結多數資訊長與資安長網路安全職責間的差異：「資訊長較著眼於確保使用正確工具讓效率最大化，並識別對公司造成影響的趨勢、持續找出可以利用並產出更好技術的契機。資安長承擔的則是確保資料安全性、一致性，並主動保障諸如此類事項的安全。」

Orange Cyberdefense 全球資安長 Richard Jones 同意這種說法：「通常，資安長角色是從營運角度看待安全性，保障企業免於網路威脅。相對地，資訊長則較著眼於將安全性建置融入企業廣泛技術堆疊與進行中的數位移轉專案裡，推動企業復原力、促進使用者體驗並最大化效率。」

網路安全架構師 Tee Patel 甚至表示，資訊長常為了安全性投資報酬率而被迫「走派系路線」，但資安長則多半需要偏向獨立，把聚焦在保障企業本身安全上。「讓企業賺錢並正中目標（CIO），與維護企業安全（CISO），乃現代資訊長與資安長職位的顯著差異。」他如此說道。

這些差異相當微妙。特許資訊安全協會（Chartered Institute of Information Security）執行長（CEO）Amanda Finch 表示，各個角色對資料的態度，正巧概括職責的差異。而資安鑑定與



認證機構 CREST 總裁 Ian Glover 告訴我們，從安全性角度完整區隔資安長與資訊長的角色越來越難。在多數企業組織裡，這些角色太過一致且相互依存。

資安長的網路安全職責

Zoom 的資安長 Jason Lee 表示，他主要將重點放在保護關鍵資訊上，例如客戶資料、員工資料與原始程式碼。「就安全性來看，宏觀考量藍圖很重要。這包括考慮與營運相關的第三方並評估怎麼管理所有風險才是最好的。我同時負責儘可能訓練員工備戰意識，確保他們做好準備並受到保護免於安全性威脅。」

對 HP 的資安長 Joanna Burkey 而言，駕馭混合工作模式時代保障企業安全，是目前安全性工作整體的一部份。「過去十八個月來遠端、在家工作模式，不得不為了網路安全在員工身上加上更多限制，因為工作多半在沒有傳統本地基礎架構保護的前提下完成。」然而，這些安全性政策與限制，是以遠端作業為例外狀況而非常態的時機下所設計，因而必須以全新視野來看待，她表示。「資安長如今必須思考仍能保障企業安全而又降低風險的其他處理方式，但也要體認到真實生活中——尤其是在全球流行病大蔓延下，不見得能夠一定確實遵守政策。」

Jones 補充，管理不斷變化的網路威脅版圖與數位轉型浪潮興起所結合的過度負載，是現代資安長角色另一個必要元素。「網路安全如今必須嵌入企業營運所有層面，還要成為上至執行長下

至初入職畢業生每個人的首要考量。」基於此，資安長必須一開始就將安全性注入公司數位環境的所有面向，確保安全性從數位專案初始就加入，最終要能降低安全團隊收到的警告數量，讓他們更能充份發揮自己的技術與資源，他如此表示。

資訊長的網路安全職責

即便資安長是負責網路安全方面各種日常事務與前瞻規劃的人，但在多數企業組織中，責任通常落在向執行長與董事會報告的資訊長身上，Finch 表示。「值此之故，資訊長不能將責任全交給資安長。反而必須保有對安全性策略的認知，確保它不會讓企業組織整體策略陷入危機，反之亦然。」

Tenable 的資訊長 Brad Pollard 認為，如今的資訊長基於可用性、效能、預算與即時專案交付等種種因素，被賦與各種安全性問責。「資訊長賦與組織內所有營運單位能力並支援它們。在做這些事的同時，他們就承接了各營運單位的資訊安全要求。」

舉例而言，資安長很有可能被要求定義安全性參數，像是漏洞修復或存取控制的服務等級協議，但要將這些需求傳達至所有營運部門、擴展所有公司技術的工作，就落在資訊長身上了，Pollard 表示。「現代資訊長面臨的網路安全重大挑戰，便是滿足營運需求，尤其是控制預算並按時完成，同時維持安全的環境。」

艾塞克斯大學資訊長 Jots Sehmbi 告訴我們，

資訊長角色變得不僅止於運作傳統營運。它已逐漸含括實施新技術為企業組織提供數位能力。

「這些技術中有些對企業組織而言很新，例如 RPA、人工智慧、物聯網」並具有潛在風險，像是資料架構的方式。因此，資訊長有責任讓公司瞭解所有新技術的網路安全趨勢。」

衝突與合作

考量到不完美世界裡的現實，Braun 表示，資安長與資訊長相異的網路安全職責與目標往往導致衝突。然而，他強調必須要團結，才能確保「使用的前瞻思維技術，是以不危及公司、公司資料或公司客戶資料的資安層級與安全性的方式實作，保障其安全。」

資訊長與資安長不能各自為政，必須瞭解雖然也許目的不同，但走的是同樣道路，Jones 表示。「這兩個角色間的協同合作與溝通，對現代企業而言是關鍵。資安長與資訊長必須協同合作，利用 SD-WAN、SASE 與零信任這類能夠安全、效率且不干擾可用性的技術與做法，為企業啟動生產力。」資安長與資訊長團結合作時也必須意識到彼此的牽制，並且在這樣的牽制下作業，他如此補充說明。

Glover 引用了監管單位在此扮演的角色，強調國際性監管社群浮現的問題，監管單位如今已認知到有責任瞭解其受監管單位提供的網路安全保障等級。「這需要同一受監管產業內資訊長與資安長彼此間緊密的協同合作。監管單位會做他們認為對的事，但通常是站在本地角度去看問題。這種主動干預的型態與資訊長與資安長傳統角色極為不同，但若謹慎且同理地進行，將能降低營運成本，讓更多資源集中在控制而不是報告上，還能透過對業務與降低成本增加效率需求展現真正的理解，提升資訊長與資安長在組織裡的地位。」

企業營運不斷進化中的網路安全角色正在改變資訊長與資安長間的凝聚力變化，Lee 補充道，這是他在 Zoom 的親身經歷。「我們都必須將網路安全放在第一位，共同對抗不斷出現的威

脅。在做任何決策時，安全性必須是我們的首要考量。對彼此的策略與關鍵舉措保持參與至關重要。我們持續彼此參與對方的策略，即便我們不認為另一方有必要確保彼此有共識與堅定的一致性。意即我們的角色比以往有更多連結，協同合作重要性甚於以往。」

網路安全主控權的未來

展望未來，專家們預測資安長與資訊長的網路安全職責會有顯著進化。「我們會看到資訊長與資安長努力讓安全性成為具有一致標準、行為模式與執行模式的可信任根源——就像法律、醫學與會計這類專業一樣，擔負同等重要責任。」Finch 表示。

Zscaler 的資安長 Marc Lueck 認為，資訊長未來幾年會有一段有趣的網路安全旅程。「這個角色與個人，若不是變得對於利用各異成本與獲益模式，平衡這兩個迥然不同的必要服務相當熟練，就是資訊長會負責 IT 安全性交付，管理、或許包括執行則由不再向他們報告的資安長負責。兩種模式將會並存，而且若這些角色用的是對的人都能成功。」他指出，網路安全失誤對資訊長來說「現在沒什麼大不了」，但網路安全對資訊長而言將變得如同效率與削減成本技能一樣重要。

Pollard 補充，這有點像現代營運單位透過 SaaS 平台，承擔部份傳統 IT 應負責任一樣，資訊長更需要負責找出營運單位裡的安全性專家。「這些專家不僅需要知道如何保障企業使用特定技術的安全，還必須要能意識到特定營運單位最大風險的威脅情勢。」他補充。

Glover 預測，資訊長與資安長的共承職責會在第三方連結和合併與收購時有所改變，雙方必須共同合作，建立有用的處理程序，加入安全性與保障。「他們將共同作業，確保屬於企業內重大舉措的一部份，透過他們的實力與權力，對第三方連結和收購與合併做出明智、深思熟慮的聲明。」