CISO－關鍵領導要角的職責與資格

資安長之必須(1)

瞭解獲得 CISO 職務需要些什麼，以及如何才能成功扮演這個角色。

文／Josh Fruhlinger 譯／Nica

資安長(CISO)是負責企業組織資訊與資料安全的高層長官。雖然過去對這個角色的定義較為狹隘，但近年來它經常與CSO及安全性VP互通，說明了這個角色在企業組織裡定義更廣了。

有企圖心的資安專家，希望登向公司企業巔峰就可能將CISO職位放在目標上。讓我們來看看，能做些什麼提升取得CISO一職的機會，當你獲得這個重要角色又將涉及哪些義務。若想將CISO加進企業組織職務名冊裡-或許是第一次，也該一讀本文內容。

CISO職責

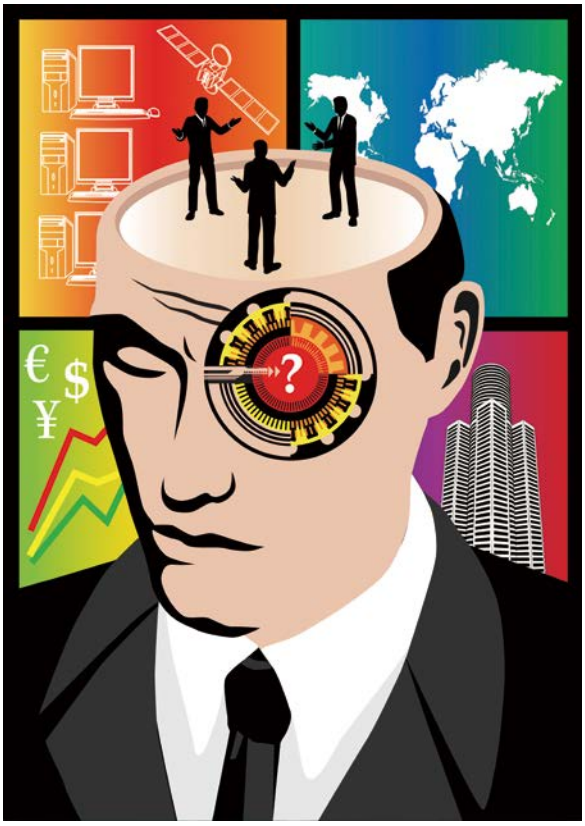
CISO工作內容有哪些？或許，瞭解CISO職務的最佳方式，就是獲悉他日常負責保護的一切。雖然沒有兩份工作完全相同，但90年代Citigroup的CISO先鋒Stephen Katz，條列了與MSNBC會談中總結的CISO責任範圍。他將這些職責切分為以下類別：

- 資安操作：即刻威脅的即時分析，以及發生問題時的情況鑒別分類
- 網路風險與網路情報：對於正在發展的安全性威脅保持最新狀態的瞭解，並協助董事會知曉，因收購或其他重大營運動作可能導致的潛在資安問題
- 資料漏失與詐欺預防：確保內部人員不會誤用或竊取資料
- 資安建構：規畫、採購與推展資安軟硬體，確保IT與網路基礎架構是以最佳安全性實作為宗旨進行設計
- 身份與存取管理：確保只有獲得授權的人擁有管制資料與系統的存取權
- 計畫管理：實作緩解風險的計畫或專案-例如定期系統修補，在資安需求上維持領先地位
- 調查與法證：確認在外洩事件出了什麼問題，若發生於內部，處理責任歸屬，並規畫如何避免相同危機一再發生
- 管理體系：確認上述所有舉措順利運作，並取得所需資金，且公司領導高層理解它們的重要性

CISO資格

這個角色的考量有哪些？概括來說，CISO需要紮實的技術基礎。Cybrdegrees.org認為，傳統預期這位候選人會擁有電腦科學或相關領域的學士學位，並具7至12年工作經驗(包括至少五年的管理職)；著重在資安上的技術性碩士學位也越來越流行。此外還有一系列預期的技術能力清單：除了所有高階技術高層預期該具備的編寫程式與系統管理基礎之外，你還應該瞭解一些以安全性為主的技術，像是DNS、路由、驗證、VPN、代理器服務與DDOS緩解技術、程式碼實作、道德駭客(白帽駭客)與威脅模組，以及防火牆與入侵偵測/預防協定。由於一般預期CISO會協助法規合規性，你也應該要瞭解PCI、HIPPA、NIST、GLBA與SOX相容性評估等內容。

不過，技術知識並非得到該職務的唯一條件，甚至可能不是最重要的。畢竟，大部份CISO職務含括管理與在公司領導層提倡安全性。IT研究人員Larry Ponemon在SecureWorld的演講中表示「多數傑出的CISO都擁有不錯的技術基礎，但通常還擁有商業背景、MBA，以及與其他CXO高層及董事會溝通所需



的技能。」

人力資源機構LaSalle Network的技術服務資深部門經理Paul Wallenberg認為，判定CISO候選人技術與非技術能力的組合，會因公司招募動作而有所不同。「大致上來說，營運層面達到全球或國際的公司企業，會尋求全面性、實用的資安背景候選人，並在瞭解職涯進程與過往成就時，採取評估領導能力的處理方式。」他表示。「另外一面，營運層面著眼於更多網路與產品的公司行號，則傾向於雇用應用程式與網站安全性相關特定技術能力組合的人。」

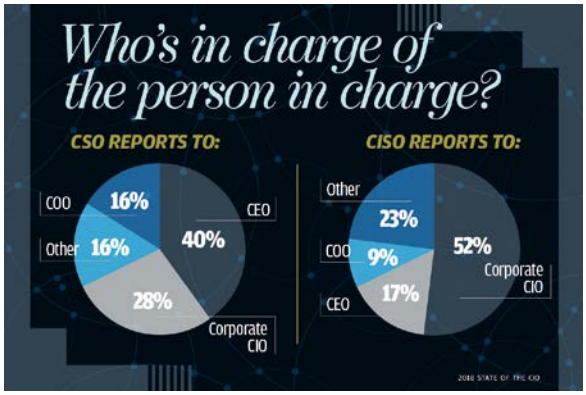
CISO證照

當你扶搖直上預期躍入CISO一職，用證照為你的履歷增添光彩有益無害。正如Information Security的看法：「這些合格證書會更新記憶、喚醒新思維、增加可信度，而且是所有健全的內部訓練課程必要部份。」不過，Cyberdegrees.org 所列的七項讓人有點不知從何選擇。我們請Lasalle Network的Wallenberg從中選擇，他給了我們前三名：

- 「Certified Information Systems Security Professional (CISSP)是提供給尋求以資安作為職涯重點的IT專業人士。」
- 「Certified Information Security Manager (CISM)廣受追求提升資安學科領域，轉換為領導階層或專案管理者所歡迎。」
- 「Certified Ethical Hacker (CEH) 是給尋求獲得威脅企業安全性議題進一步瞭解的資安專家。」

CISO vs. CIO vs. CSO

資安，是企業組織中無可避免與其他人產生衝突的角色，因為資安專家的本能是鎖住系統，讓人們難以存取，有時這會與IT人員以無衝突方式讓資訊與應用程式為大家所用的職責混淆。企業組織圖頂層戲劇性表現便是CISO與CIO之爭，鬥爭成型通常是由企業組織內部矩陣式管理的多線回報開始滋生。(在「Does it matter who the CISO reports to?」這篇文章裡有CSO的深入探討。)即便兩者頭銜裡都有「C」，但CISO向CIO報告相對常見，這會限制



CISO策略執行的能力，因為他們的願景，最終將從屬於CIO的整體IT策略。當CISO直接向CEO或董事會報告時無疑能得到權力，而這已變成日益常見的作法。據Global State of Information Survey 2018指出，這之中含括了頭銜的改變，CISO雖較可能從屬於CIO，但具有資安長(CSO)頭銜的資安高層則可能與CIO處於相同位階，啟動非技術性資安職責。

將CIO與CISO置於平等地位有助於消弭衝突，不只由於這會向整個組織傳送資安非常重要的訊息。還意謂著CISO不能只是否決技術舉措的守門員。如同杜卡迪(Ducati)的CIO Piergiorgio Grossi所表達的：「由CISO協助IT團隊提供更堅實的產品與服務，而非只是說『不。』」這種策略舉措共享職責，改變了彼此關係的動力，意謂著新CISO成敗的差異。

CISO工作描述

若你負責為企業組織尋找有前途的CISO，撰寫工作描述就是這個工作的一部份，截至目前為止的內容，已提供你如何處理的基礎。「公司行號首先要決定是否雇用CISO，並核可所屬級別、報告結構與官方位階頭銜，在小型的公司行號中，CISO可以是VP或資安總監。」Lasalle Network的Wallenberg如此表示。「他們也需要設定這個角色的最低條件與資格，接著再到市場上尋求外部候選人，或公告徵求內部申請人。」

CSO資深編輯Michael Nadeau詳述了如何撰寫CISO職務內容。他指出重點之一在於描述內容應該一開始就明確說明你的企業組織對資安的承諾。你應該強調新CISO最終將處於企業組織圖的哪個

位置，以及他們將與董事會有多少互動讓這一點明確。另一項重點則是維持職務描述的更新，即便這個角色上已經有人，畢竟你永遠不會知道那個人何時會轉換其他工作機會，而這是你絕不會想要維持空缺的重要職務。

CISO薪資

CISO屬於高階職務，因而得到相應報酬。當然，預測薪資比較像是一門藝術而不是科學，不過強烈共識是$100,000以上薪資為典型做法。本文撰寫之際，ZipRecruiter的全國平均數字為$153,117美元，Salary.com則將典型範圍訂得更高，介於$192,000與$254,000美元。

若到職場評價社群Glassdoor看看，你會看到時下開放徵求CISO職務的薪資範圍，有助於你瞭解哪個領域付得比較多或比較少。舉例來說，在撰寫這篇文章的時候，聯邦政府開放的CISO職務，薪資範圍介於$164,000與$178,000之間， 而猶他大學(University of Utah)的其中一個職位則在$230,000與$251,000之間。

CISO職務

CISO職務領域一直在變，而CSO提供豐富資訊內容讓你維持最新訊息-如何得到CISO職位，與如何確定職涯走向。你或許會想看看這幾篇文章：

「A CISO's guide to avoiding certain CISO jobs」：並非所有CISO職務建置都一樣，有些會讓你未來置於負面職涯影響的失敗之中。本文提供一些值得留意的紅旗指標提示。

「Why do CISOs change jobs so frequently?」：據市場研究調查指出，CISO平均任職時間為24至48個月。找出這樣快速變遷代表的意義，以及你可以如何反應。

「What is a virtual CISO?」CXO高層無法逃開「按需支付」員工的趨勢，這樣的員工以按時計酬的合約執行工作，無須佔去全職職位。本文將解釋虛擬CISO能與不能做的事，若你是與他們競爭工作-或想成為他們的一員，這點相當重要。 CIO