提升企業安全等級

時下資安團隊必備的八種新角色

網路安全專家的需求持續居高不下，請確保你雇用對的人。

文／Mary K. Pratt 譯／Nica

目前，美國粗估仍有五十萬個空缺的資安職務，其中含括166,000個資安分析師職缺——此乃該職業最常見的職稱。

這些空缺的職務可能還會增加。

據PwC的《Global Digital Trust Insights 2021》調查報告指出，有51%應答執行層表示來年計畫增加全職資安人員，其中有21%表示正著手增加5%或5%以上的員工。

企業團隊一直都需要安全性分析師與資安工程師，還有滲透測試工程師，這些都是許多資安部門的基本成員。但如今企業組織期望利用其他新職務、開創新角色與增加新職銜，提升企業安全等級。

本文將提供專家認為在2021年將會是IT資安關鍵的八大要角。

一、身份識別與存取管理工程師

企業資安主管逐漸將重心放在開發建全的身份識別與存取管理實作上，重心移轉的刺激因子便是居高不下的遠端存取比例、在任何時間任何地點工作的需求，以及逐漸擴大的多重雲端環境。

事實上，由 Cloud Security Alliance 所作的《2020 State of Identity Security in the Cloud》調查報告發現，有94%的應答的企業主管將人類身份識別的特權與權限管理列在高度或極高優先權，而有77%將機器列於高度或極高優先。

值此之故，資安主管著手開創利基角色，給予它們IAM工程師或IAM分析師這類職稱。

人力派遣公司 Robert Half Technology 執行董事 Jeff Weber 預期，這些專業人才的需求將會持續成長。

「未來幾個月，這個需求會受應用程式生命周期裡含括的安全性需求所驅動。」他說道，並補充表示他的公司發現CISO正在訓練具備必要技術經驗，且表現上擁有紮實問題解決與分析能力的團隊成員，填補這些角色。

二、第三方風險管理者

CISO已留意到這些威脅悄悄經合作夥伴與廠商之手介入企業營運，因而不得不投注更多注意力在此類第三方相關威脅上。資安主管、人資專員與顧問認為，因而導致出現全然專注於處理這類問題的角色。

以Benoit-Kurtz為例，她的團隊裡已有擁有專門處理內部風險與管理第三方風險的IS分析師，因為這兩者所需技能幾乎完全相同。但她預期還會需要某個人全職管理第三方風險，因為這方面工作的需求與複雜度與日俱增。

這些角色的職銜很多，端視它是否為全職職務，或是資安團隊內現有職務增添的新職責而定。

2021 年八大 IT 資安關鍵要角：
一、身份識別與存取管理工程師。
二、第三方風險管理者。
三、DevSecOps 資安工程師。
四、威脅獵捕。
五、弱點風險分析師。
六、雲端資安架構師。
七、事件應變管理師。
八、CISO。

無論哪種，專家都認為這個角色的重點一致：檢視第三方資安政策及處理程序，強制遵循合約所訂定的標準。

「你必須確保這個風險在掌控之中，而且身為資安團隊一員的你，充份瞭解供應商責任。」IT服務管理公司Involta的資訊安全長 Annalea Ilg 表示。

三、DevSecOps資安工程師

「應用程式一直都是防範外洩的最弱環節。」位於倫敦的科技暨資安專業人力派遣公司 Bestman Solutions 主管 Owanate Bestman 表示。「DevSecOps乃時下用於處理這方面問題最廣受讚譽的做法。具備DevSecOps經驗的申請者極為搶手。」

他表示資安主管希望應用程式安全性工程師，具備對DevOps全面性的瞭解、DevOps管道工具的認識、與開發團隊共同作業的能力(或實際這麼做的經驗)、健全的網路應用風險認知，以及當然要有資安方面合格身份。

有了這樣的名單，不難瞭解何以需求遠大過供給，NTT DATA Services 副總裁暨資安事務主管 Sushila Nair 如此表示，她同時也是ISACA華盛頓特區分會的董事會成員。

「DevSecOps不新，但很難找到可以融入你Scrum團隊裡的應用資安工程師。」Nair表示，並補充說明挑戰在於找到既擁有資安知識，也具備應用開發經驗的人才。

四、威脅獵捕

時下轟炸企業組織既複雜又精巧的威脅，令CISO不得不開創可以找出威脅抵禦之的新角色。

「我們需要的人才類似資安威脅分析管理師，他們著眼於所有威脅分析工具、防火牆事件記錄與其他監控工具；這個人知道什麼是威脅，並且能夠將威脅傳達給涉及的相關人員。」Southard如此說明。「他們應該要能夠留意事件紀錄，從中發現警示並察覺可疑項目，繼而發現異常行為模式、知道這是假警報還是必須注意的事件，以及指出的風險屬於緊急事件還是次要等級。」

Nair也將威脅獵捕列於關鍵角色，認為「我們需要實用的分析技能。」SolarWinds與其他進階攻擊進一步激發了我們需要獵捕攻擊者的體認。沉默且持續的攻擊，讓工具程式無法提出警告，因此我們需要知道如何獵捕網路裡的入侵者。

五、弱點風險分析師

同樣地，Southard認為，企業之中必須有人能夠追蹤並管控弱點。「這是腳踏實地修正所有漏洞的做法。」

她表示在2020年中期就發現了這個角色的必要性，這是融合了不斷有各種裝置遠端存取連結至公司系統、處理不完的弱點，與企業面臨的威脅數量持續增加等現象的發現。

Southard知道多數資安團隊裡——包括她自己的，都有專人處理弱點。但她表示，這種工作有時優先權會排在其他事務的後面。

因此，她在2021年初設立了新職位，確保注意力放在弱點管理上，她發現這樣額外的做法是相當明智的，可以讓一個人有時間與權力將此任務優先處理，甚至與廠商合作依企業組織訂定的標準補救問題。

「這麼做確保優先處理弱點，向執法機關表明我們對這些弱點的修復嚴陣以待。」她補充說明。

六、雲端資安架構師

據資安主管、人力資源公司與顧問表示，這是最搶手的角色之一。

「尋求的技能中有許多是為了因應法規：確保企業在充份利用雲端平台優勢的同時，也能降低法規與合規性風險。」Bestman如此表示。

他表示，人資主管希望員工具備雲端平台作業的經驗，理想上這個人要有特定平台訓練或認證。他們還希望這個人對資安協定有充份完整的瞭解。

「這指的是，具備開發雲端架構資安藍圖的能力，知曉需要哪個資安工具確保雲端財產安全。」Nair進一步補充說道，這些職務的最佳人選在評估工具時能夠考量企業各種選擇所造成的財務後果，再加上資安的影響。

這些要求很多，但Bestman表示他發現擁有雲端經驗的資安架構師數量正在成長，而這些人之中有許多正在取得雲端認證增加他們的市場價值。

七、事件應變管理師

Southard在2020年為她的部門增加事件應變管理師一職。她認為包括自己的資安團隊都需要至少一名成員負責跟進瞭解如何完善處理各種事件，在事件發生之際做好萬全準備。

她的新事件應變管理師——有時稱之為事件應變分析師，已有十七年類似職務的處理經驗。這份經驗對Southard而言相當重要。「我們要的是經歷過事件的人。」她表示。

Southard表示她建立這個職務是要確保資安部門可以盡快反應，還要能夠協調所有能帶來成效的各種任務。

「這個人提供分流的接觸點，把人們拉在一起、找出這是哪種型態的事件。」她解釋，並補充這類管理者應知曉如何掌控事件範疇：從電話系統斷線，到曝光身份識別資訊的外洩事件，繼而劃分出這類事件所需的關注程度。

八、CISO

CISO不是新出現的職務，但也不是常見角色。

IDC的《2020 Security Priorities》調查發現，僅42%中小型企業擁有CISO或CSO或其他資安高層，相較之下有80%企業級組織擁有這類職務。甚至部份大型企業組織還沒有這種C字頭資安高層的職務。以資安廠商Bitglass的一份報告為例，發現 2019 Fortune 500 裡有38%沒有CISO一職，這之中也僅16%有其他高層(資安副總裁之類)列名負責網路安全策略。

專家認為，這是一大錯誤。

美國伊利諾伊州弗農丘陵信用合作社BCU的資訊安全長 Stephenie Southard 表示，即便企業組織全力投入安全性，CISO仍是「向上管理全面管理並在高層設定基調的關鍵角色。這對於組織能否真正得到深度防禦策略至關重要。」。

身為長官，CISO位居與公司高層共同處理策略的位階，因此更有可能成功定義並實施與組織風險一致的資安態勢。CISO具有高層職銜的權勢，也處於讓其他人遵循資安要求的絕佳職位。

Station Casinos 的資安主管（該職務向CISO報告）Stephanie Benoit-Kurtz 補充說明，「企業組織裡沒有CISO，甚至連兼職的虛擬CISO都沒有，就設定了錯誤氛圍。」她同時也是 University of Phoenix 領導資安專案的學院主席。