完美的陌生人

CIO及CISO如何相依相存？

將安全做為策略要務的一環逐漸興起，這改變了 IT 與資訊安全領導人之間的關係。本文將探討資訊長及資安長如何成為更好的合作夥伴。

文／Esther Shein　譯／PL

一場疫情讓資訊長(CIO)及資安長(CISO)長成了陌生的盟友，時至今（2021）年，他們迫不得已要在前所未有的環境下比以往更加密切地合作。結果呢？他們的關係狀態大體上有了改善。

過去幾個月以來，組織上下都在加速它們的數位計畫，並遷往雲端，以便支援遠端員工與顧客。「這使得人們的風險偏好產生了非常非常顯著的變化，並導致資訊長及資安長的權責更加相互交纏，」Gartner研究部門副總裁 Jeffrey Wheatman 表示。

如今他們還需要一種共生關係，因為「董事會現在對網路安全提出更多、有時甚至是更好的問題，」Wheatman表示。「這使得資訊長及資安長至少要試圖讓故事或敘述保持一致。」

資訊長及資安長都同意，為了提升效率而推動手動流程與功能自動化的努力，使得彼此有必要更加密切地合作。「無論報告結構如何，資訊長及資安長都必須在規劃與策略上緊密結合在一起，」保險公司Markel的隱私暨資安長 Patricia Titus 表示。

安全如今成了一種策略

當資安長要向資訊長報告時，情況並非總是如此。「可惜地是，有些資安長在資訊長的領導下苦苦掙扎，因為最終資安長發現並需要解決的部分問題，會使得資訊長較難以完成他們的工作，」Wheatman表示。「我認為，資安長想要確保資料在移轉過程中不會被不應該看到的人看到，並保持系統完整性，以及安全與法規遵循，因此二個角色之間的目標會存在些許分歧。」

他表示，好消息是，兩個角色之間比起過去衝突更少、且綜效更多，這要歸功於企業主管及利害相關人的認可，因為他們愈來愈依賴科技。

安全做為一門學科的成熟度與日俱增。「安全如今已被看成更像是一種策略性計畫，而不是那些喊著『不，停止，不要』的人，」Wheatman表示。「我們以前總戲稱這類資安長為『不博士』。那情況愈來愈少見了。」

Wheatman補充表示，當資訊長及資安長視彼此更像是合作夥伴與同儕時，綜效便會油然而生。「當我們看到諸如物聯網及雲端等運營技術匯聚時，人們已經意識到此二者的步調必須更加緊密配合，而不是資訊長單方面將事情扔過來並說，『你們必須確保我們落實的這件事的安全。』」

資安長用手指指著資訊長說，「你得按我說的去做，否則……」，如此容易適得其反，而更應該說「我們需要共同努力解決董事會或營運長、或執行長、或財務長認為是重要的問題。」

資訊長—資安長關係的演進

Titus及Markel的資訊長 Mike Scyphers 已經共事將近五年，他們可以說是工作婚姻關係的理想典範——相互尊重與讚賞。彼此提及對方時都語帶恭維。

Scyphers表示，隨著消費性科技的普及及事業單位提升它們自己雲端服務的能力，大家非常容易聚焦於創新而忽略安全。他稱他與Titus的關係「很寶貴」，並表示，「我無法想像少了這層夥伴關係要如何部署科技。」

Titus一開始是在IT部門工作，而Scyphers表示他「完全支持」她的轉任。

「當我們之間缺乏健康的制衡時，無論何時那對話都會令我變得緊張，」他表示。「我會辯論我們不同的觀點，但是…當每件事都在IT部門時，最後我發現我自己會抱持觀望態度，而且當你總是試

的資訊長」、資安長及其他與他存在歧見的關係報告。

「有時候，你會遇到對安全和風險非常聚焦、甚至到了相互對立的資安長，那並不總是行得通，」Hayslip表示。「他們是戰術性很強的資安長，和其他人處不好，他們認為所有風險問題都必須現在、立刻、馬上處理。」

Hayslip描述自己是一個既有戰術又具策略意義的資安長。「我看待我的工作為一位剛好負責網路安全的企業主管，我必須與其它事業單位的同儕一起工作」，並向他們解釋安全的價值。

「實現此目標唯一的方法是，我不能一昧地批判他們；反之，我必須了解他們如何工作、他們的需求是什麼，他們主要顧客是誰，以及我如何支援他們，」Hayslip表示。「我用這種方式接近他們，因而獲得更多的接受度。」

他補充道，如果資安長僅僅扮演戰術性角色的話，那麼企業將「只會忍受你一段時間，再來就把你踢到一旁。」

Hayslip認為，當資安長只與小型企業合作，慣於解決急件問題，且難有機會專業地成長時，過於聚焦戰術性角色便意味著一種「成熟度的問題」。

報告結構

公司與公司之間的報告結構各異，而且也可能因產業而異。Gartner的Wheatman舉例表示，如果你身處金融服務產業，向財務長報告往往更加合情合理。而在運輸、物流貨零售業工作的資安長便最可能向營運長報告。

「我每年要接600通電話，大概有80到100通電話是詢問有關組織結構，其中的根本問題是資安

圖做對每件事時，你會產生盲點，不同觀點有助彌補自己思緒上的盲點。」

Scyphers表示，他反對扮演「黑白臉」，因此當安全議題浮出檯面時，IT部門會讓安全團隊知悉問題所在。「如果他們得到答案，我們便不會再在上面耗費時間了。」

SoftBank Investment Advisers 的資安長 Gary Hayslip 表示，人們長久以來存在一種看法，就是資訊長與資安長的關係是對抗的，其中一方向另一方報告，並且抱持「你必須按照我說去做」的態度。

Hayslip在職涯初期曾擔任過資訊長，後來轉任資安長一職，他表示，他以前認為資安長不應該向資訊長報告。「資安長的工作是運用人員、流程及科技來管理風險，而資訊長的工作則是提供服務。那些是截然不同的觀點，」他解釋。「我們使用相同的資源，但是我們處理問題的方式卻大不相同。」

Hayslip補充，意思就是，IT及安全的科技是相互交纏的，那意味著兩個團隊必須相互支援。

Hayslip向SoftBank的科技暨資訊安全負責人 Wil Bolivar 報告，並表示他們是「貨真價實的好朋友。」。他也向Softbank的財務長報告。Hayslip表示，在過去擔任過的職務裡，他曾向一些「非常好

長應不應該向資訊長報告？」他表示。Wheatman表示，在他過去所做的研究中，約有三分之一受訪的資安長表示他們不隸屬於IT部門。

他表示，當組織意識到安全是一項企業問題、而不是技術問題時，網路安全通常便會自IT部門移出。「當它屬於資訊長權責的一部分時……每個人都認為安全是一項技術問題。是的，網路安全涉及工具還有技術，但是它更是運營技術。」Wheatman表示，重點是它還支援企業流程及法律與法規要求。「這些便都不是資訊長或技術人員的問題了。」

Wheatman表示，在他加入Gartner的14年裡，據該公司安全會議的資料顯示，大約有35%的人聲稱自己是組織的安全主管，而沒有向IT部門報告。「今非昔比了。」

甲骨文（Oracle）的顧客服務副總裁暨資安長Brennan Baybeck 向某事業線負責人報告，但是他表示他向資訊長報告了七年之久，且擁有正面的經驗。

「我很幸運能與一位與時俱進的資訊長一起工作，他不僅了解安全的重要性，並且是安全的堅定擁護者，」同時也是IT治理組織ISACA董事的Baybeck表示。Baybeck表示，他能夠從企業及IT的角度向資訊長清晰說明並展現安全對公司策略的重要性。他藉由「持續向資訊長報告，教育他並讓他知道安全如何幫助我們的企業，以及了解安全狀況、風險與漏洞」，做到了這一點。

Baybeck表示，他會主動與資訊長定期會面，不僅探討安全，還分享有關如何透過安全服務讓IT部門更具效率與效力的想法。

「他將我提升到他的領導團隊裡，這意味著我不僅可以向主管提供安全建議，還可以確保安全議題深植於企業及IT策略中，彼此息息相關，」他表示。「此外，我還能夠為IT團隊提供價值。」

提升安全耗去Baybeck大約75%的時間，他利用剩餘25%的時間努力爭取更多資源。「對許多和我扮演同角色的人而言，他們面臨的情況並非如此，他們投入絕大多數時間爭取資源並證明其合理性。」

Hayslip認為，資安長不向資訊長報告是一件好事。如此一來，「風險更顯而易見，而且組織能夠從策略角度理解事物將在何處被加以管理，」他表示。

他表示，在那類情況下，資訊長及資安長的關係應該是對等的，而且仍應每週定期開會。

疫情影響

這場疫情肯定助長彼此的相互備援，IT部門努力促成遠端工作，安全團隊則努力確保在員工遠端登入網路時對其身份加以驗證、並確保資料安全無虞。「如果你的安全團隊在我們如今身處的疫情環境在沒有IT團隊的支持下展開這項任務，那麼你會瘋掉的，」Hayslip表示。

他指出，網路邊緣(network edge)已走入家庭。「因為我有680名員工，所以我有680個網路要擔心，而不是一個網絡，」Hayslip表示。

儘管 Clemson University 副校長暨資訊長 Russell Kaurloto 在疫情爆發前與資安長 Hal Stone 便已保持良好的工作關係，但是他同意COVID-19更加「鞏固彼此關係，並使我們更緊密地分享資訊、且更有效地溝通。」

Clemson University 大約有1,800名學生遠端線上上課，到了三月，這個數字躍升至大約26,000名學生，外加4,000名教職員工。「我每週都會與我們資安長一對一交談，而他也參與每日一次的COVID電話，我們會系統地了解每天發生的情況，」Kaurloto表示。

資訊長資安長齊心協力的小提示

Wheatman附和Hayslip的話表示，隨著數位事業的成長，資安長用手指指著資訊長說，「你得按我說的去做，否則……」，如此容易適得其反，而更應該說「我們需要共同努力解決董事會或營運長、或執行長、或財務長認為是重要的問題」，這樣的情況會與日俱增。

舉例而言，Wheatman與某中型金融信用合作社的資安長合作為他的審計委員會搭建一個平台。他們擬定一份計畫——從企業目標開始，然後是資安

長為建立他的網路安全計畫而採取的步驟。「資訊長看過之後表示，『我們必須與董事會討論威脅與技術，我已經和董事會談過了，他們對此並不感興趣，他們也不了解重點在哪，』」Wheatman回憶道。

他們最後不得不與一同與資訊長通話並表示，「看，這就是為什麼這個訊息不具建設性的原因，」他表示。雖然Wheatman不知道結果如何，「那樣的情境仍然普遍存在。那些問題發生的機率應該要少於5%，但是實際上大概有20%到25%。」

Wheatman告訴負責安全的領導人，他們需要弄清楚如何敘述他們的故事——不僅要告訴他們自己的老闆——還需要透過他們告訴老闆的老闆。

「我們往往迷失在技術叢林裡，最後淪為為了技術而談技術，卻缺乏對企業價值、營收、文化及風險管理的探討，」他表示。

他表示，資安長需要提出一套通用的參考術語。「我們使用諸如『網路安全』及『威脅』及『漏洞』及『風險』的詞彙。我們不一致地使用它們，因此我們需要採一致的方式溝通參考架構。」

他們還需要確保與企業目標保持一致。「這聽起來顯然很明顯，但是在許多情況下卻非如此，」Wheatman表示。「資訊長往往比較成熟，他們需要幫助資安長提升他們訊息傳送的能力，以達到更高的成熟度。」他強調，即便他們不是在每件事情上都一致，也仍需要相互協調。「他們需要擁有相同的長期願景，然而情況並非總是如此。」

Hayslip指出，造成摩擦的最大原因是預算。他表示，資訊長會被告知他們需要削減他們的預算，而資安長則聚焦於試圖建立網路安全計畫及管理風險。

「十有九次問題出在他們的優先要務是不同的。」Hayslip表示他發現，如果溝通渠道保持暢通，且資訊長及資安長每週定期開會，即使只有半小時互通有無，彼此都能學到許多東西。

「資訊長會提供你政治方面的見識，好讓你對公司的問題或企業如何改變有好的見解，」他表示。如此一來，他們才可以齊心協力找出可以節流之處。

他表示，如果資訊長及資安長彼此交談，便不會出現出乎意料的事了。「我發現當我們那樣做時，我們合作得無比美好。」

Baybeck同意，培養關係及建立合作夥伴關係是關鍵。「資安長應該努力被視為一位資訊長值得信賴的顧問，他們可以預測他們的需求，並告知他們甚至想都沒想過攸關安全風險的議題或機會，做到這樣的程度。」

所有的資訊長及資安長都同意，相互尊重或許是這段關係中最重要的要素。

「從一開始，就必須對我們每天要試圖達成與維護的事物有共同的理解，」Clemson University 的Kaurloto表示。「那是關鍵。第二件事則是建立一個相互尊重的密切關係。你們不總是會得到相同的結果，也不見得總是一致的。但是，在相互尊重的情況下，你們便會找到共同點。」

他補充道，還需要完全透明。「如果遇到你言而無信，你將無法獲得資安長對你的尊重與理解。你的資安長是你整體成功的一部分。如果你們缺乏良好的關係及真正的透明，你們不斷遇到摩擦是可預見的。」

Markel的Scyphers表示，他和Titus聚焦在企業成果，而不是安全或IT問題。「我們倆都透過自己的專業支持這一點。Patti是最絕佳的專業人員……我鼓勵存在這種信任。這很關鍵。」

Titus表示，從她的角度，挑戰彼此很重要，「而當你走出去時，你們是協同一致。你們會關起門來解決你們的問題。」

她表示，「專注於合作夥伴關係很重要」，而雙方都可能要做出讓步才能實現此共同目標。

「我們對於我們如何到達那裡可能會有些許意見不一，」Titus表示，「但是最終，我們將一起越過終點線。」

就像任何美好的婚姻一樣。