資訊科技界當今面臨最大的十一項議題

從確保物聯網（IoT）安全、到重新訓練資訊科技人才、再到尋找新的營收源，資訊長眼下仍面臨許多足以讓他們徹夜難眠的其它挑戰。

文／Paul Heltzel 譯／黃貝玲

我們每年都會與科技領導人聊聊他們在不久的未來將會面對最大的問題，從聊天內容中，我們開始看到延續自2018年的擔憂的一些不顯眼及沒那麼不顯眼的轉變。

十二個月前的一項主要問題——資料超載，逐漸演化成為新的資料渴求（data-hungry）工具，而人工智慧則協助讓資料變得有意義，並促進商業決策。資訊長表示他們今年更關心的是如何保護那些資料，因為組織得努力因應新的隱私法規。

隨著經濟環境持續改善，2019年資訊長比較不會因為緊縮的預算而受到鉗制。而且移往雲端也比較不成問題，因為許多公司已經一股腦地投入了。企業主管如今更關注如何保護他們在多重雲端環境下運作的資產。

讓我們往下看看來自企業高階主管、招聘人員及那些站在同一戰線並肩奮戰的專家們，描述他們今日的首要問題，還有——如何因應之。

一、新型態的安全威脅

Glasswing Ventures創辦人暨經營合夥人Rick Grinnell表示，近期幾起媒體極為關注的新聞事件可能會引發意想不到的新安全威脅。

「政府關門事件讓美國的政府、重大基礎設施及其它公家機構與私人組織暴露在極大的網路威脅下，」Grinnell表示。「因為關門，許多在國家層級監控威脅的安全專業人員都放假去了，這給攻擊者創造一個更大的漏洞。時間將證明，一個月的低防禦力是否會在2019年及後續產生更深層的影響。」

科技領導人也最好準備面對人工智慧帶動的新一代網路攻擊。

「安全專家對這些威脅的偵測與訓練必須格外警醒，」CGS資訊長John Samuel表示。「今年，公司將需要引進以人工智慧為基礎的保護系統，以便能夠遏制任何因為這類新一代科技而帶來的攻擊。」

Grinnell表示，人工智慧並非去年最受矚目的攻擊事件的要素，但是他預料那情況將所改變。

「我認為，2019年我們將看見諸多人工智慧攻擊事件首次發生在美國企業、重大基礎設施及政府機構，」他表示。「但願我是錯的。」

二、資料保護

具前瞻思維的組織如今會在它們的產品設計裡落實隱私政策，但是，確保這些努力符合歐盟的「一般資料保護規範」（General Data Protection Regulation，GDPR）標準是一項持續的問題。舉例，Google因為該公司如何收集資料才剛收到法國主管機關祭出的罰款。

「美國企業需要考慮採用GDPR式的政策來保護公民，甚至要在任何法規施行之前。」Samuel表示。「最終，必須有一套國際級指導準則確保全球顧客隱私與保護，並讓我們更容易遵循。」

Schellman and Co.資深經理Jacob Ansari表示，物聯網安全去年獲得許多關注，但是在業界卻只

帶來少數實務上的改變。

「物聯網設備廠商使用的仍是易受攻擊的軟體元件、貧乏的網絡及通訊安全，而且無法做到實地更新軟體，」Ansari表示。「他們仍然犯著1990年代末至2000年代初期之間其他人犯過的所有錯誤。哦，你的語音啟動家庭設備監控著你，而製造它的公司在缺少監督及責任感的情況下，時不時便會將你的資料地提供給錯誤的人。這也顯示，更完備的資料隱私法規——至少在美國——會是2019年潛在的熱門話題，尤其是牽涉到最近的選舉活動。沒有人喜歡在歐洲實施的GDPR，但是它對一般人的保護而言，卻是相當不錯的。」

資訊科技界當今面臨最大的十一項議題

一、新型態的安全威脅。
二、資料保護。
三、技術缺口。
四、多重雲的安全。
五、創新與數位轉型。
六、尋找新的營收源。
七、缺乏敏捷。
八、委外風險。
九、商業成果。
十、數位原生員工使用的工具。
十一、重建信任。

三、技術缺口

我們不只一個消息源提及資訊科技領域備受爭議的技能缺口，但是那有點扭曲——某些科技領導人如今認為，問題多半是自己造成的、而不是難以處理。

「如果你只是從美國十大大學的電算科學、或電子工程學位的大學畢業生中尋找人才，那麼是的，你幾乎找不到任何適合的候選人，而其中大部分會被五大雇主吸納，」Rapid7研究總監Tod Beardsley表示。「但是，潛在的人才庫遠遠超過於此，公司將會更充分地探索這個領域。」

RSA Conference副主席暨策展人Sandra Toms表示，資訊科技部門會藉由「與更多元化的員工拉近技能缺口，而不僅只在種族與性別方面」來幫助它們自己。多數資訊科技招募團隊都未能考慮到生活經歷、宗教、背景、性別取向及教育方面之多元性。若能以更全面的態度看待多元性，便應該可以廣納來自更多領域的候選人，進而帶來較高的生產力水平。

四、多重雲的安全

甲骨文（Oracle）雲端基礎架構的安全產品戰略結構家Laurent Gil表示，在探索以雲端為基礎的雲端服務時，資訊長現在得更加重視跨多重平台的安全性。

「傳統上，多重雲導致企業需要管理許多不同的、而且通常是不相容且不一致的安全系統，」Gil表示。「我們認為，選擇橫跨不同雲、獨立於雲架構的安全平台，現在是確保企業資產一致性，以及最重要的——完整性的基礎，無論這些資產位於何處。」

五、創新與數位轉型

根據Gartner的資料，大約三分之二的企業領導人認為，他們公司需要加速數位轉型，不然便會敗給競爭對手。

雲端諮詢公司Candid Partners的經營合夥人Merrick Olives表示，多數公司將繼續同樣的路線，直到它們被迫做出改變。

「將資訊科技支出與策略性商業能力聯結在一起，並回答『這將

如何讓我們更具競爭力？』，這一點至關重要，」Olives表示。「相較於以專案為基礎的資金，以價值流為基礎的資金模式愈來愈有效地將董事會層級的目標與預算影響聯結在一起。老舊系統的成本結構與流程效率和敏捷的數位功能有很大的不同——後者成本較低、但是效率更高。」

六、尋找新的營收源

電信費用管理軟體公司Tangoe的副總裁Ian Murray表示，雖然商業環境不斷演變，但是獲利的基本前提是不變的。

「尋找並利用營收機會的過程大抵並沒有改變——找出我們可以解決的問題，而且是尋常、普遍存在，且人們願意為了解決它而付出代價的，」Murray表示。

混合式資訊科技基礎設施供應商Peak 10+ViaWest的產品長（chief product officer）Mike Fuhrman表示，改變之處在於把重點放在落於資訊長職責範疇內的直接營收產生。

「也許我的觀念老舊了，但是我不認為資訊長應該擔憂直接產生營收的問題，」Fuhrman表示。「我開始看到這種情況愈來愈多發生在我同僚之間。為了做一位稱職的資訊長，許多資訊長努力嘗試並產品化他們自己。儘管這的思維有其利益，但是，我認為那也可以成為讓團隊和董事會去焦的一種方法。就營收產生的機會而言，資訊長的職責是聚焦在那類專案，並將企業大規模數位化成為自動化平台。我們得專注於降低企業成本，並從市場進入（go-to-market）的角度進行擴展。這才是資訊長應該如何聚焦在營收的重點……」

七、缺乏敏捷

意欲結合敏捷方法的組織有時會落得在混合模式裡蹣跚跛行，該模式結合了敏捷實務，但是也包括較為線性的「瀑布式」（waterfall）方法。簡而言之，那是兩種情況中最糟的。

Tangoe的Murray清楚解釋這一點：「開發人員是在對這個按鈕或功能如何符合整體用戶體驗（user experience，UX）幾乎沒有概念性理解的情況下，便依據特定規格表編撰程式。我們需要一套嚴守規則的方法才能成功達成這項任務，讓解決方案得以在某版本解決某特定問題。然後每個版本針對一組「衝刺」（sprint，計算開發周期的方式）做協調，如此一來，隨著版本的增加而讓UX解決方案日臻完善，而不僅只是一組能相互支持、或不能相互支持的要求功能而已。」

八、委外風險

技能缺口將促使許多組織向外尋求協助。但是，這些有時候必要的解決方案可能導致可靠及安全上的隱憂。

「我們的主要焦點是實現我們對每位顧客的承諾，」Sanchez表示。「你將你的聲譽與事業建立在這個關鍵事務上。在委外你的工作時，交付物的品質有時候係受承包公司左右。鑑於我們負責管理的專案的敏感性，我們會在專案需要我們考量委外部分或全部任務時，利用嚴謹的第三方廠商評估來評鑑合作夥伴。」

除了品質問題，委外也容易引發眾所周知的安全威脅。「資訊長應該首先考慮的具體威脅是內部人員及承包商，」MetricStream宣傳長（chief evangelist）暨前白宮網絡安全顧問French Caldwell表示。「在我們跳脫密碼憑證之前，『人』將持續是最大的威脅。」

九、商業成果

BTB Security的資訊安全顧問長Matt Wilson表示，在預留資訊科技預算與企業可衡量的成果之間，是存在脫節情況的。

「多數組織並沒有採取極為嚴格的誠實態度檢視它們目前的支出，」Wilson表示。「事情目前完成的方式背後有太多動力，解決方案有了，為了帶來有意義的改變的流程也建構超過十年了。反之，組織可能只拼湊出無法完全解決資訊科技根本挑戰的局部解決方案——例如，Equifax（譯註：美國消費者信用評分公司）無法修補某項已知漏洞。我們的生活深受資訊科技所苦。我們浪費錢。我們拿原本可解、卻因公司動力而變得完全不可解的問題來挫敗我們人才資源。前瞻2019年，我們應該拒絕繼續被同樣的問題打敗。」

十、數位原生員工使用的工具

聯想（Lenovo）全球企業事業部資深副總裁Christian Teismann認為，伴隨數位科技一起成長的新員