

關於API管理：資訊長應該要了解的眉眉角角

API 被業界人士寄予厚望，計畫利用 API 來強化企業的數位轉型，並建立起全新營收管道。從貴公司的支出組成內容，到程式化存取系統資料與服務，API 業已成為關鍵的考量。

文／Mary Branscombe 譯／兩三松

API對企業組織內部IT管理與應用程式開發流程而言，變得愈來愈重要，因此資訊長需要考慮到API管理、法規遵從與存取權限等問題：有那些人，可以動用那些企業治理模型，透過那些API，存取那一些企業資料？

資訊長還需要考量的是，企業組織應如何透過API更有效率地將工作委外，或至少是將API列為評估的獨立替代方案。一般而言，開發人員會選擇採用某個API的理由，純粹只是營運操作上的考量，像是做出企業採購決策因素，或是企業所選擇的策略方向，以及其他來自開發人員上級主管決策考量等等。

為了在不影響程式開發敏捷反應度的前提下，想要控制API的使用狀況，企業就需要制訂出相關政策。這需要清楚地了解企業組織中採用了那些內部開發和外部購買的API，以及這些API各自的用途、成本與可靠度。另外從策略角度來看的話，資訊長則是需要確認API

對企業業務提供了那些貢獻。

API的整合與組成成分

微軟低程式碼應用程式平台副總裁 Charles Lamanna 對表示：「許多微軟客戶都希望跨入一種未來情境，也就是實實在在地掌握API經濟與API完整目錄，並且能夠對企業內的各個資料孤島公開相關資料。」

Lamanna舉例說，在低程式碼平台上使用API開道或其他API管理解決方案，能夠釋出大量商機。因為開發人員可以藉此建置出相關微服務，並發布給其他開發人員使用，而非專業的素人開發者，則能透過 Microsoft Power Platform 平台來應用API。

但就算達到了「API經濟」的水準，仍是遠遠不及低程式碼和無程式碼開發要求的範疇。正如Postman公司執行長 Abhinav Asthana 所指出，企業組織在一開始規畫與設計軟體的時候，就必須優先考慮到API，而不是等到專

案完成後才列入考量。Asthana表示：「如果最後您做出了次佳決策，將可能導致更多法規遵從與企業治理的風險。如果您今天正在建置一項新的應用程式，這種做法很有可能讓它沒法與外面的世界溝通。所以請打從一開始就做好相關規畫。」

API並不僅僅是應用在企業採用外部的服務上；企業通常會開發自有的API，用以做為自助式服務存取日常業務的一般資料，或是用來簡化與供應商之間的資訊交換。如果可以方便容易取得關於發票付款與商品交付狀態等交易訊息，就能讓對新供應商或付款處理查詢的應對效率更高，但可惜的是這些資料通常會被鎖定在多個ERP系統裡頭。如果企業建置起相關API，並將它們發布到API目錄進行公布之後，就能避免掉很多技術支援需求。

提供Google技術諮詢顧問的SADA公司技術長 Miles Ward 提出的建議是：「請考慮貴公司組織的

獨特資料或系統功能，想像貴公司打算將它們對其他企業銷售出去；或是貴公司在其他地方都無法取得的資料或系統功能。API是一種連接資訊的途徑，只有在資訊流動時才會真正產生價值。如果貴公司的資料無法通過集中式、可程式化、並可擴充的介面進行存取，因此無法將資料傳送到能夠發揮作用之處的話，那麼現在就是該優先把這項考量排上時程表的時候了。」

有一些應用程式，幾乎完全需要依賴API呼叫才能建置起來。Commercetools公司產品長 Kelly Goetsch 表示，市調公司Gartner曾提到的「可組合商務（composable commerce）」，即為這種趨勢的一個好範例。

可組合技術改變了企業的傳統系統開發方法。Goetsch說：「現在貴公司不再需要依賴200名境外的委外開發人員團隊來生產大量Java程式碼。IT主管想要的是技術嫺熟的資深程式審核員，他們可以促使這些不同的應用程式結合起來一同運作，通常這是利用事件架構與API呼叫所完成的任務。但如果貴公司投入愈多這類型高階開發人員時，開發速度可能會變慢，同時困難度也會增加。」

Goetsch認為，企業資訊長真正需要的是，除了已核准和正在使用中的API目錄之外，還要加上一個更完整全面性的企業治理策略，而這項策略能透過一個通用資訊安全框架，應用在API開道上，供開發人員進行API存取。Goetsch說：「一旦確定要建置那些API，以及從外部供應商選擇出合適API之

後，API開道就是貴公司控制開發人員對這些API存取的手段。」

API開道通常是硬體裝置，但這種情形正在發生改變。目前已經出現眾所周知的API管理工具，每個主要雲端服務供應商都能提供這些商業化API管理服務，企業可以選擇API管理服務組合、執行速率限制存取控制等選購項目，還包括端點和實例過濾（在許多情況下，甚至能管理單一API裡頭的個別單項活動）。這種API管理服務可以提供企業關於API使用情況、錯誤率與其他可觀察的使用指標。另外還有類似APImetrics之類的外部API服務供應商，他們可以協助企業追蹤公用API的效能與可用度。

不受控的API

要建立起更正式API策略的第一步，是審核那些API可用與正在使用當中。因此要確認這些API是否已被列入記錄，而且可以被企業挖掘出來。

Asthana指出，在企業組織的不同單位當中，經常產生許多重複的API。他建議資訊長應讓程式開發人員參與系統架構的討論，以提高所有人員對API管理的認知。

除此之外，企業正在使用中的API卻很容易被眾人所忽略。有一家大型醫療機構建立起API目錄，在剛開始時只列出了450個正在使用的API，但最終統計出來的API數量卻高達近4000個。資訊長們其實可以利用工具檢查代理程式、日誌紀錄文件與其他鑑識工具，就能找出企業中目前存在的API，並產生OpenAPI的相關說明。

在建立API目錄之後，不僅要透過這個目錄追蹤企業API的發布與使用，更應據此建立出更具策略性的API生命周期管理策略。其中亦包含了不贊同外部API供應商對其API進行大幅度更動，或是供應商全面停止API服務時的周旋。

有一些資訊長開始聘請API架構師，並建置起卓越API中心或治理小組，以監督API的使用政策。追蹤使用中的API在整個企業組織中的分布狀況，確保對企業內部API管理系統能夠適當地分配資源（尤其是在機器人流程自動化只要透過Excel工作表就能建立API的情形下），並確認其資訊安全以避免發生資料外洩事件，而這種情形之前就曾在交友服務Bumble和消費者信用報告機構Equifax兩家公司發生過。

Digital.ai公司歐洲、中東及非洲區技術總監 Winston Bond 表示：「系統漏洞透露了現代化應用程式對API的依賴程度；以及一家企業將所持有的API私有化，而且鎖定這些API而導致的複雜度。利用一大堆依賴雲端服務提供的微服務所開發建置出來的應用程式，像是Bumble公司的系統，通常會曝露出許多原本是安全地保存在防火牆後的連接窗口。」

成本、信任與法規遵從

另一個企業必須建立有關API使用透明度的原因，就是企業的成本控制考量。企業通常會將API比照雲端服務一般對待處理，但是API比雲端服務更不容易被發現，並且它們的使用狀況通常更加難以

預測，這就可能導致使用成本超出原訂預算。

Zylo執行長 Eric Christopher 則表示：「API的訂價模型相當複雜，一般是基於使用量進行計價。但資訊長難以控制企業內人員使用應用程式的時間長短，因此最多只能進行成本預估。」

資訊長必須要事先考量，假使API無法正常運行的時候，會引發多少業務損失與其他事務中斷，而造成多少不必要的整體損失，以及那些人得負責任等問題。服務等級協定（SLA）的確是一種規範沒錯，但其內容必須細緻到足以涵蓋貴公司正在使用中的各種API才行。能夠依服務等級標的物、服務體驗與依成果計價的協定，對貴公司來說可能更為合適；因為這是依照貴公司使用結果，而不是API連接數量來衡量計價的。

綜合性交易監控能夠顯現出企業的營運與效能議題，但很少有API供應商主動提供上線測試帳號，或是驗證該公司的相關文件有效。APImetrics公司執行長 David O'Neill 就特別提醒企業資訊長：「貴團隊要如何實地測試正式上線API裡頭的任何細節？貴公司的整個正式系統環境可能因此整個當掉，而且在發生當機5小時後還一無所知。」

OpenID Foundation 基金會正在開發「信任框架」，其依據的是跨區域的正常系統運行時間與速度，提供給雲端基礎架構、金融服務與開放銀行等產業API使用。但O'Neill指出，到目前為止對信任框架並沒有相關的公開評測與排名機

制可以讓產業界欣然同意接受的。

可發現度、品質和法規遵從這三項主要考量點，對銀行、醫療保健與政府服務等受監管行業中的API來說，變得愈來愈重要。

O'Neill希望就如何衡量與監控API方面盡快達成共識，完成從測量API延遲時間、評估文件，一直到驗證API架構的品質與法規遵從等方面細節。O'Neill表示，這將需要某種評估記分卡指標，與一個能對整個產業範圍產生影響的政策規畫小組。有一些影響API的規畫應該達到全球等級，像是跨國的API協議，背後就需要有一套具備一致性的標準才行。

優先執行事項

市場研究機構 Constellation Research 公司副總裁暨首席分析師 Dion Hinchcliffe 認為，目前API生命週期管理在許多企業組織中僅僅處於起步階段。Hinchcliffe說：「朝雲端原生程式前進的開發新趨勢，促使微服務與容器成為IT領域最受重視的要角。2020年是Kubernetes在IT部門裡的成長啟始點，因此將迎來相關問題大幅爆發並尋求解答，以及在資訊長層級上被考量進行更廣泛的應用。」

Hinchcliffe說，如果認為金融服務和醫療保健等受監管行業離此一趨勢最為遙遠，一點也不會讓人感到意外。美國有一個頂級醫療保健網路已察覺其四分之一營收來自於API，並期望在未來幾年內成長到占一半以上營收。正因為具有這樣的營收成長潛力，讓API的設計、選擇、管理與治理，現在突然

變成了讓企業高階主管們的頭大問題。

Zylo公司執行長Christopher表示，放手讓業務部門自行管理所擁有API的資訊長，會對API使用狀況的了解程度最低。Christopher說：「當企業執行長對資訊長提到『你的工作就是去了解在業務部門中所發生的一切事務，躬身入局，利用技術讓這些部門能夠營運的更為順利』時，那就是資訊長開始想去了解API的細節與可見度的時候。」

Postman公司執行長Asthana則說：「如果我是一名資訊長，我想知道的是『那些API屬於外部依賴關係，又有那些API屬於內部依賴關係，以及有那些是讓它們彼此搭配運作的合適方式』。而這種做法能夠充分發揮企業資源：我會知道應當如何為程式開發團隊安排人員，我也知道可以採用那些基底程式模組（building blocks），並且可以更有效率地為這些事務妥善規畫未來的進展藍圖。」

但是反之亦然。Asthana警告說：「我的信念是，如果貴公司尚未體認以上這些事務即將到來，而解決辦法是先設定好API策略的話，那麼就有可能會遇到許許多多問題。貴公司是可以將這類問題歸咎為程式開發人員生產力問題、法規管制問題或是隱私問題；但其實以上種種在API策略中都能找到對應的解決方案。」