保持適應性是關鍵

2024 資訊長應該注意的六個警訊

隨著科技世界的快速演進，資訊長需要提高警覺性，不僅僅是發現可能的問題，還需要能夠有效地對其做出迅速且適切的回應。

文／Andrada Fiscutean　譯／Christy

在 2023 年，資訊長面臨了一系列複雜的挑戰。其中包括生成式人工智慧重新定義了技術可能性的準則，各國政府開始起草新的科技行業監管框架，以及全球衝突擾亂了企業營運。儘管面臨種種困難，資訊長必須快速適應這些變化，以因應不斷變化的環境。

在未來的一年，資訊長將能夠運用他們所學到的經驗和教訓，引領組織在一個不可預測的世界環境中進行數位轉型。

烏克蘭法律事務所 Juscutum 的創新長 Peter Bilyk 表示：「2023 年的其中一個最重要的教訓是適應能力的需求。那些能夠迅速應對新技術、市場需求或全球事件且能快速轉變的公司表現得更好。」

在進入 2024 年時，保持適應性將是關鍵。雲端原生安全公司 Aqua Security 的全球資訊長 Michal Lewy-Harush 說道：「資訊長需要保持敏捷、主動和適應性，以成功應對這些挑戰。」

今年，數位轉型仍將繼續成為所有人的議程，且現在更加注重道德考量，以因應不斷演變的監管框架。隨著組織將更先進的技術整合到其營運中，資訊安全應繼續是一個首要關注的重點。

面對未來的挑戰，對於資訊長來說，及早識別警訊或危險信號可能會帶來巨大的優勢。具有遠見和敏捷不僅僅是為了戰勝競爭對手的方法，更可能是一種生存技能。

一、AI 是一把雙刃劍

在過去的一年裡，組織和科技專業人士大量進行了 AI 的實驗。現在是時候將這種實驗推向一個新的層次，即更進一步的發展和應用 AI 技術。

愛沙尼亞前政府資訊長，目前是 IT 諮詢公司 Digital Nation 的管理合夥人 Siim Sikkut 認為：「準備好的程度取決於實驗的能力，以及將有效的實驗結果擴展應用的能力，而建立這些能力是未來成功的關鍵。對於科技領域而言，這意味著需要投入專注的時間、人才和預算，持續不斷地嘗試新事物，然後將被證明為有價值的內容納入業務中。」

南韓 SK Telecom 的資訊長 Dong-Hwan Cho 也表示贊同。他說：「在所有業務領域引入生成式人工智慧是保持競爭優勢的必要條件。」然而，並非所有金光閃閃的東西都是黃金。「能夠達到充分回收投資成本的效果是一個不同層面的挑戰，不僅僅只是看到一個出色的技術展示那麼簡單」，他補充道。

未來一年年，組織應該進一步的完善其策略，更加認真地考慮 AI 的倫理影響。Bilyk 指出：「雖然 AI 處於技術進步的最前沿，但它潛在的濫用可能性和所引起的倫理困境變得更加明顯。」

烏克蘭軟體開發商 JEVERA 的交付長 Lesia

資訊長應該注意的六個警訊

一、AI 是一把雙刃劍

二、迅速變化的 AI 法規

三、地緣政治的緊張局勢可能會干擾營運

四、公司文化和人才短缺

五、公司不能忽視安全問題

六、策略性的資料管理投資

略人的因素和社會責任，因此 AI 對於企業的轉型應該經過審慎規劃。」

她還補充說，企業應該具有極高度的適應性。Kasian 解釋著：「新技術可能會用前所未有的速度傳播，並以一種未預期的方式對企業計劃產生影響。因此企業必須準備好以明智的方式去應對變化，這需要付出努力，但成功者能獲得一切。」

二、迅速變化的 AI 法規

在 2023 年，AI 取得了巨大進展，各國政府也開始制定相應的法規。在美國，拜登總統頒布了一項有關 AI 安全使用的行政命令，在歐盟，立法者在 2023 年 12 月就 AI 法案的細節達成一致，這是全球首批為 AI 建立全面規範的法案之一。

因此，資訊長必須在整個年度內密切關注這場有關 AI 的辯論。Bilyk 指出：「隨時更新了解新的法規，特別是有關 AI 倫理、資料使用和版權問題的法規，這一點非常重要。忽視這些變化可能導致法律方面的問題，同時也可能損害公眾對企業的信任。」

公司應該確保他們有足夠的合規專業人員，初創公司應在早期階段就聘請這些專家，因為公司需要了解法規是否適用於他們，以及如何適用。此外，如果資訊長能夠清楚了解公司使用了哪些由人工智慧驅動的工具，以及內部工具的開發方式，這也會有所幫助。不知道這些會被視為一個嚴重的警告信號。

AppOmni 的安全研究員 Joseph Thacker 在接受 CSO 雜誌訪問時表示：「很多時候，領導層或法律部門甚至都不知道開發人員在建造什麼。」他補充說：「我認為對於中小型企業而言，這將會相當困難。」

三、地緣政治的緊張局勢可能會干擾營運

隨著全球地緣政治緊張局勢升高，企業正面臨各種挑戰。對於資訊長而言，保持對國際新聞的關注，並同時注意外部影響是非常重要的。

Bilyk 說道：「美中之間緊張局勢的升級可能對很多公司的供應鏈造成干擾。因此，為了減少對這兩個國家的依賴，採取多元化風險的策略變得相當關鍵。」這種方法對維持業務的連續性是必須的。

對於在地緣政治敏感地區（如烏克蘭或以色列）營運的公司，擁有堅固的應急計劃變得更加重要。

YouControl 的執行長兼創始人 Sergi Milman 表示：「在烏克蘭，由於戰爭的影響，焦點已從採用新技術轉移到保護和增強現有的基礎設施。」

四、公司文化和人才短缺

此外，資訊長應該注意員工離職率以及其背後的原因，儘管這不一定是其工作職責的一部分。瞭解這些情況可以幫助資訊長早期發現團隊動態或組織文化中的潛在問題。解決這些問題也可以制定有效的人才留任策略，進而建立一支更加穩定且高效的工作團隊。

在某些行業中，人才短缺和技能缺口是組織必須應對的重大挑戰。Bilyk 指出：「科技的迅速發展尤其擴大了技能方面的差距，特別是在新興技術領域。」

為了吸引和保留人才，組織需要提供符合勞動力需求的工作環境。Bilyk 建議，如果可能的話，應採用靈活的遠端工作策略，並在員工需要協助時提供援助。

Kasian 說道：「平凡且效率低下的任務和流程

可能使組織變得混亂不堪。對工作流程和業務流程進行修訂和改進是一個不斷重複的任務。」

她同時建議，對於公司來說，效率應該是一個優先考慮的事項。她補充指出：「僅僅是實施新軟體和採用人工智慧並不會使組織的營運自動變得更好。實際情況迫使企業更快地進行自身的轉型。同時，舊有的五年計劃可能已不再適用，需要更敏捷和快速的應變。」

五、公司不能忽視安全問題

隨著科技的進步，網路攻擊的複雜性和精密程度也在不斷的提高。單純地防禦已知的威脅是不足夠的，因此。能夠預測隨著 AI 技術進步而出現的新趨勢也很重要。

Kasian 表示：「入侵、企業資料竊取和基礎設施攻擊的風險正在增加。為了安全營運，組織必須預防性地思考安全性。如果公司尚未有安全主管和專門的安全團隊，現在是迫切需要開始改變這種狀況的時候了。」

總部位於加州的網路安全公司 Exabeam 的資訊長 Grant McCormick 指出，鑑於不斷升級的安全威脅，資訊長的角色已經與網路安全趨向融合。他說：「無論是向資訊長或是向公司內部的其他主管匯報安全情況，意識到公司的安全狀態，並使 IT 和網路安全部門能夠密切合作，這樣的做法符合每個人的最佳利益。」

Sikkut 敦促公司應更加主動，並建議資訊長從一開始就採用 Trust-by-Design 的方法，將安全和隱私保護融入到其業務流程中。

然而，儘管組織已經付出最大的努力，但往往仍難以跟上不斷演進的威脅環境。在這種情況下，尋求外部協助可能會有所幫助，例如與像 HackerOne 這樣的平台合作的獨立道德駭客就是一種不錯的方法，因為他們在找出和解決與生成式人工智慧相關的風險方面變得更加優秀和熟練。

HackerOne 的資安長兼駭客長 Chris Evans 表示：「我們社群中超過一半的駭客計劃將生成式人工智慧作為主要目標，並專門針對 OWASP Top 10 for LLMs 進行攻擊。對於對這個領域感興趣的個人來說，進入門檻較低，為未來的安全專家建立了一條包容性的道路，為每個人建立了一個更安全的網際網路。」

再一次，關鍵詞是適應性。Aqua Security的 Lewy-Harush 解釋著：「對於新的攻擊向量和新興風險的未知因素保持警覺，並且透過這樣做，給予足夠的靈活性，在不阻礙組織營運的前提下調整其安全策略。」

六、策略性的資料管理投資

最後，組織需要思考如何管理他們的資料。這意味著投資金錢和資源到可靠的系統，這些系統能夠整理、儲存和保護他們每天使用的資訊。這樣做有助於他們做出更好的決策，提高效率，並確保重要資料的安全。

資料儲存軟體開發商 Datadobi 的技術長 Carl D'Halluin 指出：「隨著資料量的增加，和對強大資料管理需求增加的情況下，如果組織沒有一個能夠應對這種需求的可擴展資料管理策略，特別是無法滿足 AI 系統即時存取和深度洞察的需求，這就是一個警告信號。」

他補充說，對於不願意採用新技術，包括 API 中心架構和網狀應用程式，也可能成為一個問題。原因在於這些新技術對於確保資料管理的互聯性和效率非常重要。