展望 2024：首席資安長 (CISO) 將面臨的 6 大資安挑戰

2024 年 1 月 2 日發布 | 專家觀點

Tom Blauvelt
網路安全架構師

你可以了解這些新興趨勢會出現什麼情況？

隨著整體網路安全情勢的不斷發展，保持領先優勢不僅僅是一個目標；更是一項任務。展望 2024 年，數位安全邊界益發複雜多變，首席資安長 (CISO) 特別要提高警覺。在這個科技不斷創新的時代，不僅要能預見潛在問題而且要積極應對各種新興的威脅，對首席資安長來說至關重要。

準備做好迎接變革的一年，我們將揭示六大網路安全趨勢，這些趨勢將徹底改變首席資安長們在 2024 年的決策方式從科技的突飛猛進到錯綜複雜的供應鏈漏洞，這是為掌舵者所做的摘要以保護數位堡壘免受不斷擴大的威脅。

1. **量子運算對加密機制的考驗**：量子運算的問世對首席資安長來說是一把雙面刃。雖然它具有徹底顛覆科技的潛力，但它也對現有加密機制構成嚴重威脅。首席資安長必須做好準備，加強數位防禦，應對即將到來的量子時代，重新評估加密協議並探索抵抗量子解密協定的解決方案，以領先網路上的對手一步。請密切關注賽門鐵克創新團隊如何掌握這些發展的更多資訊。
2. **零信任與資料保護整合**：零信任仍然是 CISO 尋求完整安全典範的基石。擁抱零信任就必須接納持續性的企業文化轉變這是至關重要認知。CISO 不僅必須專注於存取控制，還必須將資料外洩防護 (Data Loss Prevention，DLP) 整合到策略中。ZTNA、SWG、CASB 和電子郵件等保護技術使得跨不同平台擴展資料保護策略變得至關重要，無論資料存放在哪裡、如何傳遞交換，都能確保安全。賽門鐵克在這些控制措施中強調資料外洩防護，並能整合跨不同資源擴展強大的資料保護。我們完整的解決方案可確保一貫的高效穩定的偵測和回應，從而能夠無縫整合到 CISO 的整體零信任策略中，以落實整體組織的資安政策。了解更多。
3. **勒索軟體的頑強威脅活動**：勒索軟體持續困擾著首席資安長，利用合法應用程式與系統／管理工具的就地取材攻擊：「Living off the Land」(LOTL) 攻擊。LOTL 攻擊的挑戰在於如何區分合法活動和惡意活動。防禦者能透過採用「調適型防護」解決方案，提供一種在不干擾使用者體驗的情況下阻止勒索軟體的方法，達到巧妙的平衡狀態。首席資安長常常得應對不斷發展的攻擊手法，例如：LOTL，強調是面對持續威脅時保持警惕的必要性。賽門鐵克透過採用我們所謂的「調適型防護」解決這個問題。
4. **成本驅動的安全決策引人擔憂**：成本驅動的安全決策的兩難之處，特別是過度依賴那麼幾個有限的現有工具，將更加顯著捉襟見肘。未來一年的經濟不確定性可能會對安全預

算以及推動產品的整合產生影響。攻擊者將趁虛而入、伺機而動。同時，首席資訊安全長必須在成本樽節和網路安全之間取得平衡。挑戰在於打破被動安全措施的循環，並敦促企業領導者優先考慮不會損害組織安全狀況的主動解決方案。這些解決方案包括賽門鐵克的跨控制點安全產品組合，其中包括業界功能最完整的端點安全產品，該產品提供了深度安全科技來保護和防禦當今新興的威脅。

5. **面對供應鏈漏洞的挑戰**：由於組織的程式碼庫廣泛依賴第三方提供者，供應鏈攻擊仍然是一個長期存在的問題。首席資訊安全官必須在軟體生命週期的各個階段實施整體戰略，以應對不斷變化的威脅。雖然軟體物料清單 (Software Bill of Materials，SBOM) 等措施可望有些幫助，但經驗豐富的首席資安長明白，要抵禦複雜的軟體供應鏈攻擊，需要有技術熟練的人員、自我完善的流程和採用干擾最少的專用安全技術來不斷努力。
6. **負責任地整合人工智慧 (AI) 和 Chat GPT**：既要充分利用這些工具的效率和技術進步，又要保持強大的安全措施，這兩者之間的微妙平衡構成一個嚴重的難題。首席資訊安全官必須把握人工智慧部署的道德考量，確保自動決策過程的透明度、公平性和問責制。要充分開發人工智慧和 Chat GPT 推動變革的潛力，同時防範潛在漏洞並確保這些技術在不斷變化威脅環境中的可信賴程度，達成這種巧妙的平衡至關重要。瞭解賽門鐵克如何實現安全採用生成式 AI 應用程式。

面對上述的種種挑戰，首席資安長必須採取積極主動和更能適應變化的態度，擁抱創新，同時強化網路安全的基本要素。透過預測這些趨勢並制定相應的策略，他們不僅可以應對 2024 年的複雜局面，還能帶領組織走向更加安全、更具彈性的未來。

關於作者

Tom Blauvelt
網路安全架構師

Tom Blauvelt 是賽門鐵克戰略團隊的網路安全架構師。他在技術和戰略崗位上工作了幾十年，這使他能夠與首席資安長 (CISO) 以及安全監控中心 (SOC) 的分析師協作，為當今不斷變化的威脅環境量身定制解決方案。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/top-6-security-challenges-cisos-2024
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2024/1

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。