CrowdStrike 全球當機事件

資安長的 反思與應對

CrowdStrike 事件對資安長（CISO）來說無疑是一次震撼教育。這起事件讓我們看到，即使是知名網路安全公司，也可能發生意想不到的錯誤。資安長應該如何從中吸取教訓，重新審視自身的資安策略，應對未來可能出現的更複雜威脅？

編譯／Nica

網路安全公司 CrowdStrike 在日前發佈軟體更新引發全球 Windows 系統當機。驗證軟體程序於更新時出錯，導致更新內容與 Windows 系統衝突，最終引發當機藍白畫面。根據官方說法，此次事件由驗證軟體的臭蟲引發，再加上一連串錯誤導致（解釋故障細節卻未回答如何發生、為何發生）。部份人士質疑該公司是否實際測試過這項更新。此外也無法回答受影響設備的百分比，僅微軟估計的 850 萬台機器。遭嚴重影響的達美航空批評該公司事後協助不足。

針對全球大當機，CrowdStrike 的補救措施：

- 首先「**隔離問題**」，防止擴大。包括暫停有問題的軟體更新，並隔離受影響系統。
- 迅速開發並「**發佈修復程式**」，補救引發藍白當機程式碼錯誤。
- 與「**客戶密切合作**」，協助回復系統。包括技術支援、指導客戶安裝修復程式，與協助解決其他相關問題。
- 保持「**透明度**」，主動向大眾與客戶公佈事件處理進度，承諾全面調查，公開調查結果。

具體行動程序為：

- **識別問題根源**：深入分析導致藍白當機的程式碼，精確找出問題。
- **開發修復程式**：開發新程式版本，修補問題。

- **測試修復程式**：發佈給客戶前，該公司聲稱已作嚴格測試。
- **佈署修復程式**：透過各種管道發佈修復程式給客戶，並提供詳裝指南。
- **客戶驗證**：安裝修復程式後，需要進行驗證，確保問題解決。
- **持續監控**：確保修復程式有效，且沒有新問題出現。

部份嚴重影響的系統，可能需要更複雜的修復，例如重新安裝系統或回復備份。

這次事件為整個 IT 產業敲響了警鐘，提醒我們在軟體開發和佈署過程中，必須時時保持警惕，採取一切必要措施確保系統穩定性和安全性。即使是知名網路安全公司，也可能出錯。

資安長重新思考關鍵策略

資安長應主動在事件應變、災難回復、危機溝通和應變手冊中納入新教訓，重新審視與軟體廠商的協議。ForAllSecure 執行長 David Brumley 在接受美國 CSO 媒體的訪談中表示：「CrowdStrike 在三件事上搞砸了。資安長應該好好審視，確保自身服務和軟體有做好。第一、驅動程式碼內存在軟體漏洞。第二、未對客戶實際會看到什麼充分測試。第三、沒有分階段推出，

一次更新一切。」

資安長除了將這次失誤視為未來妥善處理事件的實例，還可以作其他改善，例如更新意外事件應變手冊、更新災難復原計劃、調整軟體廠商合約，在下次重大危機來臨前備妥溝通管道和應變任務。Synopsis SIG 首席顧問 Jamie Boote 便曾向 CSO 表示：「我鼓勵企業不僅回顧這類事件，還包括其他安全事故、勒索軟體、復原等所有。將此視為演練機會，『如果大問題來了，我們該怎麼做，未來有能力處理它？』這樣，就不會邊做邊想辦法。」ForAllSecure 的 Brumley 認為這種事件『絕對』會再發生。

|| 重新檢視災難復原計劃

BlackBerry 的資安長 Christine Gadsby 在 CSO 的訪談中也曾表示「只依賴一家供應商如果他們倒閉怎麼辦？這就是對那個造成社會崩潰的供應商產生了依賴。因此，災難復原計劃中要有供應商備份，且必須了解這些供應商的風險評估。」

|| 信任但驗證軟體廠商

這次事件涉及兩間最受信任的軟體公司 CrowdStrike 和微軟，我們不能依賴軟體廠商的聲譽避免災難。Gadsby 曾向 CSO 表示「我很驚訝沒有讓供應商對 SLA（服務級別協議）負責的公司這麼多，或許沒有考慮到這點，也可能不知道 SLA 什麼。…簽訂 SLA，弄清楚發生中斷時他們會做的事，成熟的供應商風險管理計劃至關重要。」還要與董事會和 CXO 密切合作，教育供應商風險管理所需的一切。

|| 危機溝通和現場人員

重新審查危機溝通，尤其內部溝通。公司企業發生狀況時不能無法與員工溝通，要有一套危機溝通計劃與平台，重大事件發生時可以與員工聯繫的替代平台。此外，可協助補救的現場人員也很重要。這次事件爆發初始之際，曾建議企業組織手動刪除有問題的更新，但對動輒數萬台電腦與系統的企業來說，這是不可能任務。要保留

一支最低限度的備用人力（現場人員）。

資安長未來應對方向

總結上述內容，CISO 未來方向建議如下：

|| 一、重新評估事件應變策略（針對更新和佈署過程的漏洞）

- 加強測試程序：確保在更新佈署前充分測試，包括內容更新和反轉測試。
- 實施分階段佈署：逐步向更大範圍的使用者佈署更新，從小範圍測試使用者開始。

|| 二、改進災難復原計劃

- 定期更新災難復原計劃：確保計劃足以因應最新威脅和技術變化。
- 確保員工熟悉復原步驟：定期演練，確保所有相關人員知道如何快速恢復系統。

|| 三、加強廠商管理

- 重新審視與軟體廠商的合約：確保合約中包含對更新和技術支援的明確要求。
- 要求更高的透明度：廠商應該提供詳細的技術說明和故障原因分析。

|| 四、提升溝通和應變工作團隊

- 建立強大的溝通管道：確保在危機過程中能夠快速傳遞訊息。
- 準備應變工作團隊：確保有足夠人力資源因應大規模 IT 事件。

|| 五、探索替代方案

- 評估其他安全性解決方案：確保選擇的解決方案能夠提供足夠的透明度與信任。
- 持續監控廠商表現：確保廠商有能力持續滿足企業組織的安全需求。

資安專家質疑該公司直接存取核心權限的合理性，除了建議自行測試修補程式，還可以考慮 Deep Instinct 或 SentinelOne 等替代方案。