當務之急 CISO 必須做好準備 — 網路復原力

資安威脅更將無所不在（1）

隨著勒索軟體盛行達到前所未有高峰，企業必須瞭解具備網路復原力意謂著超越合規性，針對企業所有層面全方位考量：從運作連續性到軟體供應鏈安全性。

文／Andrada Fiscutean　譯／Nica

2021 年五月，殖民管道（Colonial Pipeline）遭 DarkSide 駭客鎖定，執行長 Joseph Blount 作出高爭議決策，決定支付贖金 440 萬美元。這場攻擊，置美國關鍵基礎建設於高度危機之中、導致必須每天向總統拜登簡報狀況，而 Blount 主張支付贖金對這個國家而言有其必要，將此形容為他職涯中最具挑戰的決定之一。

Blount 向美國參議院國土安全與政府事務委員會表示：「我們處於令人難以忍受的局面，必須做出沒有企業想面對的艱難決定。」

隨著勒索軟體支付在 2023 年達到 11 億美元，公司領導者已然必須頻繁面對這類艱難抉擇。有更多 CSO 與 CEO 體認到問題不在於會不會發生攻擊，為是何時會發生。

據 ISTARI 與牛津大學公布的報告指出，市值 40 億美元的歐洲企業 CEO 表示「對我而言最大改變在於現在全然接受這件事會發生。相信我，接受這件事會發生與認為能抵禦這一切的企業組織之間，處理方式存有本質上的差異。

這種接受資料外洩難以避免的心態，有助於企業變得比現在更有網路復原力。十分常見的情況是，企業組織將復原力視為應對監管機構的打勾確認練習，因而無法為 CISO 提供攻擊後確實恢復原狀所需的一切。

正如 RapidFort 的執行長 Mehran Farimani 所言，抵禦網路安全意外事件並從事件中復原，需要轉換思維超越合規性。

「沒錯，你總是打勾表示已經備份所有重要軟體與資料，但有辦法快速恢復因應敵意事件？還是得花上兩周？你是否持續確保所有此類系統確實檢查？」Farimani 解釋道。

據四月份公布的復原力 Barracuda 報告指出，要求 IT 資安領導者針對處理網路風險的信心，從 1 至 10 評定等級，大部份表示悲觀。金融服務企業組織顯示準備最充份，有 55% 將其資安態勢評分為高度有效。相對之下，僅 32% 工業與製造業領域的公司表示樂觀，而零售業數字則為 39%。整體來看，小型企業在應對網路威脅時信心比較不夠。

地緣政治不穩定、人工智慧與貧富不均等日益加劇，CISO 不僅必須進一步強化企業組織的網路防禦，還必須協助企業做好最糟打算的準備，確保能從網路事件打擊的意外迅速恢復。

網路復原力成為關注焦點

網路復原力概念已進化為時下整體商業策略的關鍵要素。事實上，Trustwave 的資安長 Kory Daniels 表示，「董事會開始問這樣的問題：提供正式的復原長職銜是不是很重要？」

近期受到高度關注的網路攻擊（例如殖民管道所經歷的），強調經典 CIA（機密性、完整性、可用性）金三角中可用性元素的重要性提升。這是由於這樣的破壞不僅影響運作永續性，也影響客戶信任與企業整體市場佔有率。

Daniels 表示，針對網路復原力，必須採用考量企業所有層面與所有團隊-從員工與合作夥伴到董事會的「全方位取向」。

通常，企業組織的能力比自己體認到的還要強大，但這些資源四散在各個不同部門。負責建立網路復原力的各個群組，很可能缺乏對企業內既有能力的完整能見度。

「網路與安全性操作本身就具備極其豐富的情報，可供其他人從中獲益。」Daniels 表示。

許多企業將網路復原力整合至企業風險管理程序。他們開始採取積極措施，識別弱點、評估風險並實施適切管控。

「其中包含暴露評估、滲透測試這類正規驗證與持續監控，以便即時偵測並回應威脅。」Gartner 首席分析師 Angela Zhao 表示。

這些積極措施通常超越企業緊臨邊界，擴及廠商與合作夥伴，FS-ISAC 的全球企業復原力主管 Cameron Dicker 表示。

「公司企業都應該對自身服務供應商與軟體供應鏈進行深度分析，識別安全性風險在哪，並據此發展意外事件應變規劃。」他表示。

軟體供應鏈：復原力等式的關鍵

遺憾的是，正如 Trustwave 的 Daniels 指出，分析軟體供應鏈依舊是網路復原力未被納入討論的面向。

「企業組織應對自身供應鏈執行整體滲透測試與風險評估、對供應商實施網路安全性要求，並建立意外事故規劃，緩解供應鏈破壞運作造成的影響。」他表示。

尋求可能合作的廠商時-尤其是將連結公司私有網路的那些，安全性領導者必須確保合約或主服務協議（MSAs）確切提及整體復原力，包括網路與營運，GuidePoint Security 負責營運永續性團隊的 Bobby Williams 如此表示。

「廠商應依據合約負責確立營運永續性、災

難復原與資訊安全專案。」Williams 補充說明，「明確的測試專案可展現廠商復原力應納入合約，測試結果應提供給企業審查。」

若廠商供應軟體服務或應用，就應該在合約中確立「復原時間目標」（RTO）與定義「復原點目標」（RPO）。

「廠商應能透過必要測試體現 RTO 與 RPO。」Williams 表示。「廠商還要能夠依合約要求說明如何備份客戶資料並提供資料保存排程。」他補充表示，不應該接受以資料鏡像替代備份客戶資料。

軟體供應鏈相關風險不應輕忽。

「最近發生數起針對這部份的網路攻擊案例。」CyberMaxx 的資安長 Aaron Shaha 表示，「這是必須持續嚴格監督的領域。」

AI 增添複雜度

生成式 AI 的興起，使其成為駭客進一步破壞企業復原力策略的工具。這是由於即便懷有惡意的是技術新手，都能利用生成式 AI 執行複雜的網路攻擊，值此之故，攻擊的頻率與嚴重性將會提升，迫使企業組織自我提升。

反之，就防禦目的而言生成式 AI 工具並沒這麼有效。企業組織多半將它們用在補助性角色。AI 證實有效的領域包括威脅偵測與分析、異常偵測、行為監控與自動化應變系統。人工智慧也能用在風險管理與程式碼檢視。

「AI 演算法可以快速分析大量資料、識別模式，以及偵測潛在威脅或人類操作者可能未注意到的弱點。」Accenture Security 領導全球策略的 Valerie Abend 如此說。

在建置與維護網路復原力專案上使用 AI 也有一定的優勢。「從開發量身訂作的 AI 資安政策，到佈署進階 AI 技術並提供永續經營的支援都適用，企業組織的解決方案應確保整個 AI 歷程的可靠性、透明度與合規性。」MorganFranklin Consulting 領導網路與營運復原力的 Tamara Nolan 說道。

然而，目前 AI 在網路安全方面仍處於人為監督的輔助，而非替代。「雖然 AI 可以某種手段提供協助，但它在風險管理上的貢獻，就 AI 進化的現階段而言仍然有限。」Cossack Labs 資安工程主管 Anastasiia Voitova 表示。「它是資安專家的工具，本身並非資安專業。」

RapidFort 的 Farimani 同意這點，並補充表示 AI 工具的確能夠協助形成與傳達復原力規劃，但絕非可靠到足以任其自動導航並假設他們在保護系統。

AI 在網路安全復原力的角色，來年可能擴展。因為 AI 賦能的工具在即時偵測與應對威脅上越來越好。此外，AI 可能會被用以強化使用者驗證與存取控制機制，提升整體關鍵基礎架構系統的復原力，Abend 表示。

法規令網路復原力複雜化

全球法規版圖不斷進化，資安主管要讓企業必須遵循的一切跟上最新狀態頗具挑戰。但堅守這些法律要求，有助於緩解風險並維持企業聲譽。

「法規能夠而且確實有助於企業組織更專注於企業風險管理，除了其他優勢，還能讓企業組織在復原力策略上更負責任。」Bishop Fox 紅隊演練主管 Trevin Edgeworth 如此表示，依循這些規則，有助於提升資料外洩與安全性實作相關的透明度。

歐盟的數位營運韌性法案（DORA）與美國證券交易委員會（SEC）發佈的相關法規，正改變企業處理網路復原力的方式。

將於 2025 年 1 月 17 日生效的 DORA 法案是為了支持銀行、保險業與投資公司這類金融實體安全。歐盟以外的金融實體與資訊及通訊技術服務供應商，若為歐盟金融機構提供關鍵技術服務，也必須遵守 DORA。

「有鑑於新法規與對持續進行中網路攻擊的普遍性疑慮，諮詢顧問公司花費在全災害復原規劃上的時間較少，在 IT 復原力上耗費的心力更多 - 尤其是業務處理程序與支援應用及基礎架構間的連結。」MorganFranklin 的 Nolan 如此告訴我

們。

她建議公司企業超越只是打勾核可做到 DORA 這類法規要求，還要投注心力在復原力的各個層面上，因為「法規是假設在試圖符合 DORA 要求前，基礎的操作復原力元件皆已就定位。」

在美國市場營運的公司，也必須保持警覺並確保符合逐漸形成的法規。2023 年 7 月，證券交易委員會（SEC）對上市公司採用新的報告要求。這些規定強制要求針對重大網路安全意外事件提交 8-K 表格進行揭露，並要求公司每年提供網路安全風險管理、策略與治理方面的重要資訊。

為符合這些要求，多數上市公司採取積極措施，確保系統適切評估、衡量與回應意外事件。

「遺憾的是，在許多案例中，這些處理程序建置在營運復原力框架外，也因此沒有與公司的危機管理專案整合。」Nolan 如此表示，並建議企業組織主動銜接法律與法規框架，將之整合到企業網路復原力策略裡。這種方式有助於盡可能減少罰則並強化企業整體網路復原力態勢。

Gartner 的 Zhao 表示，DORA 與 SEC 發佈的法規往往能全球引發連鎖反應。

「在一個管轄權下的法規改變，通常會造成跨境影響，因為多國企業全球營運需要遵循多重法規框架。」她表示。「此舉導致企業組織必須協調橫跨不同市場的網路復原力策略，確保一致性安全性實作並遵循各種法規。」

Accenture Security 的 Abend 表示，法規也提升了網路復原力的重要性。它們促使企業評估自己的資安態勢，以及董事會的監督與治理。

「然而，我們發現 CEOs、企業高層與董事會，逐漸意識到這些風險，不單是由法規引發，而是真切的營運憂慮。」她說道。

雖然有法規協助，但合規性不必然代表復原力。

企業組織會「落入錯誤的安全感風險，認為他們強大的合規性態式，等同於強大的資安態勢。」Bishop Fox 的 Edgeworth 表示。

人的重要性

許多企業組織針對網路復原力投資技術解決方案，往往忽略在董事會裡要有對的人，還有培養他們的資安意識文化有多重要。

「快速找到物廉價美的網路人才，反而造成業界易受攻擊的弱點。」CyberMaxx 的 Shaha 表示。

值此之故，資安領導者必須開發穩健的、多樣的人才招募策略，確保滿足不斷進化的人才需求。

此外，還應該投資教育訓練課程，超越網路釣魚電子郵件與密碼安全性這種基本意識，Trustwave 的 Daniels 表示。教育訓練應該是「圍繞者網路威脅的深度瞭解、資料保護的重要性與維護網路復原力中所有人的職責。」他補充道。

練習與危機模擬也有幫助。「企業應確保在各種不同場景下練習，確保應變規劃能夠處理意料之外的事件。」GuidePoint 的 Williams 如此表示。「若規劃處理程序持續保持相關與最新狀態，就有信心處理這些黑天鵝事件。」

這類練習應定期執行也應該要有難度。「唯有執行具挑戰性的練習，將團隊、政策與處理程度推到極限，企業組織才會知道自己的限制在哪、哪裡需要改進。」FS-ISAC 的 Dicker 表示。「意外事件，絕對不該成為你應變規劃的第一次測試。」