供應鏈網絡資安威脅因應之道

Securing supply chains from cyber threats (I)

EY 安永

Building a better working world

“

身處萬物聯網及複雜供應鏈的新世界，建構全面資安防禦措施是生存與成長的致勝關鍵

Ashutosh Dekhne
安永美洲全球物流及配送主管暨安永美洲E2E營運轉型主管

供應鏈網絡中日漸增加的數位化與連接能力以及大量數據交換，正使供應鏈面臨前所未有的資安威脅。

這些攻擊不僅會導致組織的重大財務損失，更可能使組織與其合作夥伴及客戶間的長期信賴關係受到傷害。

我們應如何建構一個強大的現代化供應鏈，確保營運安全並提升韌性? 技術驅動的新常態是能安全營運的環境? 轉型成數位化供應鏈安全嗎? 這些是後疫情時代供應鏈主管與最高管理階層所抱持的部分疑問。

從企業觀點看來，儘管供應鏈是相當關鍵的功能之一，但在防禦潛在網路威脅方面，並未獲得應有的關注。根據安永2021年全球資安調查（EY Global Information Security Survey 2021），僅有33%的資安長（CISO）有信心供應鏈在出現網路威脅發動者時，具備滴水不漏的防禦及復原能力。供應鏈網絡攻擊可能以如下圖所列之各種型態出現。常見的供應鏈網絡攻擊動機包括勒索、資產竊取、服務或流程中斷、內部威脅，甚至出於政治或競爭目的。

供應鏈為什麼容易受到資安攻擊?

隨著供應鏈全球化程度提升與快速數位化轉型，供應鏈網絡中互聯利害關係人數量也隨之增加，對企業形成更複雜的情況，進而造成更多的資安攻擊漏洞。供應鏈中任何一環因缺乏培訓、認知或監督而未遵守資安協定，都可能使整個系統的資安防線癱瘓。

此外，生態系統中的許多當事方仍欠缺整合資訊科技（IT）系統與營運科技（OT）系統的企業層級整體資安策略，使得供應鏈中的各連接節點易受資安攻擊。

為什麼資安防禦如此重要?

供應鏈網絡攻擊可能導致在財務及信任層面的高昂代價，例如美國一家醫療管理企業於2021年遭到供應鏈勒索軟體攻擊，超過100萬人[1]受到影響，成為美國當年最大規模的健康資料外洩事件之一。

將網路防禦卓越度作為影響企業參與及策略聯盟KPI的概念也正在崛起。目前絕大多數的利害關係人將供應鏈網絡資安防禦視為業務連續性的重要因素之一，擁有健全資安防禦系統的企業較易在供應商夥伴關係、經銷合約及其他策略聯盟等各參與階段成為優先合作夥伴。

未遵守監理機關所制定的資安防禦要求不僅為企業帶來外洩風險，也可能使監管審查頻率增加並導致商譽受損罰款。2021年美國紐約州金融服務署所通報的網路資安與其他相關不合規活動，罰款共計超過600萬美元。

> 企業需轉換心態將資安防禦視為整體企業韌性策略的一環，而非只是合規要求。

Sameer Anand
EY-Parthenon美洲供應鏈主管，策略與交易諮詢服務

哪些供應鏈的環節最容易受到資安攻擊？

供應鏈各階段相關的科技、流程複雜度與第三方參與程度各有不同，因此所面臨的資安威脅及對業務連續性的可能影響程度也不盡相同。這進一步突顯出必須謹慎規劃可滿足各階段差異的資安策略並建立健全靈活的解決方案，將其與供應鏈的不同活動部分整合。

採購：

現代化供應鏈日益擴展的特性，包含進行大量資料交換的眾多參與者及功能性，讓採購成為最易遭受攻擊的環節。過去5年，企業透過數位化轉型，將軟體即服務（ SaaS ）運用在採購與供應商管理流程，然而在協助降低成本、節省時間的同時，也增加了資料及網路資料外洩漏洞，使得供應商及企業業務面臨風險。

企業資源規劃（ ERP ）軟體資料外洩是採購階段最常見的資安攻擊類型，惡意發動者將目標鎖定在客戶及供應商的敏感資料，包括財務、客戶及合作夥伴網路詳細資料、發票與訂單管理資料、帳戶詳細資料，以及其他監管與稅務證明。

過往資安攻擊顯示部分對採購端影響最大的資安事件是以供應商系統程式為目標，其次為資料與內部流程。此類事件會對供應商及客戶端營運造成傷害，因此必須改變管道或供應流程。

這種情況下，具備內部緊急應變的團隊及替代供應商網絡的客戶，在因應營運與供應中斷上會處於較有利的地位。

2022年2月，一間全球石油能源業領導廠商通報因兩間德國供應商受到網路資安攻擊，導致營運延誤，必須將其石油重新發送至替代儲存庫。

2022年3月，一間日本跨國汽車製造商通報其重要元件製造商之一的IT系統遭到攻擊，在此之前，2022年2月，該製造商也通報另一間主要日本供應商因資安攻擊造成營運暫停。持續不斷的網路攻擊與供應中斷迫使該企業修正其區域生產計畫，將4-6月產出分別減少20%、10%及5%。

製造：

絕大多數企業使用雙層技術：1）在企業層級配置IT，負責軟硬體相關資料處理與通訊；及2)負責設備、工業控制系統（ICS）及其他製造與營運使用設備的OT。

然而這兩者通常並未完美整合，使得潛在資安漏洞大幅增加。製造是影響企業運作最敏感環節之一，短暫的網路中斷可能對企業營運帶來長久負面影響，因停機、失去資料傳輸功能或庫存持有成本上升而導致鉅額損失。

在今日萬物互聯的世界，對單一供應商的資安攻擊可能造成客戶與其相關連供應商的多間工廠長時間中止製造活動，進一步導致負面連鎖反應，如生產及配送延遲、產品缺貨、供需失衡、價格上漲與消費者的不信任。

2021年，美國的水務及廢水組織收到來自聯邦調查局（FBI）、網路安全暨基礎設施安全局（CISA）、環境保護局（EPA）及國家安全局（NSA）等多個政府機構的共同警告，不間斷的網路攻擊將威脅到水廠的工業控制系統（ICS）。內容中強調了資料、勒索軟體、網路分區隔離、網路複雜度及系統維護相關風險，也特別提及威脅發動者用以癱瘓IT與OT系統及網路的手法。

因勒索軟體攻擊而導致的停機、遠端存取盜竊、未修補軟體、ICS漏洞與第三方網路相關攻擊等，都是製造階段中常見的攻擊手法。

配送及物流：

對第三方的高度依賴，使得配送及物流成為面臨高資安風險的環節之一。儘管組織擁有健全的網路定義生態系統，若其合作夥伴企業無法實施相同程度的資安解決方案，依然容易受到威脅。物流業者處理大量客戶資料也使其成為攻擊者熱點，供應鏈在此階段，資料外洩比例相當高。與採購流程類似，眾多不同的參與者使得供應鏈複雜度增加，進而更難以落實及管理標準化的供應鏈資安協定。

此外，越來越多物流業者採用自主解決方案，使其功能變得更加仰賴數位化，進而加劇資安攻擊風險。在過去，攻擊者也會利用OT的快速發展，將無線通訊頻道作為中斷整個供應鏈的破口。疫情期間物流服務業者數量呈指數型成長，使其成為勒索軟體攻擊眼中更主要的目標。

最近，數間全球最大航運業者受網路犯罪所害，影響其營運長達數週，特別是勒索軟體攻擊，造成航班延遲、敏感客戶資料外洩，以及支付鉅額贖金的企業成本壓力。

哪些產業最易受到資安攻擊?

工業4.0被認為為許多產業帶來重大改變。如先前所強調，對製造環節的資安攻擊可能對業務持續性產生長期影響，也使得半導體變成最容易成為攻擊目標的產業之一。蓄意存取敏感資料及虛擬操控的惡意行為，即是導致如健康照護、消費者產品、零售、汽車及能源等產業成為供應鏈網絡犯罪主要目標的另一項關鍵觸發點。

儘管各產業監理環境不盡相同，提升網路安全認知、主動投資入侵檢測、監控及預防工具，與落實合作夥伴網路弱點控管架構以保障合作夥伴（特別是供應商及運輸業者），正成為IT策略最優先事項。

產業	網路漏洞範圍	近期事件
半導體	此產業的傳統線性供應鏈已經進化為採用資料驅動型的智慧供應鏈架構，推動更為優化的資源管理與物流。但工廠自動化、遠距辦公、數位化供應商管理及採用動態定價系統都包含大量的資料共享，導致資料外洩風險增加。 2020年至2022年間，業界經歷了相當大量的勒索軟體攻擊、服務與生產中斷攻擊、韌體攻擊與網路癱瘓。晶片智慧財產權盜竊也呈現增加情況，尤其是在2021年全球晶片短缺時期。	► 一間全球頂尖顯示卡製造商通報敏感資料外洩資安攻擊[2]。該攻擊利用未授權存取員工憑證 **影響程度：近1TB資料遭到竊取，其中包括超過7萬筆員工憑證。此外，攻擊者發布可能影響企業績效的產品中斷相關要求。** ► 2017年，主要晶片廠之一宣布遭到勒索軟體攻擊[3] **影響程度：產線關閉近半週，導致超過1.7億美元收益損失。**
生命科學及健康照護	此產業之產品及資料的數量與關鍵性使其容易受到勒索、供應及資產盜竊，與敏感資料外洩威脅。 儘管此產業遭到網路攻擊的風險較高，嚴苛的法規壓力在某種程度上抵銷了風險，尤其是在美國，聯邦政府制定如健康保險可攜性與責任法案（HIPAA）保障敏感資料，並頒布資料外洩通報命令。	► 近期2022年發生在美國境內一間醫藥集團大廠[4]的資料外洩，是因缺乏健全授權及存取系統而導致網路癱瘓 **影響程度：超過100萬筆的個人資料遭到外洩。**

產業	網路漏洞範圍	近期事件
汽車	眾所周知，汽車產業面臨如隱私侵犯、內部威脅、透過釣魚攻擊或預裝惡意軟體等多種來源的網路癱瘓、軟體及韌體攻擊，與虛擬化惡意軟體等大量資安威脅。 隨著電動車（EV）與自動駕駛汽車（AV）迅速發展，包括開源技術社區在內的上百萬節點間之虛擬或網路互動與資料交換，預期會使攻擊數量更為增加。	▸ 韓國汽車大廠近期通報，其在美國業務因受到大規模資安攻擊[5]，而被要求支付贖金。 **影響程度：要求支付近2,000萬美元等值的比特幣，以交換資料不要外洩。此事件也導致車廠其處理客戶和經銷商之內部IT系統故障。** ▸ 2020年，一家總部位於日本的全球汽車製造商通報其在美國的網路遭受入侵[6]，並聲稱因大量的遠距辦公漏洞而導致。 **影響程度：工業控制系統運作與其他製程失效。**
消費及零售	隨著全通路策略、銷售點和配送管理創新的迅速拓展，越來越多企業採用如直接面對消費者或線上購買門市取貨（BOPIS）等新型商業模式，以及客戶與合作夥伴參與使用沉浸式技術的頻率增加，皆是消費及零售產業對數位化依賴及網路攻擊增加的一部分原因。 此產業中，攻擊者的部分關鍵動機為取得未授權資料存取（交易及帳單資料、客戶個人資料、獎勵與酬賓方案細節），以及透過分散式阻斷服務（DDoS）製造流量不平衡。	▸ 一間全球肉品加工大廠在2021年遭到資安攻擊[7] **影響程度：該業者面臨多區營運處關閉，最後不得不支付超過1,000萬美元的贖金。** **除此之外，營運處的關閉加劇了食品供應短缺的威脅，使得消費者必須面對更高昂的食品價格。** **即使營運能即時且安全的恢復，但資料的機敏性仍成為遭勒索而觸發本次事件的原因。**

產業	網路漏洞範圍	近期事件
能源	可靠的能源供應對所有產業的日常營運至關重要，包括如國防與健康照護等影響層面廣泛的產業，這使得能源產業極易受到資安攻擊。 此產業內發生大規模服務中斷時，可能導致供應短缺與價格上漲，甚至危及上百萬人性命。	▸ 2021年，美國最大燃料管線營運商之一通報遭到勒索軟體攻擊[8]，迫使其停止營運，改採人工操作模式並停用IT系統 **影響程度：服務中斷、440萬美元的贖金、導致市場短缺及恐慌性購買。**

面對資安攻擊，如何建立有效的應變生態系統?

1 組織

- 整合資安防禦措施與企業韌性策略
- 購買資安險以因應剩餘風險
- 合理配置資安防禦預算
- 使用進階分析評估常見漏洞
- 實施智慧威脅偵測解決方案
- 整合IT-OT生態系統
- 建立目標人才庫，並讓最高管理階層參與制定資安防禦策略階段

2 合作夥伴網絡

- 藉由供應商網路的多樣化來降低曝險
- 使用不同平臺廠商的解決方案以建立「零信任」的安全架構
- 使用「紅藍隊」來模擬資安攻防策略
- 為合作伙伴導入全面性的資安漏洞管理計畫
- 具備結構化的通報機制
- 將資安韌性視為選擇合作夥伴的KPI

3 監管

- 定期更新隱私管理系統以符合區域及全球隱私法規
- 促進及支援更多公私部門合作夥伴關係
- 改用更符合合規要求的基礎建設
- 針對各項業務參與進行資安盡職調查
- 評估業務情境及監控數位交易政策

企業可採取下列步驟強化其資安防禦

1. 組織：

- 整合資安防禦與韌性策略並建立緊急應變計畫，以因應資安攻擊，並有助於降低影響程度和確保營運持續。
- 企業可考量投保資安險以涵蓋實施資安計畫後的剩餘風險。例如2022年1月，全球製藥大廠在與保險公司的法律爭議中獲勝，針對2017年該公司所受到的惡意軟體資安攻擊，保險公司須賠償14億美元的損失。
- 應更合理的配置供應鏈資安的預算分配。根據安永2021年全球資安調查（GISS），39%的受訪者提到，資安花費並未充分考量到策略投資上的成本，如IT供應鏈的轉型。
- 定期執行系統更新並使用進階分析解決方案，對內部及合作夥伴進行弱點評估。此外，隨著各項新流程與產品的採用，組織應確保資安及營運的合規性。
- 實施智慧資安解決方案，利用歷史趨勢與行為能力在各接觸點進行威脅偵測。此外，採取主動措施執行預防性解決方案，例如使用功能更強大的認證協定及IAM（身分識別與存取管理）系統，以降低敏感資料外洩的風險。
- 整合並同步IT與OT系統，以確保連同監控、即時偵測並對系統的漏洞迅速反應。
- 指派技術專家與人資專家共組團隊以擴大和媒合資安人才資料庫。同時也讓最高管理層、董事會成員及其他職務的資深主管多參與制定資安策略。

2. 合作夥伴網絡：

- 供應商種類和業務管道的多樣化，有助於降低危害到營運持續之風險。前項所指之風險為過度依賴特定供應商或業務管道，以致遭受資安攻擊所造成的營運中斷風險。
- 建立「零信任」的資安架構，透過在各階段持續驗證所有數位交易，排除隱性信任並確保組織正常運作。隨著遠距工作的需求增加，企業正轉向尋求跨平臺廠商的零信任解決方案，以避免讓大型供應商集團擁有OT系統操控權。
- 透過「紅藍隊對抗」模擬的資安防禦策略，建立更妥善的內部及延伸網路之資安生態系統。此方法中，「紅隊」專家使用如滲透測試、釣魚攻擊活動等各種技巧找出既有資安防禦系統及流程中的弱點，「藍隊」執行人員則扮演保護企業系統不受資安攻擊的防守團隊。
- 採用全面的資安漏洞管理計畫，評估合作夥伴整體網路健全性及對資安攻擊的認知程度。此計畫應定期監控及評估各供應商或合作夥伴處理機敏資料的風險等級，及其可能影響營運持續性的潛在資安漏洞。
- 發展結構化且全面的通報機制，使組織能通報任何事故狀態（事前-事後、模擬）。此外，分析網路入侵的潛在影響，可透過評估組織「調查、扼制和恢復」等流程，了解企業的網路能力。
- 鼓勵所有供應商與其他合作夥伴持續增加資安在其IT預算中的比例。將資安風險準備性與網路韌性作為挑選合作夥伴的KPI，這或許有助於加速在合作夥伴網絡中實施資安防禦解決方案。

3. 監管：

- 更新隱私管理系統，以符合區域和全球的隱私法規，並平衡個別管轄權的法律，以將整體供應鏈網絡的資安協訂標準化。
- 在政府機關、企業、產業協會及非營利組織（如資訊分享與分析中心（ISACs））等公私部門間建立堅固的合作關係，共同建立不受產業限制的解決方案，以利在發生攻擊事件時，能即時交換威脅情資及獲取修復支援。以美國國土安全部的資安資訊分享與協作計畫（CISCP）為例，這是一項可靠的公私合作夥伴關係旗艦計畫，促進聯邦政府與關鍵基礎設施擁有者或營運者之間的資安資訊分享。

一間位於美國的健康照護公司建立資安團隊，與同行企業、產業協會及政府機構建立密切合作關係，分享最佳實踐並合作開發有效解決方案，以因應公部門和私部門組織所面臨日益增加的威脅及攻擊手法。

2018年，一間英國通訊領導企業與英國國家安全網路中心合作推出免費合作線上平臺，與同行分享惡意軟體及網站資訊預防資安犯罪。

- 藉由更新特定之威脅導向合規命令，以採用更符合合規要求之基礎建設。例如2022年4月，美國參議院通過網路安全法案，更有效管理及通報勒索軟體支付。
- 對各項業務參與進行資安盡職調查，遵守中心化或去中心化網路規定的通報標準。例如歐盟的一般資料保護規則（GDPR）是中心化的區域性指導方針，要求事件發生72小時內通報事件，而美國則採用去中心化法，讓各州自行制定資料外洩規定。
- 評估業務情境及監控數位交易政策，包括稅務及關稅變更，以提升合規性並降低整體網路風險。例如部分國家將高關稅作為防止資安攻擊的一種手段，使企業必須意識到並遵守此類戰術管理協定。

結論

後疫情時代下形成的商業環境，僅仰賴對資安威脅的知識已不足以保障企業經營成功並受到保護。大幅提升的互聯性與大量資料流在各項產業中皆已佔有一席之地，從營運、策略及監管角度來看，都使得供應鏈網絡資安防禦至關重要。供應鏈除了必須更靈活、更有效運用科技，也需要對抗資安威脅，避免危及營運持續性與損害長期合作夥伴關係及客戶信賴的可能性。因此，最高管理階層與董事會成員必須更重視資安防禦，並提高投入金額。

1 “Cyberattacks in healthcare surged last year, and 2022 could be even worse,” *Chief Healthcare Executive*, www.chiefhealthcareexecutive.com/view/cyberattacks-in-healthcare-surged-last-year-and-2022-could-be-even-worse, January 24, 2022.

2 “70,000 Nvidia employees reportedly affected by recent hack,” *digitaltrends*, www.digitaltrends.com/computing/71000-nvidia-employees-affected-by-recent-hack/, March 4, 2022.

3 “TSMC Suffers WannaCry Attack,” *PCrisk*, www.pcrisk.com/internet-threat-news/13286-tsmc-suffers-wannacry-attackx, August 7, 2018

4 “MCG Health Faces Lawsuit Over Data Breach Impacting 1.1 Million Individuals,” *SecurityWeek*, www.securityweek.com/mcg-health-faces-lawsuit-over-data-breach-impacting-11-million-individuals, June 23, 2022.

5 "Kia Motors America suffers ransomware attack, $20 million ransom," *Bleeping Computer*, www.bleepingcomputer.com/news/security/kia-motors-america-suffers-ransomware-attack-20-million-ransom/, February 17, 2021.

6 "Honda Hacked: Japanese Car Giant Confirms Cyber Attack On Global Operations," *Forbes*, www.forbes.com/sites/daveywinder/2020/06/10/honda-hacked-japanese-car-giant-confirms-cyber-attack-on-global-operations-snake-ransomware/?sh=2153061253ad, June 10, 2020.

7 "Meat supplier JBS paid ransomware hackers $11 million," *CNBC.com*, www.cnbc.com/2021/06/09/jbs-paid-11-million-in-response-to-ransomware-attack-.html, June 9, 2021.

8 "Colonial Pipeline Paid Hackers a $4.4 Million Ransom," *Secior*, www.secior.com/resources/news/colonial-pipeline-paid-hackers-a-4-4-million-ransom/, accessed September 16, 2022.

聯繫安永

曾韵
執行副總經理
安永諮詢服務股份有限公司
+886 2 2757 8888 Ext.88892
Christina.Tseng@tw.ey.com

陳志明
副總經理
安永企業管理諮詢服務股份有限公司
+886 2 2757 8888 Ext.67836
Jemmy.CM.Chen@tw.ey.com

藍健銘
資深經理
安永企業管理諮詢服務股份有限公司
+886 2 2757 8888 Ext. 20343
Craig.CM.Lan@tw.ey.com

安永 | 建設更美好的商業世界

安永的宗旨是致力建設更美好的商業世界。我們以創造客戶、利害關係人及社會各界的永續性成長為目標，並協助全球各地資本市場和經濟體建立信任和信心。

以數據及科技為核心技術，安永全球的優質團隊涵蓋150多個國家的業務，透過審計服務建立客戶的信任，支持企業成長、轉型並達到營運目標。

透過專業領域的服務 - 審計、諮詢、法律、稅務和策略與交易諮詢，安永的專業團隊提出更具啟發性的問題，為當前最迫切的挑戰，提出質疑，並推出嶄新的解決方案。

APAC No. 14007106
ED None

ey.com/zh_tw

加入安永LINE@好友
掃描二維碼，獲取最新資訊。