



網路安全的正面風險

AWS 方案指引



AWS 方案指引: 網路安全的正面風險

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

簡介	1
正向風險的好處	2
促進積極成果	2
提升安全狀況	2
變更風險語言	4
增加採用率	5
正面風險的範例	6
技術正面風險	6
專案管理正面風險	6
網路安全正面風險	6
網路安全風險回應	8
後續步驟	10
常見問答集	11
上行風險與正面風險	11
重要性	11
資源	12
文件歷史紀錄	13
.....	xiv

網路安全的正面風險

Greg Bell , Amazon Web Services (AWS)

2022 年 5 月 ([文件歷史記錄](#))

大多數人從負面角度看待風險，例如面臨損失或管理不良事件。然而，國際標準化組織 (ISO) 對風險的定義是「不確定性對目標的影響」。在這種情況下，影響可能是正面的，也可能是負面的。

實際風險可能因產業而異，但此標準定義適用於所有產業，並且每個產業都有負面和正面風險。在網路安全產業中，負面風險是指潛在損失，正面風險是指資產、知識、改進或資料的潛在收益。

專案管理和 IT 領域已採用評估業務報告和業務決策中正面風險的策略。但是，網路安全產業尚未將其作為一種常見做法，許多風險管理方法繼續關注負面風險。如果他們討論正面風險，那只是簡短的。

傳統上，網路安全只從負面角度來看待風險。以下是網路安全中常見的兩種負面風險類型：

- 下行風險 – 外部因素導致的損失，例如威脅。例如，網路犯罪分子可能會引入或增加安全事件的可能性。
- 上行風險 – 在追求收益的同時面臨損失，例如由於變化而導致的漏洞。例如，在實施 IT 策略時，可能會無意中增加發生安全事件的可能性。上行風險與正面風險不一樣。儘管它發生在追求收益的過程中，但上行風險也集中在潛在的損失上。

直到最近，網路安全只考慮負面風險，風險的定義集中在潛在的負面結果上。正面風險在識別風險之初就關注潛在的積極結果。排除正面風險會導致無法識別網路安全的積極結果。由於專注於負面風險，高層通常認為網路安全是被動的，而不是主動的，並低估了網路安全對積極業務成果的貢獻。

本文件定義了網路安全產業的正面風險，並討論在網路安全策略中納入正面風險的好處和重要性。

正向風險的好處

尤其是在網路安全這樣專注於保護業務免受潛在損失的行業中，很容易從負面角度界定風險。根據潛在收益重新界定網路安全風險，透過促進積極成果、提升組織的安全態勢以及增加客戶信任，從而使企業受益。

促進積極成果

採用正面風險可讓組織評估並認識到該領域對正面業務成果的貢獻。根據[高管和董事會會議室的網路安全](#) (Enterprise Strategy Group 研究報告)：

- 69% 的業務和技術負責人認為網路安全完全或主要是一個與業務幾乎沒有關係的技術領域。
- 11% 的業務和技術負責人將網路安全等同於法規遵循。
- 82% 的組織聲稱，由於網路威脅日益增加、企業內部技術的進一步整合以及不斷增長的受攻擊面等因素，網路安全風險在過去兩年有所增加。

當網路安全主管將正面風險整合到對話和報告中時，有助於提升公司內部安全 IT 操作的價值。

例如，假設一家企業在幾年前發生了資料洩露，並且資料洩露是由於缺乏修補程式管理程序而引起的。該事件仍由媒體提起，它影響了客戶對公司的看法以及與公司的互動。企業希望擺脫這一事件並擴大其服務產品，但客戶的信任阻礙了銷售。網路安全利用正面風險來說服領導層投資於可持續更新應用程式的修補程式管理程序。新程序大幅降低了資料外洩的風險，改善了公司的安全狀況。最新修補程式管理程序的新聞會傳達給媒體和潛在客戶。客戶現在可以放心地購買企業產品，銷售額大幅增加。

在風險識別過程中未考慮正面風險可能會提供不完整的評定並影響業務決策。有關可能影響業務決策的正面風險的具體範例，請參閱 [正面風險的範例](#)。

提升安全狀況和客戶信任度

網路安全是企業安全狀況不可或缺的一部分。資料洩露可能會對客戶的信任產生負面影響，但強大的安全狀況和聲譽也可以增加客戶的信任度並推動商機。

如 [促進積極成果](#) 中所述，研究表明高管領導了解與網路安全相關的負面風險，但通常不了解正面風險或商業價值。但是，研究表明網路安全領導了解強大的安全狀況如何使組織受益。

在[網路安全研究：創新加速器](#) (Vodafone 白皮書) 中，Vodafone 採訪了 1,434 位全球網路安全決策者。根據他們的資料：

- 73% 的受訪者認為強大的安全性創造了新的商機。
- 89% 的受訪者表示改善其安全性將提高客戶忠誠度和信任度。
- 90% 的受訪者還表示他們能夠提高自己的形象，接觸新的潛在客戶，並將他們變成真正的客戶。
- 89% 的受訪者認為擁有高效的網路安全是一種相關的競爭優勢，這有助於他們與競爭對手區分開來。
- 24% 的受訪者認為透過使用雲端技術和物聯網 (IoT) 以及採用有針對性的 IT 安全控制可增加營收。
- 在與高管溝通時，您還可以使用正面風險來傳達提高客戶信任度的商業價值，而不是使用潛在的負面結果。高管人員在對計畫進行資助時可以保持謹慎。在某些情況下，網路安全達到了操作所需的最低限度。在申請資金過程中內部溝通正面風險可以協助領導者了解網路安全的商業價值。這可能導致增加網路安全計畫的資金，並為企業帶來收入。

變更網路安全風險語言

對網路安全採用正面風險的部分挑戰是技術和特定領域的術語側重於負面風險，例如威脅、漏洞以及安全控制。網路安全產業必須發展和擴大其詞彙量，以納入強調網路安全為企業帶來正面業務結果 (或正面風險) 的語言。諸如業務優勢、好處以及業務價值等術語突出強調網路安全對組織的貢獻。

變更網路安全的語言有助於改變人們的看法，即網路安全是一個專注於威脅和漏洞的技術領域，它與業務無關。企業領導通常低估了網路安全對正面業務結果的貢獻。如需領導層對網路安全認知的詳細資訊，請參閱 [促進積極成果](#)。

增加相關領域的採用率

許多領域對採用正面風險的興趣日益增長，因為它認識到了該領域對業務成果的貢獻。正面風險的概念最近已被納入到常見的專案管理程序和定義中。

2013 年，專案管理協會 (PMI) 將正面風險 (也稱為機會) 的定義納入專案管理知識體系 (PMBOK) 的第五版。PMBOK 將個人風險定義為「不確定的事件或情況，如果發生，會對一個或多個專案目標產生正面或負面影響。」它將整體專案風險定義為「不確定性對專案的整體影響... 超過專案中個人風險的總和，因為它包括專案不確定性的所有來源... 表示利益相關者會受到專案結果變化的影響，包括正面和負面影響。」

不幸的是，PMI 在風險定義中將積極結果納入其風險定義中並不適用於網路安全產業。

正面風險的範例

以下是技術、專案管理和網路安全的一些正面風險範例。

技術正面風險

技術正面風險的一個範例是技術的實施可能降低工資成本。例如：

1. 實施該技術可以提高業務效率。
2. 這些效率可以減少勞動力。
3. 減少勞動力可以降低工資成本。

專案管理正面風險

專案管理中的一個正面風險範例是專案預算的錯誤計算可能導致成本節省或資助其他專案。例如：

1. 儘早實施技術專案可能會導致專案經理錯誤計算專案成本。
2. 錯誤計算專案成本可能會導致專案資金過多。
3. 過多的專案資金可能導致成本節省或為其他專案提供資金。

網路安全正面風險

網路安全正面風險的其中一個範例是實作修補程式管理可能會提高客戶信任度。例如：

1. 實作修補程式管理可減少應用程式中的漏洞。
2. 消除漏洞可降低應用程式風險，並使應用程式更安全。
3. 提高應用程式安全性可減少資料遺失。
4. 減少資料遺失可能會增加客戶信任度。

網路安全的正面風險的另一個範例是實作事件回應可能會提高員工生產力。例如：

1. 實作事件回應可能會偵測到網路流量的增加。
2. 增加的網路流量可能會導致偵測到員工透過存取與工作無關的內容 (例如音樂和視訊串流服務) 濫用資源。這些活動會消耗網路頻寬，並可能對網路和應用程式效能造成負面影響。

3. 偵測到員工濫用公司資源可能導致阻止這些服務。
4. 阻止這些服務可以減少網路頻寬的消耗並提高員工的生產力。

最後，網路安全正面風險的最後一個範例是實作事件回應計畫可能會增加商機並遵守隱私權法律。例如：

1. 實作事件回應計畫可以快速偵測和識別惡意軟體和勒索軟體。
2. 識別惡意軟體和勒索軟體可以最大程度地減少影響並減輕對公司資源的威脅。
3. 減輕對公司資源的威脅可能會帶來新的商機，並協助企業保持遵守隱私權法律。

網路安全風險回應

對正面風險和負面風險的回應有很大的不同。對於負面風險，需要採取措施將對結果的影響降到最低，但對於正面風險，需要採取措施最大限度地提高對結果的影響。下表顯示對正面風險和負面風險的可能回應。

風險類型	回應	定義
正面風險	利用	最大限度地提高風險發生的概率或可能性，以實現其積極作用。
	Share (分享)	將風險的一部分所有權或責任分配給另一方。這是與負面風險相同的方法，它試圖控制潛在的損失或收益。
	提升	增加產生風險的條件，以最大限度地提高機會。
	Ignore	忽略風險的可能性，不採取任何行動。當風險的可能性很低或潛在的積極結果的好處很小時，這種回應很常見。
	減輕	將風險發生的概率或可能性降至最低。
負面風險	轉移	將風險的責任或義務轉移給另一方，例如購買保險單，將風險轉移給保險公司。
	避免	消除產生風險的條件。
	接受	確認風險的存在，但不採取任何行動。

對於負面風險，組織會根據其風險承受能力和偏好來避免、轉移、減輕或接受風險。他們試圖防止風險的發生，如果發生，他們會盡量減少對整體任務的影響。

說明正面風險回應的最佳方法是使用範例：

- 利用 – 安全主管了解到一名合格的安全專業人員最近決定尋求新的就業機會，並安排了豐厚的簽約獎金，以吸引潛在員工加入他的團隊。
- 共用 – 業務單位負責人希望透過使用特權存取管理產品來提高安全性，但沒有足夠的預算來購買目前會計年度的工具和服務。該負責人與來自不同業務單位的負責人合作，後者將購買並實作工具作為試點專案，然後擴展安裝以支援兩個業務單位。
- 提升 – 員工發現了一個將現有業務流程自動化以減少網路安全威脅的機會，但這需要在時間和設備上進行投資。看到這樣一個過程的積極好處，經理批准加班以開發能力，並重新調整現有硬體和軟體資源，使專案得以進行。
- 忽略 – 財務主管了解到在銷售部門工作的員工開發了一種新的應用程式，它可以自動執行乏味的手動任務。該應用程式最近被授權僅在銷售部門使用。財務主管在未經明確授權的情況下獲得新應用程式的複本，以便在他的部門中獲得類似優勢。

後續步驟

技術和專案管理領域在其風險評定流程中採用了正面風險，但網路安全產業歷來將其排除在外。正面風險可能會產生正面的業務成果，網路安全產業必須轉型以接受正面風險並實現收益。

可以在所有通訊中立即開始溝通正面風險。例如，風險評定、安全評定或狀態報告應包括正面風險部分。向高管領導層提出的資金請求應包括正面風險，向企業傳達潛在利益，並強調透過批准請求獲得的任何潛在的業務優勢。

常見問答集

上行風險和正面風險有什麼區別？

儘管上行風險和正面風險聽起來相似，但是兩者實際上非常不同。在風險範圍內，存在正面或負面結果，並且在負面結果中，存在上行或下行。

正面風險是資產、知識、改進或資料的潛在收益。例如，您實作修補程式管理和快速消除漏洞的程序 (例如在一週內)。在下一年中，不會發生任何安全事件。

上行風險是在追求收益的同時遭受損失。例如，企業部署了新應用程式，您實作修補程式管理和快速消除漏洞的程序 (例如在一週內)。遭受損失 (消除漏洞的時間段) 是為了追求收益 (更安全的應用程式)，因此這被認為是上行風險。可以透過將消除漏洞的過程改為一天來增加上行風險，或將該期限改為一個月來降低上行風險。基本上，上行風險是試圖最大限度減少損失時獲得收益的不確定可能性。

為什麼將正面風險納入網路安全中很重要？

在網路安全風險評定和對話中整合正面風險，有助於為企業提升網路安全的價值。如需詳細資訊，請參閱[正向風險的好處](#)。

資源

- [高管和董事會會議室的網路安全](#) (Enterprise Strategy Group 研究報告)
- [網路安全研究：創新加速器](#) (Vodafone 白皮書)
- [整合網路安全與企業風險管理 \(ERM\)](#) (NIST 出版物)
- [闡明「上行」和「正面」風險](#) (FAIR 研究所部落格文章)

文件歷史紀錄

下表描述了本指南的重大變更。如果您想收到有關未來更新的通知，可以訂閱 [RSS 摘要](#)。

變更	描述	日期
初次出版	—	2022 年 5 月 27 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。