

探索攻擊者經濟學： 第三方風險的角色

為何網路韌性需要身分優先策略來保障第三方存取的安全。

\$9.5
兆

2024 年網路犯罪
相關的預測成本¹

若將網路犯罪比擬為國家
來衡量，其規模將排名第
三，僅次於美國與中國

其獲利高於全球所有主要
非法藥物貿易的總和

63%

的組織對於授予非員工的
存取權限不具可視性²

54%

的組織曾因非員工擁有不當
存取權限而遭遇安全問題³

59%

的組織曾因第三方而發生
資料外洩問題⁴

攻擊鏈 由此開始

存取管理效果不彰，其原因
是威脅行為者會透過下列
方法竊取憑證：

- ▶ 憑證填充
- ▶ 鍵盤側錄惡意軟體
- ▶ 網路釣魚
- ▶ 社交工程

內部攻擊者

外部攻擊者

41% 的組織表示曾對其造成
重大影響的網路攻擊源自於
第三方⁶

承包商

供應鏈合作夥伴

廠商

關係企業

越來越多公司利用第三方非員工來完成業務

儘管他們並非員工，但這些
非員工卻能存取組織最有價值的
資產

97% 的組織會將存取權限
提供給第三方非員工⁵



應用程式

001011
110010
010101

資料



開發營運



IaaS/PaaS



內部部署



SaaS

特殊權限帳戶

威脅行為者會將非員工作為
目標，是因為第三方安全通訊協定
存在漏洞、安全訓練程度較低，
以及公司對非員工存取權限的控
制及監控較為鬆散

僅有 13% 的組織會持續監控
第三方的安全風險⁷

資料外洩

勒索軟體

服務中斷

\$429萬

第三方資料外洩的平均成本⁸



保障第三方安全對於維護貴組織擴展網路而言至關重要。
以下是我們協助 Absa 銀行的做法。

12,000

具備安全身分能力的非員工人數

15

為加快第三方存取速度而省去的登錄天數

\$300

每位非員工身分登錄所節省的金額

[閱讀案例故事](#)