

安全與網絡風險

Dr Alexander Ressos, TEP

*Attorney-at-Law (Switzerland), Solicitor (Hong Kong),
Solicitor (England & Wales)*

高價值企業和富裕人士集中在一個小州，帶來了安全風險。近年來，針對瑞士企業和政府機構的網絡攻擊有所增加。2023 年，一家聯邦行政部門 IT 供應商遭受攻擊，導致聯邦機構的敏感數據外洩。¹大宗商品貿易商、加密貨幣企業和財富管理人持有有價值的數據和資產，因而成為犯罪分子和國家行為者的誘人目標。加密行業已遭受多起黑客攻擊，價值數百萬的代幣被盜。

州政府和企業已在網絡安全方面進行投資，聯邦也設立了聯邦網絡安全辦公室（BACS）。²對富裕居民及其家人的保護是另一項關切，由私人安保公司和警方負責。這些風險不太可能改變大多數企業的選址決定，但會增加在該州經營的成本。一旦發生影響金融或大宗商品基礎設施的重大網絡事件，該州在安全與穩定方面的聲譽可能受損。

1 註釋

1. 聯邦委員會，新聞稿 “Hackerangriff auf Firma Xplain: Bundesrat mandatiert politisch-strategischen Krisenstab ‘Datenabfluss’”，2023 年 6 月 28 日，admin.ch：針對 IT 服務提供商 Xplain 的勒索軟件攻擊影響了聯邦行政部門的數據；聯邦網絡安全辦公室（BACS），新聞稿 “Hackerangriff auf Firma Xplain: Bericht ... zur

安全與網絡風險

Datenanalyse publiziert”（2024 年），ncsc.admin.ch：黑客組織“Play”於 2023 年 6 月 14 日在暗網上公佈了數據，約 130 萬個對象，其中約 6.5 萬個與聯邦行政部門相關。

2. 聯邦委員會，新聞稿“Meldepflicht für Cyberangriffe auf kritische Infrastrukturen”，2025 年 3 月 7 日，admin.ch：自 2025 年 4 月 1 日起，關鍵基礎設施運營者須在 24 小時內向聯邦網絡安全辦公室（BACS）報告網絡攻擊。BACS 自 2024 年 1 月 1 日起作為國家網絡安全中心（NCSC）的繼任機構開始運作（聯邦委員會 2022 年 12 月 2 日決定；de.wikipedia.org，“Bundesamt für Cybersicherheit”）。

僅供一般參考。本文不構成法律或稅務意見，不能取代針對個別情況的專業意見，亦不建立律師與客戶關係。本文反映截至 2026 年 9 月的法律狀況。

網上版本：hk.helveticaregister.com/zug-security-and-cyber-risks