



保護您的業務和數據，
從網絡韌性與風險轉移
開始



Cyber Resilience Services

風險防範及風險轉移方案

數碼轉型步伐加快和新技術的出現，使企業容易成為網絡犯罪分子的目標。從網絡韌性以至保險，蘇黎世可為您提供一系列企業網絡安全解決方案，協助企業防範風險。

企業面對的挑戰



網絡攻擊越趨頻繁

網絡威脅形勢越趨複雜，網絡攻擊也越來越先進，企業必須跟上步伐，未雨綢繆



保護關鍵數據，防止財務損失

隨著企業收集更多數據，您必須識別對營運和客戶至關重要的數據



監管要求增多並越趨複雜

監管機構對保護數據的匯報要求越見繁複，例如個人資料(私隱)條例 (PCPD)



蘇黎世的解決方案



化繁為簡

我們可助您應對網絡複雜性，滿足最新的監管要求



結合風險防範及風險轉移方案

我們的解決方案建基於科學研究，助您實踐最有效的網絡控制措施，並滿足投保資格



提升網絡安全和抵禦網絡威脅的能力

我們提供務實而且符合經濟效益的網絡安全解決方案



中小企網絡服務方案

入門組合

營業額上限為
1,000萬美元

- 提升網絡成熟度，改善保險風險概況
- 優惠的組合價格



網絡安全概況評估

評估機構的網絡安全，提供「網絡成熟度評分」及清單



外部漏洞檢測

以自動化流程識別和檢測電腦系統和網絡中的安全漏洞



網絡安全意識培訓

增強員工識別潛在網絡威脅的能力，減少網絡攻擊的可能性

服務範疇

- 機構自訂範圍
- 從外而內檢測
- 從內而外檢測
- 一節網上培訓
- 為達至最佳效果，每節最多50人

基本組合

營業額1,000萬至
1億美元

- 提升網絡成熟度
- 改善保險風險概況
- 專享蘇黎世網絡保險條款優惠



網絡健康檢查：網絡成熟度評估

以蘇黎世和國家標準技術研究所 (NIST) 的標準問卷進行評估，並提供詳細報告和建議



財務風險評估

透過預設網絡風險情境的財務風險評估，協助機構制訂網絡投資的投放及優次



網絡安全意識培訓

增強員工識別潛在網絡威脅的能力，減少網絡攻擊的可能性



模擬釣魚攻擊

進行模擬釣魚郵件攻擊，測試員工的識別和應對能力

服務範疇

- 機構自訂範圍
- 以公開資料推行評估
- 一節網上培訓
- 為達至最佳效果，每節最多50人
- 最多50個電郵

進階組合

營業額2,500萬至
1億美元

- 大幅提升網絡成熟度
- 改善保險風險概況
- 專享蘇黎世網絡保險條款優惠



基本組合

包含基本組合內的所有服務



中小企監察及應對管理方案

設立中小企操作中心，在端點級別的網絡安全威脅進行實時監察及應對

服務範疇

- 包括上述中小企網絡服務方案「基本組合」的所有服務
- 包括下一代防病毒軟件(NGAV)以及端點偵測與回應(EDR)
- 最多99台伺服器及電腦
- 24/7全天候監控和應對
- 一年服務合約

中型企業網絡服務方案

基本組合

營業額1億至
5億美元

- 提升網絡成熟度
- 改善保險風險概況
- 專享蘇黎世網絡保險條款優惠



外部滲透測試

客製化手動模擬外部真實攻擊（駭客攻擊），用於識別漏洞及評估潛在風險



內部滲透測試

客製化手動模擬內部攻擊（內鬼駭客攻擊），用於識別漏洞及評估潛在風險



模擬釣魚攻擊

進行模擬釣魚郵件攻擊，測試員工的識別和應對能力



網絡安全意識培訓

增強員工識別潛在網絡威脅的能力，減少網絡攻擊的可能性



網絡健康檢查：網絡成熟度評估

以蘇黎世和國家標準技術研究所（NIST）的標準問卷進行評估，並提供詳細報告和建議。

服務範疇

- 3天
- 最多50個IP及系統
- 5天
- 最多50個IP及系統
- 最多200個電郵
- 兩節網上培訓
- 為達至最佳效果，每節最多150人
- 機構自訂範圍

進階組合

營業額1億至
10億美元

- 大幅提升網絡成熟度
- 改善保險風險概況
- 專享蘇黎世網絡保險條款優惠



基本組合

包含基本組合內的所有服務



網絡風險量化標準

評估網絡風險的財務影響，協助機構制訂網絡投資及策略的優次及理據

服務範疇

- 兩個客製化風險情景



大型企業網絡服務方案

基本組合

營業額10億至
50億美元

- 提升網絡成熟度
- 改善保險風險概況
- 專享蘇黎世網絡保險條款優惠



外部滲透測試

客製化手動模擬外部真實攻擊（駭客攻擊），用於識別漏洞及評估潛在風險



網絡風險量化標準

評估網絡風險的財務影響，協助機構制訂網絡投資及策略的優次及理據



模擬釣魚攻擊

進行模擬釣魚郵件攻擊，測試員工的識別和應對能力

服務範疇

- 7天
- 最多500個IP及系統
- 兩個客製化風險情景
- 最多500個電郵

進階組合

營業額50億美元以上

- 提升網絡成熟度
- 改善保險風險概況
- 專享蘇黎世網絡保險條款優惠



基本組合

包含基本組合內的所有服務



危機管理虛擬演練

模擬情境演習，用於評估和增強機構面對網絡攻擊的準備和應對策略

服務範疇

- 一個模擬風險情景
- 測試現有的應對計劃



培訓



網絡安全意識培訓 (網上培訓)

增強員工識別潛在網絡威脅的能力，減少網絡攻擊的可能性



實地培訓及網絡逃脫遊戲

客製化實地培訓，涵蓋網絡、保護數據和真實駭客體驗



模擬釣魚攻擊

進行模擬釣魚郵件攻擊，測試員工的識別和應對能力



危機管理培訓

學習對於網絡危機的組織和應對，以高效減輕和控制損失



網絡逃脫遊戲

沉浸式體驗，挑戰參與者解決網絡謎題，以有趣且引人入勝的方式提升他們的知識和技能。可在實體環境中或使用VR眼鏡進行

評估



網絡安全概況評估

評估機構的網絡安全，提供「網絡成熟度評分」及清單



網絡健康檢查：網絡成熟度評估

以蘇黎世和國家標準技術研究所 (NIST) 的標準問卷進行評估，並提供詳細報告和建議。



數據保護稽查及網絡成熟度評估

根據本港及國際數據保護法規進行合規審計，和進行網絡安全成熟度評估



ISO 27001 評估

根據 ISO 27001 評估網絡安全成熟度，協助機構準備認證



危機管理審核

評估機構對於網絡威脅和事件的應變能力和復原力



危機管理虛擬演練

模擬情境演習，用於評估和增強機構面對網絡攻擊的準備和應對策略

技術服務



外部及內部漏洞檢測

以自動化流程識別和檢測電腦系統和網絡中的安全漏洞



滲透測試

客製化手動模擬真實攻擊（駭客攻擊），用於識別漏洞及評估潛在風險



中小企監察及應對管理方案

設立中小企安全操作中心，在端點級別的網絡安全威脅進行實時監察及應對



監察及應對管理方案

設立全面安全操作中心，實時監察及應對網絡安全威脅

策略支援



網絡管治

協助機構撰寫網絡安全管治文件（存取控制、密碼、數據分類、加密等）



突發事件應變計劃

制定文件說明對網絡安全事件的應對和管理程序



財務風險評估（網絡風險量化）

持續的財務風險評估，協助機構制訂網絡投資及策略的優次及理據



網絡供應鏈

以不同評估層級為基礎的綜合框架，監測整個供應鏈的網絡成熟度



業務可持續性

制定業務持續性策略的定義，包括業務影響評估、政策發展等



CISO 服務

專業緊急支援，協助機構制定、實施和管理網絡安全策略



聯絡我們



Ruiwen Wan

Senior Cyber Risk Engineer

Ruiwen.wan@hk.zurich.com
+852 9855 0367



Vivien Bilquez

Global Head of Cyber Resilience

vivien.bilquez@zurich.ch
+41 76 310 86 91



Jean-Hermann Ly

Junior Cyber Risk Engineer

jeanhermann.ly@zurich.ch
+41 76 274 10 95

為何選用蘇黎世Cyber Resilience Solutions？



提供支援，助機構滿足投保資格



揉合豐富的理賠數據與行業指標數據



按不同企業規模和需求度身訂製的服務組合



配備科學化和內部研發的解決方案



環球團隊，可提供遙距和實地支援方案

本文件為蘇黎世保險集團商業保險業務Zurich Resilience Solutions所提供的（保險）服務，包括風險工程或風險管理服務的一般描述，並不代表或修改任何保單或服務協議。此類（保險）服務由蘇黎世保險有限公司（Zurich Insurance Group）的關聯公司提供給合資格客戶。所述價格不包括增值稅，並且可能隨時變動。

此文所表達的觀點僅代表蘇黎世Zurich Resilience Solutions在發布日期的觀點，並且可能隨時變動，恕不另行通知。本文件僅用於提供資訊目的。本文件中的所有訊息均經過可靠且可信賴的來源編輯和獲得，但蘇黎世保險有限公司或蘇黎世保險集團的任何成員對其準確性或完整性不作明示或暗示的任何表示或保證。本文件不構成法律、承保、財務、投資或任何其他類型的專業建議。蘇黎世保險集團對使用或依賴本文件所產生的任何和所有責任不承擔任何責任。本文件中的任何內容，無論明示或暗示，均不代表建立讀者與蘇黎世保險集團的任何成員之間的法律關係。

本文件中的某些陳述屬於前瞻性陳述，包括但不限於預測或指示未來事件、趨勢、計劃、發展或目標的陳述。請勿過度依賴此類陳述，因為它們本質受到已知和未知風險和不確定因素的影響，並且可能受到許多不可預見的因素的影響。本文所涉主題也不與任何特定的服務提供或保險產品相關聯，也不能確保在任何保單下獲得保障。

未經蘇黎世保險有限公司（設於Mythenquai 2, 8002 Zurich, Switzerland）事先書面許可，本文件不得全部或部分分發或複製。蘇黎世保險集團的任何成員對使用或分發本文件所產生的任何損失不承擔任何責任。本文件不構成在任何司法管轄區內出售或購買證券的要約或邀請。

Zurich Resilience Solutions

發佈日期：2024年1月