

資安險市場新趨勢

勒索軟體是當今企業面臨最緊迫的資安問題之一。平均勒索贖金要求從過去幾萬美元，至今常見對大型企業提出上千萬美金，贖金要求已經增長到甚至有時比特幣和其他加密貨幣交易所的持有量不足以及時滿足贖金需求的程度。隨著駭客在資安攻擊中變得越來越投機取巧，策略也更為縝密，勒索軟體攻擊的強度及頻率也顯著提升，造成企業巨大營運的風險，對社會造成威脅不下於恐怖攻擊。美國白宮 6 月初進一步頒布[企業勒索軟體指引](#)，要求企業採取防止勒索軟體的措施。

新興崛起的勒索軟體攻擊模式 —— 雙重加密 (Double-Encryption)*

駭客利用這種攻擊模式，可以在同一時間對目標資料進行兩次加密，進而可能導致雙倍的危險和雙倍的應對成本。我們普遍認知的雙重加密指的是一種保護性的資訊安全方法，涉及多層次資料安全。在攻擊者利用下，雙重加密成為了另一種勒索軟體攻擊模式。被攻擊者鎖定的企業可能只收到一個勒索訊息，讓受害企業在支付贖金解除第一層加密後才發現第二層加密的存在。在單一加密的勒索軟體攻擊事件中，要恢復企業正常營運已是一重大挑戰，新型態雙重加密攻擊模式對企業 IT 和資訊安全專業人士來說，意味著更大更複雜的難題。

是否要支付贖金長久以來是個棘手的問題，因支付贖金存在風險，不能保證駭客會依約提供解密金鑰。而當今雙重加密更增加了此風險，不僅受害企業最終可能要支付兩筆贖金來解除加密，也增加駭客獲得贖金後卻直接消失的機率。

雙重加密的威脅使得運用備份資訊恢復營運的能力較以往更為重要。對於那些沒有足夠備份或不願花時間從頭開始重建系統的勒索軟體受害者來說，雙重加密攻擊構成了額外的威脅，使企業預防和補救的工作大幅地複雜化。

Contacts

金融服務及專業責任險部

林鴻諭 Jova Lin

協理

T: 02 2325 2221 ext:321
jova.lin@aon.com

黃雅儀 Zita Wong

副協理

T: 02 2325 2221 ext:213
zita.wong@aon.com

李沅蓓 Kaitlyn Lee

經理

T: 02 2325 2221 ext:390
kaitlyn.lee41@aon.com

吳治霖 Calvin Wu

客戶經理

T: 02 2325 2221 ext:394
calvin.wu@aon.com

魏于華 Eva Wei

專員

T: 02 2325 2221 ext:295
eva.wei@aon.com

新業務發展部 &
Taiwan Cyber Champion

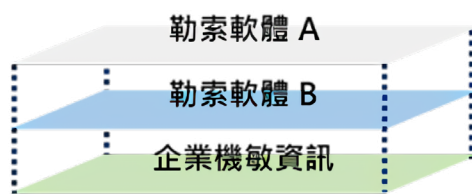
謝杰凌 Maggie Hsieh

副協理

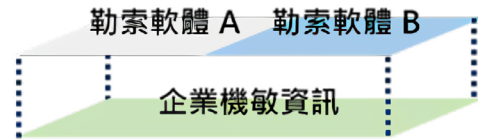
T: 02 2325 2221 ext:306
maggie.hsieh13@aon.com

*資料來源：<https://www.cybertalk.org/2021/05/19/double-encryption-ransomware-what-to-be-afraid-of/>
<https://www.wired.com/story/ransomware-double-encryption/>

勒索軟體雙重加密類型



以勒索軟體A進行加密，再用勒索軟體B重新加密同一批標的



以勒索軟體A加密企業部分的系統，剩餘部分再以勒索軟體B加密

防範勒索軟體雙重加密

- ▶ 保持企業資訊的備份維護
- ▶ 定期測試由備份恢復資訊的能力
- ▶ 遵循 CISA 關於[資訊備份的建議措施](#)

保險市場因應措施

勒索軟體攻擊事件頻傳，導致保險公司的損失案件近兩年急速增加數百倍，保險公司為了維持穩定的營運能力，紛紛開始檢視目前的風險累積程度與承保案件型態，挑出部分案件需要加強核保或重新評估風險，更特別著重於那些曾遭過勒索軟體攻擊的案件或產業，希望透過篩選風險來降低損失。以下為保險公司為了因應資安風險提升而利用的各種不同措施。

資安險保費飆升

隨著勒索軟體攻擊與各式資安事件的嚴重程度和頻率增加，各家保險公司都有各自應對方式，但共同點即是費率的飆升，過去幾年資安保險的保費成本已有顯著上漲，在 2020 年的資安險保費就相較 2019 年上漲了 5-15%，但多數保險公司認為這些漲幅仍不足以支撐索賠頻率和嚴重程度增加所帶來的負面影響，過往亞太地區由於初期發展資安險業務十分積極，保險費率及自負額通常低於歐美地區，但由於網路安全風險無法以地域區隔，自 2021 年開始，亞太地區的保險條件與保費與歐美地區逐漸趨向一致。2021 年第一季保費上漲幅度約 10%-30%，但情況在 2021 第二季出現明顯改變，保費較去年水準躍升約 30%-100% 不等，使企業投保資安險的成本大受影響。

勒索軟體相關限額限制

除了保費上漲外，部分保險公司紛紛針對勒索軟體承保範圍設定賠償子限額 (sublimit)，意味著被保險公司將只能向保險公司索賠固定較低數額。此外，共保條款的增貼也迫使被保險人分擔更多的風險。甚至有歐洲龍頭保險公司於 5 月公開聲明，不再提供勒索贖金的承保範圍。

核保作業強度提升

資安險核保過程變得更加嚴苛，保險公司特別關注企業對於勒索軟體的相關控制措施及資料備份機制；大型案件必須舉辦核保對談電話會議，部分保險公司並要求被保險公司須報告其未來一至兩年完整資安策略規劃藍圖，增加準備時間及困難度。此外，承保條件也大幅限縮，如提高自負額、營業中斷等待時間提高、外包雲端服務承保範圍限制、尚未修補軟體商公告的漏洞 (CVE) 除外不保等。

保險公司承保能量緊縮

保險公司在承保能量提供方面變得更加謹慎。大型資安保險通常使用分層結構來安排，對於基層保險，也就是承受最初衝擊的一層，排分正變得越來越艱難，巨額勒索贖金或相關賠償請求，大幅提升基層保險保單限額消耗殆盡的機率，導致越來越少保險公司願意提供基層保險承保能量，即使願意，也會要求保費必須達到特定費率。

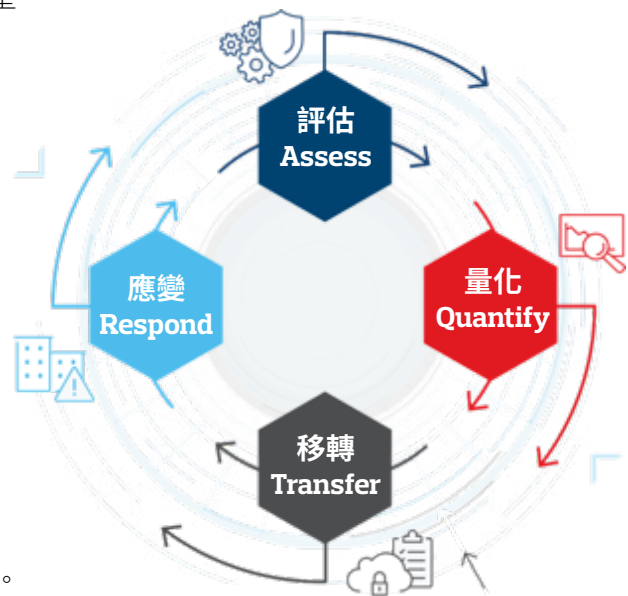
Aon 建議

勒索軟體攻擊通常並不是僅針對特定企業的，而是一種無差別式的攻擊。已投保資安險之企業，保險公司希望透過保單內容和保費的調整對企業製造激勵或誘因，試圖使企業更重視網路安全並加強資安控制。

資安保險不僅是一個風險移轉的工具，而是協助企業實踐資安風險管理的合作夥伴。處於現今保險市場十分嚴峻的情況下，建議尋找經驗豐富的保險經紀人夥伴，共同研討投保需求與策略，才能在可控成本下，獲取最適切的保障範圍。

Aon Cyber Solutions 希望透過積極主動地為企業提供預防性的解決方案，增強現有的資訊安全措施，以因應日漸壯大的資安威脅，達成企業永續經營之目標。

想要了解更多資安風險趨勢及各產業風險特性，請詳見 [Aon | 2021 Cyber Security Risk Report](#)。



Aon 簡介

Aon plc (NYSE 代號: AON) 是全球風險管理、保險經紀人、再保險經紀人及人力資源方案之領導品牌。我們在全球有超過 50,000 名同仁，透過領先業界之全球性資源及技術專家，共同為全球超過 120 個國家之客戶提供最有效且具創新性之風險管理與人力資源解決方案。Aon 多年來一再地被業界認為全球最佳之保險經紀人、再保險經紀人、專屬保險管理人、員工福利制度諮詢顧問。

若您想知道更多我們的資訊，歡迎進入我們的網站 www.aon.com。