中小企就很安全嗎？

安達保險香港
中小企網絡安全就緒度調查報告

CHUBB®

目錄

簡介

網絡風險－國際性的威脅

今時今日，企業及機構的資料正面臨前所未有的風險，就是資料有可能因外部或內部的蓄意網絡攻擊，又或者是由於系統或人為錯誤而被公開或盜取。

據香港工業貿易署統計[1]，截至 2018 年 3 月，香港有超過 330,000 家中小企業。按照定義，中小型企業是指僱員人數少於 100 人的製造業企業及僱員人數少於 50 人的非製造業企業 。這兩類企業佔香港企業總數的 98% 以上。它們亦為約 130 萬人提供就業機會，約佔就業總人數的 45%（不包括公務員）。

中小企業顯然是經濟的重要組成部分。它們與消費者及各種規模的機構緊密相連，因此，它們必須具備防範網絡風險的能力。

於 2018 年 7 月及 8 月，安達保險（全球最大的上市財產及責任保險公司）與 YouGov 合作，對 300 家香港中小企業展開一項調查，以評估它們面對網絡風險的態度。我們尤其想了解它們對自身安全程度的看法；它們如何保護自己，如何做足準備，以應對潛在風險；以及了解它們在面對相關風險時的反應。

我們的調查結果顯示，網絡風險的嚴峻現實與小型企業對網絡風險的防禦程度之間存在巨大差距。

圖一：香港中小型企業資料

[1] *https://www.tid.gov.hk/tc_chi/smes_industry/smes/smes_content.html*

數碼災難

2017 年發生兩宗重大全球網絡事件，波及多個國家的許多行業。事件促使網絡復元能力被提上政府及企業的議程。

WannaCry 病毒於 5 月份首先在歐洲爆發，隨後蔓延至全球。該病毒實施無差別攻擊，同時令中小企業及大型企業陷入癱瘓，短短數日內，已經影響 150 個國家超過 300,000 個系統。緊隨其後的是更為險惡的惡意軟件 NotPetya，該軟件導致數個美國政府部門及大型企業陷入停頓，造成數十億美元的破壞及收入損失。此類攻擊突顯我們在應對網絡事件方面準備不足，以及我們在營商方面對科技的依賴。

然而，機構不僅只注意資料外洩，同時亦要關注資料曝露－當資料被不當儲存及缺乏保安時，任何具備基本技能的人士均可存取這些資料。

2018 年，香港衞生署亦成為網絡攻擊對像，其中三部電腦遭勒索軟件侵襲，導致資料無法存取。經調查後，警方表示當用戶瀏覽不安全網站或打開電子郵件中的超連結或附件時，電腦有可能會被感染[2]。

今年較早前，約 380,000 個香港寬頻網絡客戶的個人資料因電訊公司的資料庫遭受網絡攻擊而被洩露[3]。

[2] https://www.scmp.com/news/hong-kong/hong-kong-law-and-crime/article/2158023/after-singapore-medical-data-hack-hong-kongs
[3] https://www.scmp.com/news/hong-kong/law-crime/article/2142317/personal-data-some-380000-hong-kong-broadband-customers

大型企業是否更容易受到網絡風險的影響？錯!

新聞頭條往往關注大型企業及政府部門內所發生的事故，這容易令人覺得小型企業不會發生此類事故。根據我們的調查，過半的香港受訪者 (52%) 認為，相對於其大型競爭對手，它們處於較為有利的位置。

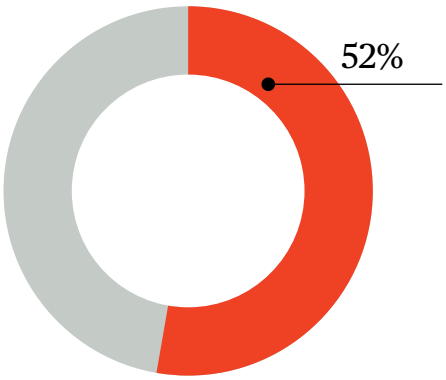
然而，這與事實相去甚遠。

我們的調查顯示，香港近四分之三的小型企業 (71%) 於過去 12 個月內網絡曾經發生錯誤或遭遇網絡攻擊。

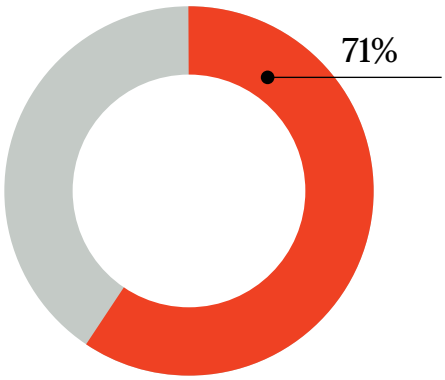
事實上，小型企業面臨更大的風險。大型企業往往在企業網絡安全方面投入巨資，構建複雜的防禦系統。縱然中小企業面臨同樣威脅，卻難以承擔實施全面保護所需的投資，因而存在重大風險隱患。

因此，倘若一家中小企業存在安全漏洞，則很有可能會在短期內成為攻擊目標。正因為如此，對網絡不法分子而言，此類企業不僅是輕易攻擊的目標，而且亦提供可觀的累積回報。事實上，於網絡安全措施方面投資較少或並無投資的中小企業，是網絡罪案的理想（亦是最常見的）目標。

圖二：中小企業對網絡風險的態度



相信對比其大型競爭對手，它們處於較為有利位置的受訪者百分比。



於過去 12 個月內網絡曾經發生錯誤或遭遇網絡攻擊的受訪者百分比

「一些中小企業認為，它們的規模相當小，不可能成為網絡不法分子的目標，又或者認為其內部問題不會對其業務造成大影響，換句話說，它們認為自己「小到不能倒」。然而，眾多有關網絡事故的報告、調查或統計數據顯示，無論大型企業或小型企業，均面臨相關風險。」

泰思博 (Andrew Taylor)
安達亞太區網絡保險
保險產品負責人

案例：
黑客竊取網上零售商的資料

行業
零售

費用
$200,000 美元

全年收入約為
$3,500 萬美元

一家零售商店透過網上交易平台銷售大部分產品。然而，由於在密碼管理及接入公司網站的虛擬專用網絡存取 (VPN) 安全程度較為薄弱，網站遭到入侵。外來黑客竊取 1,000 多名客戶的個人資料，然後針對該公司的客戶實施進一步網絡釣魚詐騙。

警方及監管機構就該公司進行調查，同時有兩名客戶對該零售商店提出民事訴訟。在調查漏洞來源方面產生了第一方費用，而識別及聯絡受影響客戶亦產生事件應變費用。其後更需委聘律師就民事訴訟進行辯護。

中小企業自擺「烏龍」

儘管小型企業遭受外部網絡攻擊的風險極高，但我們的調查顯示，大多數資料遺失事件實際上是由於系統故障或人為錯誤所致。

是項調查結果並不說明外部攻擊的影響有所減弱，而只是表明企業在防禦外部入侵其設施的同時，亦需要維持內部有序的狀態。

在我們調查的公司中，於過去12個月內發生率最高的三類網絡事故均由內部因素所引致：

- 因系統或技術故障導致資料遺失 28%
- 因系統或技術故障導致業務中斷 26%
- 因人為錯誤導致業務中斷或資料遺失，例如儲存設備遺失或被盜，或僱員無意中將公司資料暴露於風險中 22%

圖三：中小企業於過去12個月遭遇的網絡事故

事故	%
因系統或技術故障導致資料遺失	28%
因系統或技術故障導致業務中斷	26%
因人為錯誤導致業務中斷或資料遺失，例如儲存設備遺失或被盜，或僱員無意中將公司資料暴露於風險中	22%
心懷不滿的員工或其他惡意者洩露損害公司的電子郵件或其他文件	17%
第三方服務供應商因機器故障停工，而導致業務中斷	15%
黑客/網絡罪犯盜取或損害客戶記錄	13%
供應商或商業伙伴遺失資料或導致資料洩露	11%
被惡意者破壞營運	9%
被競爭對手竊取你的知識產權 (IP)，研發或其他專利資料	9%
業務被網絡罪犯詐騙	9%
網絡罪犯複合關鍵營運數據，並用之進行勒索	8%
國家贊助的機構竊取你的知識產權 (IP)，研發或其他專利資料	8%
不知道	2%
其他可察覺的網絡故或違規行為	2%

「安達保險的索償資料清楚表明，大多數網絡或資料事故均牽涉內部因素。過往 20 年的網絡保險核保經驗，讓我充分明白到，網絡風險絕非局限於技術層面，而是一個涉及整個企業層面的問題。良好的網絡緩解策略包括完善的管治流程、供應商管理及僱員教育。」

泰思博 (Andrew Taylor)
安達亞太區網絡保險
保險產品負責人

案例：
手提電腦被盜，導致洩露私隱

行業
工業

費用
$325,000 美元

全年收入約為
$2,000 萬美元

一名能源公司高級行政人員的手提電腦在公司汽車上被盜，該手提電腦存有大量客戶及僱員的個人資料。儘管相關文件已加密，但手提電腦上的整體密碼保護脆弱，且存取加密資料的個人識別號碼 (PIN) 亦被識破。

能源公司動用了 $50,000 美元，聘請司法鑒定專家及外部合規顧問。評估手提電腦內的資料後，公司主動通知相關客戶及僱員，並酌情提供電話中心、監控及恢復服務。除了第一方費用 $100,000 美元外，能源公司需多付 $75,000 以應對多州監管調查。

最終，該公司因違反其公開聲明的私隱政策而被罰款 $100,000 美元。

在管理網絡事故方面的自信－或過度自信

我們的調查顯示，大多數中小企業相信自己有能力在遭受網絡攻擊後解決資料洩漏的問題。在香港，77% 的受訪者認為自己能夠處理網絡事故，而大多數受訪者 (65%) 認為自己能夠於 12 個小時內控制資料洩漏。與此同時，在資料洩漏的情況發生之後，62% 的受訪者表示，事件令其意識到自己的安全程度低於過往所認知的水平，而 59% 的受訪者認為未來發生此類事件的可能性較小。

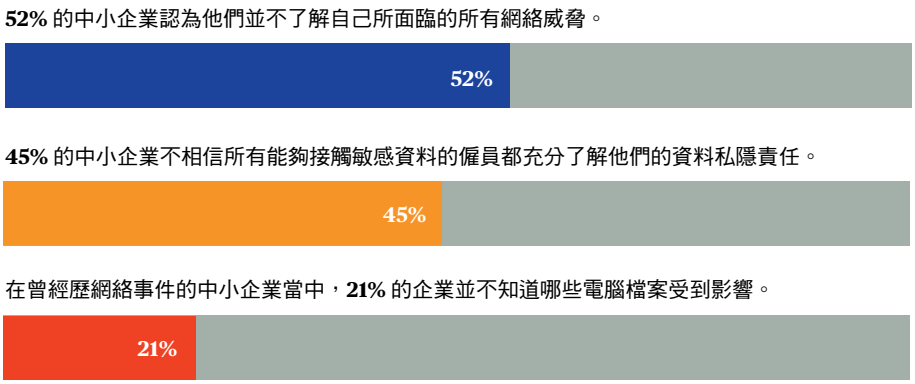
這使我們面臨困局。儘管我們發現中小企業頗有信心，但調查結果卻與之相悖。

出現這些矛盾結果的原因，或許在於受訪者對於應由何人承擔網絡安全責任並沒有一致共識。在我們的調查當中，受訪者意見不一：42% 的受訪者認為資訊科技主管或資訊總監應對此負責，而略多於四分之一 (28%) 的受訪者認為這是行政總裁的責任。

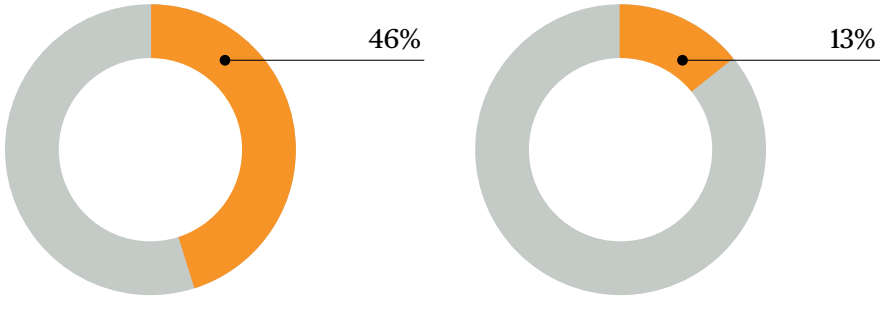
這與我們從新加坡及澳洲調查中所得的結果形成鮮明對比，在這兩個國家，大約相同比例的受訪者認為，上述兩者當中，其中一方應承擔這方面的責任。

安達保險認為，網絡安全人人有責，但應由有權實施變革的人來統領。

圖四：中小企業普遍不了解他們面臨的風險



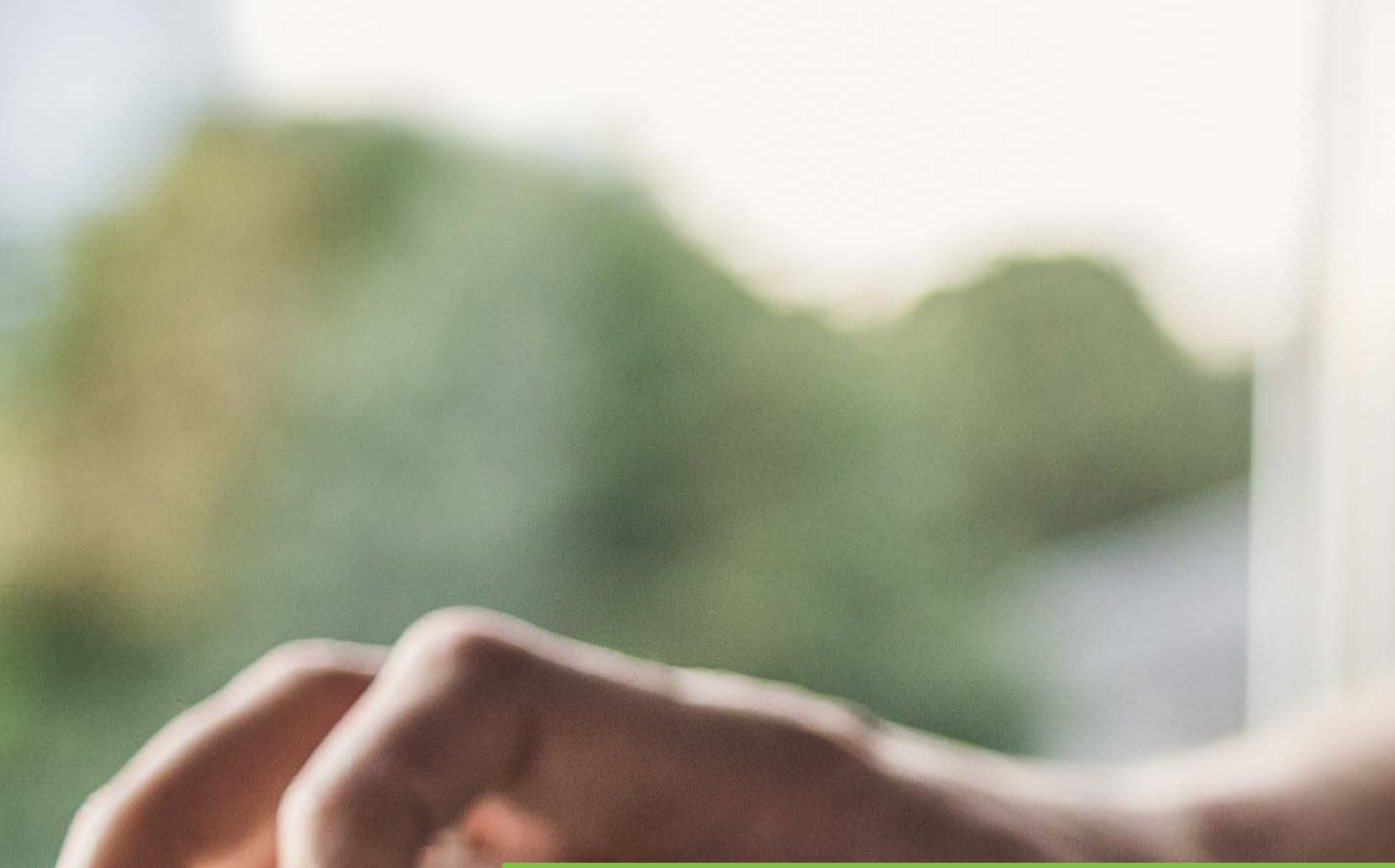
圖五：中小企業在網絡事故發生後採取的行動



「網絡風險是一種企業風險，而不是僅僅存在於一個業務部門或成本中心的風險。企業應以整個企業層面的監管來管理風險，同時需要董事會或企業東主的監督。」

「網絡風險是董事信託責任的重要一環。」

泰思博 (Andrew Taylor)
安達亞太區網絡保險
保險產品負責人



案例：
利用勒索軟件掩蓋竊取個人資料的行為

行業
零售

費用
$105,000 美元

全年收入約為
$1.50 億美元

一家全國性零售連鎖店旗下一家專營店的一名僱員點擊了來源不明的電子郵件連結，導致整個零售連鎖店蒙受損失。該電子郵件連結包含惡意軟件，導致一「後勤部門」電腦被加密。

司法鑒定調查發現，攻擊者試圖使用該勒索軟件，掩飾先前入侵該公司網絡的行為。在勒索軟件攻擊前幾個月，威脅者曾利用暴露於互聯網的端口連接作遠程存取，多次存取該電腦的資料。

不法分子的目標，正是該零售商未加密的客戶資料庫。超過 70,000 個客戶記錄被竊取，包括姓名、郵寄地址、電子郵件地址、電話號碼及其他敏感資料。

其後需要委聘外部法律顧問、司法鑒定專家、公共關係顧問及電話服務中心協助減輕攻擊造成的損失。

資料 - 需要周全保護

保護資料並非僅僅有利於企業的舉措，更是法例規定。《個人資料（私隱）條例》要求收集、持有、處理或使用個人資料的機構必須遵守《個人資料（私隱）條例》[4]。

香港是亞洲首個制訂全面個人資料私隱法例及成立獨立私隱監管機構的司法管轄區。私隱條例涵蓋私營及公營機構。然而，香港尚未與其他幾個亞洲國家一樣推行獨立的網絡犯罪或網絡安全立法[5]。

「鑒於資源有限，中小企業往往極易遭受網絡攻擊。未雨綢繆是減低風險的關鍵。其中包括兩項主要因素，首先，制定有效的網絡安全政策及程序，以及對員工進行充分培訓，便能顯著提升中小企業的應變能力，卻不致產生重大成本；其次，有效的事件應變計劃相當重要。」

叶子彬
RPC
商業糾紛、網絡
及金融科技高級顧問

[4] *https://www.pcpd.org.hk/tc_chi/data_privacy_law/ordinance_at_a_Glance/ordinance.html*
[5] *Businesses can refer to the Information Security (InfoSec) website for information on legislation introduced against computer related crimes - http://www.infosec.gov.hk/tc_chi/ordinances/corresponding.html*

發生網絡事故後中小企最關心的是....

中小企業顯然明白網絡事件可能對其業務產生的影響。我們的調查發現，中小企業最關心的是網絡事件對其與客戶關係 (64%) 的影響，其次是聲譽 (61%)、收入及營業額 (60%) 的影響，以及事件所引致的成本 (60%)。

儘管如此 — 或許正因為如此 — 僅 36% 的受訪者表示它們在網絡事故發生後通知受影響的人士。

就網絡安全事故而言，中小企業較大型機構面臨更高的風險，因為它們在應變及恢復方面所能運用的資源有限，對業務中斷及財務的影響可能更具災難性。安達保險認為，這種狀況對整體業務構成的風險是一種「骨牌效應」。

圖六: 發生網絡事故後中小企最關心的是....

64%
客戶關係

60%
收入及營業額

61%
聲譽

60%
事件所引致的成本

36%
在網絡事故發生後
通知受影響的人士

對小型企業產生的災難性骨牌效應

第一層骨牌

中小企業的網站或電腦系統受攻擊，虛擬店面和處理交易的能力被破壞，就如公司停業一樣，造成客戶流失，很大部份的客戶更不再回頭。

第二層骨牌

當攻擊涉及個人資料如信用咭號碼被盜時，負面消息動搖了客戶的信心，導致品牌形象嚴重受損，更進一步令客戶迅速大量流失。

第三層骨牌

修復電子數據，軟件和電腦系統可能需要投入大量的時間和金錢，這可促使業務破產。加上有可能需要支付贖金，可使中小企業面臨財務危機。

第四層骨牌

最後的結果可能是中小企業要面臨受網絡攻擊影響的客戶、服務商、供應商或其他人士起訴。這些訴訟往往非常耗時而且辯護費用高昂，使網絡攻擊成為另一個令業務結束的原因。

案例：
商業電子郵件洩露及竊取客戶資料

行業
專業服務

費用
$52,000 美元

全年收入約為
$2,500 萬美元

一家中型專業服務公司的一名合伙人遭網絡釣魚攻擊，導致其收件箱中的商業電子郵件被洩露。該合伙人無意中向攻擊者提供其 Office 365 的登入資料，隨後被人利用登錄其 Office 365 賬戶，存取該合伙人的聯絡人、商業附件、機密客戶資料及日程表等所有資料。所洩露的資料亦包括歐洲客戶的資料。

攻擊者使用 Office 365 刪除電子郵件，並進一步篡改該合伙人的 LinkedIn 賬戶，並持續實施網絡釣魚欺詐，並從合伙人的 LinkedIn 追隨者獲取更多資料。

其後需委聘私隱律師、公共關係顧問及電腦司法鑒定專家提供協助，以限制及減輕因此造成的損失。

保險的作用

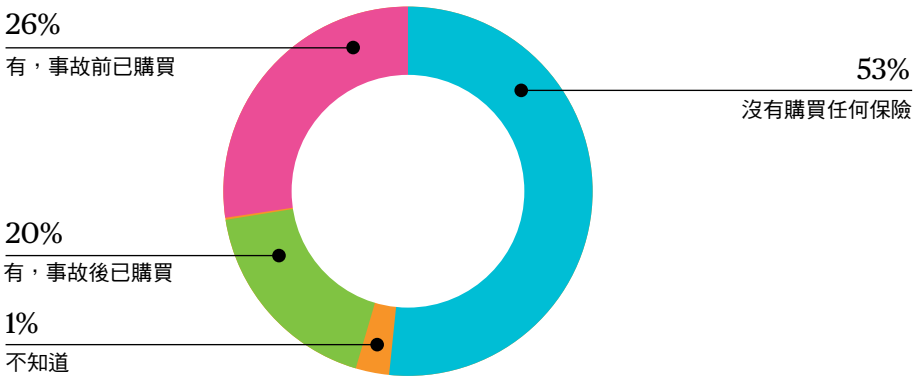
無論任何規模的企業，應對網絡攻擊的成本都是一個重要的問題，對於中小企業而言尤甚，保險能夠將中小企業的財務風險轉移至保險公司，因此可於網絡攻擊發生時減輕中小企業的負擔。然而，53% 的受訪中小企業之前從未購買過網絡保險，這可能由於他們對相關的保險方案缺乏認識，而 49% 的受訪中小企業同意這一說法。此外，54% 的受訪者重視識別及減少網絡事件影響的能力，而 53% 的受訪者重視提供實際應變服務。

因此，保險公司正着手為商界提供保障，以應付日益嚴峻的網絡風險挑戰。根據經濟合作及發展組織於 2017 年 5 月向 G7 提交的報告，安達保險正致力提高企業間對網絡損失風險的認識、分享風險管理的專業知識及鼓勵透過相關投資來減低風險。

安達保險亦同時設有可實時查詢專有資料的 Chubb Cyber Index℠，以近 20 年處理網絡索賠的經驗，紀錄相關數據及趨勢為合作伙伴及保單持有人提供有用的意見，幫助他們管理及減低未來損失的風險。

安達保險的緊急應變平台更為客戶提供進一步支援，控制事故威脅及對客戶業務的潛在損害。更重要的是，從事故中汲取經驗和教訓。

圖七：有否在網絡事故前後購買相關保險？



「顯然，代理及客戶需要更多培訓，讓他們了解網絡保險的價值。在安達保險，我們所著重的不僅是傳統的『支付承諾』，而是為受保人提供全面的企業支援方案， 這正是我們強調防患於未然以及提供全球緊急應變支援的原因。」

Tim Stapleton
安達網絡及科技部
高級副總裁

中小企業如何防範網絡風險

現代科技已在各類不同環境當中融匯交織，讓我們常處於改變之中，而這種狀況令我們面臨過往未知的風險。然而，中小企業可採取五項簡單措施，制定自身的網絡風險計劃及控制其風險，確保其網絡安全。這些建議做法符合澳洲政府的「八項關鍵」緩解策略。

制定及實施強密碼政策

網絡不法分子獲取中小企業資產的最簡單方法之一，就是透過僱員使用弱密碼而形成的虛擬「方便之門」。為糾正這種情況，中小企業應當建立一個密碼策略，規定僱員經常使用及更改強密碼（例如，字母、數字及符號的組合）。當僱員離開公司時，亦應自動更改密碼或將賬戶標記為不活躍。

定期進行網絡安全培訓

中小企業應讓僱員明白自己於防止網絡攻擊方面所能發揮的作用。當公司的手提電腦或其他設備在外面使用之後再接入內部網絡時，惡意軟件很容易乘機進入公司伺服器。定期培訓及教育是在公司團隊中建立正面及安全習慣的最佳方法。中小企業亦應限制對敏感資料的存取，僅允許管理層或需要該資料作營運用途的人接觸。

更新資訊科技設備及使用安全軟件

過時的操作系統及電腦皆存在風險，因為它們容易受到更複雜的黑客技術及新型惡意軟件的攻擊。與此同時，對中小企業而言，監控其電腦網絡的合法使用者與監控網絡本身同樣重要。儘管中小企業通常並無內部資訊安全專家，但市面上有相關軟件可供下載，只需短短數分鐘，即可部署與大型企業相同的解決方案。

制定網絡事件應變計劃

建立一個由僱員及服務供應商組成的專責團隊，在網絡事故發生時能有效作出應變。

購買網絡保險

中小企業可透過購買網絡保險，更充分地保護自己的資產及現金流，保險成本必然遠低於因網絡攻擊而停業的成本。大部份網絡保險如安達企業網絡風險管理等方案，均可預先將上述若干服務納入相關計劃。

常用網絡詞彙

網絡攻擊	影響電腦系統內資料的可用性、保密性或完整性的惡意活動。
資料外洩	敏感、受保護或機密資料被未經授權的人士有意或無意地複製、傳輸、瀏覽或使用。
惡意軟件	以任何形式感染網絡、伺服器、設備或終端用戶電腦的惡意軟件（包括病毒及特洛伊木馬），包括勒索軟件、遠程存取工具、網絡嗅探軟件及殭屍網絡軟件。
網絡釣魚	透過電子郵件、訊息、電話通訊，儘管打著合法的幌子，但事實上透過看似無害的連結或文件在系統環境中查找資料或放置錯誤資料。
勒索軟件	秘密安裝在設備上，會鎖定系統用以勒索一筆款項的電腦軟件。
魚叉式網絡釣魚	網絡釣魚是針對較廣泛受眾的普遍試探性攻擊，一旦若干資料被盜取，攻擊便會停止。相比之下，魚叉式網絡釣魚更具針對性。在魚叉式網絡釣魚中，成功竊取憑證或個人資料只是攻擊的開始，因為這只會用於存取目標網絡，最終演變為有針對性的攻擊。

關於本調查

本報告由安達保險聯同 YouGov 編製，綜合了 1,000 家來自三個市場的中小企業受訪者調查的結果；其中 400 家來自澳洲，另各有 300 家分別來自香港及新加坡。

受訪者包括來自僱員人數介乎 2 至 249 人的中小企業的董事會層次的高級行政人員 (77%) 及董事會層次以下的高級經理或總監 (23%)。

受訪者所屬行業為：專業服務 (22%)、製造業 (17%)、零售及酒店業 (13%)、教育 (6%)、金融服務 (6%)、醫療保健 (5%)、科技 (5%)、媒體及傳播 (3%)；以及其他行業 (23%)。

想知道更多關於安達保險企業網絡風險管理保障，請聯絡我們
AP.Cyber@chubb.com

關於安達保險香港

安達為全球最大的上市財產及責任保險公司，經營一般保險及人壽保險業務，立足香港超過 90 年。安達香港的一般保險業務（安達保險香港有限公司）為大型及中小企業客戶設計及提供特定的保險產品，包括財產險、責任險、海上險和意外及醫療保險服務。多年來，安達保險憑著其雄厚財務實力及市場領導地位，開創新的保險產品，提供優質服務，建立長遠穩健的客戶關係，與時並進。

如欲獲取更多資料可瀏覽
www.chubb.com/hk。

聯絡資料

安達保險香港有限公司
香港灣仔港灣道 6-8 號
瑞安中心 25 樓

電話 +852 3191 6800
傳真 +852 2560 3565
www.chubb.com/hk

Chubb. Insured.™

12/2018