RISK DOCTOR BRIEFING

管理網路犯罪風險

© *May 2014, Ben Rendle*

ben.rendle@btinternet.com

網路犯罪對全球經濟而言是一項快速成長的威脅，然而它卻沒有明確的定義，而且經常會與網路戰爭或網路恐怖主義混為一談。風險專家需要瞭解網路犯罪及其與風險管理的關連，才得以在面臨這項對商業及社會的重大威脅下，提供有價值的協助。

有些風險專家認為網路犯罪僅與技術人員有關，且應該由資訊技術部門來處置，然而網路犯罪會因為影響到組織達成策略及營運目標的能力，而造成組織的一項重大風險。不幸的是，許多企業不瞭解網路犯罪長什麼樣、造成影響的可能性有多大、衝擊可能到達什麼程度、或應該管理到什麼程度。

網路犯罪可以有許多方式影響組織，包括：

- 網路竊盜或詐騙
- 盜取身份
- 網路勒索
- 盜取顧客資料
- 盜取智慧財產
- 工業間諜

組織暴露於網路犯罪的程度與其所執行的線上活動程度有關，包括其在線的範疇、有價值的資產及資訊儲存在網路上的程度、網路安全的強度、以及組織文化中風險意識的程度。

要管理網路犯罪的風險，首先我們需界定線上活動的程度，並且決定哪些資產與活動可能會被網路犯罪所影響，然後我們便能夠開始進行辨識、評估、以及管理網路犯罪風險。以下的步驟將會有所助益：

明確地瞭解並定義組織線上活動的目標。認清我們的利益關係人其線上環境之差異與特殊性，並且評估他們的線上風險偏好。

處理文化及技術因素。包括文化藩籬、溝通難度、以及對網路犯罪風險認知差異的影響。

認清內部及外部網路犯罪的威脅。內部的威脅可能來自員工的失誤、意外的遺失資料、或惡意洩漏公司的敏感資料。外部威脅可能來自駭客、壓力團體、競爭對手甚或不懷好意的外國政府、以及病毒程式、惡意破壞程式、以及木馬程式等等。

建立保管權責與獎勵措施以應付網路犯罪風險。所有資深員工皆應該在其權責範圍內負責管理網路犯罪風險，並且挑戰那些將網路犯罪視為「不關我事」的利益關係人。

在企業風險管理（ERM）架構下管理網路犯罪風險。網路犯罪風險廣泛地影響了企業的各個領域如聲譽、企業永續經營、以及對子公司和供應商產生的連鎖效應，因此需要一貫性地視其為我們對風險整體回應的一部份來處置。

在網路犯罪風險上發展一個全球的觀點。許多組織依賴海外經濟體進行貿易、出口、以及產生財富，而這些使他們暴露在他們所不能輕忽的海外網路犯罪中 。

作為風險專家，我們必須將網路犯罪風險納入思考與實務中，這樣我們才能提供務實的針對性建議給我們的組織，以降低威脅並保護我們的事業。
