網路安全對於實體安全至關重要的原因

我意識到假設 Axis 以製作現實世界中有助於提升實體安全的智慧型產品而聞名，那麼我們為什麼要討論網路安全呢？好吧！您只要看看好萊塢的世界，就可以看到全部都是間諜、特務、策劃搶劫賭場的盜賊，甚至是使用或濫用安全攝影機、智慧門鎖、生物特徵辨識鍵盤鎖以及其他許多具有閃光燈的發光裝備的超級英雄在拯救世界/擄獲芳心/帶著戰利品逃跑。

但是，無論使用者介面多麼牽強 (我「非常想要」擁有 M16 或中情局似乎在電影中可以得到的那些電腦)，也無論所需的技術性技能多麼過度簡單化 (「按下這個按鈕，駭客就可以入侵五角大廈」)，所呈現出的不僅僅是一絲真理。

網路安全對於實體安全至關重要

在本篇文章以及接下來的幾篇文章中，我想要探索在 21 世紀網路安全對於實體安全至關重要的原因、在這種情況下網路安全的基本特徵，以及為您的企業或組織規劃任何實體安全系統時應謹記在心的一些普遍的網路安全概念。

要切記的是，**網路安全是一個過程**，而不是一個產品。威脅必須在系統層級加以管理，而保護網路、設備及其所支援之服務安全的責任則屬於整個廠商供應鏈，以及管理網路和使用者本身的人員。技術很重要，但永遠不會消除所有風險或威脅。

網路安全在基本層面上與風險管理有關，而且不可能消除一切風險。

[此外，您可以做一個小小的心理實驗：試著列出您今天早上醒來之後所面臨的「所有」可能的風險。除了像是被狗絆倒或是淋浴時被燙傷之類的事情，還有您的房子被隕石擊中或是突然湧進大量青蛙之類的事情。您很快就會了解有一些風險完全無法預測，而且您幾乎或完全沒有辦法為這些風險進行規劃]。

即使如此，防範某些風險可能相當昂貴 [防止隕石擊中您的房子可能僅花費幾美元]，因此您需要開始考慮什麼對您和您的組織很重要。找出您鑲有珠寶的皇冠並好好地守護 (這只是一個隱喻，除非您真的在倫敦塔工作)。您必須制訂出可接受的風險層級、想出消除部分風險影響的方法，並透過保險形式轉移其他風險。

在我的下一篇文章中，我將開始研究您如何分析實體安全系統的風險、實際有效的緩解方法、不同類型的攻擊，以及不同規模的組織應該如何處理這些風險。