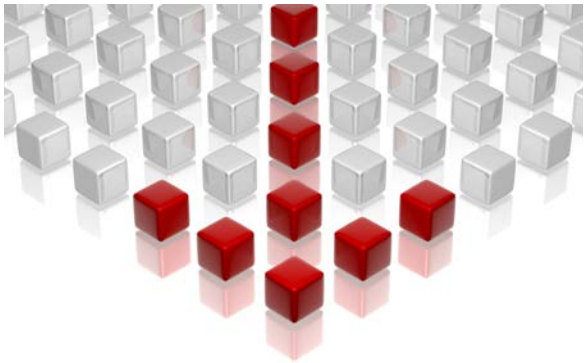
網路安全「與營運目標一致」是什麼意思？

展示安全性如何協助企業達成目標是「二階段程序」— 用業務的方式說話，再進行足以證明回報價值的成本效益分析。

文／Pete Lindstrom　譯／Nica Liu

企業的資安資深人員總會說：我們必須學著與業務方向一致。遺憾的是，我們似乎把大部份時間都用在要讓業務「與網路安全一致」，因而在做不到或不能做到時感到挫折。部份原因在於我們通常不想要（或不能）像業務一樣說話。其實，網路安全是組織的成本中心。不僅如此，它還是個很難被認可價值的成本中心，這種案例比比皆是。



讓網路安全與業務方向一致的兩步驟

基本上，與業務一致是兩階步驟。第一步是瞭解他們的語言。所有企業組織的通用語言是財務，這通常是我們最大的挑戰。多數產業皆具備自有的成本效益計算方式：想想零售業每平方英呎的銷售額，或醫療界每位病人的治療成本。就網路安全來說，我們得像企業裡所有其他部門或業務線一樣行事。這麼做才能將我們帶向第二步驟。

第二步驟是制定方式與標準，以價值（而非利潤）方式，決定利益/成本分析與投資效益。可以從作業基礎成本法這類成本會計方式計算成本，並使用收支平衡分析的方式衡量投資做為起點。它可能就像確認花費金額與在品質上確認這項投資「是否值得」那樣簡單：就像那些你已經在做但可能沒有明確定義該這麼做的事。

到這裡，你也達成了降低風險的基本要求。若花一百萬美元在這個解決方案上「是值得的」，那麼你可以預計降低風險至少到達這個金額。當我建議將這些下限也同樣套用在企業組織花費在網路安全上的總額時，人們總會感到憂心（真正有興趣的人，應該去經濟學指南瞭解「願意支付」的概念）。一旦有了基本的財務概念，一切就變得好玩了。你可以開始瞭解控制成本、互動成本（cost-per-session）與損失價值比等這類財務比率。

我曾在研討會舞台上聽一位 CISO 表示，他會「不顧一切代價」確保安全。我在這裡告訴你，這不但荒謬而且是逃避。我能理解在情感上會有這樣的想法，但這種思維相當具有毀滅性，而且與所有跟業務一致的契機相悖。瞭解網路安全對財務的影響相當具有挑戰。（嘿！瞭解它對人力資源的影響更難。）