

如何透過安全教育與訓練緩和 IT 風險

作者：Paula W. Hamm，賽門鐵克教育服務部門副總裁

IT 風險管理就是在以下兩者之間達到平衡：開發安全可靠的 IT 基礎架構需要成本，但又要考量企業組織發生資安事端的可能性與潛在損失。IT 風險管理通常可分為四個類別：

- 安全性：杜絕不良事件，保護重要資料。
- 可用性：維護系統並確保快速復原。
- 效能：使資源最佳化並確保設定正確無誤。
- 法規遵循：確保適當控制並自動收集證據。

企業 IT 相關資安事端日漸受到大眾的關注。筆記型電腦遭竊導致未加密個人資訊外流、企業 IT 系統內的信用卡號碼遭竊、電腦故障導致業務中斷，以及負載過重導致 IT 基礎架構無法為企業客戶提供服務，這類新聞時有所聞。

讓人員參與其中

教育員工，讓他們瞭解 IT 風險對企業組織有何影響，這是妥善管理這類風險所不可缺少的措施。企業組織往往著眼於透過投資新技術來緩和風險，但卻無法善用最重要的資產 - 人員。

企業 IT 相關資安事端的常見內部原因包括：密碼保護不力、未能更新防護軟體、未能掃描檔案、工作時不當瀏覽網頁與下載檔案，以及社交工程術（用於操控人員執行動作或洩露機密資訊的技術）。這些資安事端的潛在影響會讓基礎架構處於暴露狀態，使企業組織容易遭受入侵、攻擊，並遺失專屬資訊。這些安全漏洞還可能促使病毒感染（以及再度感染）比率居高不下，並降低可用的網路頻寬。最終，這所有一切將由於停機而導致生產力下降，以及由於修復程式及更換遺失或遭竊設備而導致成本增加。

人員是寶貴的資源，在確保 IT 基礎架構安全方面扮演了重要的角色。透過適當的訓練與教育，員工可以在緩和 IT 風險方面發揮重要作用。根據 Gartner 所發佈的報告，實行有效的安全認知方案可以減少花在回應資安事端上的時間，因而節省 25% 的生產力。¹ 這意味著，員工可專注於他們最擅長的工作。

透過教育緩和風險

與一般觀點不同的是，管理風險的責任並不應該由 IT 部門單獨承擔。安全工作人人有責，就資訊安全而言，人員與技術、政策、程序及指導原則同等重要。然而，期望員工在毫無準備的情況下，處理現今安全環境的複雜與微妙之處並不切實際。透過適當的教育與訓練，員工即可成為企業組織的最強防線和最寶貴的安全資產。

IT 組織在設計訓練方案時，應牢記四大風險管理類別：安全性、可用性、效能與法規遵循。此外，還應該遵循一些最佳實務準則，概述如下。

¹ Gartner：資訊安全認知訓練是保護 IT 資產的重要環節。Witty, Roberta J 等人 (2005 年 1 月 11 日)

安全風險

- 改善資安事端的回報與處理方式
- 妥善分類與保護智慧財產
- 減少即時通訊之類不安全的通訊管道
- 設計並實作更安全的應用程式與基礎架構
- 教育全體員工有關安全認知的重要性

可用性風險

- 採取更主動的方法來處理 IT 可用性問題
- 示範正確備份程序的重要性
- 提高對於常見病毒與木馬程式攻擊媒介（電子郵件附件與檔案下載）的認知
- 教育應用程式開發人員有關建置可靠穩定應用程式的重要性

效能風險

- 示範網路資產的正確使用方式（例如：不在上班時間觀賞線上影片）
- 在 IT 系統設計中提高對於系統效能的注意力
- 教育應用程式設計師與開發人員，有關他們在正面影響 IT 系統中的效能問題方面的能力

法規遵循風險

- 支援並遵循內部 IT 保護與企業政策需求，以協助符合 FISMA、Gramm-Leach-Bliley、HIPAA、Sarbanes-Oxley、COBIT 與 ISO 17799:2000 等法規遵循標準

若要成功保護資訊資產，從上至下每個層級的員工都必須對於安全風險與政策，以及各自在保護公司資產方面的責任有基本瞭解。否則，企業組織將無法使員工負起保護組織資源的責任。

總是在資安事端發生後再進行處理的「反應式」安全模式早已落伍。現今的安全環境已變得極為複雜，反應式的公司將始終處於落後地位。進步的公司必須採取主動方法，讓員工更深入瞭解公司的 IT 風險管理策略。從長遠看，唯有如此才能降低相關的成本並維護任何層級的安全。

###