機構應對網絡事故的「黃金準則」

在 AI 時代，數碼轉型深入各行各業，網絡安全事故早已不再是「會否發生」，而是「何時發生」。因此，企業與個人必須將網絡安全視為日常運營的核心，而非附屬選項。當機構遭遇勒索軟件攻擊或大規模數據洩漏時，反應的速度與透明度，直接決定品牌聲譽的影響。

第一步：預防與準備

事故尚未發生之前，機構必須建立完善的安全策略，包括定期風險評估、漏洞掃描及系統加固，確保基礎設施能抵禦潛在威脅。員工的安全意識培訓亦不可或缺，因為人為疏忽往往是攻擊者最容易利用的弱點。清晰的應急響應計劃、定期演練、可靠的備份與復原機制，以及持續的監控與預警系統，都是事故前就應準備好的防線。

第二步：事故應對

一旦機構遭遇勒索軟件攻擊或大規模數據洩漏，在事故應對階段，應急速度與透明度是維護品牌聲譽的關鍵。機構必須立即切斷受感染系統，防止損害擴大，並迅速確認受影響範圍。同時，依照相關法規(如《私隱條例》)，機構有責任及時向受影響人士及監管部門通報。

第三步：事故後復原及優化

每一次網絡危機都是對現有防護體系的「壓力測試」。在復原階段，機構除須確保系統恢復正常運作外，還須徹底修復安全漏洞、優化備份與還原機制，並加強員工培訓。

網絡安全是一場長期的攻防戰，唯有透過不斷的優化與資源投入，才能將教訓轉化為更穩固的防禦體系。HKIRC 的免費員工培訓平台(cyberhub.hk)正是其中一個有效資源，提供針對不同崗位的網絡安全課程，讓員工在面對突發事故時，已經清楚知道第一步該如何處理。

黃家偉工程師

行政總裁
香港互聯網註冊管理有限公司 (HKIRC)