ISO/IEC 27001 資訊安全管理系統認證

做好預防措施 減低資訊安全風險

惡意勒索軟件事件在全球各地時有發生，令各界不能不重視網絡安全問題。此外，網絡駭客及病毒軟件無處不在，稍有不慎電腦便很易被攻擊或入侵，對各行各業的資訊安全構成嚴重威脅。

資訊安全管理系統(Information Security Management System，簡稱ISMS)是專門針對企業和機構的資訊安全管理而設計，透過建立和控制業務風險，加強機構的應變能力，從而提升工作效率。而ISO/IEC 27001則是國際標準化組織就ISMS發布的國際標準，為系統的開發與運作提供規範性的要求。

國際認可標準 協助保障資訊安全

ISO/IEC 聯合技術委員會轄下負責ISMS的工作小組副召集人Dale Johnstone(莊士敦)指出，無論大企業或中小企，甚至公營機構都有機會受到駭客攻擊。ISMS能系統化地協助機構確保資訊安全，減低因內部員工不小心或惡意洩露機構敏感資料(如涉及客戶私人密碼等)而帶來的損失，或因在互聯網受到駭客攻擊而引致信息被破壞、不當獲取、財務詐騙等不良後果的風險。

ISO/IEC聯合技術委員會轄下負責ISMS的工作小組副召集人Dale Johnstone(莊士敦)

ISO/IEC 27001是一套國際認可的資訊安全管理系統標準，為保障資訊安全提供實踐方案，透過人員、流程和資訊系統的協作實踐風險管理，全方位增強員工保護資訊的意識，並就不同情況制定合適的應變措施，以防範問題發生和減低機構因一時疏忽而蒙受損失。

莊士敦指出，機構在實施ISO/IEC 27001時最大的挑戰，往往是辨識什麼資料最需要保護。他建議機構將資料分門別類，並從小部份開始做起，例如針對涉及客戶私隱等敏感的資料先訂立保安措施，逐步累積經驗，以求更有效全面保護機構的所有信息資產。他認為，獲得ISO/IEC 27001認證除了能協助機構保障資訊安全外，更可增強客戶的信心，帶來更多商機和增加收入。「實施ISO/IEC 27001的成本並不高，遠低於系統受侵襲後帶來的金錢和信譽損失。」

由上而下 推動執行

艾博士安全系統(香港)有限公司首席安全顧問潘永明指出，公司為滿足一些投標項目的要求，率先於2003年獲取ISO/IEC 27001認證。執行認證並不須額外添置器材，最重要是讓負責資訊保安的部門，養成定期檢討、進行內部審計及建立文檔的良好習慣，做好預防措施，並預計各項風險及制訂應變策略，以減低資訊系統受襲的風險和影響。

艾博士安全系統(香港)有限公司首席安全顧問潘永明

潘永明稱，獲得ISO/IEC 27001認證讓他們對網絡風險有更充分的準備，可及早作出針對性部署；而且認證能增強客戶信心，對投標新項目亦有幫助。他認為各行各業，特別是醫療界、金融界及涉及客戶資料的行業如數據中心等，都應實施ISO/IEC 27001以減低風險。他期望龍頭企業能帶頭實施ISO/IEC 27001，上行下效，令認證大大普及。

管理資訊科技風險 全局員工有責

要儲存管理全港考生的資料，以及計算和發放公開考試成績，並要確保試題不會事先洩露，香港考試及評核局（考評局）在資訊保安方面必須做到準確無誤。考評局資訊科技總經理曾廣納指，考評局自2008年引入ISO/IEC 27001認證後，全局上下均根據認證的要求，養成良好管理習慣；除了資訊部門負責人會經常進行風險評估，預先就潛在風險制訂應變措施和記錄相關文檔外，亦會要求每位員工做好自身崗位的資訊保安工作，例如要求員工定期更換電腦密碼及離開座位時把電腦的重要資料收妥，以減低發生事故的機會。

香港考試及評核局資訊科技部總經理曾廣納

曾廣納表示，認證機構每年會派員進行審核，查找管理系統是否有漏洞，為他們提供極大參考作用。他更分享說，實踐ISO/IEC 27001 所須投放的資源並不多，最重要是建立全局所有員工的防護意識，讓他們明白為何要跟從管理措施去做，便自然事半功倍。他認為，不論公私營機構，都值得推行認證的要求，以提升資訊保安。

(資料由客戶提供)