做好政策管理 符合支付卡產業規範

影片：30 分鐘掌握支付安全的強化策略

在企業「合規」的重要性遽增的今日，政策遵循（policy compliance）在企業組織的重要性也顯著提升，不亞於人力資源、資訊等部門。一套完整及受到充分支持的安全政策，奠定著組織的基調，同時向員工傳達組織對他們的要求。無法測量、監控與管理政策遵循，可能造成對企業與個人的聲譽損傷，導致組織受到懲處及營收的損失。

信用卡支付安全是主要的信用卡品牌（美國運通、Discover、JCB、萬事達卡和 Visa）非常重視的問題。因此，支付卡產業資料安全標準（Payment Card Industry Data Security Standard, PCI DSS）的第 12 項要求─維護針對所有人員的資訊安全政策，即在確保接受信用卡付款的商家和服務提供者改變其組織文化，以確保流程和系統的安全性可以得到應有的重視。

負責發展和維護 PCI DSS 的支付卡產業安全標準協會（Payment Card Industry Security Standards Council, PCI SSC），正透過改善組織政策與風險評估流程，來強化支援安全性（security）的相關流程。具體來說，該協會期望能確保企業組織全年性的遵循 PCI DSS，並做到經常性的妥善管理和評估。誠如 PCI SSC 的資訊長 Troy Leach 所言：「PCI DSS 可以協助企業回答：『我們是否具備無時無刻保護好顧客持卡人資料的企業文化？』」

強化政策管理

一般來說，全權負責 PCI 合規的執行長或財務長，都非常瞭解相關要求。然而，問題在於這些 PCI 政策是否能夠被確實執行。要克服這個常見的挑戰，定期針對負責卡片支付工作的員工進行溝通和教育，便非常關鍵。同時，若要確保任何需要改進的事項能在適當的時間、對適當的人員，在組織內部進行適當的溝通，則健全政策管理將是最有效的做法。

展示健全的政策與程序

在網路攻擊事件越來越普遍的現在，組織成員不僅要能正確行事，並且要能被看到。因此，政策文件必須：

- 可取得
- 保持更新
- 清楚明確
- 在合規提報（compliance reporting）時可識別

每個政策的遵循都要加以追蹤，以便組織能證明其合規，並且展現出治理的成果。

企業已經意識到，要符合現行 PCI DSS 日益細化的規定，在表格中打勾的模式已經不再可行。現在，他們必須證明整個企業體都遵循新的政策、對政策有充分瞭解，並且持續合規。改變的動力最初可能來自避免組織違規或被罰款，但現在大家越來越意識到，改善流程的結果將使企業、員工和顧客都獲益。

BSI 雲端安全及支付標準產品經理吳晟熙在今年度的「BSI Standards 管理系統標準年會」演講中也指出「企業組織要將法規要求化為控制措施，法遵人員與資訊部門需要多溝通」，顯見組織成員對規範和流程的了解，左右合規的成敗。吳經理同時也建議企業組織可以從 ISO/IEC 27001 資訊安全管理系統的基礎，收納各式資訊安全要求，並強化組織員工的遵循意識(包括業務單位及資訊單位)。更多吳經理的演講內容請參考：

1. 〈支付安全的威脅與強化策略〉演講精華摘錄
2. 〈支付安全的威脅與強化策略〉演講內容影片

> 「將法規要求化為控制措施，法遵人員與資訊部門需要多溝通」

吳晟熙 產品經理
BSI 英國標準協會

PCI DSS 支付卡產業資料安全標準 系列課程

強化電子支付卡資料安全及法規遵循課程 1 天
PCI DSS 內部稽核員課程 3 天
PCI DSS 主導稽核員課程 5 天

T: +886 2 2656 0333 Ext. 133
E: training.taiwan@bsigroup.com
課程訊息請按此>