美國發表網路安全框架

2014年2月12日，美國發表「網路安全框架(Cybersecurity Framework)」，該框架係由美國政府、企業及民間機構花費一年的時間共同發展而成，其蒐集了全球現有的標準、指引與最佳實務作法，最後由國家標準技術局（National Institute of Standard and Technology, NIST）彙整後所提出。

本框架主要可分成三大部份：

1.框架核心（Framework Core）

框架核心包括辨識(Identify)、保護(Protect)、偵測(Detect)、應變(Respond)、與復原(Recover)等五項功能。這五項功能組成網路安全管理的生命週期，藉由這五項功能的要求項目與參考資訊的搭配運用，可使組織順利進行網路安全管理。

2. 框架實作等級（Framework Implementation Tiers）

共分成局部（Partial）、風險知悉（Risk Informed）、可重複實施（Repeatable）、合適（Adaptive）四個等級。組織可以透過對風險管理流程、整合風險管理計畫以及外部參與等三個面向的觀察，瞭解組織目前的安全防護等級。

3. 框架側寫（Framework Profile）

框架側寫係組織依照本框架實際操作後所產出的結果，可以協助組織依據其企業需求、風險容忍度，決定資源配置的優先順序，進一步調整其網路安全活動。

此一安全框架旨在提供整體規劃藍圖予尚未建立網路安全架構的組織參考，而針對已有建立網路安全架構者，該框架並未意圖取代組織原先的風險管理程序和網路安全計畫，而係希望協助公、私部門改善資通訊科技和工業控制系統風險管理的能力。

相關連結

- Launch of the Cybersecurity Framework,The White House
- White House pushes cybersecurity framework for critical infrastructure, PCWorld

相關附件

- Framework for Improving Critical Infrastructure Cybersecurity [pdf]

郭俊仁 編譯整理

上稿時間：2014年03月

資料來源：

White House pushes cybersecurity framework for critical infrastructure, PCWorld ,http://www.pcworld.com/article/2097320/white-house-pushes-cybersecurity-framework-for-critical-infrastructure.html（last visited May.3,2014）
Launch of the Cybersecurity Framework,The White House ,http://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework（last visited May.3,2014）

延伸閱讀： Framework for Improving Critical Infrastructure Cybersecurity,http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

推薦文章