外國金融監理快訊

FDIC 及 OCC 對「網路風險升溫」聯合聲明 (Heightened Cybersecurity Risk)

本公司國關室翻譯

壹、宗旨

美國聯邦存款保險公司 (Federal Deposit Insurance Corporation, FDIC) 及美國財政部金融管理局 (Office of the Comptroller of the Currency, OCC) 於 109 年 1 月發表聯合聲明，提醒金融機構相關網路安全風險管理原則。此原則涵蓋「金融監理機關發布金融機構建立資訊安全標準指導方針 (Interagency Guidelines Establishing Information Security Standards)」及聯邦金融檢查委員會 (Federal Financial

本文中譯內容如與原文有歧義之處，概以原文為準。原文網址連結如下：
https://www.fdic.gov/news/news/financial/2020/fil20003a.pdf

Institutions Examination Council, FFIEC) 成員提供此類議題之相關資源，如 FFIEC 發布之「破壞性惡意軟體聲明 (Statement on Destructive Malware)[註 1]」。

金融機構採行上述原則及相關網路風險降低方法，可降低網路攻擊者成功攻擊的風險，並將中斷式及破壞性網路攻擊之負面衝擊降至最低。儘管預防性控管措施極其重要，然金融機構管理階層仍應為最壞情境做預備，建置並維護業務持續計畫程序，以期迅速復原、重新開業並使機構持續營運。

貳、重點

實施暨維護有效的網路安全控管措施，對保護金融機構免於惡意網路攻擊活動（特別是在風險升高階段）尤其重要。健全的網路安全風險管理包含以下面向：

一、事件因應及回復彈性能力 (Response and resilience capabilities)：檢視、更新及測試事件因應措施與業務持續計畫。

二、認證 (Authentication)：防止未經授權存取。

三、系統組態 (System configuration)：安全配置暨設定系統及服務。

參、背景

網路安全威脅之風險升溫，如地緣政治加劇致局勢緊張及侵略威脅，可能導致以美國為目標及其利益進行網路攻擊。近年來，針對金融機構的中斷式及破壞性網路攻擊之頻率及嚴重性日益增加。網路攻擊者經常使用惡意軟體攻擊金融機構的電腦及網路漏洞，採取的做法係藉偽照使用者登入資料 (credentials) 及以社交工程技巧誘導金融機構員工或其承包商下載惡意軟體進行釣魚式或魚叉式網路攻擊，以取得金融機構系統及網路存取權限。另一種攻擊方式即藉可移除式裝置，使金融機構之電腦及系統遭病毒感染。

入侵金融機構系統的破壞性惡意軟體可能會修改、刪除或以其他方式使其系統無法運作。依據金融機構被攻擊之範圍、其備份流程方法及其他所使用之控管措施，金融機構的資料與系統備份亦可能遭破壞性惡意軟體攻擊而產生類似影響，嚴重影響其恢復營運能力。

金融機構業務持續及復原能力計畫應妥適考量針對備份流程及其系統的網路

威脅與漏洞，包括涉及鏡像及資料複製 (mirroring and data replication) 功能之威脅與漏洞，渠等功能幾乎可即時進行系統備份。近年來許多金融機構採用的鏡像及資料複製功能，可縮短復原時間及提高業務回復能力。然此種功能亦可使金融機構暴露在快速複製惡意軟體的風險，破壞原始及備份資料或導致產生處理錯誤 (processing errors)，致使損害無法逆轉。

肆、風險管理

鑑於嚴峻網路威脅環境，管理高層應重新評估資訊科技防範措施是否足以抵禦網路威脅，尤其是來自勒索軟體及其他破壞性惡意軟體之威脅。日益增加的網路攻擊突顯網路安全防範準備及復原能力為優先要務之重要性。實施暨維護有效的網路安全管控措施 (包括威脅監控) 對保護金融機構免於網路惡意活動攻擊十分重要。關鍵管控措施包含下列六大面向：

一、事件因應、回復彈性及復原能力 (Response, Resilience and Recovery Capabilities)

縱使備有預防性管控措施，金融機構仍可能成為破壞性惡意軟體攻擊的受害者。管理階層應考量採取措施強化系統及營運回復彈性，以抵禦網路及實體攻擊，包括網路分段或離線 (如磁帶裝置) 等方式之維護系統備份。此外，在關鍵網路元件與服務 (如核心處理、交易資料、帳戶資料及備份) 及高度敏感的網路環境物件之間，進行邏輯分段 (logically segmenting) 及從網路連結的系統中隔離出來，可降低網路惡意活動在整個網路散播的風險。

金融機構進行復原能力測試，以應變勒索軟體或其他破壞性惡意軟體損壞或加密其資料 (包括備份資料)，將有助其降低被攻擊情事。在破壞性惡意軟體損害主要資料及備份系統的情境下，未遭感染的備份資料便顯得格外重要。

此面向尚包括以下內容：

(一)維護完整、已建檔及當前事件暨業務回復彈性計畫，包括因應破壞性網路攻擊及後續之復原措施

1.將被網路攻擊後的復原措施與要項整合至業務持續管理計畫中。

2.與聯邦和地方執行網路安全法規之機構建立關係並維繫之。

3.識別可用於協助處理網路安全事件的鑑識與復原專業技術。

4.定期進行網路安全事件復原演練或規劃測試，確認該項功能的復原能力如預期進行。

5.將網路保險視為大範圍的風險管理策略之一。網路風險管理策略包括辨別、衡量、降低及監控網路風險。

(二)實施一套完整的系統及資料備份策略

1.將所有關鍵資料及系統組態資訊，以符合資料量、資料種類及其重要性的備份頻率，進行備份。

2.將系統及資料備份檔安全存放在不同的地理位置並保持離線，或可與主系統進行實體或邏輯隔離。

3.定期測試破壞性攻擊事件發生時重建資料的能力。

4.思考備份及還原作法是否符合產業標準及架構，俾利破壞性惡意攻擊發生時，藉資料倉儲 (data vaulting) 保護關鍵資料。

二、身份識別及存取管理 (Identity and Access Management)

釣魚式網路攻擊激增及網路威脅者成功偽造使用者登入資料，亦促使金融機構建置妥適的身份及存取管理措施，其中包括客戶、員工及第三方廠商存取系統的身份認證管控措施。身份識別及存取管理管控措施案例如下：

(一)使用並驗證身份認證管控措施（如多因子認證）的有效性，以切割及保護連線之關鍵系統及資料的存取。

(二)確認身份認證及存取控管措施的強度係依風險設定之。

(三)設定用戶權限，依其職務角色設定存取管控措施，並僅限為其工作職務所需。

(四)限制及監控系統管理員及其他特殊權限使用者之帳戶。

(五)定期檢視已授權存取權限的妥適性。

三、 網路組態及系統之安全強化 (Network Configuration and System Hardening)

網路及軟體系統設定應以安全及完善方式檢視與配置。金融機構管理階層應檢視預設系統設定是否適當、變更預設使用者之設定檔、配置安全性設定及採用安全監控工具。安全檔更新及系統修補程序對維護系統安全十分重要，應及時進行。其他系統組態控管措施及網路安全防衛 (cyber hygiene) 原則包括：

(一)妥善設定網路元件，確保僅被授權的通訊埠、協定與服務可運作，並停用所有不必要的服務、通訊埠及協定。另記錄及核准作業系統及系統元件的安全性設定標準。

1. 在使用系統前，依據需求檢視及停用或調整預設使用者之帳戶及其設定。
2. 限制可卸除式裝置自網路存取資料。
3. 進行弱點掃描，包括所有網路元件、硬體元件 (桌上型及筆記型電腦、行動裝置、路由器及防火牆)、韌體及作業系統，以確保關鍵修補程式皆已安裝。
4. 定期執行及更新反惡意程式的軟體，俾持續監控及防禦網路及所有連線裝置。
5. 設定電子郵件系統，以偵測及防止一般電子郵件攻擊手法，如含惡意連結或附件的詐騙或釣魚式電子郵件。
6. 邏輯性地分段關鍵網路元件及服務（如核心處理、交易資料、帳戶資料及備份資料），且於適當情況下，將關鍵及高度敏感性項目元件與外部網路環境進行隔離。

(二)以符合風險特性，配置設定並持續監控內部網路連接到服務提供商，特別是提供關鍵服務的內部網路。

管理階層評估其內部攸關破壞性惡意軟體及營運回復彈性之風險時，也需將下列四至六點列入考量。

四、 員工訓練

應瞭解員工係金融機構網路安全計畫的關鍵管控點。由於社交工程手法是惡

意攻擊者入侵機構系統的主要管道，故對員工進行社交工程訓練應考量下列二項因素：

(一)持續對識別網路威脅、釣魚式網路攻擊及可疑連結等事項，進行員工訓練。

(二)評估前述網路安全訓練計畫的有效性。

五、安全性工具及監控

(一)聘僱合格的網路安全人員或合格的資訊安全代管服務商 (managed security service provider)，取得來自相關產業提供之網路威脅及漏洞資訊，如美國金融服務資訊共享及分析中心（FS-ISAC）與美國電腦緊急處理小組（US-CERT），以利監控機構系統。另應建置並維護一個利用威脅及漏洞資訊，進行辨別與因應潛在網路威脅的流程。

(二)以手動或藉由安全資訊與事件管理工具檢視系統及網路稽核日誌是否有異常活動。此工作事項應由合格人員定期進行。

(三)實施足夠範圍的滲透測試，包括定期內外部測試，檢視銀行偵測及因應網路攻擊之能力，並及時追蹤與修正測試結果。

六、資料保護

(一)維護資料分類計畫 (data classification program)，俾識別敏感及關鍵資料。

(二)加密或代碼化 (tokenize) 傳輸中或靜態的敏感及關鍵資料。

本聯合聲明僅提供關鍵風險管理及控管注意事項之案例。金融機構管理階層應利用資源開發並維護有效的網路安全風險管理計畫，包括與服務提供商、軟體商、承包商及其他第三方之密切協調合作。

註釋

註 1： FFIEC 於 2015 年發布此篇「破壞性惡意軟體聲明」，資料連結：https://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf