主旨：有關近期國內多家重要能源及科技公司遭受網路駭客攻擊事件，請貴公(協)會依下列事項轉知所屬會員廠商重新檢視，請查照。

說明：

一、依據法務部調查局(以下簡稱調查局)於109年5月15日發佈國內重要企業遭勒索軟體攻擊事件調查說明，內容略以：「109年5月4日至5日國內多家重要能源及科技連遭勒索軟體攻擊，駭客入侵並將勒索軟體植入公司內部系統、個人電腦及伺服器等資訊設備，儲存的重要檔案均無法開啟，除營運受到嚴重影響外，駭客亦要求交付贖金。為穩定重要能源及科技企業營運，並遏止網路犯罪，調查局成立專案小組迅速偵辦本案。」

二、為避免上開事件影響國內金屬相關產業，請協助轉知會員廠商依調查局提供建議進行資安漏洞檢視，說明如次：

(一)檢視企業網路防護機制，如對外網路服務是否存在漏洞或破口、重要主機應關閉遠端桌面協定(RDP)功能等。

(二)觀察企業VPN有無異常登入行為或遭安裝SoftetherVPN及異常網路流量，如異常的DNS Tunneling、異常對國內外VPS的連線等。

(三)注意具軟體派送功能之系統，如網域/目錄(AD)伺服器、防毒軟體、資產管理系統，尤其注意AD伺服器的群組原則遭異動、工作排程異常遭新增等。

(四)更新防毒軟體病毒碼，留意防毒軟體發出之告警，極可能是大範圍感染前之徵兆。

(五)加強監控網域中特權帳號，應限定帳號使用範圍與登入主機。

(六)建立備份機制，並離線保存。

三、有關調查局發佈旨揭駭客攻擊事件相關新聞，請查詢網站https://www.mjib.gov.tw/news/Details/1/607