00000000000000000000公司
威脅弱點衝擊影響判定表

更新日期:　　流水編號： YYY-XXXX

（一） 威脅等級

指威脅發生的機率或可能性

威脅發生可能性	評等	說明	威脅頻率
低	1	防制脆弱性被利用的安全對策有效	平均每年發生次數2次以內或沒發生過但可能發生
		威脅來源缺乏動機或能力不足	
		發生頻率低	
中	2	威脅來源有動機也有能力	平均每季都可能發生一次以上；或平均每月人為阻止事件或威脅發生2~3次
		防制脆弱性被利用的安全對策有效	
		有可能發生	
高	3	威脅來源有強烈的動機與足夠的能力	平均每月都可能發生一次以上；或平均每月人為阻止事件或威脅發生超過四次(含)
		防制脆弱性被利用的安全對策無效	
		時常發生	

（二） 弱點等級

是指資訊資產之脆弱點被利用的難易度

難易度	評等	說明	一般分級原則
低	1	脆弱點很難被利用； 或是會受到損害後能立即回復	1.僅限深入瞭解脆弱點技術，並於特定條件或環境下方能利用脆弱點 2.不會損害資訊資產價值，或是受到損害後能立即回復 3.必需運用特殊的方法才能利用脆弱點進行攻擊 4.威脅來源必須花費長時間(可能需一個月以上)的資料收集，突破各層防護，才能接觸到關鍵資訊攻擊成功：可能要1~數個月以上
中	2	脆弱點被利用的難度適中； 或是會受到損害，且無法立即回復	1.具備瞭解脆弱點技術知識，方能利用脆弱點 2.資訊資產價值受到損害，且無法立即回復 3.不需用特殊的方法就能利用脆弱點進行攻擊 4.已實施保護的機制，威脅來源必須花費一段時間(可能是數天)進行資料收集始能接觸到關鍵資訊擊成功：可能是數天以上
高	3	脆弱點很容易被利用； 或是會受到嚴重損害，影響或中斷資產相關業務運作，導致資訊資產消失無法復原	1.任何人不需具備任何能力均能有意或無意的利用脆弱點 2.資訊資產價值受到嚴重損害，影響或中斷資產相關業務運作，或導致資訊資產消失無法復原 3.利用簡易的方法就能利用脆弱點進行攻擊 4.未實施保護或保護機制無效，威脅來源於短期內即可攻擊成功攻擊成功：可能是一天內到數天
	瞭解脆弱點技術知識：如必須學過開鎖才能解鎖，必須知道取得exploit的方法才能攻擊系統弱點 深入瞭解脆弱點技術：如必須瞭解系統內部設計架構，並學習過組合語言才能攻擊系統弱點 特定條件或環境：如特定的作業系統、特定的時間、或特定的操作方式		

（三）衝擊程度評估等級

指指各資產在發生資訊安全事故後，對組織業務運行所可能造成的損害狀況。訂定等級時，應依據該資產對組織形象、業務持續、人員安全影響程度。

衝擊程度	評等	說明
微弱	1	對於業務執行沒有影響
		造成的損失可能僅影響影響僅個人或少數幾人
		可以立即完成復原或修復
輕微	2	對於組織整體業務執行影響不大
		已影響組織業務之運作，但在組織可承受範圍內。
		造成的損失可能僅影響單一單位或業務或系統
		修復或進行復原的措施可以在4小時內完成
嚴重	3	事件處理不當可能對組織形象造成嚴重損害
		已嚴重影響組織業務之運作，超出組織可承受範圍內。
		造成的損害可能影響組織整體業務或二個以上業務或系統
		修復或進行復原可能要超過8小時才能完成