勒索軟體事後回復檢核表

檢核表使用原則：

基礎項目：企業在防護勒索軟體時的一般性原則，確認事前的技術預防是否已達成，事中、事後則是建議事項或是用在確認處理動作是否遺漏。

進階項目：當較大規模的企業具備多網段、AD 管控、虛擬平台等複雜的網路環境，除基礎項目需達到以外，建議落實進階等級的項目，達成更好的防護效果；同時，在資產方面也產生重要性的排序需求，可快速釐清事件處理順序，提升減輕影響與系統回復的效率。

事件階段	檢核面向	基礎項目	進階項目	檢核欄
3.事後回復	3.1 設備恢復	-	3.1.1 依據關鍵資產清單及 2.2.4.2 受駭影響評估結果，排定資產恢復優先順序，以及對高重要性資產的資安保護規劃	
		3.1.2 重置該設備的所有密碼、憑證	-	
		3.1.3 使用備份資料進行還原	-	
		3.1.4 重新恢復的設備安裝防毒軟體，並執行全系統掃描	-	
	3.2 事後分享	3.2.1 將事件相關資料通報 TWCERT/CC，協助分享(去識別化後)給國內企業，防止更多企業受害	-	
	3.3 檢討改進	3.3.1 依受駭原因，於事件應變後，規劃管理層面對應改善措施並執行	-	

勒索軟體事後回復檢核表

參考資料

美國

https://www.cisa.gov/stopransomware

https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf

https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

https://jenner.com/system/assets/assets/11480/original/memo-what-we-urge-you-to-do-to-protect-against-the-threat-of-ransomware.pdf

英國

https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

資安廠商

https://www.trendmicro.com/en_no/forHome/campaigns/ransomware-protection.html

https://www.nomoreransom.org/zht_Hant/prevention-advice.html