工業技術研究院
Industrial Technology Research Institute

2021智慧商業論壇暨成果發表會

推動國際物流業資訊安全升級

工業技術研究院 服務系統科技中心
王亦璋 副理

大綱

- 資安即國安
- 企業資安事件發生頻率與復原速度
- 國際案例: 一段代碼癱瘓一個國家！
- 國際物流資安特性
- 國際物流資安注意事項與防護措施

資安即國安

蔡英文總統出席「2021台灣資安大會開幕典禮」時表示，政府將推出「資安即國安2.0」戰略。

- 提升關鍵基礎設施及核心資料庫的防護韌性。
- 邁入物聯網及5G時代，確保產業研發中的資訊安全，打造能被世界信賴的資安系統及產業鏈，將是台灣在全球競爭中最重要的優勢。
- 持續用下一個世代的數位思考強化資安運用，提升台灣整體數位產業的實力。

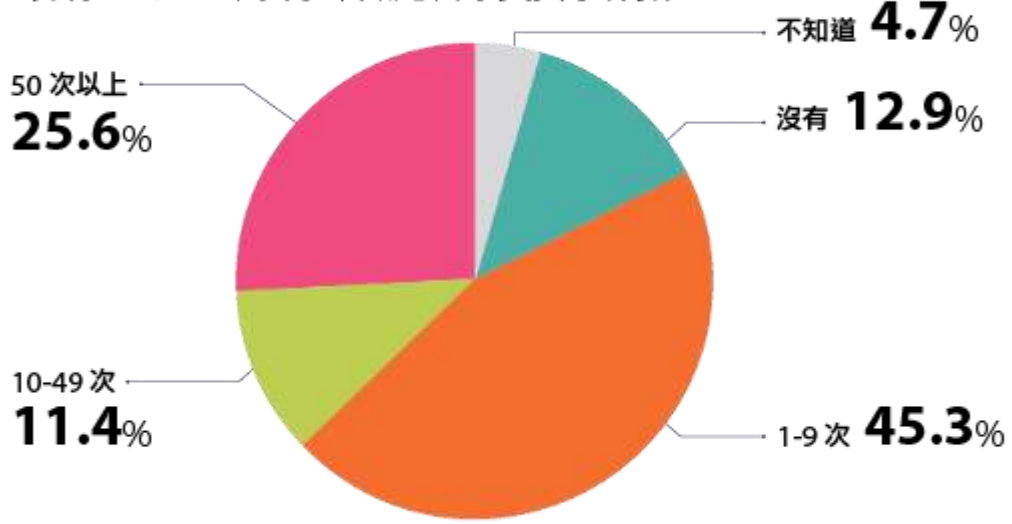
資料來源: 2021-05-05
https://www.chinatimes.com/newspapers/20210505000441-260118?chdtv

ITRI Industrial Technology Research Institute

企業資安發生頻率與復原時間

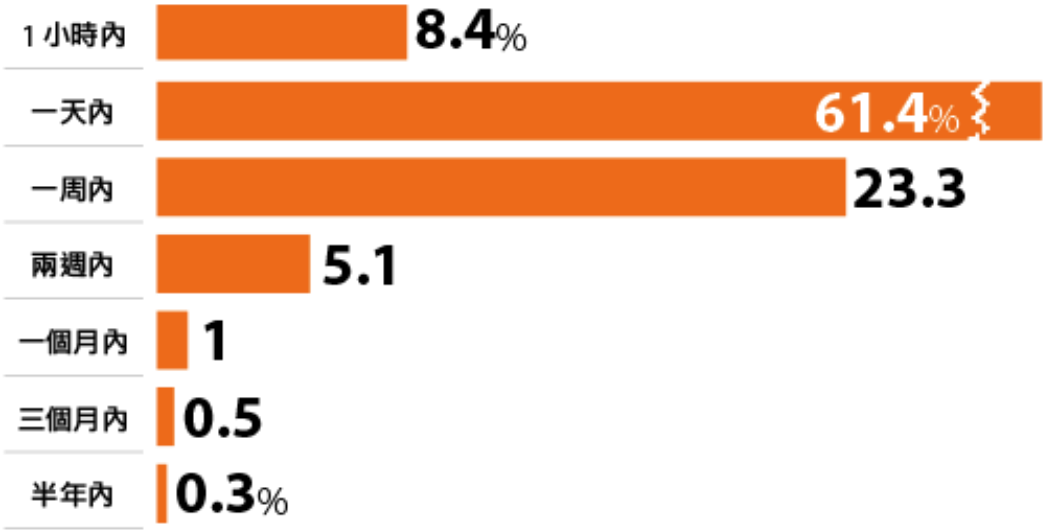
2020年企業資安事件發生頻率

每 4 家企業就有 1 家超過 50 次資安事件，且比例已連續三年增高，並仍有 4.7% 企業表示不知道自家資安事件數



企業遭遇資安事件復原時間要多久?

資安事件復原的快慢，可看出企業應變能力，近 7 成企業可以在 1 天內復原，但也有近 3 成企業需要 2 天到 2 周



資料來源: 2021-05-12
https://www.ithome.com.tw/article/144234

ITRI Industrial Technology Research Institute

一段代碼癱瘓一個國家！

全球最大貨櫃船運業者「快桅」遭勒索軟體攻擊 損失超過2到3億美元 影響遍及全球

快桅集團 (Maersk)

維基百科

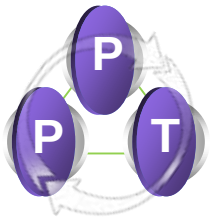
- 總部設於丹麥哥本哈根，是世界知名跨國企業集團
- **世界上最大的貨櫃船運經營者及貨櫃船供應商**
- 主要業務核心: **運輸**(貨櫃運輸船隊)及**能源**(離岸石油開採和運輸)

資料來源: 2018-08-28
https://news.cnyes.com/news/id/4191150

ITRI Industrial Technology Research Institute

國際物流業的資安特性

- 擁有的資料量大，但運用的應用程式較少
- 因應全球客戶需求 E化程度越高越能創造服務價值
- 但隨之而來的資安風險越大
- 而當眾多物流業者在E化程度也都迎頭趕上，接下來會分出勝負的部份，除了服務、效率以外，就是可能為客戶所帶來的風險高低。資安控管越嚴謹，資安風險就越低，客戶黏著度越高
- 國際物流業屬於產業供應鏈的一環，需要配合上下游的系統去做客製化介接，每個系統對於資料保護方式都不盡相同， 因此要配合每一個客戶不是一件容易的事，因此物流業者會去評估是否要導入資安的國際標準驗證，因為國際標準驗證是與客戶溝通之間的一道重要橋樑。



資安事件、情境、風險與資安技術 ＋ **資訊安全管理標準 (ISO、NIST)** ＋ **國際物流組織對於供應鏈安全的規範**

https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=5653

ITRI Industrial Technology Research Institute

國際物流資安注意事項與防護措施

國際物流常見資安事件 ⟶ 可能肇因與資安風險

電子郵件釣魚攻擊	• 點擊含有商業發票的不明電子郵件，遭網路釣魚攻擊。
電子郵件滲透詐騙	• 國際詐騙集團滲透國外代理商的電子郵件並要求付款，造成財物損失風險。
端點防護不足	• 倉儲管理與監視系統無使用者連線控管與入侵偵測，增加貨物資料外洩風險。
系統安全漏洞	• 海空運承攬報關系統開發技術、環境與版本如未升級或更新，且未定期實施安全檢測，增加駭客攻擊風險。

注意事項：企業應建立事前預防、事中應變、事後復原之管理制度來提升整體資安防護力

(一) 國際物流電子郵件管理

常見資安事件的類型

商業電子垃圾郵件	電子郵件釣魚攻擊	商業電子郵件詐騙
• 未經請求或允許而發送的商業廣告或非法的電子郵件	• 藉由傳送電子郵件方式，騙取收件者信任，進而開啟郵件內容的駭客攻擊模式	• 竄改仿冒合作廠商來信的電子商務郵件
		

商業電子郵件詐騙資安事件情境：

A國際物流公司財務人員與國外代理正進行對帳及匯款，遭到國際詐騙集團滲透國外代理的電子郵件，截取原始通訊的郵件內文，仿造往來郵件(含：郵件抬頭、內文、簽名等)，並要求付款，A國際物流公司財務人員在未仔細檢查不經意情況下將郵件回覆至國際詐騙集團所指定的地址，並進行匯款，造成財物損失。

注意事項與防護措施建議

People

- ✓ 不輕易點擊不明來源之電子郵件。
- ✓ 不輕易點擊不明來源之電子郵件中網頁連結或附件。
- ✓ 不隨意在網路上公布或留下電子郵件地址。
- ✓ 電子郵件中，不輕易提供個人隱私安全相關資訊，如帳號、密碼。
- ✓ 傳送含機敏個人檔案前先加密發送加密附件，密碼需以另一封寄出。
- ✓ 不利用公司網路轉寄垃圾郵件，不回覆垃圾電子郵件訊息。
- ✓ 落實電子郵件公私領域區分，避免將公務信箱用於私人用途。

Process

- ✓ 收件者須仔細觀察外部郵件寄件者資料，確認寄件者/收件者的名稱、主旨、主題關聯性、郵件地址無誤；
- ✓ 如收到未知寄件者或少往來對象來信須特別注意，若無法判斷的信件可向寄件者求證，並依循組織舉報程序主動回報；
- ✓ 企業應增加多步驟審核與驗證的流程，尤其在付款授權流程或對現有帳戶資訊的任何更改時，需與對方求證；
- ✓ 向IT或資安專責人員確認信件真實性、是否為釣魚郵件或藏有其他病毒等，未經查證前勿輕易回覆或匯款；
- ✓ 透過通知信或郵件記錄器來設定個人專用的黑白名單。

Technology

- ✓ 安裝郵件防毒軟體。
- ✓ 架設郵件攔截過濾與追蹤系統。
- ✓ 點擊連結及附件前，先進行檢測。
- ✓ 加強密碼管理，定期更新密碼並確保密碼複雜度。
- ✓ 不定期透過社交工程演練確保企業員工具備資安意識。

ITRI Industrial Technology Research Institute

(二) 國際物流系統安全漏洞管理

常見資安事件的類型

勒索軟體	進階持續性滲透攻擊(APT)	植入惡意程式
• 要求受害者繳納贖金以取回對電腦的控制權，或是取回解密金鑰	• 針對性、持續性、隱密性且經過策劃後，對目標對象進行入侵滲透攻擊	• 設計程式破壞獨立的電腦或已連接網路的個人電腦，如：病毒、蠕蟲或特洛伊木馬程式

勒索軟體資安事件情境：

S國際物流公司遭駭客攻擊，駭客疑似利用漏洞，誘騙公司人員下載勒索軟體後，將使用者裝置內的資訊進行加密，甚至橫向擴散至其他電腦，S國際物流公司重要業務文件被加密，多數電腦無法使用，駭客更利用勒索軟體要脅被害人依指示交付財物換取解密。然而鑒於勒索軟體付款機制精密而難以追查，且自行解密恐耗費時日，本案件造成S國際物流公司營運中斷與財損，而使企業蒙受重大損失。

注意事項與防護措施建議

People

- ✓ 避免在工用電腦上使用個人應用程式和網站，如電子郵件、通訊軟體。
- ✓ 未經防毒掃描或仔細檢查，避免開啟可疑、不明來源之檔案或連結。
- ✓ 不使用免費WiFi登入個人網路銀行、公司網路或其他需要帳號密碼登入的系統。
- ✓ 一般使用者不要使用管理員權限的帳戶。
- ✓ 當作業系統提示更新時(即Windows Update)應盡早完成更新。
- ✓ 下班後應確實關閉電腦。
- ✓ 除非已採取額外的安全措施，應禁止在公司網路上使用個人設備。
- ✓ 除非已採取額外的安全措施，應禁止在公司網路上開放遠端登入操作或遠端維護。

Process

- ✓ 一旦發現電腦疑似遭到入侵時，立即關閉電源，拔除實體網路線及任何USB儲存裝置，停止使用網路與外界連線，並依循組織舉報程序主動回報；
- ✓ IT或資安專責人員啟動可信度高的防火牆管控與外界連線，並使用防毒軟體做系統全盤掃瞄，將可能入侵途徑系統隔離，評估並找出可能潛在的主動式木馬程式；
- ✓ 若遭受駭客入侵的情況依然無改善則須立即停用網路，並考慮重新安裝作業系統；
- ✓ 報告相關單位，連絡可能受到影響的個人或單位，並更改重要系統與核心業務營運服務的帳號密碼；
- ✓ 確認更新實體主機、虛擬主機之防毒軟體，並搭配以安全模式抽查方式，檢查是否還有潛伏期內的主機；
- ✓ 倘若遭到駭客入侵的影響甚鉅，包含重大機密資料遭竊或相關財務損失，則需考慮向警方報案尋求協助處理。

Technology

- ✓ 安裝防毒軟體，並開啟自動掃描功能。
- ✓ 定期更新修補程式，保持所有電腦均完成安全更新。
- ✓ 採用可防制勒索網站的安全產品或服務。
- ✓ 設定作業系統或利用軟體管制應用程式使用者權限。
- ✓ 資料庫應控管於內部網段，不可直接暴露於外網。
- ✓ 以白名單限制存取系統並鎖定來源IP，若有資料交換需求，應於防火牆或伺服器設定存取控制，僅允許特定來源IP存取資料庫。
- ✓ 加強密碼管理，定期更新密碼並確保密碼複雜度。
- ✓ 重要服務之系統應設置相關備援機制，並配合定期資料備份。
- ✓ 定期執行資安檢測，如：網路活動檢測、網路設備、伺服器及終端設備檢測、網站安全檢測及安全設定檢測等項目，針對檢測的內容加以修正及改善。

ITRI Industrial Technology Research Institute

(三) 國際物流端點防護管理

常見資安事件的類型

勒索軟體	植入惡意程式	分散式阻斷服務攻擊
• 要求受害者繳納贖金以取回對電腦的控制權，或是取回解密金鑰	• 設計程式破壞獨立的電腦或已連接網路的個人電腦，如：病毒、蠕蟲或特洛伊木馬程式	• 駭客利用大量偽造且無意義的封包，消耗被攻擊者的網路頻寬與系統資源，導致網路癱瘓
		

端點防護漏洞的資安事件情境：

P國際物流公司使用某軟體開發商的連網監視器攝影機，在使用前未更改裝置的預設密碼，遭駭客輕易破解，在未設置隔離措施下使感染範圍擴散，駭客利用監視器攝影機組成的殭屍網路，針對某一雲端服務發動了分散式阻斷服務攻擊，癱瘓系統主機致其無法正常作業。

注意事項與防護措施建議

- **People**
  - ✓ 新購設備應立即變更預設帳號密碼，不使用連網裝置預設密碼。
  - ✓ 不使用公開與來路不明的網際網路位置。
  - ✓ 依產品韌體更新指示盡早完成系統更新。
  - ✓ 定期盤點內部所有的物聯網設備，若發現已不再使用或非必要的設備應下線處理。
- **Process**
  - ✓ 一旦發現電腦疑似遭到入侵時，立即將連網設備中斷連線，並依循組織舉報程序主動回報；
  - ✓ IT或資安專責人員確認並排除問題，更新韌體版本至最新版本；
  - ✓ 重置設備、變更連網裝置預設帳號密碼。
- **Technology**
  - ✓ 定期檢視並更新設備系統與韌體版本。
  - ✓ 定期追蹤檢查系統漏洞。
  - ✓ 帳號權限強化權限區隔。
  - ✓ 連網設備限縮來源IP或對外服務埠進行網路控管。
  - ✓ 強化資訊平台存取控管機制，防止無授權帳號不當的存取資訊。
  - ✓ 採取多層次的防禦架構來阻絕不同類型的攻擊。
  - ✓ 關閉設備非必要之功能。
  - ✓ 安裝入侵偵測系統、資訊系統監控工具。
  - ✓ 加強資訊存取的監控與紀錄，提供事後追蹤分析，找出可能的資安威脅。

110年度商業司資安計畫推動作法與案例分享

人員(People)	流程(Process)	技術(Technology)
社交工程演練	標準作業程序	報關承攬通關網路系統優化
資安意識提升	資訊安全管理系統(ISMS)	物流作業連網端點資安強化
資安人員培育	緊急應變措施	網路分割與權限控管落實
資訊安全組織	-系統和資料的復原與重建	-資安漏洞偵測與修補
-電子郵件釣魚詐騙	-勒索病毒贖金交付的談判	-病毒木馬程式的清理
-電子郵件攔截竊取	-重要營運服務不中斷的維持	-駭客襲擊事件偵測與應變

工研院 服務系統科技中心

王亦璋

03-5916592/0910338893

ycw@itri.org.tw