
CYBERSEC 2022 臺灣資安大會
CHANGE
NOW
數位轉型 資安升級
SEP. 20-22 臺北南港展覽二館

講者簡介

姓名: 宋曉青 Carey Sung

現任: TRI 上市公司稽核主管

經歷:

1. 會計師事務所: Auditor 審計查核員
2. 同協電子:上櫃公司總經理室稽核員
3. Cashbox Company: 上櫃公司稽核主管/會計部經理
4. Holiday Company: 上市公司稽核主管
5. 福來國際企業: 大陸稽核總監/特助
6. JM集團食品(股)公司: 台灣區稽核主管
7. TRI上市公司:稽核主管

證照:

1. CIA 國際內部稽核師
2. CRMA 國際風險管理師
3. 資安管理系統主導稽核員(BS7799 LA)
4. 外語導遊;領隊/華語導遊證照

學歷: 警大犯防所博士生/運休所EMBA/會計系

企業內控 VS 資安事件與因應策略

- 企業內控制度與規範簡介
- 企業資安事件與內控缺失之犯罪態樣
- 常見資安事件態樣 V.S 傳統因應策略
- 情境犯罪預防策略--新因應策略介紹
- 現行法規要求-資安長與資訊長(制度規劃)

Next:聽眾請準備好手機QR Code APP

請問您

Mentimeter

Please enter the code

42701031

Submit

Click to download as image

https://www.menti.com/njgjqpiqd4

mentimeter - 搜尋 (bing.com)

內控制度制訂與責任

- 三目標:”銀髮族很有錢(財)”

第 3 條　公開發行公司之內部控制制度係由經理人所設計，董事會通過，並由董事會、經理人及其他員工執行之管理過程，其目的在於促進公司之健全經營，以合理確保下列目標之達成：

一、營運之效果及效率。

二、報導具可靠性、及時性、透明性及符合相關規範。

三、相關法令規章之遵循。

內控自評內容--內控三目標與五要素

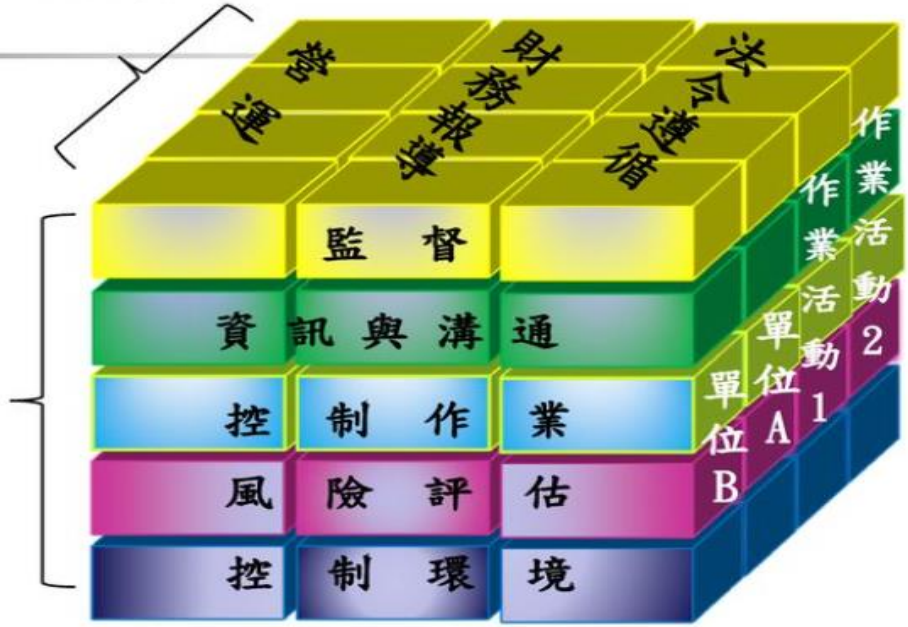
內部控制之目標及要素

三大目標：

- 營運效果與效率
- 財務報導之可靠
- 相關法令之遵循

五大要素：

1. 控制環境：機關文化、內部控制認知
2. 風險評估：辨認、估計與評量風險
3. 控制作業：政策及程序、SOP
4. 資訊與溝通：資訊處理及傳達
5. 監督：評估內部控制制度執行有效性



三維立方體模式，在呈現目標、要素、組織單位及作業活動之間的靜態關聯性。

資料來源：張信一 經濟部會計長 中華民國100年4月13日 中華民國100年6月14、17日 - ppt download (slidesplayer.com)

資安事件-重訊公佈

臺灣證券交易所股份有限公司　新聞稿

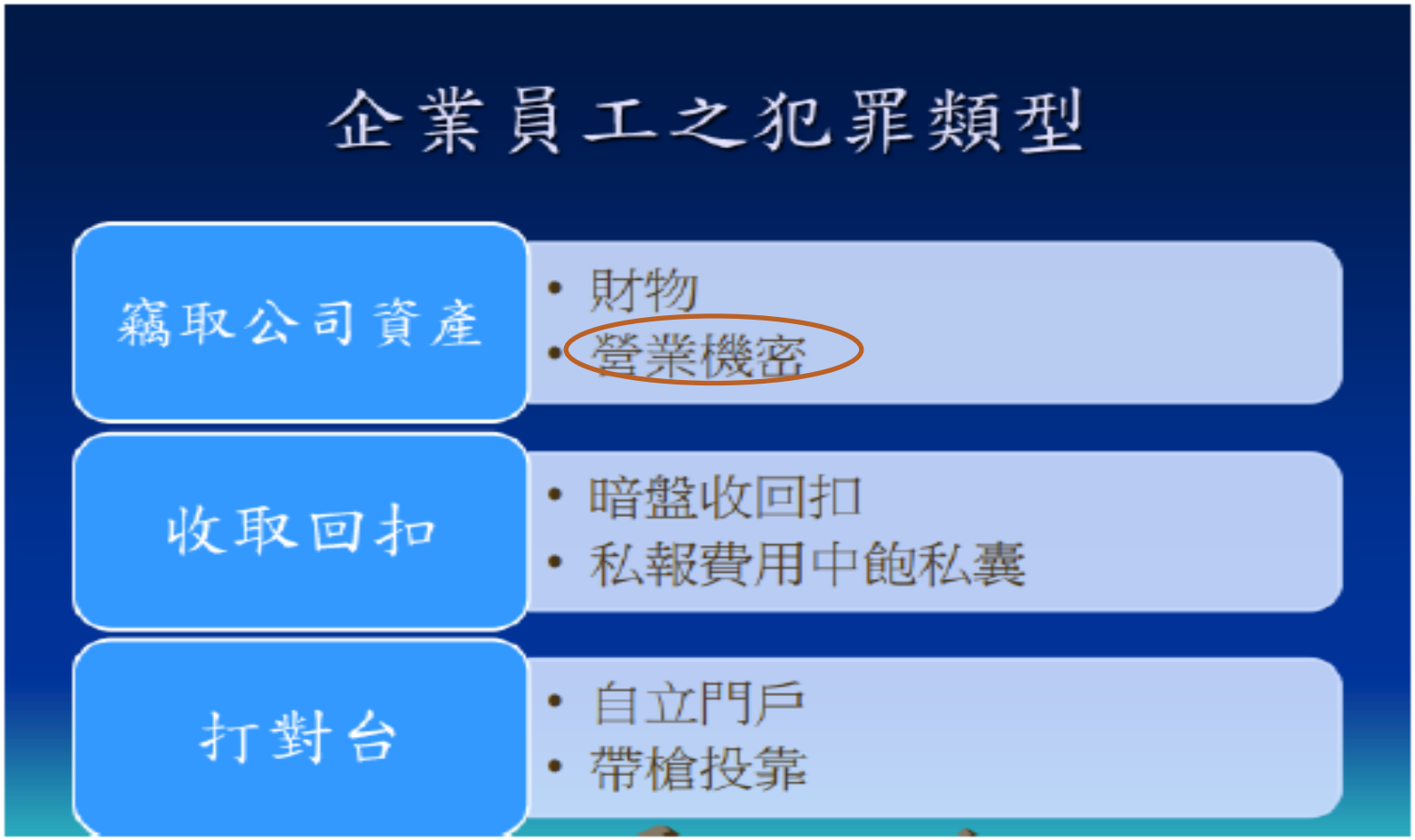
中華民國110年4月27日

上市一部

重大訊息與時俱進，臺灣證券交易所明訂上市公司發生重大資安事件應發布重大訊息

臺灣證券交易所表示，國內外資安攻擊事件態樣眾多，網路駭客透過社交工程或工作排程散播惡意程式等，攻擊手法層出不窮，資通安全已衍然成為重要議題，考量發生資通安全事件對財務業務之影響性逐漸上升，且對公司商譽等可能有重大影響，為強化該類事件重大訊息發布之重要性暨使法源依據明確，修訂重大訊息處理程序明訂上市公司發生重大資通安全事件應發布重大訊息。

內控疏失重大事件—(參考:證期局資料)



主題1：企業內部稽核常見缺失及違規案例解析

講師：證期局　鍾怡如　專門委員

重訊公佈—以資安事件為例

2021年4月27日，臺灣證券交易宣布修訂重大訊息處理程序，明訂上市公司發生重大資安事件時，需發布重大訊息對外揭露。2021年4月29日，證券櫃臺買賣中心也發布消息，同樣表示已修訂相關公開處理程序，要求上興櫃公司發生資安事件造成重大損害或影響，應發布重大訊息。

代號	簡稱	日期	序號	主旨
2353	宏碁	110/03/20	1	說明媒體報導
2382	廣達	110/04/22	1	廣達針對媒體報導提出說明
3260	威剛	110/05/26	2	威剛針對部分資通系統遭病毒攻擊事件說明
8091	翔名	110/06/03	3	本公司部分資通系統遭到病毒攻擊事件說明
2376	技嘉	110/08/06	2	公告本公司遭受駭客攻擊
6605	帝寶	110/10/18	2	說明本公司部分工廠廠區伺服器遭受病毒攻擊及影響
2353	宏碁	110/10/19	1	說明媒體報導
2014	中鴻	110/10/27	1	說明本公司輔助性伺服器遭受病毒攻擊及影響
2547	日勝生	110/10/29	1	說明本公司及子公司部分資訊系統遭受駭客網路攻擊
6257	矽格	110/11/01	1	公告本公司網路安全事件
2942	京站	110/11/02	1	說明本公司部分資訊系統遭受駭客網路攻擊
4728	雙美	110/11/09	1	說明本公司部分資訊系統遭受駭客網路攻擊
6697	東捷資訊	110/12/20	6	說明本公司部分資訊系統遭受駭客網路攻擊

2021年國內上市櫃公司至少14件資安事件重大訊息，平均每月一起 | iThome

資安事件(定義) V.S 內控因應策略

法規名稱：司法院及所屬各機關資訊安全事件通報及應變作業處理程序

四、資安事件分類與影響分級：

（一）資安事件類別分為三類：

1. 內部資安事件：如惡意破壞毀損、作業不慎、未依規定操作等。
2. 外力入侵事件：如病毒感染、駭客攻擊（或非法入侵）。
3. 天然災害或重大突發事件：如颱風、水災、地震、火災、爆炸、核子事故、重大建築災害等。

司法院及所屬各機關資訊安全事件通報及應變作業處理程序 (rootlaw.com.tw)

內控案例-態樣1 與傳統策略考量..

釣魚郵件釣什麼？

釣魚郵件看中的目標，大略可分為三種：竊取機敏資料、騙取金錢財物、誘導執行惡意程式。

竊取機敏資料	冒充金融或網路服務通知信，主要騙取金融相關服務的登入帳號及密碼，可能也是為了後續騙取金錢財物目的；其次是電子郵件或其它網路服務的登入帳密
騙取金錢財物	多半在郵件內容中聲稱有不錯的財務合作方案，或是通知受害人中了大獎，以誘騙受害人匯款
誘導執行惡意程式	通常在釣魚郵件中放置惡意程式、惡意連結，並誘騙受害人開啟，目的在取得受害者電腦的控制權

- 定期的教育訓練與社交工程演練，提高員工的警覺性、強化安全意識(only?)，以降低風險。

攻擊手法與工具

- BEC信件中沒有惡意程式-→可輕易規避傳統防毒檢測機制?!
- 合作廠商匯款帳號清單管理?!

BEC 手法-(論文參考資料)

根據 FBI 的定義，所謂的「商務電子郵件入侵」(Business Email Compromise，簡稱 BEC) 是一種精密電子郵件詐騙，專門鎖定需定期匯款給廠商的企業。BEC 其實就是之前大家所知道的騙，這類詐騙一開始都是先入侵企業高層主管的電子郵件帳號名義發送電子郵件給不知情的員工，指示他們電匯一大筆款項

儘管有些案例會運用到惡意程式，但絕大多數的 BEC 詐騙的「社交工程技巧」，因此一時很難察覺，從近期的一些案例可易被假冒公司高層主管要求提供資訊的電子郵件所騙。BEC 詐騙本。

(一) 假發票詐騙

此版本通常稱為「假發票詐騙」、「假供應商詐騙」或「發的一般都是跟國外供應商有往來的企業。企業通常會接到歹徒子郵件要求更改發票中的匯款目的地，或者要求將發票上的金所掌控的帳戶。

(二) 執行長(CEO)詐騙

此版本通常是冒用企業高層主管的電子郵件帳號，假借高某員工將款項匯至歹徒掌控的帳戶。在某些案例中，這類要求子郵件是直接發給金融機構，指示金融機構緊急匯款給某家銀稱為「執行長詐騙」、「企業高層主管詐騙」、「假冒名義」或「金融匯票匯款詐騙」。

(三) 入侵電子郵件帳號

某家企業的某位員工電子郵件帳號遭到歹徒直接入侵，而非冒名，歹徒利用此員工的帳號發送電子郵件給該員工通訊錄中的廠商，請廠商將發票上的金額匯到歹徒掌控的帳戶。

(四) 假冒律師

在這個版本當中，歹徒會假冒成律師或法律事務所的代表，透過電話或電子郵件的方式，和企業的員工或執行長聯絡，宣稱自己正在處理某項機密的緊急事務，催促對方盡快將款項暗中匯到某個帳戶。這類 BEC 詐騙會刻意安排在營業日結束或周末前夕，也就是員工正準備下班、容易慌亂的時候。

(五) 偷竊資料

此手法會入侵企業內特定員工 (通常是人力部門) 的電子郵件帳號，然後利用這個帳號發送郵件給其他員工或高層主管，要求提供個人身分識別資訊，而非要求匯款。再利用取得的資訊對該公司進行下一階段的 BEC 攻擊。

資安事件-駭客

國外

從2020年開始，美國便不斷指控中國入侵多家醫藥公司及學術單位，試圖竊取疫苗研發機密，這次事件很可能將使中美之間的關係進一步惡化。至於華為、TikTok等中國服務是否會受到這次駭客事件波及，則暫時還不明朗。

資料來源：Bloomberg、New York Times、華盛頓郵報、Krebs on Security
責任編輯：錢玉紘

國內

延伸閱讀：宏碁遭駭客REvil勒索天價14億元！成微軟漏洞受害者，官方證實：已通報各國執法機關

宏碁3月才剛遭同樣的駭客團體REvil透過零時漏洞，從海外子公司以釣魚信件滲透進主機，竊取資料後向宏碁兜售威脅，但宏碁並未理會，以各國報警處理及內部斷網掃毒方式強硬處理，一毛都沒支付。對此，宏碁董事長陳俊聖指出，因為無法確知駭客到底拿走多少資料，是真是假，所以根本不該理會。

責任編輯：錢玉紘

https://www.bnext.com.tw/article/62421/revil-quanta-hacker-macbook-air-leak

集團風險

犯罪黑數

去年起，台灣科技業、電子業不斷遭到駭客攻擊，牽連股東權益。（圖／本刊繪圖組）

Next

A+ A-

由於愈來愈多上市公司遭駭客勒索，證交所規定自4月27日起，上市公司若發現重大資通安全事件，必須及時發布重訊，以維護投資人權益；近來受惠於挖礦熱潮的威剛（3260），成了首間因重大資安事件而發布重訊的公司。

然而，並非每間公司都會遵守規定，本刊調查，新北市一間專營電子代工的上市公司旗下事業，比威剛早3天受到勒索軟體攻擊，且被要求支付500萬美元贖金，該上市公司卻未發布重訊，簡直就是漠視小股東的權益。

遭駭不重訊1／不甩證交所　上市公司旗下企業遭勒索卻裝死 | 財經 | CTWANT

妨害電腦使用案—刪除 資料庫 客戶資料

裁判日期：民國 110 年 12 月 09 日 裁判案由：妨害電腦使用.

事　實

一、詹逸鈞於民國105年3月30日起至106年9月30日，任職於喬美國際網路股份有限公司（下稱喬美公司），擔任JAVA技術經理，負責該公司所經營TFE臺灣資金交易所網站（該網站係儲存於AWS亞馬遜臺灣代理商鉿鍇國際股份有限公司雲端服務，下稱本案網站）前台及後台之程式開發，並取得本案網站得以PROBE方式透過外部網際網路直接登入、且具有刪改該本案網站資料庫權限之外掛帳號、密碼（下稱本案外掛帳密）等資訊。詎其離職後，竟以本案外掛帳密基於無故刪除他人電腦相關設備之電磁紀錄之犯意，於107年3月25日下午1時許，在臺北市○○區○○路0段000號11樓財團法人資訊工業策進會（下稱資策會）數位教育研究所，以所內電腦設備連結網際網路後，以PROBE方式透過外部網際網路直接登入本案網站，無故刪除本案網站客戶帳戶資料之電磁紀錄，致生損害於喬美公司對本案網站之管理運作。

✓ 詹逸鈞犯無故刪除他人電腦相關設備之電磁紀錄罪，處有期徒刑伍月，如易科罰金以新臺幣壹仟元折算壹日。

判例-妨害電腦使用罪-主文(刑事罪)

司法院法學資料檢索系統

匯出時間：111/09/12 01:36

裁判字號：臺灣士林地方法院 96 年訴字第 509 號刑事判決

裁判日期：民國 99 年 08 月 31 日

裁判案由：妨害電腦使用等

臺灣士林地方法院刑事判決　　96年度訴字第509號

公　訴　人　臺灣士林地方法院檢察署檢察官

被　　告　癸○○

選任辯護人　陳俊傑律師

上列被告因妨害電腦使用等案件，經檢察官提起公訴（95年度偵字第4126號），本院判決如下：

主　文

癸○○連續犯無故取得他人電腦之電磁紀錄罪，處有期徒刑壹年貳月，減為有期徒刑柒月。扣案筆記型電腦壹部沒收。

事　實

一、癸○○自民國95年1 月10日迄同年3 月9 日止，受雇於國際

資料來源：司法院法學資料檢索系統

罰則-刑法359條

【附表二】威林公司主張享有著作權之電腦檔案明細表及清冊。

附錄本判決論罪法條全文

中華民國刑法第359 條

無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處5 年以下有期徒刑、拘役或科或併科20萬元以下罰金。

行為時著作權法第91條第1項

擅自以重製之方法侵害他人之著作財產權者，處3 年以下有期徒刑、拘役，或科或併科新臺幣75萬元以下罰金。

判例-妨害電腦使用罪-上訴

裁判案由：
妨害電腦使用等
智慧財產法院刑事判決

99 年度刑智上訴字第 82 號

上　訴　人　簡威珉
即　被　告　　號
選任辯護人　張啟祥律師

上列上訴人因妨害電腦使用等案件，不服臺灣士林地方法院中華民國 99 年 8 月 31 日 96 年度訴字第 509 號第一審判決（起訴案號：臺灣士林地方法院檢察署 95 年度偵字第 4126 號），提起上訴，本院判決如下：

主　文

上訴駁回。

保密同意書/伺服器權限表

司事前書面同意，不得重製、「不可閱覽也不可重製」項下之檔案，則係指被告依威林公司伺服器使用權限表之規定，被告無權閱覽之檔案，且依保密同意書之約定，非經威林公司事前書面同意，不得重製，是被告將該等檔案內容重製存檔於扣案筆記型電腦內，被告使用之目的違反約定，又幾乎重製威林公司所有電腦檔案資料，利用之結果有害威林公司之研發市場競爭，顯非合理使用，其辯稱依著作權法第91條第4 項規定免責云云，亦無足採。

㈢承上，本院認定係屬遭被告侵害如附表二所示之285 筆著作，並非威林公司抄襲或複製他人作品，具有原創性，且具一定之表達形式，且非著作權法第9 條第1 項所定不得為著作權標的之著作，應認係受著作權法保護之著作，而由威林公司享有著作財產權，被告以其筆記型電腦非法擅自重製附表二所示之285 筆著作，違反著作權法第91條第1 項之犯行，亦堪認定。

控制作業 V.S 執行有效性

結果，伊將這些檔案存檔在接 HPLC 儀器之電腦內，未存檔於其他電腦，因此等數據檔案需特殊之軟體才能打開，連接 HPLC 儀器之電腦沒有設定權限，但只有研發部才能取得該等數據檔案，其他部門的人可以進來實驗室，但不可接觸連接 HPLC 儀器之電腦，伊有簽署保密同意書

1. 權限-特定人
2. 密碼管理
3. 檔案存取:
   限制範圍判斷
4. 書面同意

，查獲上開數據顯示之路徑中「LC 電腦資料」指連結 HPLC 儀器之電腦，「D 碟」指該電腦之 D 槽，「SISC32B」是操作 HPLC 軟體儲存數據的地方，上開路徑代表以進入「LC 電腦資料」、選取「D 碟」、「SISC32B」、「yujean」之順序取得檔案，非研發部人員可能進入實驗室，使用隨身碟將連接 HPLC 儀器之電腦後下載複製檔案，查獲之數據資料是在實驗室連接 HPLC 儀器之電腦列印出來，不是轉為 WORD 檔後之報告等語（見原審卷第 5 冊第 66 至 73、75 頁）。

(6)證人林晃儀證稱：伊在威林公司擔任協理之權限，伊接觸不到 HPLC 儀器，查獲之「新藥專利數據」伊無法接觸也看不到，即使輸入伊之電腦帳號、密碼也看不到，這不是伊之權限範圍，伊接觸不到研發、生產部門，伊有簽署保密同意書等語（見原審卷第 6 冊第 39、41、44 頁）

(7)綜上，附表一「第 8 頁檔案名稱明細表」、「第 9 頁檔案名稱明細表」所示之 438 筆「新藥實驗數據」電磁紀錄，係儲存於告訴人研發部門連接 HPLC 儀器電腦之檔案，並未存檔於公司伺服器，亦非被告基於協理職務之使用電腦權限範圍，係屬被告「不可閱覽也不可複製」之電磁紀錄。

控制作業(控制點)V.S 訴訟爭點

**書面同意

5.綜上所述，附表一右方所示屬於被告使用權限範圍內之「可閱覽但不可複製」電磁紀錄242 筆、非屬被告使用權限範圍「不可閱覽也不可複製」之電磁紀錄659 筆，共901筆，依被告與告訴人所簽訂之「保密同意書」約定，非經告訴人事前以書面同意，被告不得下載複製。

調查局資通安全處資安鑑識實驗室

鑑識結果 V.S 時間設定關鍵

鑑識意見認為：上開三個時間點，為**檔案上三個獨立之時間**標記，無必要之先後順序關係，一般而言，正常的應用軟體在設計時，檔案建立、修改，皆屬存取動作，故「Last Accessed 」（最後存取日期）通常會是最後的日期，但上述三種時間，皆會因使用的應用軟體設定而改變，網路上很容易可 取得隨意設定此三種檔案時間的小工具；就扣案筆記型電腦而言，使用人自其他電腦與附表一所示檔案從其他電腦下載、複製、貼上筆記型電腦時，未修改或編輯檔案內容，「Last Written」（最後修改時間）會記錄著該檔案原來在其他電腦時之最後修改時間；若使用人下載、複製、貼上檔案後曾修改或編輯檔案，「Last Written 」（最後修改時間）會變成檔案修改或編輯後存檔當時電腦的系統時間，至於「Last Written」（最後修改時間）是否會在「File Created」（檔案建立日期）之後，則需視當時電腦的系統時間是否正確或錯誤而定；以EnCase工具查看本案**電腦的系統資訊**，電腦的Last Shutdown Time最後關機時間為「2005年11月1 日」，明顯與檔案時間不符，故判斷因電腦系統時間設定錯誤，使檔案存取日期錯誤.

鑑識意見:出自調查局資通安全處資安鑑識實驗室

檢查頻次 V.S 資源度

證券期貨市場資通安全事件通報作業流程

每月至少查核乙次	AC-17010	(共用)通訊與作業管理－網路安全管理
每月至少查核乙次	AC-18000	(共用)存取控制
每半年至少查核乙次	AC-14000	(共用)資訊分類與控制
每半年至少查核乙次	AC-15000	(共用)人員安全
每半年至少查核乙次	AC-16000	(共用)實體及環境安全
每半年至少查核乙次	AC-17020	(共用)通訊與作業管理－電腦系統及作業安全管理
每半年至少查核乙次	AC-19000	(共用)系統開發及維護
每半年至少查核乙次	AC-20000	(共用)營運持續管理
每半年至少查核乙次	AC-21000	(共用)符合性
每半年至少查核乙次	AC-22000	(共用)其他
每年至少查核乙次	AC-12000	(共用)資訊安全政策
每年至少查核乙次	AC-13000	(共用)安全組織

資訊安全風險管理機制.pdf (gfortune.com.tw)

內控案例-態樣2-內神通外鬼

臺灣新竹地方檢察署新聞稿

發稿日期：110 年 12 月 24 日
聯絡人：主任檢察官高如應、鄒茂瑜
聯絡電話：03-6677999
編號：1101224001

本署聯手友○光電揪內鬼
起訴銷售部主管中飽鉅額回扣近億元
友○光電蒙受 24 億餘元價差損失

本署於 110 年 1 月間接獲法務部調查局新竹市調查站陳報，指出國內面板知名大廠友○光電經內部稽核發現銷售部主管有主導異常交易造成公司損失之情事，因金額鉅

承辦檢察官於起訴書特別敘明：被告蘇○寧及宮○治身為我國面板大廠友○光電銷售部高階主管，握有面板銷售之訂價權限，且業已坐領高薪，卻不思為雇主爭取最佳利益，反而利用己身所掌握的市場價格資訊，設計各種價差交易等非常規交易模式，藉以牟取私利，不惟造成友○光電的鉅額損失，且已造成臺灣廣大投資股民的損失，又將不法利益輸至大陸地區，間接削弱我國經濟實力，所為實屬不該，該 2 人犯後猶飾詞狡辯，隱藏犯罪所得，顯毫無悔改之心，建請從重量刑。

稽核制度-偵知機制

▲友達光電廠驚爆一名蘇姓銷售處長非法交易，不法獲利金額高達24億。（示意圖／記者湯興漢攝）

記者陳凱力／新竹報導

新竹地檢署今年1月間接獲竹市調站陳報，知名面板大廠友達光電(AUO)經內部稽核發現，銷售部蘇姓處長有主導異常交易造成公司損失情事，因金額鉅大，不只直逼友達一年淨利，還攸關投資大眾權益，新竹地檢署對其中2名犯嫌提起公訴，並請求法官從重量刑。

高層與專業人士白領犯罪-態樣3

潤寅詐貸470億 史上最高// 楊文虎夫婦 判25年、27年定讞

此外，楊文虎夫婦的女兒楊宇晨犯湮滅隱匿刑事證據、洗錢等罪，二審判刑2年2月，併科罰金100萬元。檢察官針對二審認定楊宇晨部分洗錢犯行無罪上訴，今天遭最高法院駁回，楊宇晨判刑2年2月定讞。

潤寅實業負責人楊文虎、王音之夫婦，以不實文件向12家銀行詐貸470億餘元，創下史上最高詐貸金額，高等法院判楊文虎25年、王音之27年，最高法院昨駁回上訴定讞。（資料照，本報合成）

高院認定楊文虎夫婦**犯十三件詐欺銀行罪**，各判廿五年、廿七年獲三審支持而確定。

專業人士(法官律師)犯罪/人性..??

公司資料

統一編號	13137009
公司狀態	核准設立，但已命令解散
公司名稱	潤寅實業股份有限公司
公司英文名稱	NEW SITE INDUSTRIES., INC.
資本總額(元)	329,000,000
負責人	楊文虎
登記地址	臺北市信義區信義路4段456號16樓

- 資料來源:https://youtu.be/MwxmHx4CS6g

2008~2020 12年歷程

潤寅集團以紡織貿易起家，從事化纖原料、橡膠、輪胎原料進口，旗下有潤寅、潤琦、易京揚、顥兆四家公司。楊氏夫婦二○○八年起以現金、水果禮盒收買多家上市公司和廠商幹部，合作製作假合約、發票、交易紀錄等不實申貸文件，向台企銀、星展、土銀、元大、王道、一銀、合庫、中信、玉山、上海、華南、兆豐等十二家銀行融資，十二年間詐貸四七○億餘元，得款除支付集團開銷，還買豪宅過奢華生活；夫婦雖「邊貸邊還」，至今仍滯欠四十三億四千多萬元。

向 12 家銀行邊貸邊還 仍欠 43 億多

串聯舞弊?
吹哨者制度?
內控與稽核制度?

高階犯罪手法-情境與被發現時間點

- 楊氏夫婦二〇〇八年起以現金、水果禮盒收買多家上市公司和廠商幹部，合作製作假合約、發票、交易紀錄等不實申貸文件，向台企銀、星展、土銀、元大、王道、一銀、合庫、中信、玉山、上海、華南、兆豐等十二家銀行融資，十二年間詐貸四七〇億餘元

銀行業者表示，潤寅集團提供的部分應收帳款，往來業務對象都很大咖，銀行也按正常程序去信徵信，只是部分往來對象沒有即時回應，等到發現異常，才察覺潤寅早與這些公司停止往來，提供的資料，可能是假交易。

1. 銀行函證—失效?→系統功能…?
2. 康友-KY…現金蒸發…..CPA/財報…???

內控制度與情境犯罪預防

Source: Internal Control—Integrated Framework, COSO 1992

- COSO於1992年發表了一份名為《內部控制—整合框架 Internal Control—Integrated Framework》的報告，COSO認為一家企業的良好內部控制必需擁有五大要素，包括Control environment (內控環境)， Risk assessment (風險評估)，Control activities (控制活動)，Information & communication (資訊與溝通)，和Monitoring (監督)。

情境犯罪預防內涵 V.S 資安新策略

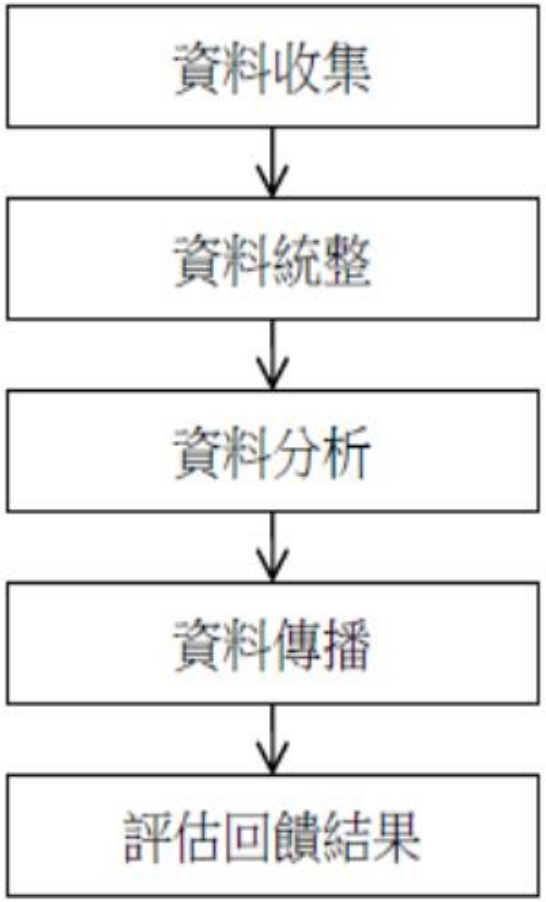
- **情境犯罪預防理論** 由克拉克(Situational Crime Prevention，Clarke，1980)首先提出，該理論強調犯罪受情境因素的影響，例如犯罪的時空、機會和條件等因素都可以影響犯罪人理性選擇和犯罪決定。

✓ **理性選擇:**
犯罪通常是由犯罪人對自己行為可能付出的代價與可能獲得的收益之間作成本效益分析的結果

✓ **日常活動:**
人們的**日常活動**影響著犯罪的三個必要條件，即犯罪動機、合適目標和缺乏犯罪抑制物在時間和空間上的聚合。

情境犯罪預防 與 犯罪分析步驟

- (一) 蒐集有關特定犯罪(資安案例)之因素與範圍等資料。
- (二) 分析助長犯罪可能性之情境條件。
- (三) 特定犯罪機會與成本效益分析。
- (四) 實施可行性最高且經濟預防方案。
- (五) 監視成效,並持續改善。



「情境犯罪預防」（Situational Crime Prevention）的五大策略內涵

主要策略內涵:

一、「增加犯罪阻力」的強化標的物防盜裝置等
二、「增加犯罪風險」的改善街道照明等防衛空間設計/CCTV…
三、「減少犯罪酬償」的車籍登記及機車烙印等
四、「減少犯罪刺激」的避免公布做案手法
五、「移除犯罪藉口」的公告性企業相關防治規範(霸凌/性騷擾/職安..)等。

。(資料來源:https://talk.ltn.com.tw/article/paper/1409780)

一般企業也適用-情境犯罪預防與內控

【超市收银员每天偷钱连偷7年 只为让丈夫刮目相看】湖南株洲一超市收银员，因工资低被丈夫瞧不起，于是偷盗超市的营业款，竟然还连偷7年！该女子几乎每天都要从收款机里拿走300元左右，最多的一天能拿走四五百，11年至今已经盗窃了50多万的营业款，自己买了两套房和一台车，而超市老板一直以为是经营状况不佳，多年来从未发觉……

情境犯罪預防技術

- Cornish 及 Clarke (2003) 說明的25項情境犯罪預防技術.

一、增加犯罪困難度	二、增加犯罪風險	三、減少犯罪後報酬	四、減少犯罪誘因	五、去除犯罪藉口
1.強化標的物 (1)門鎖 (2)商店連鎖	**6.延伸監控者身份** (1)職員便衣監控與公告 (2)加強賣場內部巡邏密度 (3)鼓勵顧客檢舉。	**11.藏匿標的物** (1)模型展示 (2)電視廣告 (3)空盒展示 (4)相片展示 (5)僅存放一個展示品(庫存放倉庫)	**16.降低挫折與壓力** (1)優惠價格 (2)增加服務品質 (3)增加附加價格達到一物多用的效果	**21.制定規範** 訂定商品優惠專案規定 健全社會制度、福利，避免將貧窮當藉口。
2.控制進入機構 (1)門禁管制 (2)倉儲／業務區禁止進入	**7.增強天然監控** (1)增加天然監視人潮 (2)明亮的照明 (3)透明牆壁	**12.標的物移除** (1)線上虛擬展示服務 (2)模型機展示	**17.避免爭執** (1)網路論壇提供討論 (2)提升服務態度 (3)投訴信箱 (4)顧客滿意度調查	**22.張貼告示** (1)宣傳竊盜檢舉獎金與公布檢舉方式 (2)警告標語
3.出口監控 (1)ＣＣＴＶ (2)便衣巡邏、監視	**8.降低匿名性** (1)會員卡 (2)特殊區域刷卡進入	**13.財物標示** (1)電磁感應標籤 (2)購買證明貼紙	**18.降低情緒誘因**	**23.激發道德意識** 政府及新聞媒體宣揚竊盜是不道德的行為
4.轉移犯罪意圖者 (1)免費贈品 (2)試用區	**9.運用管理人員** (1)售貨人員監控 (2)管理者不定期巡視	**14.瓦解犯罪市場** (1)加強查緝銷贓管道「二手商品拍賣市場」 (2)查緝夜市贓物。	**19.消除同儕壓力** 播放輕鬆音樂，使能舒暢身心購物。	**24.促進遵守規定** 妥善規劃設計商店內部設施，避免人潮洶湧引誘竊盜。
5.控制犯罪工具／促進物 (1)金屬探測器 (2)超音波掃描儀 (3)偵測偷竊、破壞工具	**10.強化正式化監控** (1)加強保全訓練 (2)制服人員巡邏	**15.否定犯罪利益** (1)正式購買附贈贈品及點數 (2)正式購買可上網增加保固年限	**20.防止模仿** (1)避免在新聞媒體播放竊盜手法。 (2)學校禁止傳播竊盜手法。	**25.控制毒品與酒類供應** (1)賣場及附近商店禁止販賣酒類 (2)對於有酒味顧客禁止進場或特別注意。

資安VS 個資外洩-個體損失28萬元-提告CASE…

9/10，TVBS報導
佳德鳳梨酥客人個資又外洩　團購主訂貨遭詐25萬元

台北知名糕點名店佳德今年1月遭駭客入侵竊取會員資料，造成顧客被詐騙集團騙走28萬元，當時佳德曾表示已加強電腦防護。但近日又有一名女客人下單後接到詐騙集團佯裝佳德客服人員騙走25萬元，導致她戶頭只剩下8百元，氣得向警方報案，揚言要告佳德。

資安事件-個資外洩與保護為例

‧‧‧‧案例一：旗下擁有萬豪、君悅、喜達屋及洲際飯店等多家飯店品牌的 HEI 飯店集團，日前傳出飯店系統遭植入惡意程式，導致集團經營的餐廳、飯店或其他休閒設施的顧客信用卡片資料外洩。客戶的信用卡片資料已被竊取，竊取的時間約在 2015 年 3 月 1 日至 2016 年 6 月 21 日間[6]。

‧‧‧‧案例二：鉅亨網記者陳慧菱 台北日盛金(5880)旗下日盛銀行新營分行行員，以不法方式在 5 年間挪用 17 位客戶款項，總共 4400 萬元，金管會對日盛銀行重罰 600 萬元。金管會銀行局表示，日盛銀行新營分行沈姓行員，從 2011 年至 2016 年 5 月間，以不法方式取得客戶網銀密碼私自轉帳、以投資高利或行員親屬存款誘騙客戶款項、謊稱投資保單，以及將客戶以金錢信託投資的基金贖回後挪用等方式，竊取客戶款項高達 4400 萬元，目前沈姓行員已被銀行解職，並遭警方收押。銀行局指出，日盛銀行內部稽核作業中未能發現異常情事，顯示日盛銀行有內部控制規定疏漏、未能落實執行內部控制等嚴重缺失[7]。

‧‧‧‧案例三：統一投信遭爆客戶個資外洩，因其內部網站未設定，造成目錄公開外洩客戶開戶文件、會員大名、電子郵件等相關個資，對此，統一投信坦承，已在第一時間啟動專案補救措施，除先以電話、郵件專案通知客戶，也向金管會報告，預計下周會將實質補償方案送金管會核准後就會立即執行[8]。

表 2:·個資安全保護措施與個資事件分析

個資法規範之安全保護措施	案例一 將客戶個資外洩--顧客信用卡片資料被竊取	案例二 員工以不法方式取得客戶網銀密碼，並私自轉帳，並以基金贖回後挪用等方式，竊取客戶款項	案例三 將客戶個資外洩-因內部網站未設定，造成目錄公開外洩客戶開戶文件
(A)配置管理之人員及相當資源	□	□	□
(B)界定個人資料之範圍	□	□	□
(C)個人資料之風險評估及管理機制	□	□	□
(D)事故之預防、通報及應變機制	□	□	□
(E)個人資料蒐集、處理及利用之內部管理程序	X	X	X
(F)資料安全管理及人員管理	X	□	□
(G)認知宣導及教育訓練	□	□	□
(H)設備安全管理	□	□	X
(I)資料安全稽核機制	X	X	X
(J)使用紀錄、軌跡資料及證據保存	□	□	□
(K)個資安全維護之整體持續改善	□	□	□
註:·標註X表示案件中明顯不符[個資法安全保護措施]要件			

資料來源:作者自行整理

內控防護 V.S 新因應措施考量面向METRIX

表 3:個資法安全保護措施與情境犯罪預防策略

個資法之安全保護措施	犯罪預防策略				
	增加犯罪阻力	提升犯罪風險	降低犯罪酬賞	削弱犯罪動機	移除犯罪藉口
(A)配置管理之人員及相當資源	V				V
(B)界定個人資料之範圍					V
(C)個人資料之風險評估及管理機制	V	V			V
(D)事故之預防、通報及應變機制				V	
(E)個人資料蒐集、處理及利用之內部管理程序	V	V			
(F)資料安全管理及人員管理	V	V			
(G)認知宣導及教育訓練				V	V
(H)設備安全管理	V		V	V	
(I)資料安全稽核機制	V	V		V	
(J)使用紀錄、軌跡資料及證據保存	V	V		V	
(K)個資安全維護之整體持續改善	V			V	

資料來源:作者自行整理

整合情境犯罪預防與內控防護措施

1. 事前預防措施 - 保護系統為例

1.未使用防毒軟體，未及時更新系統、軟體和應用程序：

2.-未安裝防毒/防惡意軟體並保持其病毒碼/惡意特徵碼更新: 每周至少對系統和路執行一次掃描

移動儲存設備(如：隨身碟)連接時應執行防毒掃描。

3. 未將系統、應用軟體更新到最新版本，並下載最新的安全更新檔。

4.未有效管理與啟用 Microsoft Office巨集：誘使受害者啟用巨集以查看檔案內容。

5.未執行最小化開放埠的設置：勒索軟體可能會利用對外曝露的服務和開放埠（例如 RDP埠3389和SMB 埠445）在網路中傳播。

6.未適當設定人員的最小使用權限：為了減少攻擊者獲得管理權限的機會，控制和限制存取權限，僅限於需要完整存取權限才能執行工作的人員獲得授權。

7.未禁用非活動帳戶。

8.未實施多因子身份驗證。

9.提高資安意識：未應定期對員工進行培訓,例如識別可疑電子郵件，不要隨意點擊連結，不打開未知或不受信任來源的電子郵件的附件，並進行社交工程演練，提高訓練成效。

10.保護資料為例: 3份備份、2種儲存媒體、1個不同的存放地點

增	提	降	削	移
加	升	低	弱	除
犯	犯	犯	犯	犯
罪	罪	罪	罪	罪
阻	風	酬	動	籍
力	險	賞	機	口

結論: 人與(資安)內控防護制度—企業基石

資安長 V.S 資訊長

強化資安 113家上市櫃今年要設資安長

工商時報 魏喬怡、彭禎伶 2022.06.21

Segregation of Duty （SoD）

法規要求—資安長/JD...

類別	標準	人力編制要求
銀行	國內所有銀行	指派副總經理以上，或職責相當之人兼任資訊安全長
保險	國內所有保險業者	1.都要設置資安專責單位及主管 2.資產達一兆元的業者，指派副總經理以上或職責相當的人兼任資訊安全長，同時也要設置資安專責單位，並指派協理以上或職責相當的人擔任主管
證期業	1.實收資本額100億元以上的證券商 2.實收資本額20億元以上的期貨商	資訊長= 資安長? 指派副總經理以上，或職責相當之人兼任資訊安全長

序號	2	發言日期	111/04/27	發言時間	17:18:45
發言人	谷元宏	發言人職稱	總經理	發言人電話	(02)2162-6688
主旨	公告本公司董事會通過設置資安長				
符合條款	第	8	款	事實發生日	111/04/27
說明	1.人員變動別（請輸入發言人、代理發言人、重要營運主管(如:執行長、營運長、行銷長及策略長等)、財務主管、會計主管、公司治理主管、研發主管、內部稽核主管或訴訟及非訟代理人）:資安長 2.發生變動日期:111/04/27 3.舊任者姓名、級職及簡歷:無 4.新任者姓名、級職及簡歷:林合壎；本公司資訊科技處處長 5.異動情形（請輸入「辭職」、「職務調整」、「資遣」、「退休」、「死亡」、「新任」或「解任」）:新任 6.異動原因:新任 7.生效日期:111/04/27 8.其他應敘明事項:無				

資安長向誰報告?

https://www.cio.com.tw/what-does-the-minister-of-security-report-to/

> *報告關係不只是組織圖上的線條而以，他們是權限的分派。最終，資安長報告向誰報告，反映的不只是個人的效率問題，而且更反應了組織的成熟度。*

文／Josh Fruhlinger 譯／高忠義

CIO.com 所進行的2019年資訊長當前情勢調查(State of the CIO survey)調查轉型中的產業。調查發現23%的高階安全主管向執行長報告，而將近45%的高階安全主管向資訊長報告。受訪者對於安全議題日益獲得高階管理人應有的考量似乎頗有信心：64%受訪者表示IT安全策略已緊密整合而變成公司整體IT策略與發展路線圖的一部分。

換句話說，安全長需要跳脫IT的巢穴。「資安長完全以IT為重心，因而棲身在資訊長之下的時代已經過去」Verodin 的資安長Brian Contos 這麼說。「安全效能管理與風險管理事務已經超越IT的領域，而且必須有高管層級的營運才能讓技術面與非技術面的決策者獲得有證據基礎的資料，藉由知情的地位提升事業決策的效率與效能。」

制度預防--風險/情境/機會(機率)-(調查局資料)

Q3 各部門發生貪瀆類型風險情事

白領犯罪與內稽人員
道 德 倫 理 之 衝 擊

調查專員兼組長 吳惠明

2021/08

部門名稱	股市犯罪	金融貪瀆	掏空資產	侵害營業秘密
財務部	32.5%	26.0%	27.9%	13.0%
業務部	20.5%	28.0%	20.6%	25.4%
研發部	7.3%	7.7%	6.7%	29.7%
採購部	34.4%	36.4%	41.7%	30.0%
其他	5.3%	1.9%	3.1%	1.9%
總計	100.0%	100.0%	100.0%	100.0%

資料來源:調查局專員 IIA例會分享資料

THE END-共好~!

- 情境犯罪預防與內控防護做得好,
- 達成內控三目標-”**銀髮族很有錢(財)**”~!
- 報告完畢/謝謝聆聽