



致理科技大學

資訊管理系專題報告

台灣 50 成份股企業 CSR 資安與個資保護觀察站

Taiwan's Top 50 Listed Companies CSR Information Security and Personal Data Protection Observatory

專題生：(10410209)張光祐
(10410210)楊子鎡
(10410225)王兆立
(10410230)張家豪
(10410237)李昱昌
(10410244)徐偉倫

指導教授：林裕淇 老師

中華民國 107 年 6 月

致理科技大學

資訊管理系

畢業專題

台灣50成份股企業CSR資安與個資保護觀察站

一〇六學年度

致理科技大學

專題報告審核書

本校 資訊管理 系（所） 張光祐

(10410209)、楊子鎰(10410210)、王兆立

(10410225)、張家豪(10410230)、李昱昌

(10410237)、徐偉倫(10410244)

等君所提論文 台灣50成份股企業CSR資

安與個資保護觀察站

經本委員會審定通過，特此證明。

口試委員會

委員： _____

指導教授： _____

系主任： _____

中華民國 107 年 6 月

致理科技大學

授權書

本授權書所授權之專題報告在致理科技大學

106 學年度第 2 學期所撰寫。

專題名稱：台灣 50 成分股企業 CSR 資安與個資保護觀察站

本人具有著作財產權之論文或專題提要，授予致理科技大學，得重製成電子資料檔後收錄於該單位之網路，並與台灣學術網路及科技網路連線，得不限地域時間與次數以光碟或紙本重製發行。

本人具有著作財產權之論文或專題全文資料，授予教育部指定送繳之圖書館及本人畢業學校圖書館，為學術研究之目的以各種方法重製，或為上述目的再授權他人以各種方法重製，不限時間與地域，惟每人以一份為限。並可為該圖書館館藏之一。

本論文或專題因涉及專利等智慧財產權之申請，請將本論文或專題全文延至民國 年 月 日後再公開。

上述授權內容均無須訂立讓與及授權契約書。依本授權之發行權為非專屬性發行權利。依本授權所為之收錄、重製、發行及學術研發利用均為無償。

(上述同意與不同意之欄位若未勾選，本人同意視同授權)

同意 不同意

學生簽名：

(親筆正楷簽名)

指導老師姓名：

(親筆正楷簽名)

中華民國 107 年 6 月 11 日

摘要

專題報告名稱：台灣 50 成份股企業 CSR 資安與個資保護觀察站 頁數：總頁數

校系別：致理科技大學資訊管理系

完成時間：106 學年度第 2 學期

專題生：張光祐、楊子鎡、王兆立、張家豪、李昱昌、徐偉倫

指導教授：林裕淇

關鍵詞：50 成分股企業、CSR 企業社會責任、資訊安全、個資保護

隨著科技快速的發展，資訊交流的狀況一言難罄，企業間的資安與個資保護也逐漸成為人們所關注的議題之一，但人們所能得知的相關資訊多而複雜，使得無法清楚瞭解相關內容，此狀況為促使我們訂定專題题目的發想。

在本專題之中提出了一個 CSR 資安整合搜尋平台，來解決使用者搜尋上的問題及提升人民基本素養。經過問卷調查，我們所擬規劃建置的 CSR 資安整合搜尋平台實現在解決使用者搜尋問題上。本專題所提出的方法，有以下的優點：

1. 相關類似網站較少，2. 符合最新流行趨勢，3. 提升公民素質等(請參考研究目的與系統功能綜合扼要描述)。

ABSTRACT

Thesis Title :

Pages :

University : Chihlee University of Technology

Graduate School : Department of Information Management

Date : June, 2018

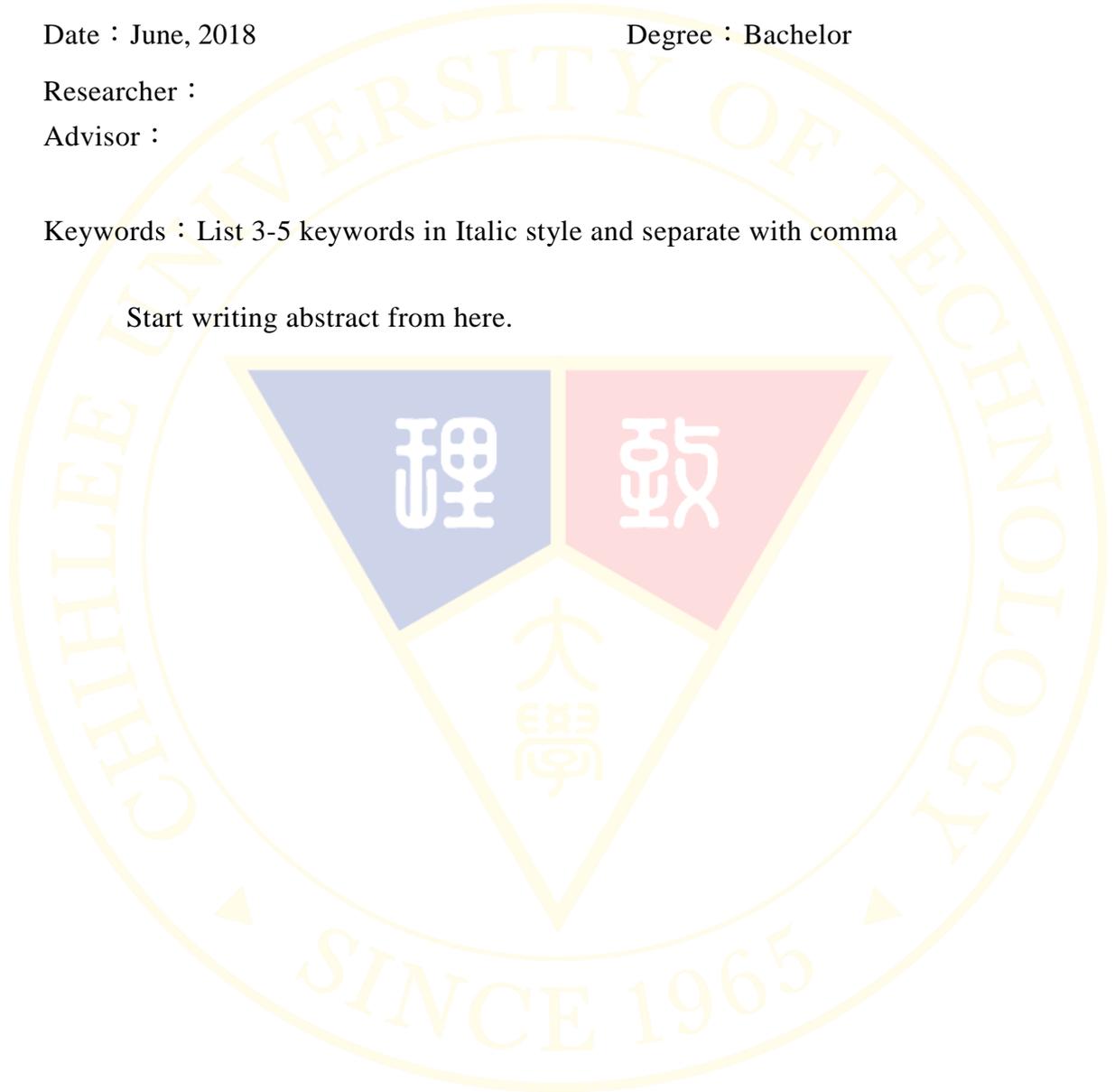
Degree : Bachelor

Researcher :

Advisor :

Keywords : List 3-5 keywords in *Italic style* and separate with comma

Start writing abstract from here.



誌謝

本次專題受到許多人的幫助，在此深表感謝。

首先，感謝指導老師林裕淇博士，在專題製作中有耐心的給予我們適當的建議與指導，使本次專題能夠順利完成。

感謝張慧老師，花了一學期的時間教導我們企畫書及簡報的製作，使我們呈現出來的報告能夠更專業及完整。

感謝陳昭伶老師，在我們建置網站的過程中遇到問題時，願意伸出援手，給予我們建議與相關資訊。

感謝所有陪伴我們完成專題的同學、朋友及家人，是你們給予我們鼓勵及支持，才使我們能熬過此次的專題製作。

最後感謝本組專題組員，在這一年之中，風雨無阻的到學校開會與討論，盡心盡力的找尋資料與程式撰寫，因為有你們的付出，才能完成這次的專題，謝謝你們，辛苦了。

徐偉倫、楊子鎰、張光祐

張家豪、李昱昌、王兆立 謹致

致理科技大學 資訊管理系學士班

中華民國 107 年 6 月

目錄

| | |
|-----------------------|-----|
| 中文摘要 | i |
| ABSTRACT | ii |
| 誌謝 | iii |
| 目錄 | iv |
| 圖目錄 | v |
| 表目錄 | vi |
| 第壹章 緒論 | 1 |
| 第一節 研究背景 | 1 |
| 第二節 研究動機 | 1 |
| 第三節 研究目的 | 2 |
| 第貳章 文獻回顧與探討 | 3 |
| 第一節 企業社會責任 | 3 |
| 第二節 資訊安全與個資保護 | 4 |
| 第三節 近年資安數字 | 8 |
| 第四節 2017 四大資安趨勢 | 12 |
| 第五節 ISO 27001 | 14 |
| 第參章 系統結構與運作 | 17 |
| 第一節 研究流程 | 17 |
| 第二節 研究方法 | 19 |
| 第三節 SWOT 分析 | 23 |
| 第肆章 網站建置與展示 | 00 |
| 第一節 產業現況分析 | 00 |
| 第二節 網站建置 | 00 |
| 第伍章 結論與未來展望 | 25 |
| 第一節 結論 | 25 |
| 第二節 未來展望 | 25 |
| 參考文獻 | 26 |
| 附錄 | 27 |
| 附錄一 畢業專題 系統操作手冊 | 28 |
| 附錄二 問卷 | 45 |

圖目錄

| | |
|---------------------------------------|----|
| 圖 3-1-1 研究流程圖 | 8 |
| 圖 3-2-1 男女比例 | 19 |
| 圖 3-2-2 年齡比例 | 19 |
| 圖 3-2-3 職業比例 | 20 |
| 圖 3-2-4 教育程度比例 | 20 |
| 圖 3-2-5 關注企業對社會貢獻 | 20 |
| 圖 3-2-6 何處得知資安資訊 | 21 |
| 圖 3-2-7 時常於網路提供個人資料 | 21 |
| 圖 3-2-8 您知道 CSR 嗎 | 21 |
| 圖 3-2-9 評論企業依據 | 22 |
| 圖 3-2-10 企業致力於資安保護程度 | 22 |
| 圖 3-2-11 您希望提供什麼服務 | 22 |
| 圖 4-1-1 Microsoft Visual studio | 24 |
| 圖 4-1-2 000webhost | 24 |
| 圖 4-1-3 SQL Server-1 | 25 |
| 圖 4-1-4 SQL Server-2 | 25 |
| 圖 4-1-5 SQL Server-3 | 26 |
| 圖 4-2-1 後台控制台 | 26 |
| 圖 4-2-2 後台頁面 | 27 |
| 圖 4-2-3 後台外掛 | 27 |
| 圖 4-2-4 會員登入與站內搜尋 | 28 |
| 圖 4-2-5 搜尋結果畫面 | 28 |
| 圖 4-2-6 數據資料庫 1 | 29 |
| 圖 4-2-7 數據資料庫 2 | 29 |
| 圖 4-2-8 訪客統計 | 30 |
| 圖 4-2-9 平台超連結 | 30 |

第壹章 緒論

本研究目的在於製作一個企業 CSR 資安與個資保護觀察網站，本網站將整合各大企業的 CSR 企業社會責任報告書及資安與個資保護相關關鍵字，以便於民眾及相關人士查詢。企業社會責任是一種道德或意思型態的理論，主要討論政府、股份有限公司、機構及個人是否有責任對社會做出貢獻，以報告書的方式，公開公司在社會責任及永續經營的目標規畫及成果發展。

第一節 研究背景

隨著科技不斷進步，網路犯罪不再是可以輕視的一件小事。在這充滿龐大資料的大數據年代，對於各大企業及政府機關在資安及個資保護方面，民眾早已不再置若罔聞，如何獲得民眾對企業的支持與信賴，已成為各大企業首當其衝的目標之一。

全球網路資安問題解決方案公司「趨勢科技」於今年初發佈 2016 資訊安全總評報告，並以「企業威脅刷新紀錄的一年」為題指出，勒索病毒與變臉詐騙越來越受網路詐騙集團的青睞，成為勒索企業的利器，其中光是勒索病毒就造成了全球各大企業損失高達 10 億美元，且勒索病毒新家族數量較 2015 年增加成長 7 倍，而台灣遭受此攻擊的次數排名更往前增加 20%，顯示資安問題對各大企業的影響有逐年增加之趨勢。

自 20 世紀初起，歐美等西方國家企業已意識到企業成長與社會發展的關係，逐漸以捐贈的方式來援助社會弱勢，並開始有了企業社會責任的發展。到了 20 世紀末期，全球化經濟持續蔓延，促使各國企業對傳統價值觀的改變，逐漸往自然資源、生態保護、勞工權益及企業倫理發展，更加承擔了社會及利益相關者的責任，國際上各企業也形成共識，逐漸改變原先企業的社會責任守則並創新，形成了全球性的社會責任契約。SA8000 是第一個用於第三方認證的全球社會責任標準，是一個自主而非強迫性的社會責任標準，但已經對於全球各大企業的經營、管理及活動帶來了不可小覷的影響。

我們這次的研究方向為企業社會責任中對於資安與個資保護的相關發展，現在網路社群發達，有心人士取得個資的方式變得容易且多元，為了解決大多數人對企業於個資保護方面的疑慮，我們選擇蒐集各企業的 CSR 報告書並整合出各企業對資安及個資保護所做的努力以及各企業對未來所做的防範趨勢，以供查詢。

第二節 研究動機

近年來有關資安及個資保護的事件頻傳，人民對政府及各大企業的信賴遞減。為了提供方便查詢及瞭解近幾年各大企業對資安及個資保護的相關策略，我們想整合各大企業所提供的 CSR 報告書，希望透過整合、分析能更清楚的知道相關議題，此為本研究動機之一。

大多數人並不知道企業每年均有提供 CSR 報告書供外界檢視，因此我們想利用這個機會，製作一個觀察網站，裡面統合了各企業近五年的 CSR 報告書，並利用相關關鍵字便能查詢相關事件，此為本研究動機之二。

藉由透過此觀察站的分析，再進階整理出台灣人較熟悉的 50 成份股企業針對資安相關問題所做的貢獻，並能清楚瞭解個企業未來對於資安問題所做的防範及趨勢，更加入關鍵字搜尋系統，使相關內容清楚分類，以便查詢，此為本研究動機之三。

第三節 研究目的

本研究依照動機方向規劃出三個目的：

- 目的一、本研究將收納整合台灣 50 成份股企業 CSR 相關報告數據。
- 目的二、本研究將分析所整合報告中與資安及個資保護相關關鍵字。
- 目的三、本研究將呈現近五年各大企業對資安及個資保護相關趨勢。



第貳章 文獻回顧與探討

我們將相關的文獻資料分為五節來探討，分別為企業社會責任、資訊安全與個資保護、近年資安相關數字、2017 資安趨勢及 ISO27001 的介紹，統整各界專家學者對相關議題的發言，讓我們對資安的世界更加瞭解。

第一節 企業社會責任

一、企業社會責任的三大理念

台灣證卷交易所公司治理中心網站(2014)指出，企業社會責任泛指企業在創造利潤、對股東利益負責的同時，還要承擔對所有利益關係人的責任，以達成經濟繁榮、社會公益及環保永續之理念。

(一) 經濟繁榮

1. 積極研發
2. 拓展通路
3. 專注本業經營
4. 創造股東價值
5. 創造就業機會
6. 帶動經濟發展

(二) 社會公益

1. 重視人權、兩性平等
2. 關懷社會、回饋鄉里
3. 勞資和諧、完善薪酬結構
4. 注重勞工安全
5. 保障消費者權益
6. 營造健康職場環境
7. 提供優良產品服務
8. 完善資安保護機制

(三) 環保永續

1. 實行節能減碳、推動綠色環保
2. 注重生態平衡、減少能源消耗
3. 炭足跡、水足跡盤查
4. 溫室氣體減量

二、國際間對企業社會責任的定義與規範

(一) 歐盟(2011)

企業對社會影響的責任。

(二) 世界企業永續發展協會(WBCSD)

企業為達成永續發展，共同與員工、家庭、社區與地方社會營造高品質生活的一種承諾。

(三) 世界銀行

企業與關鍵利害關係人的關係、價值觀、遵紀守法以及尊重人、社區和環境等有關政策和實踐的集合，是企業為改善利害關係人的生活品質而貢獻於永續發展的一種承諾。

三、全球化的企業社會責任

黃正忠(2006)於證券櫃檯月刊指出，全球化已經是不可避免的趨勢，而今反全球化抗爭卻又不斷擴大，因為勞動力、原料、市場、人才與群聚效應的競爭優勢等考量，國家與企業自然也都必須尋求對自身最有利的全球性投資與經營布局。楊雅智(2015)於證券暨期貨月刊指出，隨企業社會責任的盛行，國際間有關企業社會責任的規範、行為準則及相關資訊揭露及認證等發展日漸蓬勃，較廣為人知及重視者如聯合國全球盟約 (The UN Global Compact)、國際勞工組織公約 (International Labor Organization)、OECD 多國企業指導綱領 (The OECD Guidelines for Multinational Enterprises)、國際標準組織 ISO26000 社會責任指引及全球永續性報告第四代指南 (GRI G4 Guidelines) 等，這些規範及標準之發展與演進，係由包含政府、企業、勞工組織及非政府組織等不同利害團體共同參與討論而形成的，並多由公司治理、環境及社會等三大構面據以推動企業社會責任，以達到經濟、環境生態及社會之平衡及永續發展。

第二節 資訊安全與個資保護

一、資訊安全

中央研究院資料管理組網站指出，資訊可以有許多存在的形式，例如書寫、列印、電子媒體等；傳輸方式除了傳統郵寄、傳真之外，也能透過電子方式傳輸各種格式的電子檔案，包括影音、文件、圖片等等。不管任何形式的資訊，都應被視為資產，受到完整良好的保護，使資訊不會因為時間推移、存放地點變更，或者軟硬體升級而無法取得或識別，而資訊安全就是要保障機構內的資訊資產免於不可承受的風險。資訊安全有以下三項特性：

1. 機密性：適當保護資訊資產，讓資訊資產均為合法使用。
2. 完整性：維持資訊資產內容的正確與完整。
3. 可用性：確保資訊資產能隨時提供使用。

若上述三種資安的特性無法達成，造成服務的失效，對機關形象的影響為害甚大，因應各機關為確保資訊資料、系統、設備及網路通訊安全，並能有效降低因人為疏失、天然災害等導致之資訊資產遭毀損等風險的需求，資訊安全管理系統(Information Security Management System，簡稱 ISMS)是全世界普遍使用的方法，透過控制措施把資訊風險降到各機關可以承受的範圍。

二、個人資料與保護

林紫晴(2013)認為，個人資料的判斷標準為「得以直接或間接方式識別該個

人之資料」，及便未指名道姓，只要接露，及足以辨識為某一特定人之資料，及有個資法之適用。個人資料包含：自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。並提及以下相關資料：

(一) 個人資料保護法

台灣於 2012 年 4 月份完成修法，並經立法院三讀通過的《個人資料保護法》，簡稱個資法，行政院隨即在當年度 8 月份拍板定案決定分兩階段實施，其中除第 6、54 條條文施行日期，由行政院定之外，其餘較無爭議性的條文，定於 2012 年 10 月 1 號正式施行，且不再有緩衝寬限期，其適用對象包含了一般人(自然人)、企業(法人)或其他任何 3 人以上之團體。

早在 1995 年間，政府便已公布施行了《電腦處理個人資料保護法》，當時針對公務機關、教育、金融等八大行業，訂立以電腦系統處理個人資料的規範，故 2012 年施行的《個人資料保護法》，也被稱為新版個資法，因兩法案相距十餘年的時間，其時空背景皆已相差甚遠，法條內容也做了不小的更動，如表 2-1。

表 2-1.新舊版個資法比較

| | 舊版個資法 | 新版個資法 |
|------|---|------------------------|
| 全名 | 電腦處理個人資料保護法 | 個人資料保護法 |
| 適用對象 | 公務機關及徵信、醫療、學校、金融、 電信、證券、保險、大眾傳播等八大行業 | 所有行業、自然人、法人 |
| 保護範圍 | 經電腦處理之個人資料 | 所有個人資料(不限型式) |
| 賠償金額 | 每人二萬元至十萬元 單一事實最高總額二千萬元 | 每人五百元至兩萬元 單一事實最高二億元 |
| 舉證責任 | 受害者 | 被告單位 |

新版個資法與舊版個資法最主要差異為：適用範圍的擴張，不再侷限於特定行業以及數位資料；加重刑罰，相同原因產生的賠償金額合併計算，最高可達到 2 億元；採用被告舉證，由負責保管個資的單位提出資料安全無洩漏的證據。

(二) 自我個資保護

劉若芬(2012)認為，除了透過法律規範之外，民眾自我的警覺也不可或缺，尤其身處在危險的網路世界中，不得不更加謹慎，很有可能一不小心就洩漏的自己的個資，而遭到冒用，或是不小心就觸犯個資法。現今科技詐騙技術層出

不窮，養成好的電腦與網路使用習慣，可以防範在網路上洩漏個人資料，提供以下方法：

1. 安裝防毒軟體、防間諜及防火牆等保護軟體，定期掃描並時常更新病毒碼，將安全防護設定盡可能設定到最高等級。
2. 使用複雜密碼，包含數字、符號及大小寫英文字母，勿與個人名字或身份資料相關，並時常更新密碼。
3. 不要在電子郵件中索取銀行和信用卡資訊。
4. 進行線上購物時，盡量避免使用信用卡交易，若必須使用信用卡交易，確認在可信任的購物網站，並且在有安全保護機制，以 https:// 開頭之網址下進行信用卡交易。
5. 進行網路線上交易時，使用可信任的電腦，避免使用公用電腦，與無線網路。

除了防範自我個人資料洩漏外，也必須當心是否在網路上不小心觸犯個資法，例如網路群眾活動：人肉搜索，若沒有特定目的，而不當蒐集其個人資料並公開，或者在網路上未經當事者同意而蒐集並利用他人的個資，都有可能觸法。除了文字形式，影像紀錄也有可能涉及他人隱私，例如面貌、車牌、門牌等，在盡情享受網路自由時，網友們也應謹慎處理網路個人資料保護問題。

(三) 企業個資保護

張景皓(2012)指出，企業因應個資法該做好的安全維護措施分為以下 11 點。

1. 配置管理人員及相當資源

- 指派專員或成立因應小組，成員要涵蓋有個資的部門。
- 執行推動高層制定的個資政策或是同時負責制定企業個資政策與執行推動。
- 最重要的是要獲得高層的支持及有可支配的資源。
- 長期任務是審視企業個資保護落實情況，持續改善個資保護制度。

2. 界定個人資料之範圍

- 用個資盤點找出企業內部所有人的資料。
- 要從個資生命週期來盤點個資。
- 找出任何存放個資的載具，包括紙本或電子型式的個資。
- 可藉助盤點工具加快清查速度，但需瞭解盤點工具的局限。

3. 個人資料之風險評估及管理機制

- 先評估資料的價值才能採取適當的風險措施。
- 可依資料機密性、完整性和可用性來評估價值。
- 不同等級的風險要有不同的應變措施。
- 可參考 ISO27001 風險評鑑的作法來評估個資風險。
- 可採取隱私權衝擊分析的作法來評估個資風險。

4. 事故之預防、通報及應變機制

- 依不同風險等級來制定通報應變程序和通報對象。
- 個資事故依法必須通知個資當事人。
- 從事故中記取教訓找出預防措施。
- 積極處理事故，若處理得宜可補救企業形象。

5. 個人資料蒐集、處理及利用之內部管理程序

- 依蒐集、處理及利用的法令規範來訂定作業流程。
- 蒐集個資時要告知使用目的。
- 間接蒐集的個資則用於使用前補行告知。
- 個資處理及利用要符合目的。
- 增加新的用途時要重新告知當事人。

6. 資料安全管理及人員管理

- 資料要分級管理，可依資料敏感程度、風險高低來分級訂定不同管理方法。
- 個資使用或傳輸時若沒有必要完整顯示時，就要部份遮罩或去識別化處理。
- 建立紙本文件與電子檔案的存取控管流程。
- 內涵個資的資料傳輸過程要加密以避免外洩。
- 要依員工職務分級管理個資存取權限，而非人人都可以查詢。

7. 認知宣導及教育訓練

- 用教育訓練讓員工瞭解日常工作處理個資的態度和原則。
- 可依不同的職務規劃不同課程內容。
- 教育訓練內容和實施的紀錄要保存備查，訓練教材也要對內公開。
- 可用個資考試來檢驗教育成效。

8. 設備安全管理

- 凡是可儲存個資的設備，不論是固定設備或行動設備都要納入制度管理裡。
- 設備管理政策要充分告知員工。
- 存放大量個資的資料庫及機房要嚴加控管。
- 開放員工自帶設備上班要加強端點控管。

9. 資料安全稽核機制

- 舉行內稽可瞭解企業個資保護制度落實程度，找出需改善的問題。
- 稽核有三種，分別是內部稽核、行政檢查和外部稽核。
- 稽核過程分為文件審查及實地審查兩階段。
- 稽核小組成員要有良好的溝通技巧。
- 內部稽核人員不能稽核自己的職務。

10. 使用紀錄、軌跡資料及證據保存

- 要從日後訴訟舉證角度來保存各種軌跡證據使用紀錄。
- 可成立專責文件控管小組來保存紙本文件。
- 個資使用紀錄和軌跡紀錄至少要保存 5 年。

11. 個人資料安全維護之整體持續改善

- 要定期持續檢討，並非發生事故才需要改善。
- 高層主管要定期召開審查會議，審視個資保護制度落實程度。
- 持續改善制度文件、會議紀錄與實施紀錄都要保留。

第三節 近年資安相關數字

一、企業高層最易成為詐騙目標

趨勢科技(2016)資深技術顧問簡勝財指出：「最常見的變臉詐騙手法為社交工程攻擊，主要鎖定需與國外廠商合作，並定期匯款的國際貿易公司，透過入侵其電子郵件帳號方式，進行詐欺性轉帳。根據趨勢科技進一步針對變臉詐騙的全球監控資料研究分析顯示，最常遭詐騙份子假冒的職務是執行長，其次為總裁和總經理。詐騙份子會入侵企業高層主管電子郵件帳號，並假冒該主管名義進行公司內部電子郵件發送，要求員工將款項匯至歹徒掌控的帳戶進行詐騙，通常具有匯款權限的財務長(CFO)則是歹徒最常鎖定的目標，高達 40.38%。」

根據 FBI 的最新統計，過去兩年當中，變臉詐騙攻擊或稱為商務電子郵件入侵 (Business Email Compromise, 簡稱 BEC) 詐騙案例總計已至少造成了將近 31 億美元的損失，全球約有 22,000 家企業受害。從 2015 年 1 月至今，企業機構通報的損失金額已成長了 1,300%，平均每一詐騙案例的損失高達 140,000 美元，由於這類詐騙行動的潛在損失與影響驚人，FBI 不得不發出一份民眾服務公告來詳述 BEC 詐騙的運作過程，以及可能對受害員工和企業造成多大的損失。

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，專門鎖定有外國合作廠商且需定期匯款給廠商的企業。BEC 其實就是之前大家所知道的中間人電子郵件詐騙，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，然後假冒該主管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到外國帳戶。

儘管有些案例會運用到惡意程式，但絕大多數的 BEC 詐騙都是單純利用所謂的「社交工程技巧」，因此一時很難察覺，從近期的一些案例可以看到，員工很容易被假冒公司高層主管要求提供資訊的電子郵件所騙。BEC 詐騙共分為以下五種版本。

(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「發票更改詐騙」，受害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的電話、傳真或電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額匯到另一個歹徒所掌控的帳戶。

(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，假借高層主管的名義要求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「緊急匯款」的電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行，這類詐騙一般稱為「執行長詐騙」、「企業高層主管詐騙」、「假冒名義」或「金融產業匯款詐騙」。

(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。

二、ATM 相關資安事件頻傳

趨勢科技全球技術支援與研發中心(2016)指出，資安產業和執法機關已意識到，ATM 也開始成為駭客攻擊的目標。早在幾年之前就有資安研究人員發現專門攻擊 ATM 提款機的惡意程式，而且也實際看過歹徒得逞的案例。在這些案例中，歹徒使用的是專門針對 ATM 設計的惡意程式。從實體轉到數位的犯案手法，意味著犯罪集團已經發現一項事實，那就是：採用惡意程式來竊取提款機中的鈔票或提款卡資料，反而更輕鬆、更隱密。看來，這股趨勢未來只會更加嚴重，因此值得我們來探討一下網路犯罪集團目前已知的幾種 ATM 攻擊手法。

(一) ATM 相關事件與實體攻擊

ATM 相關詐騙和攻擊數量在過去幾年大致呈現上揚的走勢（ATM 相關詐騙與攻擊從 2014 至 2015 年成長了 15%）。意味著精明的網路犯罪集團已意識到駭客工具在該領域的潛在應用商機。儘管我們手上並無 ATM 惡意程式在美國地區的攻擊數據，但根據歐洲 ATM 資安團隊指出：「國際上已出現許多損失案例，在單一歐元支付區（Single Euro Payments Area，簡稱 SEPA）之外的國家和地區就有 53 起案例，而在 SEPA 區域內則有 10 起案例。前三名的地區分別是美國、印尼和菲律賓。」（趨勢科技，2016）。

(二) ATM 惡意程式如何興起

趨勢科技與歐洲刑警組織（Europol）的歐洲網路犯罪中心（European Cybercrime Center，簡稱 EC3）針對 ATM 網路威脅的發展進行了一項共同研究。根據我們的研究顯示，犯罪集團之所以會利用駭客工具來搭配傳統的 ATM 竊盜手法，背後有多項因素。其中一項主因是某些 ATM 提款機仍在使用過時而再也無法獲得安全更新的作業系統（如 Windows XP®）。另一項原因是犯罪集團意識到數位犯罪手法的風險更低，而且可以暗中移動。還有另一項重要因素是 ATM 廠商會透過一個名為「金融服務延伸功能」（eXtensions for Financial Services，XFS）的中介軟體所提供的應用程式開發介面（API）來操控各類型的提款機周邊裝置（如：密碼輸入鍵盤、吐鈔機等等）。簡單來說，若我們將今日的 ATM 提款機看成一台 Windows® 電腦加上一個軟體操控的鈔票箱，這樣就不難理解為何 ATM 提款機會成為惡意程式作者覬覦的目標。（趨勢科技，2016）。

三、IoT 與 DDoS 攻擊

趨勢科技全球技術支援與研發中心(2016)指出，DNS 服務商 Dyn 所遭遇的大規模分散式阻斷服務攻擊 (DDoS)攻擊敲響了一記警鐘：物聯網生態鏈已經徹底、完全地被破壞。缺乏支援和不安全的設備造成網際網路基礎設施一個重要的部分斷線，影響了許多知名網站。臺灣 2016 年 10 月 21 日傍晚 19 點 10 分，Dyn 管理的 DNS 服務系統遭到 DDoS 攻擊，造成多數網站無法使用，其中較知名的有：CNN、Airbnb、Spotify、Netflix、HBO 等。這起攻擊中，駭客控制數千萬件物聯網 (IoT) 裝置，包含網路攝影機、監視系統、無線網路基地台等，命裝置發動攻擊。影響延續約 8 小時，直到台灣時間隔日早上 8 點才完全修復。

(一) 攻擊起因：監視/網路攝影機感染 Mirai 僵屍網路

這起攻擊來自何處？大部分都是感染了 Mirai 惡意軟體的物聯網設備所造成，趨勢科技將其偵測為 ELF_GAFGYT.DGB/ELF_BASHLITE.SM。(Mirai 魁儡殭屍網路原始碼已經在 10 月初公開發布，恐遭有心人士惡意利用)。關於攻擊的大部分原因是一家白牌的數位網路監視攝影機和網路攝影機。這家廠商已經公開召回他們一些具有漏洞的設備，這是一個值得鼓勵 (可能代價高昂) 的舉動。不過，也很可能有其他廠商的設備也參與其中。(趨勢科技，2016)。

(二) 類似攻擊未來未必不再發生

要將這些攻擊說是「前所未有」是有點勉強，Brian Krebs 也曾遭受到 Mirai 「Botnet 傀儡殭屍網路」的 DDoS 攻擊。可以肯定的是，在找到方法保護好物聯網前，這起攻擊並不會是最後的一次。而關於物聯網 (IoT, Internet of Thing)，現在的優勢是在攻擊者那方：有太多物聯網設備是不安全，無法保護，也不會受到保護。阻斷服務攻擊成為更加有力的威脅：威脅公司會斷線變成實際可行也更具說服力的說法。

物聯網產品自己也會因分散式阻斷服務攻擊 (DDoS) 攻擊而產生對現實世界的影響，當這些設備無法連到中央伺服器時會發生什麼事？比如這個例子，一個可根據溫度來智慧決定要不要加熱的恆溫器，因為網路斷了拿不到數據，結果就不停的加熱，號稱比較省電的裝置卻適得其反，無法正常運作。DDoS 攻擊曾經只是會造成困擾的事情。而現在隨著越來越多重要功能放到網路上，這成為了嚴重的威脅。(趨勢科技，2016)。

(三) 購買家電的潛在威脅

根據趨勢科技美洲地區公共建設之網路安全報告。分析連網裝置受到攻擊的方式，約有七成曾受過釣魚式攻擊 (Phishing)、五成受過漏洞攻擊 (Unpatched vulnerabilities)、四成則受過分散式阻斷服務攻擊 (DDoS)。另外，勒索病毒 Ransomware (勒索軟體/綁架病毒) 攻擊也是一新犯罪趨勢。

很顯然地，必須做些什麼來保護物聯網。不幸的是，再怎麼說這有多困難都有些輕描淡寫了。我們不能期望使用者突然成為專家來保護自己的設備，因為使用者不會關心他們家的網路攝影機，或是智慧型電視機等聯網裝置，正對別人發動 DDoS 攻擊，除非突然電視掛掉不能看了，因為人們通常只關心類似這樣的問題：我要看電視時要隨時可以看。當人們購買冰箱，電視...等智慧型家電時，會考慮價錢、外型和功能，鮮少有人會將連網設備的安全列入採買要素。(趨勢科技，2016)。

(四) IoT 生態鏈缺口

網路安全專家把這種威脅比作「好像每個人都有一顆核彈」，那物聯網產品賣家呢？他們並非每個人都足夠的技術和能力來解決自己所賣東西的問題。在某些情況下，這些賣家只是拿白牌產品來貼牌而已。經銷商和進口商是否真的能夠支援自己所賣的產品？答案是：可能不行。

加拿大網路安全專家在接受 CBC 採訪時說，侵入工作站或 Windows 的裝置是比較困難的。但是由無數小公司生產的便宜的智能電子產品，在安全防護上非常初級。而目前對這個行業的管理缺乏相關法規，使那些不想在安全上投資的小公司有漏洞可鑽。駭客侵入這些產品如入無人之境，然後可以透過它們發動大規模的網路攻擊，例如發送海量垃圾信息導致網站癱瘓。另一位網路安全專家把這種威脅比作「好像每個人都有一顆核彈」。

那麼物聯網產品的實際製造商呢。不幸的是，業務壓力讓這些設備的售後支援都很差。安全性並非優先考慮的事項「易於使用、全新功能和快速上市才是。物聯網代工並沒有理由投資在安全性上」不會有廠商因為產品安全性不夠而沒有生意。此外，長期支援需要花費時間、資源和金錢 - 這些都是製造商希望減少的事情。總之，沒有人有動機去做對的事情 - 保護他們的物聯網設備。就安全性而言，物聯網生態鏈是崩壞的。(趨勢科技，2016)。

(五) 物聯網安全性

長遠來看，物聯網的安全性將會變得更好。不安全的物聯網產品所造成的後果顯而易見，將被認為不安全甚至是非法的。你不能販賣不安全的汽車或電器 - 未來你可能也不能販賣開放 telnet 連線的網路攝影機。

物聯網產業該如何更好地製造安全的設備？他們必須學習更佳的安全實作，不然就可能無法銷售自己的產品。對安全風險具備簡單的認知就足以消除目前物聯網設備最嚴重的漏洞。趨勢科技等安全廠商也在致力於一般消費者可用來保護自家網路的技術和產品。(趨勢科技已經能夠偵測 Mirai 惡意軟體，我們的 TippingPoint 產品也能夠偵測 Mirai 的相關網路流量)。

我們已經看到進步的跡象，無論是產業或監管單位。歐盟委員會正在考慮新法規來涵蓋物聯網設備的安全性。產業團體發布了防護物聯網設備的藍圖。我們看到這整個生態鏈開始認真地對待安全性，而這時間點已經有些急迫了。

要從不安全的生態鏈轉變成安全並非一蹴可幾。在我們想辦法達成目標前，還可能會看到不安全物聯網產品所造成更加嚴重的安全事件。需要物聯網產業、安全廠商和監管單位的協助來盡快地完成此一轉變。(趨勢科技，2016)。

四、行動裝置勒索病毒

趨勢科技全球技術支援與研發中心(2016)指出，近年來，趨勢科技目睹個人電腦勒索病毒 Ransomware (勒索軟體/綁架病毒) 稱霸資安威脅版圖，不論數量和破壞力都前所未見。但現在，網路犯罪集團已開始將矛頭指向另一個目標：Android 行動裝置平台。根據我們的研究顯示，2016 年 6 月 Android 勒索病毒威脅較 2015 年 4 月成長了 15 倍。

(一) 行動裝置如何散播勒索病毒

行動勒索病毒會冒充正常應用程式、熱門遊戲、Flash 播放程式、視訊播放程式或是系統更新，經常出現在非官方應用程式商店（趨勢科技至今仍未在 Google Play 商店上發現任何勒索病毒威脅）。此外，你也可能因瀏覽色情網站、網路論壇或點選簡訊中的垃圾連結而遭到攻擊。（趨勢科技，2016）。

(二) 行動裝置勒索病毒如何運作

趨勢科技首次發現行動裝置勒索病毒是在 2014 年 4 月。當初發現的是會「鎖住螢幕」的變種，它會鎖住你的行動裝置，直到你支付贖金為止。你若不支付贖金，那就得重新購買一支手機，如果你檔案都已經儲存在雲端，或許心不會這麼糾結。有時，勒索病毒會謊稱你的裝置已被當地的執法機關鎖住，你必須支付一筆「罰款」才能解開。趨勢科技曾發現一個特殊的行動裝置勒索病毒會竄改你解鎖裝置的 PIN 碼。我們首次發現是在 2015 年 3 月，它跟鎖住裝置的勒索病毒類似，差別只是它利用裝置本身的安全機制來對付你，直到你付錢為止。（趨勢科技，2016）。

第四節 2017 四大資安趨勢

黃泓瑜、黃彥霖(2017)指出，資料外洩事件頻傳，2016 年光美國外洩資料高達 15 億筆。勒索軟體災情哀鴻遍野，7 成企業認賠付款。殭屍木馬挾持百萬 IoT 裝置，DDoS 攻擊威力更達到了 Tb 級，關鍵基礎設施網攻威脅拉警報，破 6 成業者嚴陣以待。

一、資料外洩事件翻倍爆增

雅虎在 2016 年 9 月揭露在 2014 年遭到駭客入侵資料庫，造成 5 億筆用戶個人資料外洩，之後又在 11 月坦承有超過 10 億筆帳戶也在 2013 年被駭客竊取，總計有超過 15 億雅虎用戶的個人資料流傳在各個駭客論壇之中。大多數長期使用雅虎服務的用戶，擔心自身是否也是在外洩名單裡面，被有心人士做不當的使用，動搖對雅虎信任。

雅虎這兩起外洩事件，讓 2016 年成為近五年來資料外洩筆數最多的一年。根據美國隱私權資訊中心 (Privacy Rights Clearinghouse) 數據顯示，2016 年共有 1,583,926,656 筆資料外洩，跟 2015 年相比多了 9 倍，發生資料外洩案件數比 2015 年增加近 1 倍，甚至駭客還在地下論壇免費提供 2.7 億個 Gmail、Hotmail、Yahoo 用戶個人資料給其他人利用。

美國隱私權資訊中心指出，駭客侵入資料庫以及植入惡意程式的行為，是 2016 年發生資料外洩案件最主要的原因，駭客鎖定 POS 機和 ATM 植入惡意程式，讓用戶使用信用卡或支付卡感應付款時，能同時竊取信用卡資料。例如 2016 年 6 月美國溫娣漢堡就有 300 家連鎖店支付系統遭惡意程式感染，竊取了使用者支付卡資料，以及 10 月印度國家支付公司所使用的 POS 機，也遭惡意程式感染，造成 326 萬張支付卡資料外洩。（黃泓瑜，2017）。

二、勒索軟體風暴狂襲

由於勒索軟體是最熱門的網路犯罪手法，美國 FBI 評估，2016 年勒索軟體美國網路犯罪規模超過 10 億美元，相較 2015 年全年勒索軟體犯罪規模只有 2,400 萬美元，成長超過 40 倍。

勒索軟體危害在 2016 年達到高峰，除了出現勒索軟體即服務 (Ransomware-as-a-service) 或是拉 2 位下線可免費解密的營運模式外，勒索軟體綁架對象已經從傳統電腦和伺服器，擴散到手機及智慧連網電視等新興連網裝置。上述這樣的轉變，也讓勒索軟體仍然是 2017 年最嚴重的資安威脅之一。

不過，勒索軟體帶來的嚴重威脅，卻也促進資安業者的團結，例如，包括許多執法單位和資安公司便通力合作，推出「No More Ransom」(勒索軟體不要來) 專案網站，提供各種勒索軟體解密金鑰，希望遏止勒索軟體帶來的危害。以下為常見 5 種勒索軟體類型。(黃彥茶，2017)。

1. 加密檔案勒索型:加密個人檔案和目錄來勒索贖金，常要求用比特幣來躲避追蹤。
2. 鎖定螢幕勒索型:鎖定電腦螢幕勒索贖金但不加密檔案，已出現攻擊數位電視案例。
3. 加密網站伺服器勒索型:利用常見 CMS 軟體漏洞，入侵網站伺服器，加密內部檔案來勒索。
4. 綁架 MBR 勒索型:綁架作業系統 MBR 開機磁區，導致電腦無法開機，付款才解鎖。
5. 行動裝置勒索型:目前鎖定的行動裝置以 Android 作業系統最常見，經常使用「路過式下載」手法入侵行動裝置後將裝置變磚塊，付錢才解凍。

三、Tb 級 DDoS 攻擊越演越烈

殭屍網路 Mirai 於 2016 年 9 月現身之後，造成全球網路世界開始發生好幾起大規模 DDoS 攻擊事件，最高攻擊流量甚至超過 1Tbps，超越過去 10 年以來 DDoS 攻擊的最高流量紀錄。它掌控著超過 200 多萬臺 IoT 裝置作為攻擊的兵力，隨時發動超過 500Gbps 以上規模的 DDoS 攻擊都是家常便飯。

駭客近年開始侵入 IP 攝影機、CCTV 攝影機、路由器等有嵌入 Linux 作業系統的 IoT 裝置，作為殭屍網路的兵力。例如，2016 年 9 月的 OVH 遭攻擊事件，殭屍網路 Mirai 操控超過來自全球 14 萬臺 CCTV 網路攝影機發動攻擊。同月，知名資安部落格 Krebs On Security 也遭到殭屍網路 Mirai 所操控的 24,000 臺的 IoT 連網裝置攻擊。

資安業者 Flashpoint 分析前述兩起攻擊事件發現，遭到控制的 IoT 裝置大部分來自中國製造商「雄邁」生產的機板。這些遭駭客控制的 IoT 裝置，都是內建同樣的憑證、採用固定預設的使用者名稱 root 及固定密碼 xc3511，並且允許遠端駭客透過 Telnet 存取。駭客可以更輕易地利用這些 IoT 裝置上的安全漏洞，植入惡意程式感染其裝置，收服這些 IoT 裝置成為殭屍網路的攻擊火力。除此之外，殭屍網路 Mirai 作者 Anna-senpa 在去年 10 月時，在地下駭客論壇公開 Mirai 原始碼，促成新變種殭屍網路形成。

根據 Level 3 威脅研究中心研究估計，開放原始碼之後，殭屍裝置的數量從

21.3 萬臺增加到 49.3 萬臺，Mirai 殭屍網路的規模成長了一倍。之後，資安公司 Imperva 發現新的殭屍網路 Leet，可發動高達 650Gbps 的 DDoS 攻擊，攻擊規模與殭屍網路 Mirai 攻擊 Krebs On Security 的強度相當。

目前，根據 Malwaretech 殭屍網路偵測網站監控結果，發現殭屍網路 Mirai 的攻擊裝置來源遍布全世界，而且每天幾乎都有 5 萬臺以上的殭屍裝置上線，隨時都做好攻擊的準備。此外，Incapsula 分析殭屍網路 Mirai 發動 DDoS 攻擊裝置來源國家顯示，臺灣也在殭屍網路 Mirai 的攻擊裝置來源前十名的國家裡面，位居第 8。說明臺灣也處在這股 IoT 殭屍網路攻擊風暴，難以置身於事外。(黃泓瑜，2017)。

四、連網威脅驟升

隨著工控系統連網比例逐漸增加，也對關鍵基礎設施 (CIP) 隨之帶來許多網路攻擊和威脅，根據市場研究調查公司 MarketandMarkets 在 2016 年 6 月做的統計，全球工控系統安全的產業規模預估從 2016 年的 90 億美元，成長到 2021 年 126 億美元，年複合成長率 7%。

而工控市場規模的增加主要是因為網路威脅，使得這些大量使用工控系統的關鍵基礎設施業者，必須大幅增加相關的安全解決方案而造成的結果。

根據 MarketandMarkets 研究，北美地區也是工控安全最大的市場，會在 2016 年~2021 年掌控全球工控網路安全市場，而大型的工控安全業者，則包括 IBM、CSC、McAfee、洛克西德馬丁 (Lockheed Martin)、Palo Alto 等。而這些工控安全業者則希望協助電廠、交通、水資源與垃圾處理、汽油和瓦斯以及其他的製造工廠等關鍵基礎設施業者，可以確保免於像是 Stuxnet、Blackenergy 以及 Night Dragon 等網路威脅，有效提升網路安全防護與偵測能力並減緩潛在的威脅。

也因為工控市場資安產業規模增加，許多關鍵基礎設施成為駭客鎖定攻擊標的，2015 年耶誕節前夕，烏克蘭電廠爆發長達 6 小時的大停電，影響超過 70 萬人，這起事件就是工控系統被感染惡意程式 Blackenergy 所造成。經此事後，更提升各國對關鍵基礎設施安全性的重視。(黃彥茶，2017)。

第五節 ISO 27001

一、ISO 27001 資訊安全標準

沈柏村(2010)於金融聯合徵信雙月刊第十一期中介紹，國際標準組織 (International Organization for Standardization, ISO) 於 2005 年 10 月 15 日公佈 ISO 27001 資訊安全標準 (全名是 ISO/IEC 27001:2005 - Information Security Management Systems Certification)，是一種國際認可的資訊安全管理體系 (Information Security Management Systems) 驗證標準；ISO 27001 資訊安全標準是從英國標準協會 (British Standards Institution) 提出之 BS7799-2 標準 (全名是 BS7799 Information technology-Security techniques Information security management systems Requirements)，延伸整合而成的國際資訊安全標準，其演進過程如下：1995 年：英國公佈 BS7799 Part I 1998 年：英國公佈 BS7799 Part II 1999 年：英國公佈新版 BS7799 Part I、Part

II 2000 年：ISO 通過成為 ISO/IEC 17799 Part I 2002 年：BS7799：2-2002，成為資訊安全管理系統驗證規範 2005 年：ISO/IEC 17799：2005 2005 年：BS7799：2-2005，2005 年 10 月 15 日 成為國際標準 ISO27001，ISO 27001 資訊安全標準的規範要求，是一般性且可廣泛應用的，適用於任何型式的組織，並不限制組織規模大小和營業性質；因此，只要組織在經營策略上有必須取得 ISO 27001 資訊安全標準認證，皆可參考及依照 ISO 27001 資訊安全標準的規範，訂定欲取得認證的範圍，制定符合且適當的資訊安全制度文件及控制措施，運用「計劃、執行、檢查、行動」(Plan-Do-Check-Act, PDCA) 持續改進模式運作，在整體資訊安全管理制度落實後，即可請驗證單位（例如：BSI、SGS、DNV）進行 ISO 27001 資訊安全標準驗證作業。（沈柏村，2010）。

二、通過驗證之效益

通過 ISO 27001 資訊安全標準驗證，對於組織（企業）而言，至少可以產生以下三點效益：（一）確保企業核心競爭力，保護營業機密，防止資訊之濫用；（二）保護客戶財產，對提供作為使用或組合成為產品之顧客財產（包括智慧財產），可予以識別、查證、保護及安全防護；（三）確保企業生產力，防止資訊之誤用與意外災害，確保業務永續運作。（沈柏村，2010）。

三、ISO 27001 資訊安全標準驗證簡介

組織於確認驗證範圍、並建立及實施 ISO 27001 資訊安全管理制度三個月後，即可申請取得 ISO 27001 資訊安全標準認證，申請驗證必須要通過驗證單位（例如：BSI）的稽核驗證，由驗證單位向發證單位（例如：UKAS）提出建議發證申請，最後由發證單位決定發證 並頒發 ISO 27001 證書。ISO 27001 驗證流程，可以分成以下三個程序。（沈柏村，2010）。

（一）申請驗證前應注意事項

第一個程序為驗證前的準備，組織開始向驗證單位申請驗證前需注意下面條件要準備完成：

1. 系統文件完成且符合標準要求，並符合相關法規要求。
2. 全員認知公司之政策、目標、承諾。
3. 所有關鍵人員依訓練需求及計畫接受訓練。
4. 管理系統程序執行中，且有完整之管理循環及三個月執行紀錄。
5. 已執行過系統稽核，並舉行獨立審查。

然後決定驗證範圍，並與驗證單位確認實際驗證工作人天數與價格，雙方簽約並安排時程進行驗證作業，一般為早期發現正式驗證可能會有的問題，並使正式驗證能順利進行，於正式驗證前會安排預評作業，就是模擬正式驗證的作業，在預評作業完成後，再進行下一階段。

（二）文件審查作業

第二個程序為正式驗證作業之第一階段驗證（Initial Audit Step 1, IA1），即文件審查作業，主要驗證重點如下：

1. 驗證範圍與適用性聲明是否適當。
2. 確認管理系統的運作型態和文件化程度。
3. 管理系統是否依風險評估結果所建立。
4. 審查及驗證是否可信賴。

在此階段如果沒有「不符合事項」，則不需矯正措施確認或追蹤稽核。

(三) 實地審查作業

第三個程序為正式驗證作業之第二階段驗證(Initial Audit Step 2, IA2)，即實地審查作業，主要驗證重點如下：

1. 文件化的管理系統是否符合相關標準。
2. 管理程序是否確實執行。
3. 管理系統方面是否能達到持續改善及法規遵循。

在此階段如果沒有「不符合事項」，則不需矯正措施確認或追蹤稽核，驗證單位會建議發證，並頒發 ISO 27001 證書。



第參章 系統結構與運作

第一節 研究流程

在此次研究中，大致分為三個研究流程，其一為研究目的，包含了收納、分析、呈現等三個部份，為此次研究中最基本及最重要的工作。其二為文獻探討，收錄了相關資安的研究報導，提供我們在研究中所需的資料及幫助。其三為可行性分析及問券設計，以 SWOT 分析優勢、劣勢、機會及威脅，可清楚得知此次研究中的目標，接著再以問券的形式，訪問一般民眾及相關人士有關資安的議題，幫助我們修改研究動機及目的。統合三個研究流程進而進行系統開發，並分為三個部份：網站架設、資料庫架設及資料分析，最終以網站方式呈現，研究流程如下圖 3-1-1。

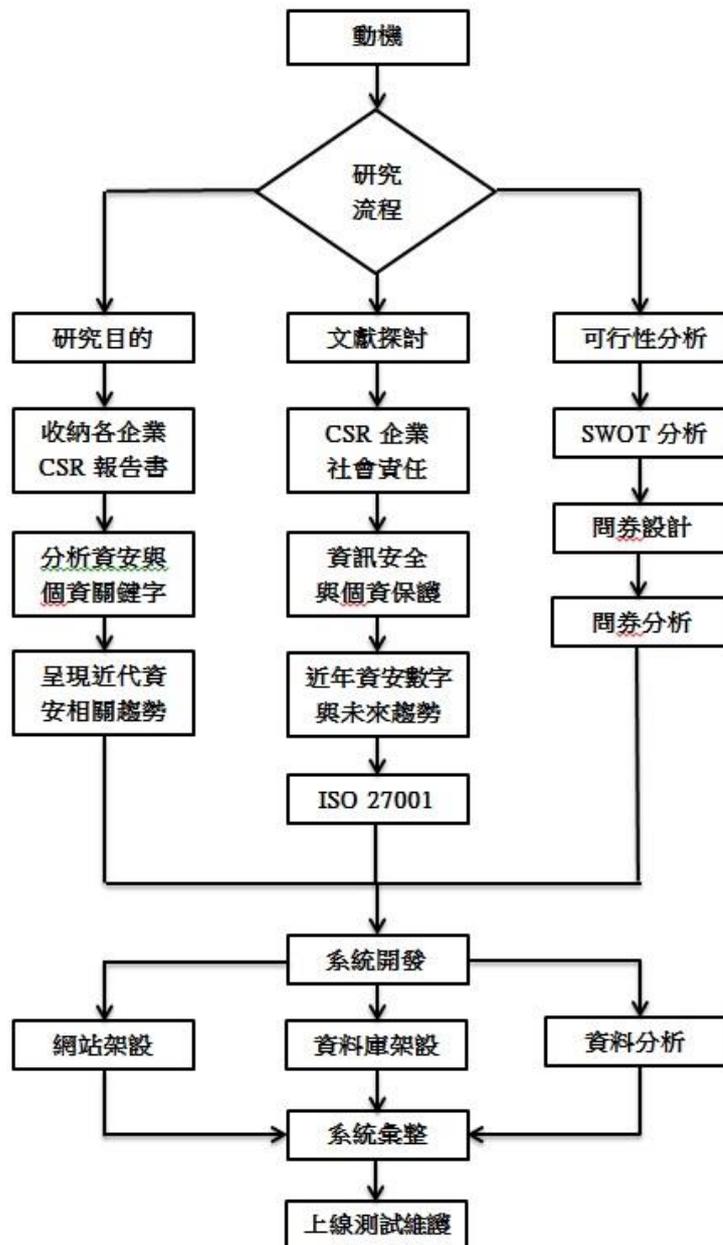


圖 3-1-1. 研究流程圖

第二節 研究方法(問卷調查)

此章節為研究結果分析，將蒐集到的資料統整進行分析。

一、研究範圍及問卷發放

本研究以探討有關民眾對於 CSR 企業社會責任及資訊安全的認知，實際關注企業在資訊安全上的貢獻程度及民眾想法。問卷發放時間為 2017 年 11 月 16 日至 2017 年 11 月 26 日止，由 google 表單發放，共收回了 200 份有效問卷。

二、樣本結構分析

(一)基本資料分析

依圖 4-2-1 可知，在問卷中，男性共有 97 位，女性共 103 位，女性共占全部樣本之 51.5%。在圖 4-2-2 可知年齡分布方面，18-25 歲之間共有 139 人為最多，佔全部樣本的 69.5%。12 歲以下及 50 歲以上的人數最少皆只有 4 人，各佔全部樣本的 2%。依職業來區分，以學生為大多數，共有 141 人，共佔全部樣本的 70.5%，而以家管及軍公教人數最少，皆只有 2 人，各佔全部樣本 1%。依教育程度來區分，以大學專科為大多數，共有 153 人，共佔全部樣本的 76.5%，而碩士以上人數最少只有 6 人，佔全部樣本的 3%。

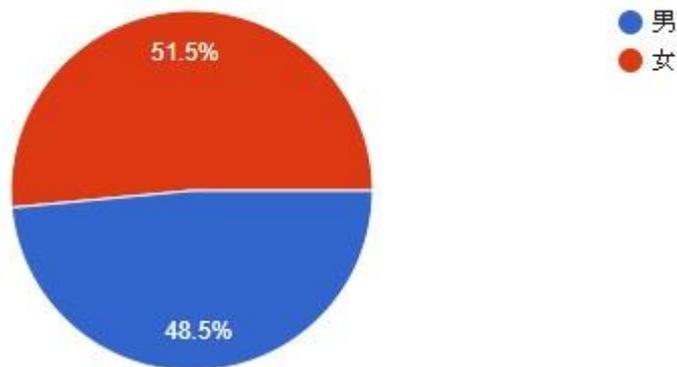


圖 4-2-1. 男女比例

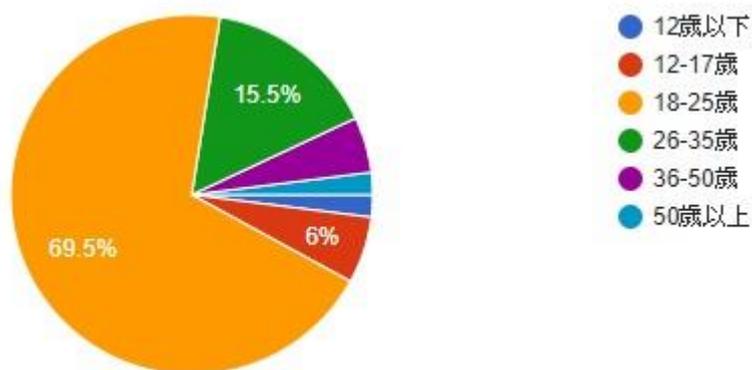


圖 3-2-2. 年齡比例

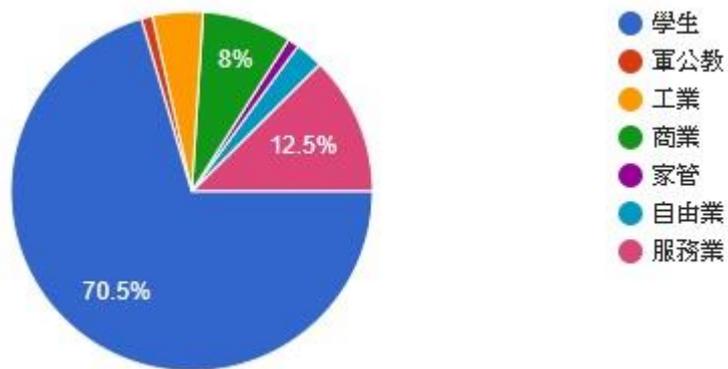


圖 3-2-3. 職業比例

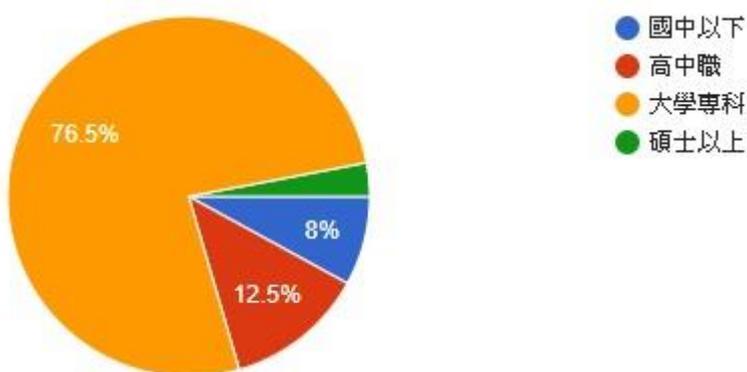


圖 3-2-4. 教育程度比例

(二) 相關議題關注程度分析

依圖 4-2-5 得知，平時有在關注企業對社會貢獻程度的人為五五分配，幾乎將近一半的人平時沒有在關注相關議題。依圖 4-2-6 得知，大多人都是從網路及新聞媒體得知資訊安全相關資訊，而從公司宣導得知者只有 1 人，佔全部樣本的 0.5%。依圖 4-2-7 得知，有 142 人常常於網路提供個人資料，佔了全部樣本的 71%。

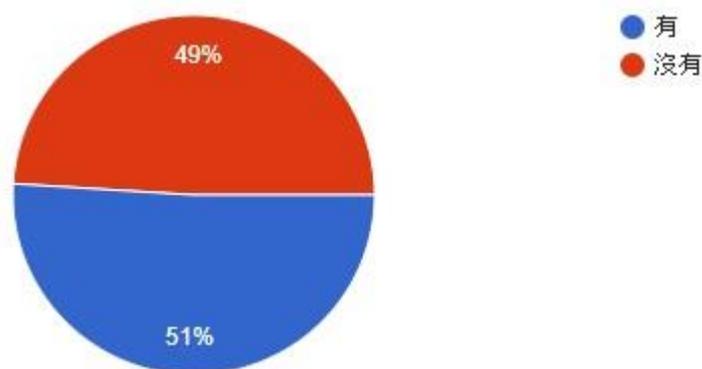


圖 3-2-5. 平時有在關注企業對社會的貢獻嗎

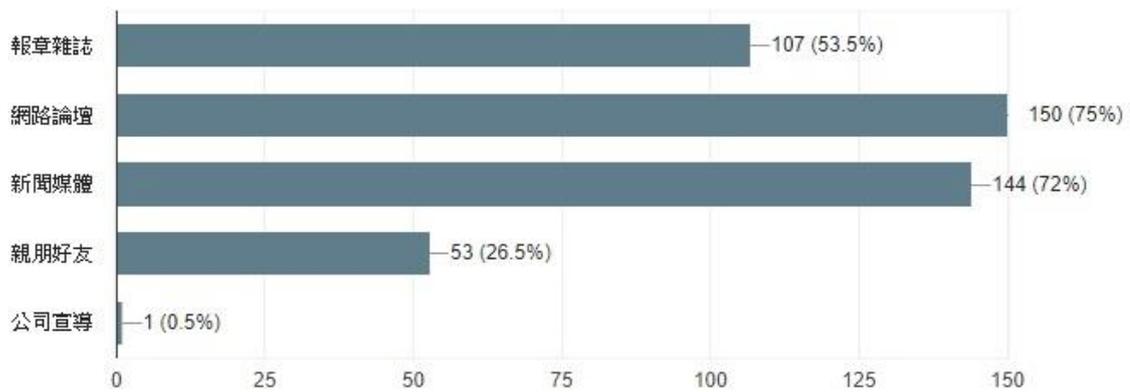


圖 3-2-6. 會從何處得知資安相關資訊

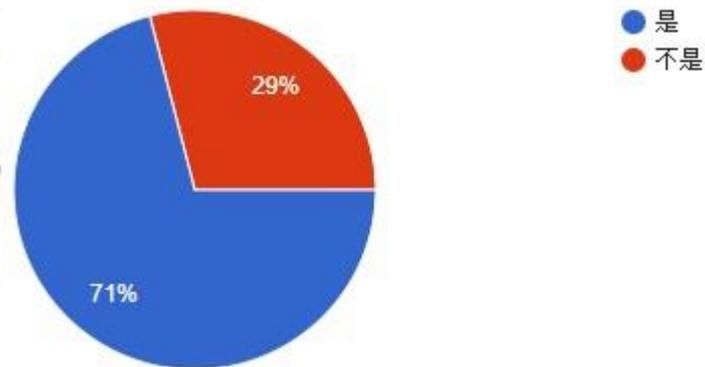


圖 3-2-7. 時常於網路上提供個人資料嗎

(三) 主觀感受及需求分析

依圖 4-2-8 得知，有 133 人不知道 CSR 企業社會責任，佔全部樣本的 66.5%，意謂大多數人皆不知道有此規範。依圖 4-2-9 得知，有 135 人都會以企業對社會的貢獻程度來評論該企業，佔了全部樣本的 67.5%，可知大多數民眾還是有在關心相關議題。依圖 4-2-10 得知，有 95 人覺得企業對社會貢獻的程度為 3 分，屬於中間值，可知大多數人還是覺得各企業在此方面還需努力。依圖 4-2-11 得知，大多數人對於資安未來趨勢發展較有興趣，其次為關鍵字搜尋。

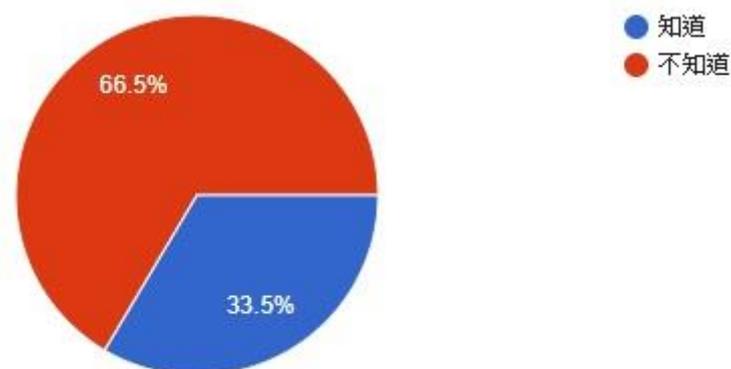


圖 3-2-8. 您知道 CSR 企業社會責任嗎

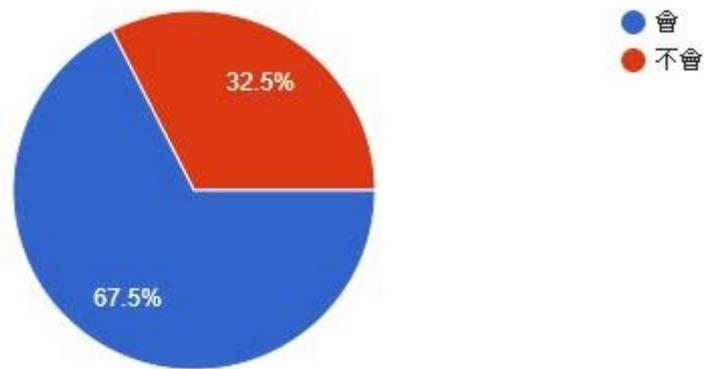


圖 3-2-9. 您會依企業對社會的貢獻程度最為評論該企業的依据嗎

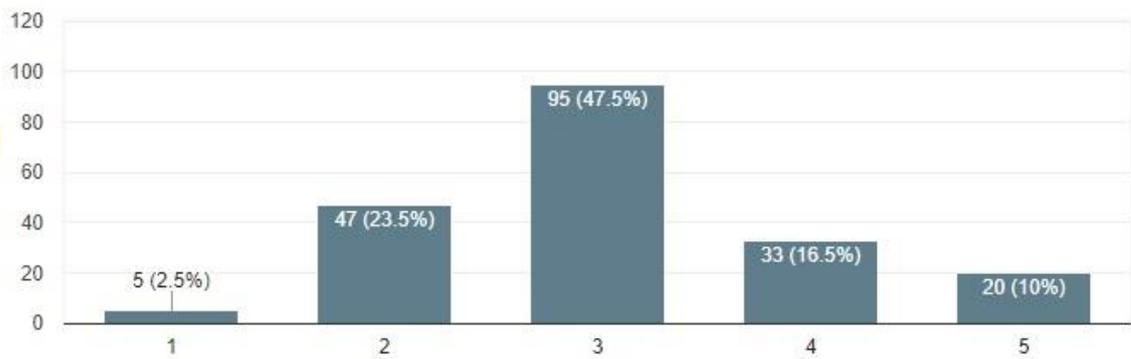


圖 3-2-10. 您覺得現今各企業致力於資安保護的程度為何

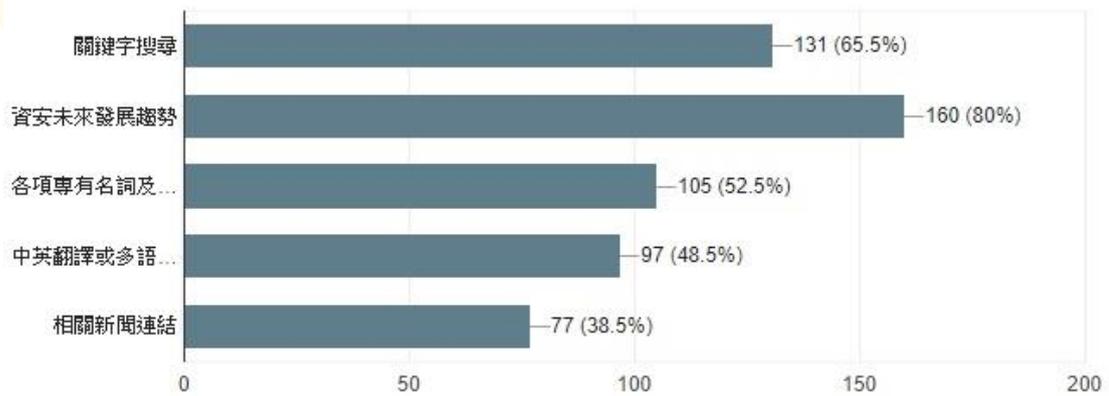


圖 3-2-11. 您希望此觀察站能提供什麼服務

第三節 SWOT 分析

在本研究中，我們進行 SWOT 分析，藉以明瞭本研究之優勢所產生之機會，以及因為劣勢所可能產生之威脅。如表 3-1 所示。

表 3-1. SWOT 分析表

| | | | | | |
|--|--|----|----|----|----|
| <ul style="list-style-type: none"> • 相關類似的網站較少 • 符合最新流行趨勢 • 會員制方便使用 • 免費使用減少負擔 • 提升公民素質 | <ul style="list-style-type: none"> • 知道 CSR 的人為少數 • 經驗不足經營較困難 • 龐大資料量不易收納 | | | | |
| <ul style="list-style-type: none"> • 提供關鍵字快速搜尋 • 提供中英翻譯減少代溝 • 提供相關報告整合 • 提供最新資安趨勢 | <ul style="list-style-type: none"> • 有更知名專業的網站競爭激烈 | | | | |
| <table border="1"> <tr> <td>優勢</td> <td>劣勢</td> </tr> <tr> <td>機會</td> <td>威脅</td> </tr> </table> | | 優勢 | 劣勢 | 機會 | 威脅 |
| 優勢 | 劣勢 | | | | |
| 機會 | 威脅 | | | | |

此觀察站其主要優勢為符合流行趨勢，現在資安問題頻傳，各公司的資訊安全及個資保護已成為人們關心的議題之一。劣勢在於知道 CSR 報告書的人較少，一般人較少關心這方面的資訊，市面上相關的網站也不多，不易引起人們注意。我們的機會在於關鍵字的搜尋功能，加入關鍵字搜尋功能方便查詢相關的內容。唯一威脅是在我們的相關經驗不足下，還有其他更知名的付費網站存在於市面上，因此推廣困難。

第肆章 網站建置與展示

第一節 網站建置

一、網站架設

(一)Microsoft Visual studio

SQL 資料庫引導建置網站，建置 GridVeiw 表格引進資料庫資料顯示 50 企業關鍵字及五年資安發展進程，利用 000webhost 之 wordpress 超連結連至完成之資料庫網頁，SQL server 可隨時做更新頁面，利用 SSMS 及時上傳更新資料庫資訊。

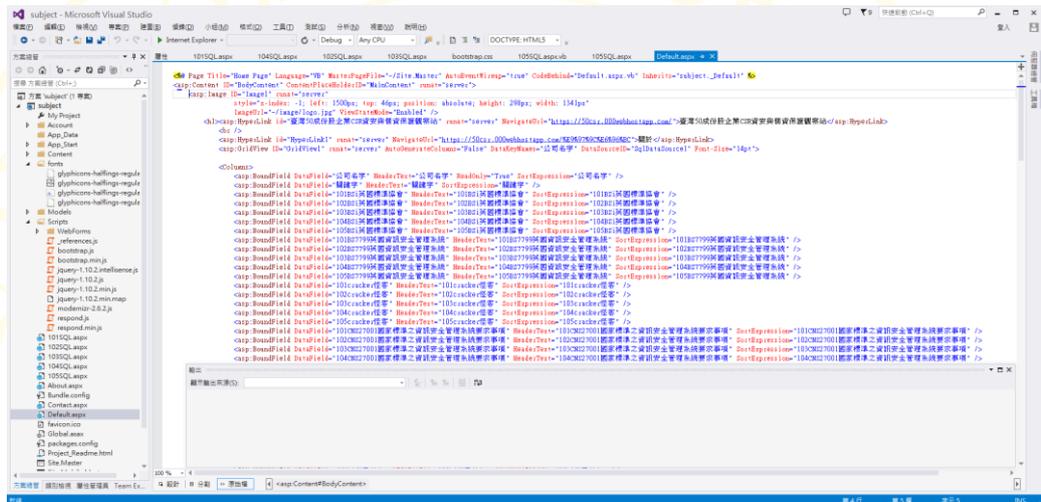


圖 4-1-1. Microsoft Visual studio

(二)000webhost

提供相關外掛程序，引入會員管理申請、討論及留言板與會員交流、瀏覽在線人數及總瀏覽數及各平台聯絡超連結。



圖 4-1-2. 000webhost

二、資料庫架設

SQL 2017 Developer Edition 版本安裝，並啟動 SQL Server Browser 服務，切換至通訊協定啟用 TCP/IP 並至工作管理員服務查看相關 SQL 服務的啟用狀態，架設完成相關資料庫資料即完成之資料庫網頁丟置主機伺服器資料夾提供更新資訊上傳 C:\inetpub\wwwroot，配合 Visual Studio 完成之輸出檔建置首頁 index。

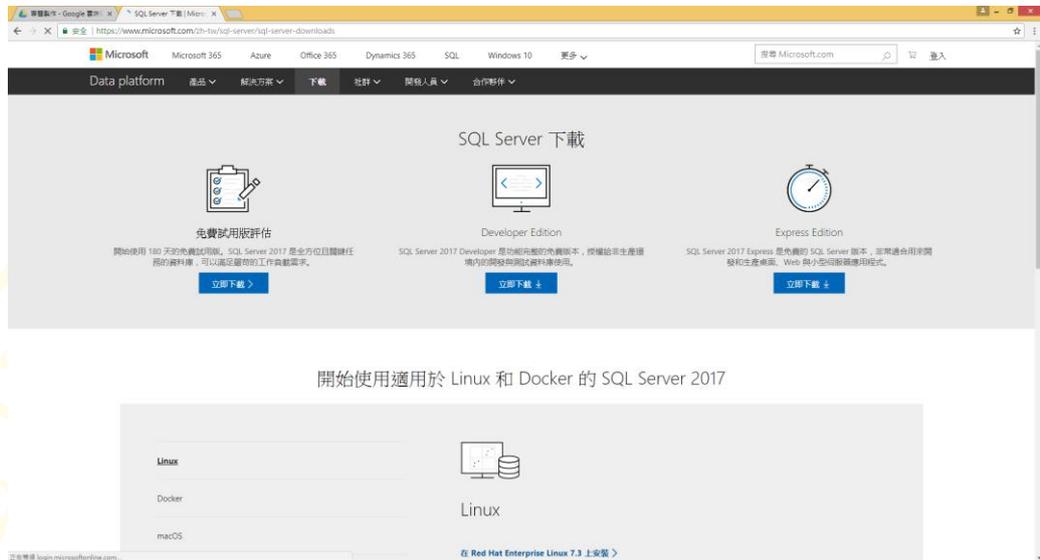


圖 4-1-3. SQL Server-1

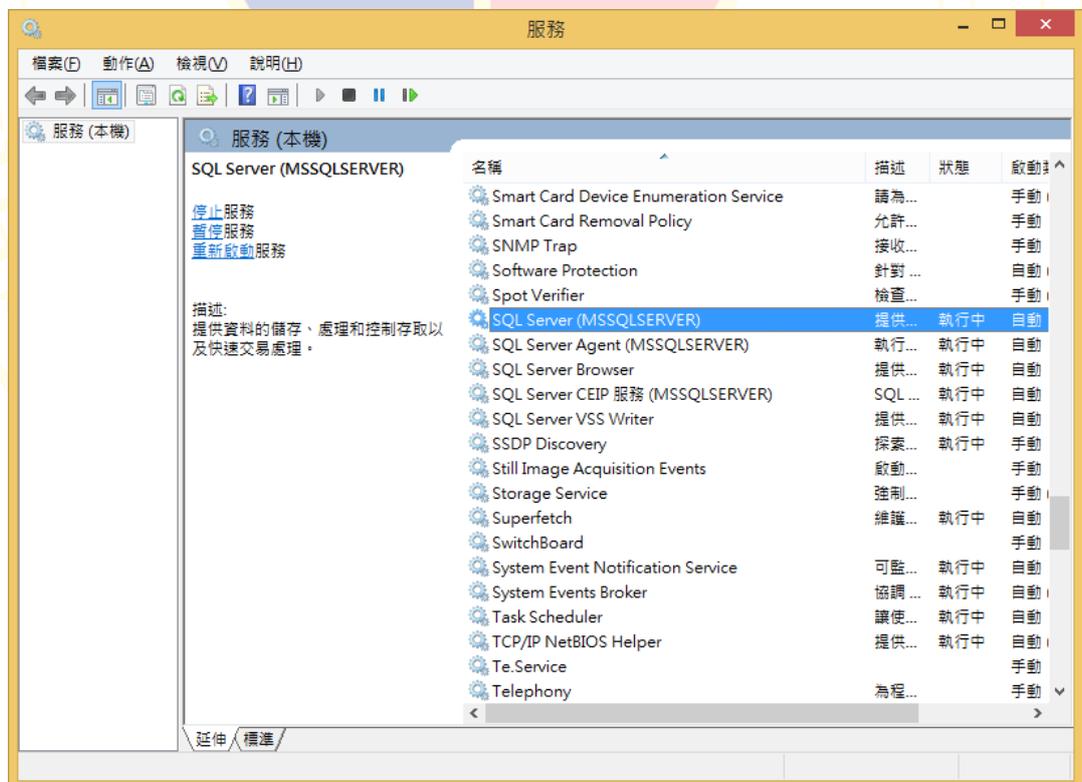


圖 4-1-4. SQL Server-2



圖 4-1-5. SQL Server-3

第二節 成果展示

一、後台架構

透過 000Webhost 內的 Wordpress admin 控制台尋找需要的外掛以及會員權限的控制，頁面的新增和原始碼可以透過預覽做即時調整。

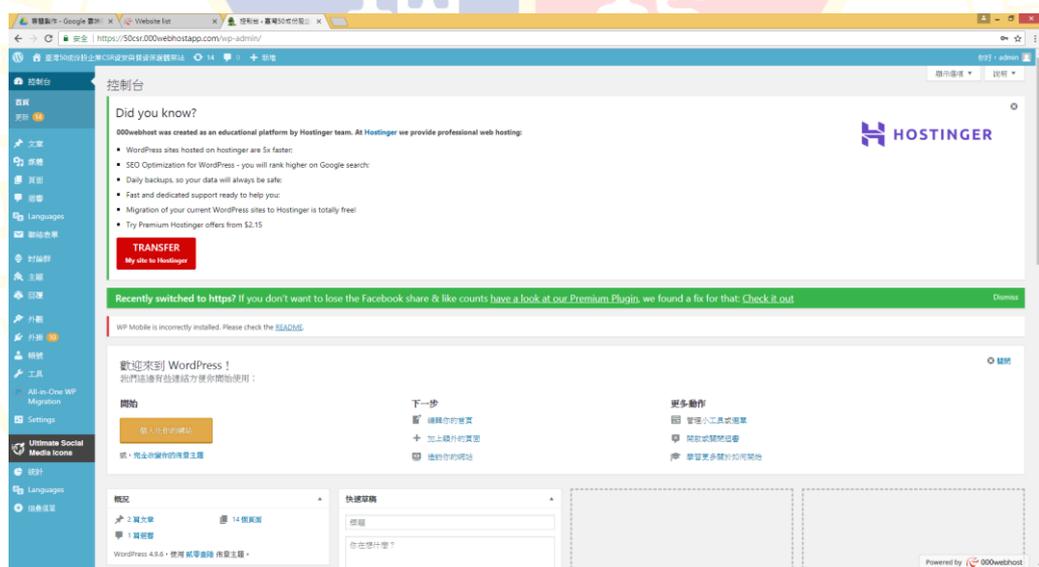


圖 4-2-1. 後台控制台



圖 4-2-2. 後台頁面

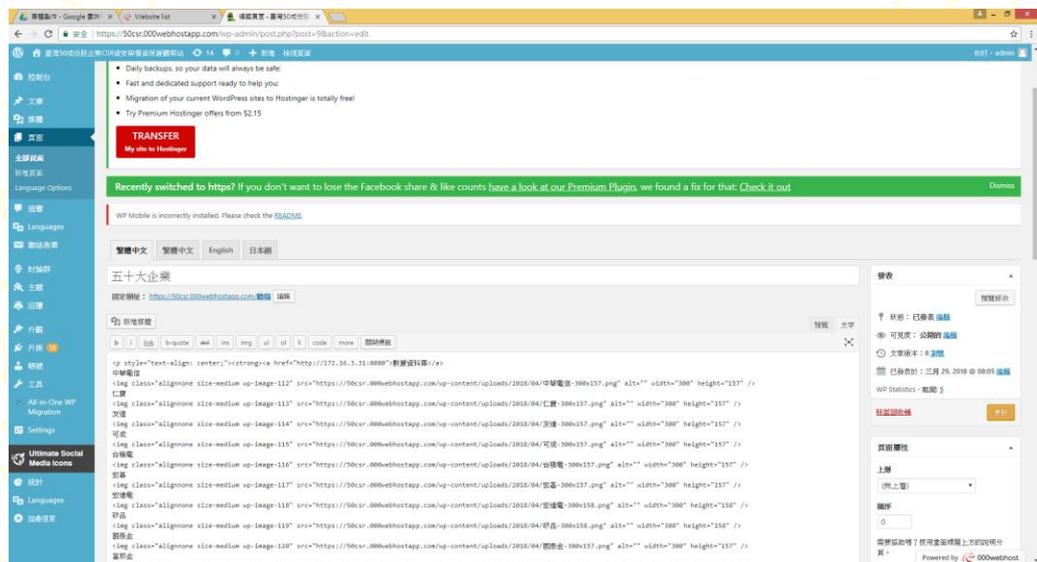


圖 4-2-3. 後台外掛

二、功能介紹

(一)會員登入與站內搜尋

會員登入系統分為登入、註冊、忘記密碼三部份，第一次使用需先進行註冊，之後要登入會員時只需輸入註冊時的電子郵件及密碼即可。

站內搜尋可輸入欲查詢之關鍵字，方可顯示站內所有相關文章及內容。下圖為會員登入及站內搜尋畫面及結果。



圖 4-2-4. 會員登入與站內搜尋

宏碁 的搜尋結果：

中華電信 仁寶 友達 台積電 宏碁 宏達電 矽品 國泰金 富邦金 華南金 華碩 開發金 影銀 廣達 聯強 聯發 ... [繼續閱讀](#)

3rd 四月 2018 / 資安 / 50企業, 分析圖, 資安 / 留下一則迴響

五十大企業

數據資料庫 中華電信 仁寶 友達 可成 台積電 宏碁 宏達電 矽品 國泰金 富邦金 華南金 華碩 開發金 影銀 ... [繼續閱讀](#)

會員登入

使用者名稱:
密碼:
 記住我
[註冊](#)
[忘記密碼](#)

站內搜尋

宏碁

圖 4-2-5. 搜尋結果畫面

(二)數據資料庫

透過網址超連結連至建置好的資料庫網頁，資料庫網頁透過 SQL Server 上傳之資料再利用 Microsoft Visual Studio 製成，如下圖。

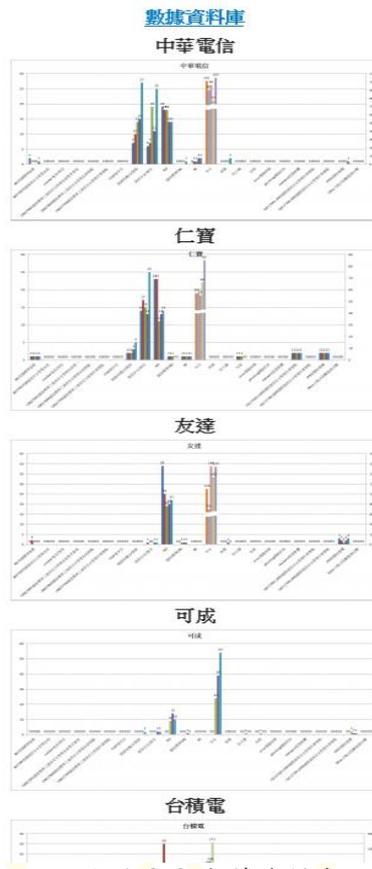


圖 4-2-6. 數據資料庫 1

| 公司名稱 | 101BSI 英國標準 字準協會 | 102BSI 英國標準 準協會 | 103BSI 英國標準 準協會 | 104BSI 英國標準 準協會 | 105BSI 英國標準 準協會 | 101BSI7799 英國資訊安 全管理系統 | 102BSI7799 英國資訊安 全管理系統 | 103BSI7799 英國資訊安 全管理系統 | 104BSI7799 英國資訊安 全管理系統 | 105BSI7799 英國資訊安 全管理系統 | 101cracker 評者 | 102cracker 評者 | 103cracker 評者 | 104cracker 評者 | 105cracker 評者 | 101CNS27001 國家標準之資 訊安全管理系 統要求事項 | 102CNS27001 國家標準之資 訊安全管理系 統要求事項 | 103CNS27001 國家標準之資 訊安全管理系 統要求事項 | 104CNS27001 國家標準之資 訊安全管理系 統要求事項 | |
|------|------------------------|-----------------------|-----------------------|-----------------------|-----------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------|------------------|------------------|------------------|------------------|--|--|--|--|--|
| 大立 | | | | | | | | | | | | | | | | | | | | |
| 光 | | | | | | | | | | | | | | | | | | | | |
| 中 | 3 | 2 | 4 | 3 | 2 | | | | | | | | | | | | | | | |
| 德 | | | | | | | | | | | | | | | | | | | | |
| 中 | 2 | | | | 1 | | | | | | | | | | | | | | | |
| 華 | 1 | 1 | | 1 | 1 | | | | | | | | | | | | | | | |
| 仁 | 1 | 1 | 1 | 1 | 1 | | | | | | | | | | | | | | | |
| 寶 | 1 | | 4 | 5 | 5 | 1 | | | | | | | | | | | | | | |
| 元 | | | | | | | | | | | | | | | | | | | | |
| 大 | | 2 | | | | | | | | | | | | | | | | | | |
| 新 | | | | | | | | | | | | | | | | | | | | |
| 日 | | | | | | | | | | | | | | | | | | | | |
| 月 | | | | | | | | | | | | | | | | | | | | |
| 光 | | | | | | | | | | | | | | | | | | | | |
| 通 | | | | | | | | | | | | | | | | | | | | |

圖 4-2-7. 數據資料庫 2

(三)000webhost 外掛支援

000Webhost 提供瀏覽人數流量統計及各連絡平台圖示超連結，方便用戶迅速聯絡以及流量統計，如下圖。

訪客統計

- 線上使用者: 1
- 今日瀏覽次數: 28
- 今日瀏覽者數量: 13
- 總瀏覽次數: 117

圖 4-2-8. 訪客統計



第五章 結論與未來展望

在專題製作中共享收集資訊成究相關專題研究，以下為此專題研究之結論與未來展望的感想。

第一節 結論

資訊可以有許多存在的形式，由於現在是一個資訊爆炸的時代資訊傳遞的技術日新月異，傳統郵寄、傳真之外，也能透過電子方式傳輸各種格式的電子檔案，包括影音、文件、圖片等，不管任何形式的資訊都被視為重要資產，應受到完整良好的保護，而資訊安全就是要保障機構內的資訊資產免於不可承受的風險進而造成損失。

近年來個資外洩頻繁造成許多詐騙等案件，個人資料包含：自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料，而判斷標準為「得以直接或間接方式識別該個人之資料」，如何避免外洩為現代重點課題之一。

此專題研究所要得到的成果是收納整合台灣 50 成份股企業 CSR 相關報告數據、分析所整合報告中與資安及個資保護相關關鍵字、呈現近五年各大企業對資安及個資保護相關趨勢，並且利用整合得到的資訊匯製成相關網頁提供給需求資訊者一個網路平台使用，此網路平台的效益為造就提升人民資訊安全與個資保護之素養。

第二節 未來展望

收集 50 成份股企業 CSR 相關報告數據數量為台灣較為重要之企業，為提升對相關資訊理解程度不高之人民作初步統計及介紹，未來展望為增廣其企業數量及數據精密度，並增進其專業層面深度成究更為完整的網路平台提供給較為專業之人士研究數據使其推廣分享給各界人士。

該網路平台目前為提供研究數據給需求者閱讀，在未來希望成究成一個互動式平台，以會員式讓相關興趣及專業人士共同探討，也可提供資訊給平台及時更新時事及資料。

參考文獻

中文部分

林紫晴(2013)，個資保護於校園資訊系統中之研究，聖約翰科技大學，電機工程研究所，碩士學位論文。

台灣證券交易所公司治理中心(2014)，企業社會責任簡介，

擷取自 <http://cgc.twse.com.tw/front/responsibility>

趨勢科技(2016)，盤點2016十大資安數字-企業機構篇，

擷取自 <https://blog.trendmicro.com.tw/?p=34234>

張景皓(2012)，企業因應個資法該做的維護措施，

擷取自 <https://www.ithome.com.tw/article/88078>

黃泓瑜、黃彥茶(2017)，2017CIO必看四大資安趨勢，

擷取自 <https://www.ithome.com.tw/article/111211>

沈柏村(2010)，ISO27001資訊安全標準及驗證流程簡介，金融聯合徵信雙月刊第11期，20-22頁。





附錄一、畢業專題 系統操作手冊

【專題執行計畫表】

| | | | |
|-------------------|--|------------|---------------|
| 組名 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | | |
| 組員 | 班級 | 學號 | 姓名 |
| | 資三 B | 10410209 | 張光祐 |
| | 資三 B | 10410210 | 楊子鎰 |
| | 資三 B | 10410225 | 王兆立 |
| | 資三 B | 10410230 | 張家豪 |
| | 資三 B | 10410237 | 李昱昌 |
| | 資三 B | 10410244 | 徐偉倫 |
| 選定合作單位 | 名稱 | 無 | |
| | 負責人 | 無 | 聯絡人 無 |
| | 電話 | 無 | 電話 無 |
| | 地址 | 無 | |
| | 業務描述 | 本次專題無合作單位。 | |
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | | |
| 專題資訊系統功能描述 | 本網站將提供使用者方便搜尋各企業 CSR 報告書中有關資安與個資保護的相關資訊。 | | |
| 指導老師簽名 | | 日期 | 106 年 8 月 1 日 |
| 備註 | | | |

【專題工作分配表】

| | | | |
|------|---|------|---------------|
| 組名 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫人 | 徐偉倫 |
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫日期 | 107 年 3 月 1 日 |
| 姓名: | 工作分配: | | |
| 張光祐 | 網站架設 程式撰寫 圖表製作 意見整合 內容策化 | | |
| 楊子鉉 | 資料蒐集 資料整合 資料分析 內容策化 會議協調 口頭報告 | | |
| 王兆立 | 資料蒐集 資料整合 資料分析 內容構思 | | |
| 張家豪 | 網站架設 程式撰寫 圖表製作 意見整合 口頭報告 | | |
| 李昱昌 | 資料蒐集 資料整合 資料分析 圖表製作 報告書製作 | | |
| 徐偉倫 | 圖表製作 資料整合 意見整合 內容策化 簡報製作 報告書製作 | | |
| | | | |

【GANTT 圖】

| | | | |
|------|------------------------------|------|----------------|
| 組名 | 台灣 50 成份股企業 CSR 資安與個人資料保護觀察站 | 填寫人 | 徐偉倫 |
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個人資料保護觀察站 | 填寫日期 | 107 年 2 月 28 日 |

以下為本專題的 GANTT 圖(甘特圖)，長條圖代表任務工作，其長度代表執行時間之長短，以不同顏色代表工作之性質，藍色長條圖為「專案起草」工作，長度為 4 周工作時間，紅色長條圖為「需求分析」工作，長度為 2 周工作時間，綠色長條圖為「系統分析」工作，長度為 2 周工作時間，最後橘色長條圖為「系統建置」工作，長度為 5 周工作時間，此專案從 2018 年 3 月 10 日開始，預計在 2018 年 5 月 26 日前完成。

| 識別碼 | 工作名稱 | 開始 | 結束 | 期間 | 2018 年 3 月 | | | | 2018 年 4 月 | | | | 2018 年 5 月 | | | |
|-----|------|------|------|-----|------------|------|------|------|------------|------|------------|------|------------|------|------|------|
| | | | | | 10 日 | 17 日 | 24 日 | 31 日 | 7 日 | 14 日 | 21 日 | 28 日 | 5 日 | 12 日 | 19 日 | 26 日 |
| 1 | 專案起草 | 3/10 | 3/31 | 4 W | [Task Bar] | | | | | | | | | | | |
| 2 | 需求分析 | 4/1 | 4/14 | 2 W | | | | | [Task Bar] | | | | | | | |
| 3 | 系統分析 | 4/15 | 4/31 | 2 W | | | | | | | [Task Bar] | | | | | |
| 4 | 系統建置 | 4/15 | 5/19 | 5 W | | | | | | | [Task Bar] | | | | | |

【開發工具清單】

| | | | |
|------|----------------------------|------|-----------------|
| 組名 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫人 | 張家豪 |
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫日期 | 106 年 12 月 18 日 |

| 名稱 | 功用 |
|------------------------|---------|
| MySQL Server | 網站後台資料庫 |
| 000WEBHOST | 介紹頁面 |
| Microsoft VisualStudio | 架站程式 |

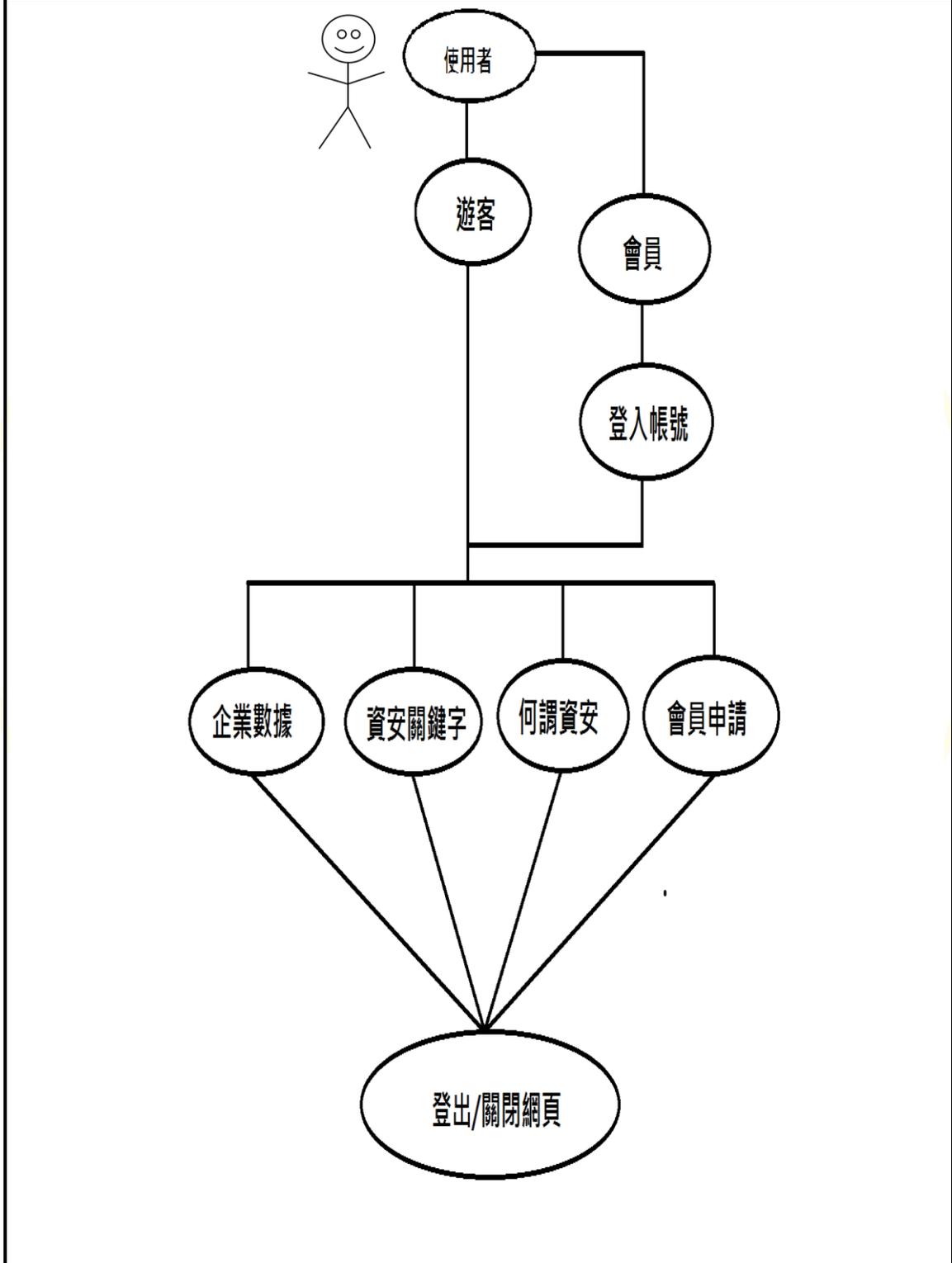


【需求訪談計畫表】

| | | | |
|---|----------------------------|------|-----------------|
| 組名 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫人 | 徐偉倫 |
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫日期 | 106 年 12 月 31 日 |
| <p>106.11.16 問卷發放 106.11.26 問卷結束 發放地點：GOOGLE 表單 回收有效問卷份數：200 份 問卷內容：</p> <p>一、基本資料</p> <ol style="list-style-type: none"> 1.男女比例 2.年齡比例 3.職業比例 4.教育程度比例 <p>二、相關議題關注程度</p> <ol style="list-style-type: none"> 1.平時關注企業對社會貢獻的程度 2.從何處得知資安相關資訊 3.時常於網路提供個人資料頻率 <p>三、主觀感受及需求</p> <ol style="list-style-type: none"> 1.是否知道 CSR 企業社會責任 2.是否依企業對社會貢獻程度評論該企業 3.現今各企業致力於資安保護的程度 4.希望提供什麼服務 | | | |

【使用個案圖】

| | | | |
|------|------------------------------|------|-----------------|
| 組名 | 台灣 50 成份股企業 CSR 資安與個人資料保護觀察站 | 填寫人 | 張家豪 |
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個人資料保護觀察站 | 填寫日期 | 107 年 12 月 18 日 |



【藍圖】

| | | | |
|----------|--------------------------------|------|-----------------|
| 組名 | 台灣 50 成份股企業 CSR 資安與個 資保護觀察站 | 填寫人 | 張家豪 |
| 專題 名稱 | 台灣 50 成份股企業 CSR 資安與個 資保護觀察站 | 填寫日期 | 106 年 12 月 18 日 |

: :

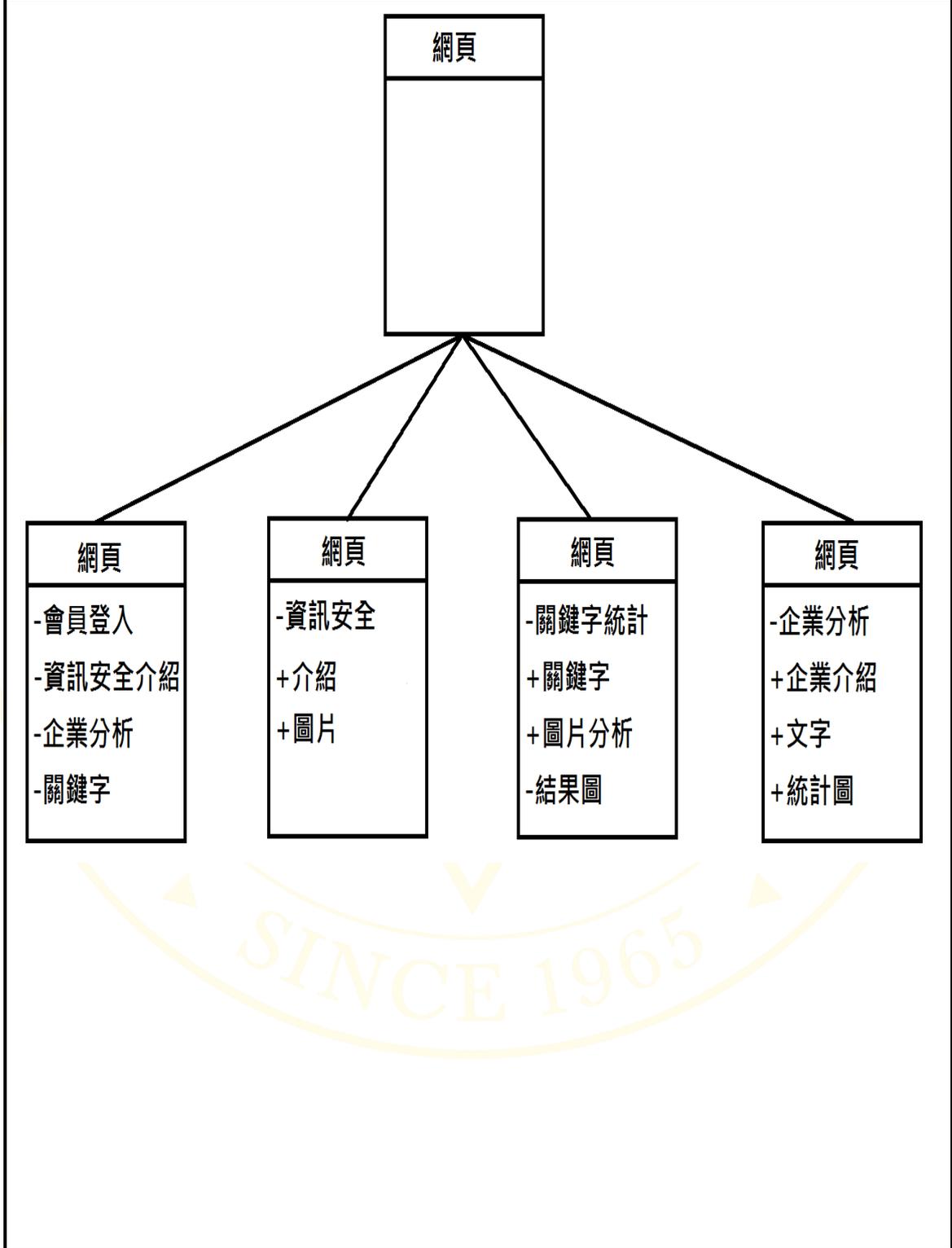
40

【資料詞彙】

| | | | | |
|-----------|----------------------------|----------|-------------------|-------|
| 組名 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫人 | 張光祐、張家豪 | |
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫日期 | 107 年 3 月 1 日 | |
| <<首頁>> | | | | |
| 編號 | 欄位名稱 | 型態 | 格式 | |
| A1 | 資安介紹 | Button | ImageButton, text | 資安介紹 |
| A2 | 企業分析 | Button | ImageButton, text | 企業分析 |
| A3 | 關鍵字分析 | Button | ImageButton, text | 關鍵字分析 |
| <<資安介紹>> | | | | |
| 編號 | 欄位名稱 | 型態 | 格式 | |
| B1 | 何謂資安 | nVarchar | Text | 何謂資安 |
| B2 | 首頁 | Button | ImageButton, text | 首頁 |
| B3 | 統計圖 | Button | ImageButton, text | 統計圖 |
| <<企業分析>> | | | | |
| 編號 | 欄位名稱 | 型態 | 格式 | |
| C1 | 企業介紹 | nVarchar | Text | 企業介紹 |
| C2 | 首頁 | Button | ImageButton, text | 首頁 |
| C3 | 企業分析 | Button | ImageButton, text | 企業分析 |
| <<關鍵字分析>> | | | | |
| 編號 | 欄位名稱 | 型態 | 格式 | |
| D1 | 關鍵字分析 | nVarchar | Text | 關鍵字分析 |
| D2 | 首頁 | Button | ImageButton, text | 首頁 |
| D3 | 連結資訊 | Button | ImageButton, text | 連結資訊 |

【類別圖】

| | | | |
|------|----------------------------|------|---------------|
| 組名 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫人 | 張家豪 |
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫日期 | 107 年 5 月 1 日 |



【使用者操作手冊】

| | | | |
|-------------|----------------------------|-------------|----------------|
| 組名 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫人 | 徐偉倫 |
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫日期 | 107 年 5 月 29 日 |

| | | | |
|-------------|----|-------------|----|
| 畫面編號 | 01 | 畫面名稱 | 首頁 |
|-------------|----|-------------|----|

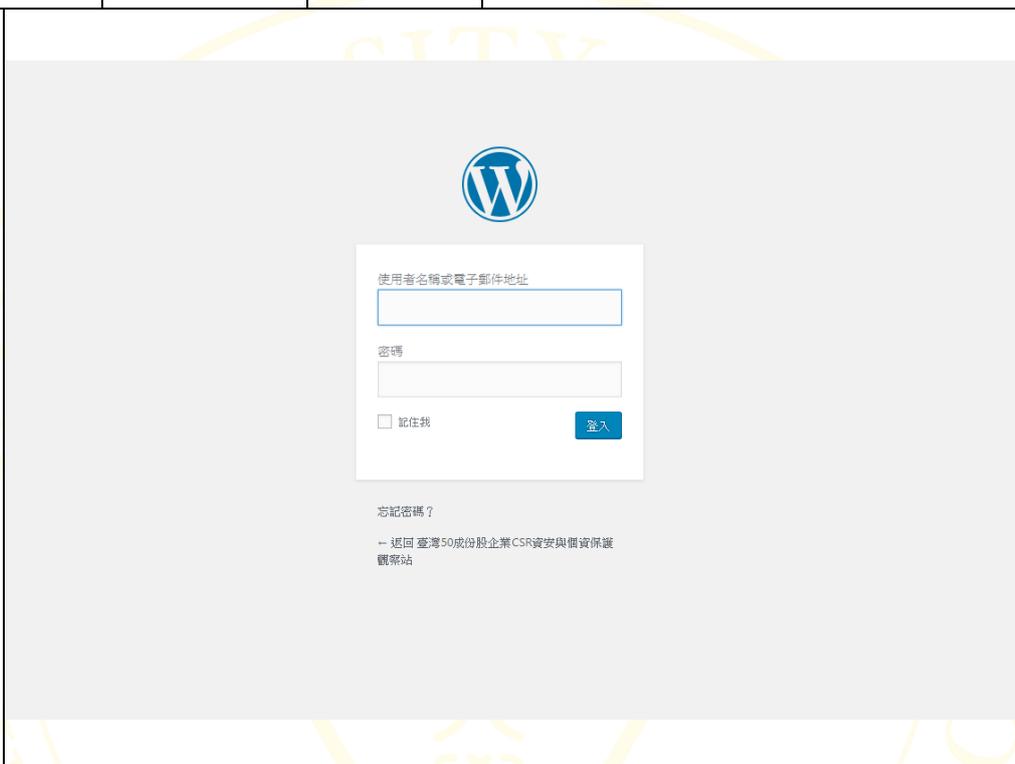
| | |
|------|---|
| 系統畫面 |  |
| 操作說明 | <p>點選首頁關於連結至新頁面，即有粉絲團、信箱、網站創作者資料等資訊。</p> |

【使用者操作手冊】

| | | | |
|------|----------------------------|------|----------------|
| 組名 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫人 | 徐偉倫 |
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫日期 | 107 年 5 月 29 日 |

| | | | |
|------|----|------|------|
| 畫面編號 | 02 | 畫面名稱 | 登入畫面 |
|------|----|------|------|

系統畫面



操作說明

點選首頁登入畫面，進入登入視窗。

【使用者操作手冊】

| | | | |
|-------------|---|-------------|------------------|
| 組名 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫人 | 徐偉倫 |
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫日期 | 107 年 5 月 29 日 |
| 畫面編號 | 03 | 畫面名稱 | 首頁(五十大企業) |
| 系統畫面 |  <p>The screenshot shows a web browser window with the URL https://50csr.000webhostapp.com. The page title is '臺灣50成份股企業CSR資安與個資保護觀察站'. There are navigation links for '首頁', '關於', '五十大企業', and '資安用語詞彙數量數據圖'. A large 'INFORMATION' banner is centered. Below it, there is a section for '五十大企業' with a bar chart and a '數據資料庫' link circled in red. A '會員登入' form is on the right.</p> | | |
| 操作說明 | <p>點選首頁五十大企業即可顯示五十大企業名單及圖表分析。</p> | | |

【使用者操作手冊】

| | | | |
|------|----------------------------|------|----------------|
| 組名 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫人 | 徐偉倫 |
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | 填寫日期 | 107 年 5 月 29 日 |

| | | | |
|------|----|------|------|
| 畫面編號 | 04 | 畫面名稱 | 資料畫面 |
|------|----|------|------|

系統畫面

資料庫網頁

臺灣50成份股企業CSR資安與個資保護觀察站關於

| 公司名字 | 101BS | 102BS | 103BS | 104BS | 105BS | 101BS | 102BS | 103BS | 104BS | 105BS | 101cracker | 102cracker | 103cracker | 104cracker | 105cracker | 101CN | 102CN | 103CN | 104CN | 105CN | |
|------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|------------|------------|------------|------------|------------|-------|-------|-------|-------|-------|--|
| 王立元 | | | | | | | | | | | | | | | | | | | | | |
| 光華 | 3 | 2 | 4 | 3 | 2 | | | | | | | | | | | | | | | | |
| 華南 | | | | | | | | | | | | | | | | | | | | | |
| 中華 | 1 | 1 | | 1 | 1 | | | | | | | | | | | | | | | | |
| 仁美 | 1 | 1 | 1 | 1 | 1 | | | | | | | | | | | | | | | | |
| 元大 | 1 | | 4 | 5 | 5 | 1 | | | | | | | | | | | | | | | |
| 安達 | | 2 | | | | | | | | | | | | | | | | | | | |
| 日月 | | | | | | | | | | | | | | | | | | | | | |
| 光華 | | | | | | | | | | | | | | | | | | | | | |
| 成發 | | | | | | | | | | | | | | | | | | | | | |
| 台一 | | | | | | | | | | | | | | | | | | | | | |
| 隆 | | | | | | | | | | | | | | | | | | | | | |

操作說明

點選首頁五十大企業連結至資料庫網頁，即可顯示五十大企業有關資安的關鍵字。

【測試相關計畫】

| | | | |
|------|------------------------------|------|----------------|
| 組名 | 台灣 50 成份股企業 CSR 資安與個人資料保護觀察站 | 填寫人 | 徐偉倫 |
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個人資料保護觀察站 | 填寫日期 | 107 年 5 月 29 日 |



【專案結案報告】

| | | | |
|------|------------------------------|------|-----|
| 組名 | 台灣 50 成份股企業 CSR 資安與個人資料保護觀察站 | 填寫人 | |
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個人資料保護觀察站 | 填寫日期 | 年月日 |



【會議記錄】

| | | | | | |
|--|---|--------|--|------|------------------|
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | | | | |
| 會議編號 | 01 | 召集人兼主席 | 楊子鎔 | 紀錄者 | 徐偉倫 |
| 討論主題 | 專題主題定案及分工 | | | 會議時間 | 2017/09/19 17:00 |
| | | | | 會議地點 | 綜合教學大樓 7F |
| 上次會議 | 決議事項 | | 執行狀況 | | |
| | 無 | | 無 | | |
| 本次會議 | 本次工作進度 | | 本次會議內容 | | 負責人員 |
| | 專題主題及內容發想 組員工作分配 | | 1. 訂定專題主題 2. 報告內容架構討論 3. 工作進度分配 4. 組員分工 | | 全體 |
| 本次會議內容 | 本次會議將決議本次專題製作的主題及內容，並進行工作分配。會議中各組員提出各自意見，並與指導老師討論，及排訂日後工作進度及開會日期。 | | | | |
| 決議事項（與主席裁示） | | | | | |
| 訂定主題為「台灣 50 成份股企業 CSR 資安與個資保護觀察站」，並各自進行所分配之工作內容。 | | | | | |
| 請簽名 | 請簽名 | 請簽名 | 請簽名 | 請簽名 | 請簽名 |
| 下次會議 | 召集人 | 楊子鎔 | 紀錄者 | 李昱昌 | 時間 |
| | | | | | 2017/09/29 17:00 |
| 預定討論主題 | 專題製作方向及內容 | | | | |
| 指導老師意見 | | | | | |

【會議記錄】

| | | | | | | |
|-------------------------------------|--|--------|--------------------------------------|------|------------------|------------------|
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | | | | | |
| 會議編號 | 02 | 召集人兼主席 | 楊子鎔 | 紀錄者 | 李昱昌 | |
| 討論主題 | 專題製作方向及內容 | | | 會議時間 | 2017/09/29 17:00 | |
| | | | | 會議地點 | 綜合教學大樓 7F | |
| 上次會議 | 決議事項 | | 執行狀況 | | | |
| | 訂定主題及前製作業 | | 確實執行 | | | |
| 本次會議 | 本次工作進度 | | 本次會議內容 | | 負責人員 | |
| | 決議資料搜集內容方向 專題報告書內容撰寫 | | 1. 報告書內容提案 2. 資料蒐集整合 3. 專題方向討論 | | 全體 | |
| 本次會議內容 | <p align="center">本次會議將決議專題的製作方向，經組員共同討論後選定最合適的方式，並同時進行報告書的內容發想。</p> | | | | | |
| 決議事項（與主席裁示） | | | | | | |
| <p align="center">專題報告書第一章緒論完成。</p> | | | | | | |
| 請簽名 | 請簽名 | 請簽名 | 請簽名 | 請簽名 | 請簽名 | |
| 下次會議 | 召集人 | 楊子鎔 | 紀錄者 | 王兆立 | 時間 | 2017/11/14 17:00 |
| | | | | | 地點 | 綜合教學大樓 7F |
| 預定討論主題 | 資料統整及分析 | | | | | |
| 指導老師意見 | | | | | | |

【會議記錄】

| | | | | | | |
|--------------------|--|--------|---------------------------------------|------|------------------|------------------|
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | | | | | |
| 會議編號 | 03 | 召集人兼主席 | 楊子鎰 | 紀錄者 | 王兆立 | |
| 討論主題 | 資料統整及分析 | | | 會議時間 | 2017/11/14 17:00 | |
| | | | | 會議地點 | 綜合教學大樓 7F | |
| 上次會議 | 決議事項 | | 執行狀況 | | | |
| | 專題製作方向及報告書製作 | | 確實執行 | | | |
| 本次會議 | 本次工作進度 | | 本次會議內容 | | 負責人員 | |
| | 資料統整及分析 | | 1. 企業資料統整及分析 2. 報告書內容撰寫 3. 問券調查 | | 全體 | |
| 本次會議內容 | <p>搜尋台灣前 50 成份股企業的 CSR 企業社會責任的報告書，並對於當中與資安及個資保護相關的關鍵字進行整理。</p> <p>報告書第二章內容發想。</p> <p>問卷題目分為三個議題：一、基本資料調查，二、相關議題關注程度調查，三、主觀感受及需求調查。並於 11/16 開始進行問卷發放，截止於收集 200 份有效問卷。</p> | | | | | |
| 決議事項 (與主席裁示) | | | | | | |
| 專題報告書第二章文獻探討與回顧完成。 | | | | | | |
| 請簽名 | 請簽名 | 請簽名 | 請簽名 | 請簽名 | 請簽名 | |
| 下次會議 | 召集人 | 楊子鎰 | 紀錄者 | 張光祐 | 時間 | 2017/12/28 08:20 |
| | | | | | 地點 | 圖書館 601 教室 |
| 預定討論主題 | 網站架設構思 | | | | | |
| 指導老師意見 | | | | | | |

【會議記錄】

| | | | | | | |
|---|--|--------|---|------|------------------|------------------|
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | | | | | |
| 會議編號 | 04 | 召集人兼主席 | 楊子鎔 | 紀錄者 | 張光祐 | |
| 討論主題 | 網站架設構思 | | | 會議時間 | 2017/12/28 08:20 | |
| | | | | 會議地點 | 圖書館 601 教室 | |
| 上次會議 | 決議事項 | | 執行狀況 | | | |
| | 資料統整及分析 | | 確實執行 | | | |
| 本次會議 | 本次工作進度 | | 本次工作內容 | | 負責人員 | |
| | 網站架設構思 報告書依進度完成 問券分析 | | 1. 網站架構設計 2. 網站內容討論 3. 報告書內容撰寫 4. 問券分析 | | 全體 | |
| 本次會議內容 | <p>報告書第三章內容構思。</p> <p>網站架設選使用 000WEBHOST 及 Microsoft VisualStudio，並進行網頁功能及作用的討論。</p> <p>問券統整及結果分析。</p> | | | | | |
| 決議事項 (與主席裁示) | | | | | | |
| <p>專題報告書第三章系統結構與運作完成。</p> <p>架設網站相關設施討論及功能發想。</p> | | | | | | |
| 請簽名 | 請簽名 | 請簽名 | 請簽名 | 請簽名 | 請簽名 | |
| 下次會議 | 召集人 | 楊子鎔 | 紀錄者 | 張家豪 | 時間 | 2018/02/27 15:30 |
| | | | | | 地點 | 綜合教學大樓 7F |
| 預定討論主題 | 網站建置 | | | | | |
| 指導老師意見 | | | | | | |

【會議記錄】

| | | | | | |
|------------------------------------|---|------------|---------------------------------------|----------|------------------------|
| 專題 名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | | | | |
| 會議 編號 | 05 | 召集人 兼主席 | 楊子鎔 | 紀錄者 | 張家豪 |
| 討論 主題 | 網站建置 | | | 會議 時間 | 2018/02/27 15:30 |
| | | | | 會議 地點 | 綜合教學大樓 7F |
| 上次 會議 | 決議事項 | | 執行狀況 | | |
| | 網站架設構思 報告書第三章完成 | | 確實執行 | | |
| 本次 會議 | 本次工作進度 | | 本次工作內容 | | 負責人員 |
| | 網站建置開始 報告書完成 簡報完成 | | 1. 網站架設討論 2. 資料庫伺服器架設 3. 報告進度討論 | | 全體 |
| 本次 會議 內容 | 網站架設開始，多方嘗試各類型外掛及功能測試，預計於 5 月底完成 網站架設。 報告書及簡報進度分析，預計於 5 月底完成所有內容。 | | | | |
| 決議事項（與主席裁示） | | | | | |
| 網站架設於 5 月底完成。 報告書及簡報預計於 5 月底完成。 | | | | | |
| 請簽名 | 請簽名 | 請簽名 | 請簽名 | 請簽名 | 請簽名 |
| 下次會議 | 召集 人 | 楊子鎔 | 紀錄者 | 徐偉倫 | 時間 2018/05/29 09:00 |
| | | | | | 地點 圖書館 505 教室 |
| 預 定 討論 主題 | 成品討論及修改 | | | | |
| 指導老師 意見 | | | | | |

【會議記錄】

| | | | | | | |
|----------------|--|--------|-----------------------|------|------------|------------|
| 專題名稱 | 台灣 50 成份股企業 CSR 資安與個資保護觀察站 | | | | | |
| 會議編號 | 06 | 召集人兼主席 | 楊子鎔 | 紀錄者 | 徐偉倫 | |
| 討論主題 | 成品討論及修改 | | | 會議時間 | 2018/05/29 | |
| | | | | 會議地點 | 圖書館 505 教室 | |
| 上次會議 | 決議事項 | | 執行狀況 | | | |
| | 網站架設完成 報告書及簡報完成 | | 確實執行 | | | |
| 本次會議 | 本次工作進度 | | 本次工作內容 | | 負責人員 | |
| | 網站及資料庫除錯優化 報告書及簡報預覽 | | 1.網站完成及測試 2.專題發表籌畫 | | 全體 | |
| 本次會議內容 | <p>網站及資料庫測試。 籌備 6/11 專題發表內容，排定報告者、報告內容、報告方式。</p> | | | | | |
| 決議事項 (與主席裁示) | | | | | | |
| 報告者、報告內容、報告方式。 | | | | | | |
| 請簽名 | 請簽名 | 請簽名 | 請簽名 | 請簽名 | 請簽名 | |
| 下次會議 | 召集人 | 楊子鎔 | 紀錄者 | 李昱昌 | 時間 | 2018/06/12 |
| | | | | | 地點 | 圖書館 505 教室 |
| 預定討論主題 | 專題發表檢討 | | | | | |
| 指導老師意見 | | | | | | |



附錄二、問卷

CSR企業社會責任與資訊安全

親愛的受訪者 您好：

這是一份關於「CSR企業社會責任與資訊安全相關」問卷，採用匿名設計；您所提供的資料將予以保密，僅供本研究分析使用，不會做任何的商業用途，亦不會洩漏任何可辨識的個人資訊，請您安心填寫問卷。您的寶貴意見將成為本研究的重要資訊。

本問卷需佔用您一點時間填答，問題並無標準或對錯，請依照您心中主觀感受與想法進行填答，謝謝！

敬祝

平安快樂

致理科技大學 資訊管理系

台灣50成分股企業CSR資安與個資保護觀察站製作團隊

*必填

您平時有在關注政府或各企業對社會的貢獻嗎？*

- 有
- 沒有

您會從何處得知資安相關事件或知識呢？*

- 報章雜誌
- 網路論壇
- 新聞媒體
- 親朋好友
- 其他： _____

您時常於網路上提供個人資料嗎?(申辦帳號等) *

- 是
- 不是

您知道CSR企業社會責任嗎? *

- 知道
- 不知道

您會依企業對社會貢獻的程度作為評論該企業的依據嗎? *

- 會
- 不會

您對於現今各企業致力於資安保護的貢獻程度為何? *

1 2 3 4 5 6 7 8 9 10

最低 最高

如果要建立一個整合CSR有關資安與個資保護的網站，您會希望該網站提供什麼服務? *

- 關鍵字搜尋
- 資安未來發展趨勢
- 各項專有名詞及法規解釋
- 中英翻譯或多語言翻譯
- 相關新聞連結
- 其他： _____

您的性別? *

- 男
- 女

您的年齡? *

- 12歲以下
- 12-17歲
- 18-25歲
- 26-35歲
- 36-50歲
- 50歲以上

您的職業? *

- 學生
- 軍公教
- 工業
- 商業
- 家管
- 自由業
- 服務業
- 其他： _____

SINCE 1965