National Taiwan University

CSIE5500: Public Interest Cybersecurity Practices and Society

問題擬定與深度訪談實戰工作坊

國立臺灣大學圖書資訊學系 副教授 鄭瑋

協力：國立臺灣大學圖書資訊學系 研究生 龔俐霏、林語婕

暖身：今天早上，要一直說話

1. 請小組同學再次自我介紹，
2. 在自我介紹之後，小組可以一起討論以下問題：

3. 在日常生活中，你（或聽聞過的別人）採取了哪些措施來保護自己的資訊安全？
4. 講到「資安專業人員」，形象可能會是什麼？

最後請用自己的方法（推舉、抽籤...）讓一位同學總結小組的討論。

網路安全實務與社會 - 課程目標

- 評估非營利組織（NPO）之資安風險，進而協助解決其面臨的真實資安問題
- 為達到此目標，你會學到：
  - **理解** NPO 面臨的資安困境
  - **運用**資安檢核表、檢測工具、面談等方式蒐集所需資料
  - **分析**資料，指出核心業務之潛在資安威脅和影響
  - **提出**可落實之解決方案

密集課程主題總覽

	溝通面	管理面	技術面
風險評估相關技能	盤點組織內外部議題 （的訪談技巧）	威脅建模 風險緩解策略	資安檢測工具與操作 OSINT Framework 風險緩解技術方案
基礎知識	問題擬定與訪談技巧 Meet with your client	如何改變人的資安行為 假訊息對於組織的影響	資安威脅和趨勢 OWASP Top 10

	量化典範 預測或檢驗差異	混合典範	質性典範 解釋現象、理解脈絡
資料收集、研究設計方法舉隅	實驗法 問卷調查法（封閉）	日誌法（開放與封閉） 德菲法（專家調查法）	問卷調查法（開放） 訪談調查法 焦點團體法 行動研究法 田野調查、民族誌 案例研究
資料分析方法舉隅	資訊計量學 次級資料分析 社會網絡分析 敘述、推論統計	內容分析	歷史（文獻）分析

	量化典範 預測或檢驗差異	混合典範	**質性典範** **解釋現象、理解脈絡**
資料收集、研究設計方法舉隅	實驗法 問卷調查法（封閉）	日誌法（開放與封閉） 德菲法（專家調查法）	問卷調查法（開放） 訪談調查法 焦點團體法 行動研究法 田野調查、民族誌 案例研究
資料分析方法舉隅	資訊計量學 次級資料分析 社會網絡分析 敘述、推論統計	內容分析	歷史（文獻）分析

問卷調查法—有問題的「問題」

1. 你不覺得我們的產品是最好的嗎？
2. 請給與你工作和家庭情況的整體幸福感。（1-5, 5為最幸福
3. 你是否不喜歡不健康的食物？
4. 在過去的幾年裡，你經常使用我們的服務嗎？
5. 作為一個年輕人，你怎麼看待現在的教育制度？
6. 你同意大多數人認為環境保護很重要這個說法嗎？
7. 請簡要地詳細描述你上一次購物的體驗。
8. 你每週在 threads 上花費多少時間：（0 - 1小時、1 - 3小時、3 - 5小時， 5 小時以上？
9. 為什麼你認為我們的競爭對手的服務品質不如我們？
10. 在疫情期間，你是否因為害怕感染病毒而減少了購物？

問卷設計原則

1. 意義清楚原則
2. 客觀公正原則
3. 選項窮盡與互斥原則
4. 敏感性問題原則
5. 回答默從問題的處理原則

雖然是「問卷設計」原則，我們將部分原則借用來發展晤談問題

Source: 俞振華-**問對問題找答案**： **調**查方法與問卷設計

晤談問題設計 –意義清楚原則(1/2)

有意識使用術語或專業詞彙（隨著受眾調整）

- [X] 對資安術語不熟悉的實習生：「您有實施端點防護嗎？」
- [O]「您在所有使用中電腦和設備上有裝了什麼可以保護資訊安全的軟體？」

避免超過受訪者角色能力的問題：

- [X]「您的組織在過去三年中的預算是多少？」（問工程師）
- [X]「您對第七期國家資通安全發展方案的看法是什麼？」
- [X]「您對於九二一大地震的印象是？」（問還沒出生的20代實習生
- [O]「您或周遭親友提及地震經驗中，對九二一地震的描述是什麼？」

小練一下

有意識使用術語或專業詞彙（隨著受眾調整）

- [X] 對資安術語不熟悉的實習生：「您有實施端點防護嗎？」
- [O]「您在所有使用中電腦和設備上有裝了什麼可以保護資訊安全的軟體？」

面對不熟悉資安術語的受訪者，請調整這個問題：

您的組織中，高權限帳號是否有開啟 MFA（多重要素驗證）？

晤談問題設計–意義清楚原則(2/2)

避免雙管問題(Double-Barreled Question, DBQ 又稱雙重負載問題)

- [X]「您是否同意將員工餐廳關閉，並且開設遊戲中心？」
- [X]「您是否有備份並加密敏感資料？」

避免雙重、多重否定敘述

- [X] 您是否不同意不應該在資源有限的情況下優先加強資安防護？

11

你是否同意在國民教育階段內 (國中及國小)，教育部及各級學校不應對學生實施性別平等教育法施行細則所定之同志教育？

白話文：你是否反對國中、小施行同志教育？

同意	不同意
反對同志教育	支持同志教育

09

你是否同意政府維持禁止開放日本福島 311 核災相關地區，包括福島與周遭 4 縣市 (茨城、櫪木、群馬、千葉) 等地區農產品及食品進口？

白話文：你是否反對福島核災食品進口？

同意	不同意
反對核災食品	支持核災食品

https://www.thenewslens.com/article/106137

晤談問題設計–公正客觀原則

避免情緒性的言語及植入研究者之偏見、避免引導受訪者至社會可接受價值之問題，或其他具有誘導性問題

- [X]「 對於那些罪大惡極的網路駭客，政府的政策是否適當？
- [X]「說謊被普遍認為是不好的行為，您在過去三天內是否說過謊？」

避免失衡的陳述句

- [X]「您不贊成...?」
- [O]「您是否贊成...?」

晤談問題設計–選項窮盡且互斥原則

使答案之類類別或選項互斥、窮盡、且達到平衡

- [X]「請問您在工作，還是失業中？（那對於正在待業的人士？）」
- [X]「您如何評價公司員工的整體資安意識？ 是較低還是一般般？（沒有正面的選項）

晤談問題設計–敏感性問題處理原則

若存在科學證據，或基於事實，不妨說明這種情況很正常

- [O]「科學實證顯示一個人平均一天會說謊2.2 次，是否方便和我們分享…？」
- [O]「選舉時有些人會去投票，有些人不會去投票。請問去年的選舉您有沒有去投票？」

晤談問題設計–回答默從問題的處理原則

人對於不熟悉、抽象、又是一長串的敘述的問題，傾向回答正面的回應

- [X]「 考慮到當前日益複雜的網路威脅環境，包括但不限於分布式阻斷服務攻擊（DDoS）、社交工程釣魚郵件、勒索軟體、零日漏洞利用、SQL注入、跨站腳本攻擊（XSS）、中間人攻擊、供應鏈攻擊，以及考慮到物聯網（IoT）設備的大幅增加帶來的新的安全挑戰，再加上遠距上班這樣的工作趨勢，並且鑑於人工智能和機器學習在網絡攻擊中的應用日益普遍， 淨零碳排的政策下，您是否同意我們公司應該顯著增加對先進持續性威脅（APT）防禦系統的投資，包括但不限於下一代防火牆、端點檢測與響應（EDR）解決方案、安全資訊與事件管理（SIEM）系統、使用者與實體行為分析（UEBA）工具，以及威脅情資，以確保我們能夠有效地檢測、預防、響應和緩解這些不斷演變的複雜威脅，從而保護我們的數位資產和敏感資料免受潛在的攻擊？ 」（ㄜ...好，為什麼有淨零碳排啊）
- [O] 拆成：

- 「在您的日常工作中，您在工作中最常遇到哪些資安挑戰？」
- 「如果公司要增加資安投資，您認為應該優先考慮哪個領域？」

深度訪談（in-depth interview）

深度訪談法如同問卷法，也是提出問題達到蒐集資料的研究方法。不過，除了「一問」與「一答」，深度訪談更像是一種有目的、程度上面對面的對話過程。

研究者與研究參與者的關係，會和問卷法比起來，更加靠近、平等、有互動。

為什麼這門課程想要讓大家培養訪談技巧

- **了解脈絡的多樣性與獨特性**：深度訪談可以使師生能夠根據每個組織的具體情況，而收集需要的資料。
- **探索議題背後的細節**：在討論非營利組織的資安問題時，可能涉及各種獨特且具挑戰性的原因，如外界無法第一時間想到的內外部問題等。訪談技巧可以幫助大家一起探索這些議題背後的細節。
- **協助揭示個人經驗與感受**：訪談技巧幫助師生洞察到所服務之組織或企業，對一些挑戰還有解方的想法和態度。

深度訪談的大致過程

- **訪談前**：決定訪談對象（抽樣）、覺察議題、決定訪談類型（結構式、半結構、非結構；正式、非正式？）、**設計訪談問題、尋找合適地點**、聯絡潛在受訪者（如何確保託付給最可靠的人...）、準備設備與現場材料（錄音筆？錄影設備？到時候是否使用專業軟體協助做筆記、便條紙）
- **訪談中**：詢問問題、 檢核、摘要、與受訪者討論（debriefing）、 行政程序（是否有知情同意書或是車馬費之領據需要簽署）
- **訪談後**：盡快回憶相關細節並且標示重點、進行逐字稿與後續分析

深度訪談-訪談前

- 決定訪談對象（利益關係者）
- 覺察議題（e.g., ISO27001內外部議題）
- 決定訪談類型（結構式、半結構、非結構；正式、非正式？）
- 設計訪談問題
- 尋找合適地點、聯絡潛在受訪者
  準備設備與現場材料：錄音筆？錄影設備？到時候是否使用軟體、工具協助做筆記、便條紙（莫小看道具的力量，沒帶筆有時候會很慘）

訪談前｜問題的內容外，順序很重要

- 留意訪談問題的順序、保持訪談內容的彈性

研究者要保持訪談過程與內容的彈性，切勿期待一開始的訪談、或是一次的訪談就能蒐集到核心切題的資料（對某些議題來說，回訪是必要的），宜視整體情況做彈性調整。

一般來說，安排訪談問題的順序是：

先簡單（基於事實性的、較不敏感的、容易回想的），
再複雜（聚焦於研究問題的、情感交織的、涉入個人價值的、擁有特殊個人意見的）。

訪談中｜避免引導性問題，讓受訪者自在表達

- 鼓勵自由表達：給予充分時間思考和回答、使用開放式問題
- 適度追問細節：當回答不夠清楚時，使用「能幫我們多說一些嗎？」、「能幫我們多說一些關於這次全新購置的NAS的情況嗎？」等開放性問句

訪談中｜避免引導性問題，讓受訪者自在表達

實際操作方式：

1.「檢核」：即是在訪談的途中，研究者與受訪對象確認自己捕捉到的概念是否有誤解，則需要請對方澄清。

- 受訪者：「我們最近改善了密碼政策，現在員工都使用更安全的密碼了。」
- 訪談者：「這聽起來是個很好的改進。能否請您詳細說明一下，改善後的密碼政策是怎麼樣的？」
- 受訪者：「我們建議員工每兩週就要換一次密碼，而且密碼需要15碼以上。」
- 訪談者：「讓我確認一下我是否正確理解了您的政策。您要求員工每兩週更換一次密碼，並且新密碼必須至少有15個字，對嗎？」
- 受訪者：「是的，沒錯。我們認為這樣可以大大提高安全性。」
- 訪談者：「謝謝您的解釋。這確實是一種改革。不過，我想進一步了解一下，您有觀察到員工對這個政策的反應嗎？」

訪談中｜避免引導性問題，讓受訪者自在表達

實際操作方式：

- 2.「摘要」則是遇到一長串原話，研究者可使用此法將訪談的 flow 拉回原本的研究問題，這個時候提供摘要給對方，要注意摘要部分也要忠於原話，另也要注重語氣中立，不然就像是強迫對方接受您的解讀啦。
- 訪談者：「非常感謝您的分享。讓我稍微總結一下我們剛才討論的要點，請您確認我是否理解正確：貴公司實施了每兩週更換一次、至少15字的密碼政策，但發現員工對於遵守這個政策有些難處。接續我們討論了如此一來員工可能選擇更簡單的密碼或將密碼寫下來，因此您也提及正在考慮的替代方案，如重因素認證。我的理解正確嗎？有什麼要補充的嗎？」
- 受訪者：「總結得很好。我想補充的是，我們也在考慮加強員工的資安意識培訓。」

訪談者：要維持訪談節奏靈活輕巧（1/2）

⇢ 利用「轉場」形式的語句促使訪談過程的流暢

如同對話，研究者在問題之間應有相互聯繫的技巧，這樣訪談過程中才能自然與流暢。教科書整理了四種轉場技巧與例子，以「 詢問設計者打造網站使用體驗 」類似的主題，供同學參考：

- 一般轉換（最普通的）：「我們剛剛已經討論到您所設計之網站的潛在使用者可能遇到的困難，接下來，想請問您的網站設計了什麼樣的方法來排除這個情況呢？」
- 摘要轉換：「在我進到下個問題之前，我先確認一下我有完整紀錄您剛剛的回答，...，分為 1, 2, 3, 4 這四點困難，請問您有任何需要補充的嗎？好的，謝謝您，那我們現在進到下一題。想請問您的網站設計了什麼樣的方法來排除這個情況呢？」
- 直接宣告（可讓節奏輕快但也要注意禮節喔）：「那麼，現在想請您分享，自從您設計了這樣的方法來排除狀況，後續是否能看到使用者流量的改變呢？」
- 喚起注意：「下一個問題就進入到我們今天訪談的重點了，您覺得一個成功的網站應具備哪些排除錯誤的能力？」

訪談者：要維持訪談節奏靈活輕巧 (2/2)

（補充）應用這些技巧的注意事項

1. **一般轉換**：適用於大多數情況，能自然地將話題從一個方面引導到另一個方面。
2. **摘要轉換**：在轉向一個較不相關的議題時，或是受訪者剛剛的回答有些模糊特別有用，能確保雙方對前面討論的內容有共識。
3. **直接宣告**：當需要快速轉向相關的新話題時使用，但要注意保持禮貌和專業性。在討論敏感的資安問題時要特別謹慎。
4. **喚起注意**：適用於引入特別重要或可能需要深入討論的話題，如關鍵的資安決策或最佳實踐。

小組練習！

一般來說，安排訪談問題的順序是先簡單（基於事實性的、較不敏感的、容易回想的），再複雜（聚焦於研究問題的、情感交織的、涉入個人價值的、擁有特殊個人意見的）。

⇢ **原始的問題順序**

1. 您在公司工作多久了？職責範圍是什麼？
2. 您對公司未來的資安政策有什麼個人的看法？
3. 貴公司目前使用哪些資安工具？
4. 您如何評價這些工具的效果？
5. 貴公司是否考慮過採用外部資安服務？為什麼？
6. 您認為採用外部資安服務可能帶來哪些影響（e.g., 好處或挑戰）？
7. 在選擇資安服務提供商（如捐款網站），您會考慮哪些因素？

訪談剛結束｜合作愉快！餘韻無窮

與受訪者討論（Debriefing）是訪談結束時的重要環節，提問者可以提供輕鬆自然的對話緩衝。在正式問題結束後，研究者可以揭示完整研究目的，或就剛剛訪談中提到的話題進行輕鬆閒聊。例如，「您剛提到的工具我也用過，真的很不錯！」

⇢ 實戰技巧：

- 結合行政程序（如簽署車馬費領據、再次宣讀權利義務、確認下次開會時間）進行debriefing，既有效率又不占用過多時間。
- 靈活調整：若受訪者趕時間，應就速速結束。

深度訪談-訪談後

訪談後：盡快回憶相關細節並且標示重點、進行逐字稿與後續分析

為什麼要即時記錄？

- 捕捉語氣、態度與熱情的差異
- 反映訊息的不同「重量」(weight)
- 防止記憶消退
- 逐字稿完善可能需要數天或數週時間
- 及時記錄有助於重建現場感受和重拾靈感

一些收穫到（harvested）資料的範例

日期: 2024年9月27日 受訪者: 張經理（IT部門主管）
地點: 公司會議室 時間: 14:00-15:30
現行密碼政策：每兩週更換，至少15碼
張經理談到密碼政策時顯得非常自信，但提到員工抱怨時語氣明顯變得有防衛心
提到“每兩週換一次密碼”時，張經理的語速加快，由衷覺得可以改善目前的問題
當安Ｊ提醒到頻繁換可能的安全風險時，張經理看起來是驚訝的。安Ｊ的態度很友善，並不會讓張經理感到被冒犯，學長，好穩丫。
整個訪談過程中，張經理經常提到"符合行業標準"，這似乎是他決策的主要依據
談到多重因素認證時，張經理感覺是願意嘗試的！

一些收穫到（harvested）資料的範例

初步分析與思考

公司的主理人的兒子最近被網路詐騙過

似乎處於資安策略的轉折點，可能是研究深入探討的好時機

預算vs安全需求的權衡是一個重要主題，值得在未來的訪談中進一步探討

要注意訪談結果可能受到主理人個人動機和近期事件的影響

- 留意參與者之動機對研究產生的影響
- 正式訪談前可以先進行預訪談或試訪

照顧資料的源頭：因為，人是人

- 注意訪談長度、訪談情境的適切性，以開放和尊重的態度對待受訪者：
- 確保他們感到被重視和舒適
- 提問者應真誠尊重受訪者的隱私

有效的訪談姿態：

- 提問者應保持中立態度，避免對受訪者的回答做出評價。
- **總是讓受訪者掌握回答的主控權**，同時保持專注聆聽和適當的眼神交流。
- 創造一個讓受訪者事前就敢於拒答的氛圍（這...不容易！更常見的是：受訪者勉為回答，但可能事後越想越不對勁而投訴...

訪談團隊配置建議

理想上，訪談團隊應至少由兩人組成：

- 主問者專注於聆聽和提問，而記錄者則負責記錄筆記。
- 如果只有一位提問者，建議將訪談大綱印出，並用圈寫或手寫關鍵字的方式記錄重點，同時保持與受訪者的互動。
  （一直看著筆電飛速打字，很難有眼神接觸
- 訪談後應盡快整理細節和重點。

36道練習題：拉近小組成員的距離

友誼升溫、墜入友誼的小河