用遊戲打開資安世界

一場讓學生不想輸的資安人生挑戰賽！

【計算機概論】課程中的資安議題，常被學生視為抽象、遙遠且難以應用。陳昱圻老師嘗試將奧義智慧科技研發的《資安人生》桌遊融入課程設計，透過遊戲情境讓學生化身為「資產守護者」，在有限預算下對抗各種攻擊事件，親身體驗資安策略的決策歷程。

在遊戲過程中，學生不只是記憶資安名詞，而必須依據防護架構進行整體布局，思考如何從辨識風險、防禦攻擊到復原損失，逐步建立「防禦縱深」的策略觀念。遊戲中「被炸扣錢」的即時回饋，也讓學生因為「不想輸、不想破產」，因而積極參與參與，有效提升學習動機與課堂互動。

也由於遊戲情境與自身生活經驗連結（如：攻擊事件對應日常使用的線上平台），讓專有名詞轉化為生活經驗的一部分，使學生更能理解資安概念並建立風險意識，縮短理論與實務之間的距離。資安學習不再只是「聽懂」，而是「用得出來」！

<table>
<tr><th colspan="5">課程基本資料</th></tr>
<tr><td>授課教師</td><td>陳昱圻</td><td>教學單位</td><td colspan="2">資訊工程系</td></tr>
<tr><td>課程名稱</td><td colspan="2">計算機概論（必修）（3 學分）</td><td>修課人數</td><td>46</td></tr>
<tr><td>欲解決的
教學現場問題</td><td colspan="4">在現今資安教育的教學現場中，常面臨學生學習動機低落、資安知識理解片段，以及缺乏生活化連結等問題。學生普遍認為資安議題抽象且與自身無關，導致課堂參與度不高，學習成效有限。即使具備部分資安知識，也常無法整合應用於真實情境中，形成知識與實務的落差。此外，資安教學若未貼近生活經驗，學生難以建立資安意識與行動力。為解決上述問題，本計畫將導入奧義智慧科技研發的《資安人生》桌遊，透過遊戲化學習設計，讓學生在互動情境中主動參與、整合知識並體驗資安事件，進而提升學習興趣、強化應用能力，並建立資安與日常生活的連結。</td></tr>
<tr><th colspan="5">遊戲導入之教學設計</th></tr>
<tr><td rowspan="3">第一次導入之教學設計</td><td>當週主題</td><td colspan="3">資訊安全</td></tr>
<tr><td>教學目標</td><td colspan="3">■ 讓學生知道：資訊安全的基本概念，包括社交工程、資安事件應對等。
■ 讓學生能夠：辨識日常生活中常見的資安風險與防範措施。</td></tr>
<tr><td>遊戲名稱</td><td colspan="3">資安人生（市售實體遊戲）
網址：https://www.cycraft.com/news/board-game-cybercans-3th-anniversary （無公開販售）</td></tr>
</table>

	遊戲簡介	《Cybercans：資安人生物語》是由奧義智慧科技研發的資安教育桌遊，結合真實資安事件與策略思考，讓玩家在遊戲中扮演企業資安長，面對各種資訊安全挑戰。遊戲以「Cyber Defense Matrix」為架構，涵蓋裝置、應用程式、網路、資料與使用者等五大資產類別，並對應識別、防護、偵測、回應與復原等防禦階段。玩家需在有限資源下擬定資安策略、購買防禦卡、應對新聞與攻擊事件，提升企業資安韌性。透過擲骰前進、抽卡互動與角色扮演，遊戲不僅提升資安知識，更強化風險評估與決策能力，適合教育場域、企業訓練與資安推廣活動使用。活動方式類似大富翁。		
	遊戲時間	預計 60 分鐘	**參與方式**	個人
	遊戲內容	人數限制	遊戲規則中限制之人數上限：6	
		故事情境	在不遠的未來，全球資訊環境陷入混亂，駭客組織掀起一波波網路攻擊浪潮，企業機密外洩、系統癱瘓、詐騙訊息如病毒般蔓延。你身為公司的資安決策者，正面臨前所未有的挑戰。公司即將發表一項劃時代的創新產品，卻在倒數階段接連遭遇資安事件：釣魚郵件滲透內部網路、員工帳號遭破解、雲端資料庫頻頻被掃描。面對有限的預算與時間壓力，你必須迅速擬定防禦策略，部署資安設備、強化員工意識、建立應變機制。每一次選擇都將左右企業的命運！你是否能在這場資安風暴中穩住陣腳，守住企業的最後防線？	
		運作規則	《資安人生》是一款以資安防禦為主題的策略型桌遊，玩家(以個人為單位)扮演企業資安長，目標是在資安風險環伺的環境中，妥善運用資源保護企業資產。遊戲採回合制進行，玩家輪流擲骰前進棋盤，根據停留格子觸發事件（如攻擊、新聞、資源獲得等），並透過卡牌配置與資源管理，建構企業的資安防線。 • 擲骰移動：每位玩家輪流擲骰，依點數前進棋盤。 • 事件觸發：根據停留格子抽取對應卡牌（如攻擊事件、新聞事件），並執行卡牌效果。 • 資源管理：玩家擁有預算點數，可用於購買防禦卡，部署於資安矩陣中。 • 防禦配置：依照「Cyber Defense Matrix」架構，將防禦卡放置於對應資產類別與防禦階段。 • 勝利條件：遊戲結束時，成功抵禦最多攻擊、維持企業穩定者獲勝。	

<table>
<tr><td rowspan="7"></td><td>課程關聯</td><td colspan="3">《Cybercans：資安人生物語》桌遊與資訊安全的關聯性極為密切，其設計核心即是為了推廣資安知識與實務應用。遊戲架構採用「Cyber Defense Matrix」資安防禦模型，涵蓋五大資產類別（裝置、應用程式、網路、資料、使用者）與五個防禦階段（識別、保護、偵測、回應、復原），完整呈現企業資安防禦的全貌。透過模擬真實資安事件（如釣魚攻擊、密碼外洩、勒索病毒等），玩家需在遊戲中進行風險評估、策略部署與資源管理，實際體驗資安決策的過程。這不僅強化玩家對資安概念的理解，也培養其應變能力與防禦思維，使資訊安全不再只是抽象理論，而是可操作、可體驗的實務技能。特別是在《計算機概論》課程中，資訊安全章節常涵蓋資安基本原則、常見威脅類型、防護技術與個人資安習慣等內容，本桌遊可作為該章節的延伸教學工具，透過情境式學習讓學生將課本知識轉化為實際行動，提升理解深度與學習動機。因此，《資安人生》不僅是教學媒介，更是資訊安全素養培養與計算機概論課程在資安這個段落整合的實踐橋樑。老師介紹基礎資安管理概念與遊戲規則，桌遊進行時，老師安排助教作為引導者提供協助。</td></tr>
<tr><td rowspan="6">當次課程
2節100min
流程安排</td><td>時間</td><td>規劃內容</td></tr>
<tr><td>10 min</td><td>基礎資安管理概念、課程導入與情境設定</td></tr>
<tr><td>15 min</td><td>遊戲規則與分桌</td></tr>
<tr><td>60 min</td><td>桌遊進行</td></tr>
<tr><td>10 min</td><td>小桌分享與回饋問卷填寫
（桌遊進行以個人為單位，此階段為小桌的策略分享時間）</td></tr>
<tr><td>5 min</td><td>教師總結此次遊戲式教學目的，並對遊戲與課程關聯做補充</td></tr>
<tr><td rowspan="6">第二次導入之教學設計</td><td>當週主題</td><td colspan="3">資訊安全</td></tr>
<tr><td>教學目標</td><td colspan="3">■ 讓學生知道：資訊安全的基本概念，包括社交工程、資安事件應對等。
■ 讓學生能夠：透過上回經驗，重新研擬資安策略。</td></tr>
<tr><td>遊戲名稱</td><td colspan="3">The Storymatic Advance（市售實體遊戲）
網址：https://www.amazon.com/Storymatic-Classic-Creative-Writing-Prompts/dp/B004PICKDS?ref_=ast_sto_dp</td></tr>
<tr><td>遊戲簡介</td><td colspan="3">同第一次遊戲</td></tr>
<tr><td>遊戲時間</td><td>預計 60 分鐘</td><td>參與方式</td><td>個人</td></tr>
<tr><td>遊戲內容</td><td>人數限制</td><td colspan="2">遊戲規則中限制之人數上限：6</td></tr>
<tr><td></td><td>故事情境</td><td colspan="2">一覺醒來，發現上週在教室是在夢裡擔任資安決策者，有了夢裡的經驗，你手上又剛好有一家公司，那就自己實際以自己公司的角度出發，擔任自己公司的資安決策者吧！</td></tr>
</table>

		運作規則	同第一次遊戲
	課程關聯	**學生們將藉由已發展的部分故事內容加以衍生創作延續故事，訓練接續故事脈絡邏輯以及激發創意。在第二次導入《資安人生》桌遊時，雖然遊戲內容可維持原架構，但應透過經驗回饋 → 策略反思 → 優化實踐的歷程，讓學生展現學習成長與策略深化。特別是重新調整重新調整資安矩陣(如下)配置，鼓勵學生提出更新方案，例如：加強使用者教育、防範社交工程、提升偵測能力等。**	
	當次課程 2節100min 流程安排	**時間**	**規劃內容**
		20 min	說明遊戲與當週課程主題的連結，介紹遊戲中的情境與玩法
		50 min	進行遊戲，同學們以分組方式在固定的時間內完成遊戲發表
		20 min	同學們互相評比，投票選出最佳的組別並延伸討論內容
		10 min	讓學生進行問卷回饋

學生回饋 與 教學優化

	第 1 次
課後學生反饋	一、 高風險攻擊帶來的震撼與資安現實感 學生對 Chimera 的 Skeleton Key、DoppelPaymer 勒索軟體等高傷害攻擊卡印象最為深刻。回饋中多次提到，即便抽到防禦卡，面對這類攻擊仍可能面臨巨額損失(如噴掉 6000 元或面臨破產)，這讓學生深刻體認到資安防禦並非「萬靈丹」。學生從中學到：即便事前有所準備，一旦遭受針對性強或供應鏈攻擊(如 Solargate)，企業仍需付出慘痛代價，這種「無法全身而退」的挫折感成功轉化為對資安現實艱難度的理解。 二、 防禦策略的價值辨析與層級認知 學生在遊戲中展現了對不同防禦階段(Identify, Protect, Detect, Respond, Recover)的思考。Red Team(紅隊演練)與 Threat Intelligence(威脅情資)因能於攻擊前期(Identify/Detect)攔截損害而被公認為高價值卡牌；相對地，部分學生對 Disaster Recovery(災難恢復)等事後補救卡牌感到沮喪，認為其成本高且無法減少既定損失。此外，學生也觀察到 User(使用者端)的防禦相對稀缺且難以判定成功，進而反思內部威脅(Insider Attack)與社交工程在實務上的防護難點。 三、 資安概念與日常生活經驗的連結 問卷顯示，當抽象的資安術語與學生的生活經驗結合時，學習效果最為顯著。例如：學生透過 Apex 遊戲遭 DDoS 攻擊的經驗，秒懂了阻斷服務攻擊的威力；透過

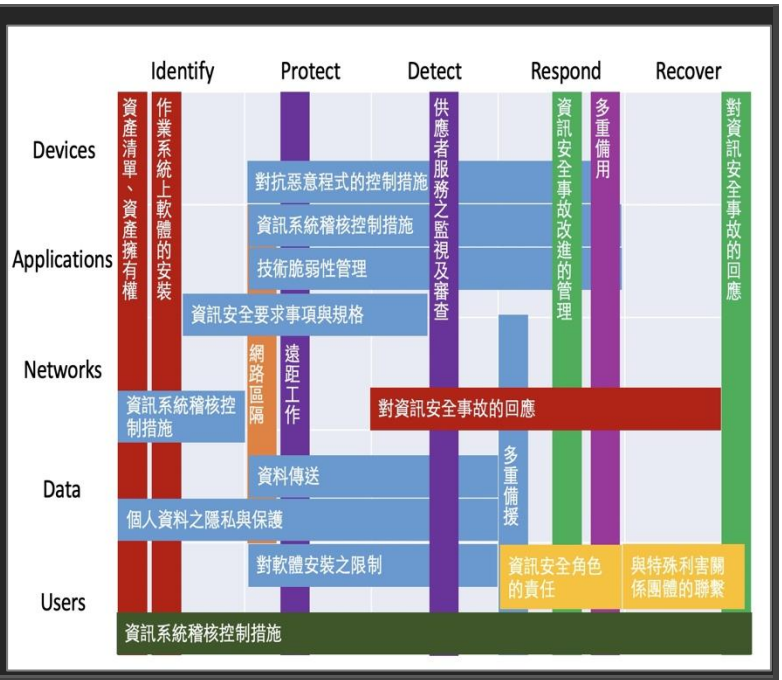
	Authy 等應用程式理解了 **2FA (二階段驗證) **的必要性。這種將「課本知識」與「個人生命經驗 (如高中研究過的加密技術、對水熊蟲的好奇)」掛鉤的反應，大幅拉近了學生與資安議題的距離，提升了學習動機。 四、 遊戲機制驅動的情緒參與與反思 遊戲中的隨機性 (如新聞卡的強制扣款、骰子點數決定成敗) 引發了強烈的情緒波動。學生提到「一直被攻擊卻抽不到防禦卡」的無奈，以及「資安發大財」或「Bug Bounty」帶來的轉機，這些機制模擬了現實中資安攻防的不可預測性。學生在懊悔「忘記使用卡片」或「丟錯牌」的過程中，不僅是在玩遊戲，更是在反思資源配置的優先順序，並透過與隊友交換卡牌或「夥伴募集」等互動，體驗到資安防護中「資訊共享」與「策略協作」的重要性。。
對應教學優化策略	一、 強化「風險管理」與「殘餘風險」的量化概念 • 導入 BIA (企業衝擊分析): 針對學生對「Skeleton Key」造成巨大損失的恐懼，可以引導學生計算「預期損失 (ALE)」。 • 討論殘餘風險：藉由「防禦成功仍要付錢」的機制，解釋現實中即便有完善防禦，仍有調查、鑑定與商譽損失等「殘餘風險」，教育學生資安目標非「零風險」而是「風險控管」。 • 優化教具：提供一張「風險評估表」，讓學生在遊戲中途記錄遭遇攻擊的損失，並在課後分析哪種投資 (卡牌) 的投資報酬率 (ROI) 最高。 二、 深化 NIST 網路安全框架 (CSF) 的策略運用 • 可視化防禦縱深：利用 NIST CSF 的五大階段 (辨識、保護、偵測、響應、復原)，要求學生在下一場遊戲前，根據手牌分類並畫出其「防禦架構圖」。 • 策略對比教學：針對學生提到的「偵測型 (Red Team)」與「復原型 (Disaster Recovery)」卡牌，組織辯論或小組討論：在預算有限下，應該優先投資「事前辨識」還是「事後韌性」？這能幫助學生理解資安資源分配的兩難。 三、 擴展「情境式」與「生活化」的案例研究 • 案例對齊遊戲：將學生感興趣的 Apex DDoS 攻擊、SolarWinds 供應鏈攻擊或 半導體業 Skeleton Key 案例 寫成詳細的 Case Study。 • 時事新聞卡更新： 邀請學生根據最近一週的資安新聞 (如 AI 詐騙、電商個資外洩)，自行設計「新聞卡」或「攻擊卡」，這能訓練其觀察產業動態的能力，並提升參與感。 • 生活防護連結：延續學生對 2FA/Authy 的興趣，介紹 MFA (多因素驗證) 的各種實作方式及其在遊戲中對應的「User 分類」卡牌。 四、 針對「人為因素」與「社交工程」的專題補強 • 探討「最弱的一環」: 針對學生觀察到「User 防禦卡較少」且「內部威脅難防」的點，開設專題討論「人性弱點」。

	• 角色扮演擴展： 在遊戲中加入「社交工程」回合，允許玩家透過口頭溝通（或欺騙）來交換資訊或資源，模擬社交工程攻擊中的心理博弈，讓學生對人性在資安中的影響有更深體會。 五、 建立「結構化」的遊戲後引導（Debriefing） • 錯誤學習清單：學生提到「忘記用 Bug Bounty」或「丟錯牌」，這類「人為疏失（Human Error）」本身就是極佳的教導點。建立一個「事故檢討會議（Post-Mortem）」環節，讓學生分享：如果重來一次，在資源有限下會如何調整防禦排程？ • 數據化反饋：收集全班的「最終資產」與「遭受攻擊次數」進行簡單統計，展示「積極投資防禦」與「被動承擔風險」在長遠來看的財富曲線差異。
	第 2 次
課後學生反饋	一、 策略佈局與防禦階段的價值權衡 學生對於防禦資源的配置展現出顯著的策略分歧。部分玩家傾向於「左移防禦」（Shift Left），優先購買 Identify（識別） 階段的卡牌（如紅隊演練），認為在攻擊前期就擋下最具效益，避免「到最後一層才擋」的無力感。然而，也有玩家採取「風險平均分攤」策略，在五大功能項目中各配置一張卡牌，或嘗試將點數集中於特定的 Detect（偵測）或 Respond（回應）防線。這些反饋顯示學生已開始思考資安防禦的縱深佈局與投資優先順序。 二、 隨機威脅（運氣）與現實資安的不可預測性 「運氣」與「隨機性」是反饋中的高頻關鍵字。學生深刻體會到，即便有精密的配置（例如：在 Detect 佈滿防線），若遇到連續的高頻攻擊（如抽到 18 張攻擊卡）或防禦判定失敗（骰到 6），企業仍會面臨破產或負債。這種遊戲體驗成功類比了現實中的「未知威脅（Zero-day）」與「機率性失效」，讓學生意識到資安並非 100% 的保證，而是在不確定性中尋求生存與韌性的過程。 三、 資安投資的成本效益（ROI）與財務思維 部分學生從企業決策者的角度出發，開始質疑防禦的成本合理性。有反饋指出，若「防禦卡價格加上授權費」高於「受攻擊的損失」，則傾向採取不購買或只買便宜卡片的「賭博式策略」。這種從純技術轉向「財務風險管理」的思維，反映出學生理解了企業在有限資源下，必須在「資安建置成本」與「潛在損失」之間進行艱難的權衡。 四、 角色認同與動態環境中的生存策略 遊戲機制的互動性引發了強烈的情緒參與，如「併吞隔壁同學資產」、「防禦卡被搶走後的裸奔狀態」等。學生在扮演「老闆」、「小企業」或「負債者」的過程中，體驗了從負債到翻身的動態歷程。這讓學生體認到資安防護並非靜態的配置，而是必須隨時根據財務狀況、外部突發事件（新聞卡）以及對手行為來靈活調整策略的動態博弈。

對應教學優化策略	優化成效之對應說明 若將上述反饋應用於第二次導入的優化，預期將能達到以下成效： • 從「盲目買卡」轉向「情境配置」：學生在反思「後端防禦效益不大」後，第二次配置時會更自覺地強化使用者教育（User）與前期偵測（Detect），降低防禦成本並提升攔截率。 • 提升決策的韌性：經歷過「瘋狂被炸」的學生，會學會預留現金流（Risk Buffer）以應對不可控的運氣因素，而非將點數全部鎖死在固定資產中。 • 強化社交工程意識：針對「卡片被搶」或「策略大失敗」的經驗，學生會更關注內部威脅與人性漏洞，進而主動在資安矩陣中加強對人的管理與防範。

課程實況

照片一：情境模擬，課堂問題演練。



照片二：桌遊實作，策略擬定

建議與回饋

遊戲導入課程後教師及學生的教與學之歷程變化	**教師**	遊戲導入後的變化核心在於：授課教師不再需要費力「推銷」知識，因為遊戲創造了「需求」。 學生因為「不想輸/不想破產」，主動產生了對資安知識的渴求，這正是教學歷程中最本質的優化。
	學生	從學生的角度來看，遊戲化學習最大的價值在於「賦權 (Empowerment)」。他們不再是被動等待老師灌輸知識的容器，而是手握預算、面對威脅、必須為自己生死負責的 CEO。這種「痛過才會記得」**的歷程，是傳統講述式教學難以取代的深層變化。
應用遊戲式學習後，是否解決申請表上設定的教學現場問題？		針對「學生學習動機低落，課堂參與度不高」的問題： 是，根據前述分析，遊戲機制將枯燥的資安理論轉化為「資產保衛戰」。學生從被動聽講轉變為「不想輸、不想破產」的積極參與者 (如反饋中提到「瘋狂被炸」引發的情緒波動)。這種「生存模式」激發了強烈的情緒涉入與求勝心，成功將學習動機從外在應付轉為內在驅動力。 針對「資安知識理解片段，無法整合應用」的問題： 是，學生在遊戲中必須運用 NIST 框架 (Identify 到 Recover) 進行整體佈局。反饋顯示，學生已從死背單字進化到思考「防禦縱深」與「連鎖效應」(如：發現只買最後一層 Recover 沒用，進而整合前端 Identify 與 Detect 的策略)。這證明遊戲能強迫學生將片段知識串聯成「系統化的防禦邏輯」。 針對「資安議題抽象且與自身無關，缺乏生活化連結」的問題： 是，遊戲將抽象的攻擊具象化為具體的「扣錢」痛感，並成功連結學生的生活經驗。前述反饋中，學生主動將遊戲中的 DDoS 攻擊連結到 Apex 英雄的遊戲體驗，將

	2FA 連結到 Authy 的使用經驗。「經驗掛鉤」讓資安不再是遙遠的技術名詞，而是與生活息息相關的切身議題。 針對「知識與實務落差，難以建立行動力」的問題： 是，傳統教學難以模擬「資源有限」的決策困境。遊戲透過預算限制與隨機風險（運氣/骰子），讓學生體驗真實世界中的「風險管理」與「成本效益分析（ROI）」。學生從反饋中展現出「計算預期損失」、「預留殘餘風險資金」等實務行為，成功橋接了理論知識與實務決策間的鴻溝。
是否持續以「遊戲式學習」優化後續課程教學？	是，持續以「遊戲式學習（Game-Based Learning, GBL）」之精神優化後續課程，但形式需從「桌遊體驗」進化為「實戰競技」與「機制整合」。 單純重複遊玩同一款桌遊會有邊際效益遞減（枯燥）的問題，因此後續優化應著重於將桌遊建立的「心智模型」遷移至「技術實作」。 後續優化的核心在於「鷹架作用（Scaffolding）」的搭建。透過桌遊完成第一階段的「引起動機」與「建立廣度」後，第二階段必須透過 CTF 與情境演練進入「技術深度」與「管理維度」。如此一來，才能確保學生從「覺得資安好玩」成功過渡到「具備資安專業能力」，實現從體驗到實戰的完整學習路徑。