ISSN 1023-2842
中山管理評論 2023 年三月號
第三十一卷第一期 p.171-200
DOI: 10.6160/SYSMR.202303_31(1).0006

凱舟濾材-中小企業透過數位技術防堵 BEC 詐騙

Caware Filtering Corporation- SME Use Digital Technology to Prevent BEC Fraud

張敏華 *Min-Hua Chang*
國立中山大學企業管理學系
Department of Business Administration,
National Sun Yet-sen University

黃子佳[*] *Tzu-Chia Huang*
國立中山大學企業管理學系
Department of Business Administration,
National Sun Yet-sen University

戴佑真 *You-Zhen Dai*
國立中山大學行銷傳播管理所
Department of Institute of Marketing Communication,
National Sun Yet-sen University

本文引用格式建議：張敏華、黃子佳、戴佑真，2023，「凱舟濾材-中小企業透過數位技術防堵BEC詐騙」，中山管理評論，31卷1期：171~200。
Suggested Citation: Chang, M. H., Huang, T. C., and Dai, Y. Z., 2023, "Caware Filtering Corporation- SME Use Digital Technology to Prevent BEC Fraud," **Sun Yat-sen Management Review**, Vol. 31, No. 1, 171-200.

[*] 通訊作者：黃子佳，地址：高雄市楠梓區德賢路 220 巷 58 號，Tel: 07-3686633，E-mail: jiajia1491@gmail.com。

摘要

網際網路、電子郵件其無國界、低成本、即時性及多元互動等特點，是凱舟跨國商務溝通高度依賴的科技媒介。2019 年變臉駭客利用「社交工程技巧」，獲取凱舟業務部員工電子郵件帳密，並接管其帳戶長期監看。根據與客戶往來郵件中洩漏的信息，設定縝密且合理的攻擊手法，多方交叉發信。詐騙客戶將貨款匯至其所預設的假帳戶，造成財損、客戶關係破裂和高管引咎辭職等刻不容緩的挑戰。

透過凱舟 BEC 攻擊始末，主旨在培養學生辨識與學會防範 BEC 的能力，提升資安意識。這包括理解駭客使用的技術與非技術性的手法，體會凱舟與客戶遭受經濟與非經濟面的損害。以有限資源組合有效的解決方案，強化商務經濟活動的安全，並帶來數位應用思維質變的成果。

關鍵詞：商務電子郵件詐騙(BEC)、數位轉型、資訊安全、社交工程、網路攻擊

Abstract

Caware’s international business highly relies on the convenient benefits from internet-web tech due to its features of cross border, low cost, real time and multi-parties communication. In 2019, The BEC hackers alter "social engineering technics" to snatch the log access of Caware sales employee's email account, and follow with consequently surveillance all emails within this account. By monitoring the leached messages and information of emails back-and-forth between Caware & her customers, the hackers locate the target customer & timing with a logical and meticulous manner written scrip. The hackers played the role of customer and supplier between Caware and her customer by sending-and-replying emails in order to hitch the trust of Caware & her supplier. Eventually, the fraud of BEC with hitched trust of Caware & her customer works to let the customer wire order payment into a new bank account which is a fraud bank account. The loss of money, infringement of customer relationship, and job quitting of some related core staffs are all timely crucial challenges for Caware's business operation. From understanding the story of Caware's BEC case, the main goal of this case coaching is to develop the students' sensibility and judgement against BEC attack, prevention skill, and to raise

cyber security sensibility therefrom. The acquisition from this coach session includes majorly the illustration of BEC hacker technics of either technical or non-technical manner and to figure the loss of Caware and her customers in the economic-wise or non-economic-wise as well. The side effect of coaching goal shall also shape out how to propose the most optimized solution portfolio by leverage limited resource, the security enhancement of business trading, and to alter the digitalization transformation in decision maker's mindset.

Keywords: Business Email Compromise(BEC), Digital Transformation, Information Security, Social Engineering, Cyberattack

個案本文

在 2019 年 4 月，凱舟與義大利客戶 Martech 公司在一場交易中，被駭客設局。凱舟員工 Maria 電子郵件遭入侵後，犯罪者註冊多個極為相似的電子郵件地址以假亂真，竄改通訊內容等方式，導致 7 萬歐元的貨款被騙走。

壹、淨水濾材的模範生成為肥羊

凱舟濾材網站、社群(FB/LinkedIn)、國內外媒體報導皆可搜尋，總經理 Carren 於 2006 年創辦「Caware」品牌行銷全球，致力於製造優質淨水濾材與設備，以滿足世界各地不同水質。2011 年以中東市場的家用飲水為起點，接而從貿易轉向產線建置，也廣布綠能、商業、工業，近年轉以生技醫材專攻歐美市場做為公司第二曲線。

凱舟是一間典型的中小企業，數十年來，以高品質的濾芯研發，提供客戶解決方案。組織現逾七十名同仁，背景領域不乏醫管、材料、工管的博碩士。即便凱舟內部皆是高知識、高學歷的專業人才，銷售經驗遍及六十余國，在高度仰賴資訊科技作為溝通管道，卻從未編列資安預算。每年資安投資不到台幣 5 萬，資安漏洞像蝴蝶效應凸顯一連串的管理破口，造成客戶財損、不信任，員工驚嚇出走、責任推諉，產線出貨收款流程大亂，可謂是成也數位，敗也數位，數位變革勢在必行。

本篇個案角色介紹：

Carren 凱舟濾材總經理，負責公司營運與治理。
Tina 凱舟濾材財務部主管，負責應收帳款對帳及核對。
Judy 凱舟濾材業務處主管，綜理客戶服務事項/代理各業務員。
Maria 凱舟濾材業務處經理，處理客戶訂單/出貨/款項追蹤。
Kyle 凱舟濾材業務處經理，同 Maria。
Stanley 凱舟濾材之總管理處經營管理專員，擬訂及執行內部管理辦法、流程制訂/稽核事項。
Yale 凱舟濾材總管理處資訊管理專員，維持內部資訊服務、資訊設備硬體等運作。
Marta 凱舟濾材的客戶，Martech srl 業務經理。Martech srl 主要經營家用電器零配件與耗材買賣。總部位於義大利，以自有品牌「Martech」行銷全歐洲，員工數約莫十人。客戶包含家電經銷商、區域批發商至鄉鎮零售商，其供應商遍集全球，凱舟為其濾芯耗材 ODM[1]代工廠。

莊顧問凱舟濾材委外資安顧問，協助資訊方案提案建議/遠程資安事項監控/異常狀況查核。

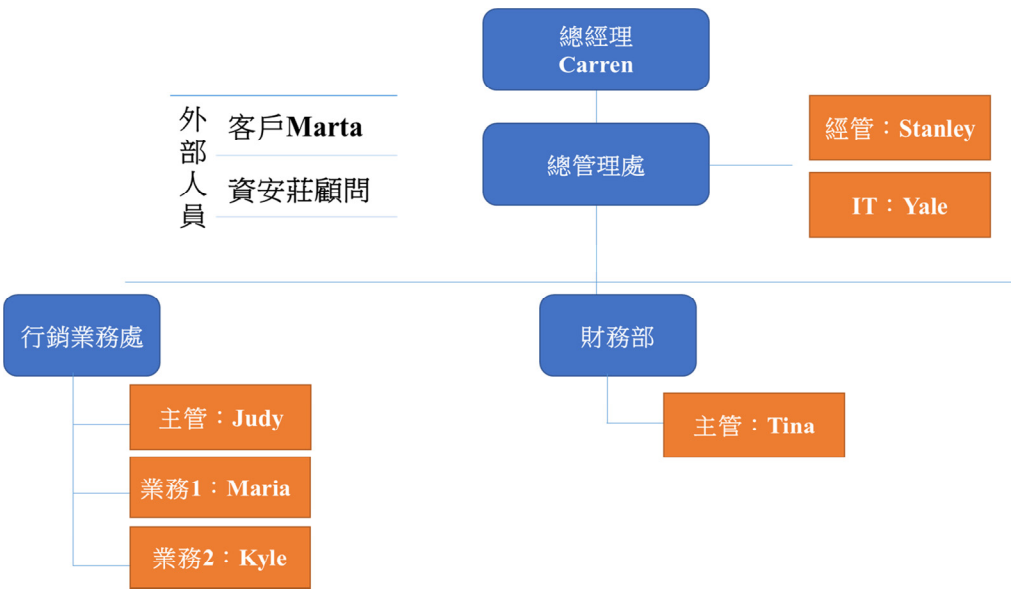

圖 1：凱舟個案人物之間的關係
資料來源：本研究整理

[1] Original Design Manufacturer「原廠委託設計」從客制化產品設計到生產完成後，交給品牌公司貼他們的 LOGO 出售。

貳、悄悄駭入的不速之客

事情是這樣發生的….，2018 年 10 月 Maria 收到 Microsoft 寄來的電子郵件，說目前的版本需要更新應用程式，於是便點選連結，在頁面上以信箱帳號及密碼登入並安裝。

首部曲、電子郵件頻遭退信

2019 年 4 月 8 日，凱舟負責船務同仁，正在準備 10 日要出貨給義大利客戶 Marta(個案人物說明如圖 1)，是價值 7 萬歐元的客制化濾芯訂單。以電子郵件傳送提單[2]給相關同仁時，就會收到業務 Maria 的退信通知。之前，船務同仁還提醒 Maria，問她是不是 Webmail 信箱滿了，請她清理一下垃圾郵件跟廣告信，不然郵件常被退回來。Maria 跟部分凱舟同仁習慣回到家，透過自己的筆電或手機以 Webmail 接收公司的郵件。Maria 在公司用 Outlook 準備寄提單、出貨付款通知給義大利客戶 Marta，同時 cc[3]給其他相關同仁照會時，也會收到退信通知，感覺怪怪的。於是，請負責 IT 的 Yale 來檢查一下郵件伺服器設定。Yale 看完雖覺得無異狀，但也為求安全起見，順便用卡巴斯基防病毒軟體進行掃毒，偵測後並無病毒感染，隨後請 Maria 持續關注，並回報是否還有異常發生。

殊不知此時在看不見的角落，駭客早已虎視眈眈，埋伏監看凱舟與客戶往來的郵件內容。退信問題持續了一周，狀況仍未改善，因此 Yale 打電話問 ISP 業者中華電信，他們提供凱舟 hiBox 企業全能信箱服務，有郵件雙重過濾防護機制，以及專屬、多語系使用管理介面。電信專員建議檢查公司郵件 Webmail 端設定，Yale 進入後臺時發現，Webmail 介面變成簡體中文，而轉信機制也被開啟，且使用許久，Yale 心想可能一開始便是如此，應不屬於特殊異狀。

二部曲、駭客出手電子郵件交叉發信

監看凱舟郵件已久的駭客眼見時機成熟，準備出手了…。4 月 12 日，登入 Maria 的 Webmail，假借 Maria 名義發信告知義大利客戶 Marta 表示：因為公司兆豐國際商業銀行的帳號，目前稽核中，無法收款，當您要安排匯款時，敬請

---

[2] 提單（B/L）是對外貿易中托運人運輸貨物的憑證，具有法律效益。證明承運人已收到提單上注明的貨物數量和狀況，便於托運人與收貨人之間的付款，提單也是貨物所有權和交換的憑證，僅在收貨人出示原始提單（B/L）時才會放行這些貨物。

[3] CC 是 carbon copy 的縮寫，副本的意思。寄送郵件給主要收件者時，也同時傳送副本給其他相關人，例如直屬上司、內部其他部門、或者外部協辦人員，同步追蹤進度。

告知，屆時我們會提供正確的收款銀行帳號。

Marta 不疑有他，回信給 Maria 表示：感謝告知，請提供新的匯款帳號等相關訊息。此時 Marta 是直接「回覆所有人」郵件，殊不知 cc 給凱舟同仁信箱全是假的，但顯示名稱皆相同(如表 1)，只有 Maria 電子郵件地址不曾被竄改，但駭客早在 Maria 收信前即已轉走郵件。收到信的駭客隨即在西班牙開立新銀行帳戶，並回信給 Marta，信中附上凱舟濾材公司英文名稱、新銀行帳號 IBAN 與 SWIFT CODE 等，並且叮囑 Marta：請確認銀行訊息，需按照指示安排付款，以避免收款時，出現任何問題。

表 1：真假電子郵件地址對比列表

職稱	顯示名稱	正確電郵地址	顯示名稱	仿造電郵地址
總經理	Carren	carren@caware.com.tw	名稱未改	carren.caware.tw@mail.com
業務	Kyle	kyle@caware.com.tw		kyle.caware.tw@mail.com
業務	Maria	maria@caware.com.tw		(Webmail 被盜用，未被仿造)
業務主管	Judy	judy@caware.com.tw		judy.caware.tw@mail.com
客戶	Marta	marta@martechsrl.com	marta@martechsrl	marta-martechsrl@mail.com

資料來源：本研究整理

4 月 16 日，賓果！大魚上鉤了。Marta 回信給假冒 Maria 的駭客表示：昨日(4/15)已匯款，水單請見附加檔案，並請給予提單正本，後續報關用。當駭客一收到郵件，於 4 月 17 日，用以假亂真的郵件地址(Marta-martechsrl@mail.com)，冒充 Marta 寫信給凱舟 Maria 表明已匯款，要索取提單正本，並竄改 Marta 的信(4/15 改成 4/16)、附件水單內容及電話號碼。

4 月 17 日，Maria 收到信後，直接回覆給 Marta-martechsrl@mail.com 表示：感謝告知匯款，待會計確認入帳後，再郵寄提貨報關文件跟樣品 AP2。此時信件中的人除了凱舟同仁為正確的電子郵件地址，其餘的皆是駭客用來魚目混珠的郵件地址。如圖 2。

主旨：RE：Caware Official Shipping Notice – PICAW-190122-EIT01
日期：2019-04-17 14:00
寄件者：”Maria – Caware Filtering Corp.,”<maria@caware.com.tw>
收件者：” ‘ marta@martechsrl ’ ” <marta-martechsrl@mail.com>
副本：” ‘ carlo ’ ” < carlo-ciemmeservicesrl@mail.com>, ‘cristina ’ < cristina-martechsrl@mail.com>, ” ‘ Kyle – Caware Filtering Corp.,’ ” <kyle@caware.com.tw>, ” ‘ Carren – Caware Filtering Corp.,’ ” <carren@caware.com.tw>, vivian@caware.com.tw

Hi Marta,
Thank you for your wiring notice with the bank receipt.
After we receive it, I'll let you know and send the original shipping document (for custom purpose) with the sample of AP2 together.

Best regards,
Maria

FROM: marta@martechsrl [mailto:marta-martechsrl@mail.com]
SENT: Wednesday, April 17, 2019 4:21 AM
TO: Maria – Caware Filtering Corp.,
CC: carlo; cristina; Kyle – Caware Filtering Corp;
Carren – Caware Filtering Corp.,; Judy- Caware Filtering Corp.,
SUBJECT: R: Caware Official Shipping Notice – PICAW-190122-EIT01

Hi Maria,

圖 2：Maria 回信待確認入帳

資料來源：本研究整理

4 月 17 日，駭客再用相同手法登入 Maria 的 Webmail，再將同樣內容回覆給 Marta，此時信件中的人除了 Martech 的員工是正確的電郵地址，其餘的已遭變造。如圖 3。

Da: Maria - Caware Filtering Corp.,”< maria@caware.com.tw >
Inviato: mercoledi 17 aprile 2019 10:27
A: Marta<marta@martechsrl.com>
Cc: carlo< carlo.marcelli@ciemmeservicesrl.com>; cristina < cristina@martechsrl.com>; Kyle – Caware Filtering Corp., <kyle.caware.tw@mail.com>; Carren – Caware Filtering Corp., <carren.caware.tw@mail.com>; Judy – Caware Filtering Corp., <judy.caware.tw@mail.com>
Oggetto:RE: Caware Official Shipping Notice – PICAW-190122-EIT01

Hi Marta,
Thank you for your wiring notice with the bank receipt.
After we receive it, I'll let you know and send the original shipping document (for custom purpose) with the sample of AP2 together.

Best regards,
Maria

From: marta@martechsrl.com
Sent: Tuesday, April 16, 2019 3:16 PM
To: Maria – Caware Filtering Corp.,

圖 3：駭客將同樣內容的信發給客戶

資料來源：本研究整理

三部曲、Email 誘出機密資料

預知Marta定會在匯款後未收到提單而催促，4 月23 日駭客即先假冒Marta寄信，試探 Maria 入帳狀況及要求提供提單正本。此時，凱舟業務部 Kyle 成為 Maria 的職務代理人，不疑貳地回覆駭客：Maria 因車禍請傷假，後續事宜暫由我接手。

駭客暗自竊喜 Kyle 與 Maria，都未發現其他人電郵地址的異樣，4 月24日，掌握時間點趕緊告知 Kyle：與銀行核對這筆付款的結果，由於銀行的新政策，需要凱舟的營利事業登記證及提單副本(B/L，Bill of lading)才能匯入解付[4]，造成不便深感抱歉，也請 Kyle 理解與配合。隨即 Kyle 便向甫上任的業務主管 Judy 轉述郵件內容，從 10 日出貨到現在，遲遲未收到貨款，原來錢是卡在銀行端，需要凱舟公司的相關文件才能完成手續。Judy 同樣地不做他想，遂將公司營業登記證及提單副本(B/L)，以郵件提供給假 Marta。

參、亡羊補牢猶未晚？

4 月 24 日，Marta 的一通電話擾亂了正在拉斯維加斯參展的 Carren，Marta 語調略高且急促地說「Carren 我們公司已經把貨款付給你們好幾天了，為什麼 Maria 總是回覆沒有收到錢，不能放行提單，我們急著出貨給客戶！」Carren 安撫 Marta 說，「可否先把水單傳給我，我請會計 Tina 盡速再同銀行確認，若貨款收到了，即刻放行提單。」Marta 用 Whatsapp 傳來水單，Carren 一看到收款行是西班牙銀行，心揪了一下！這不是凱舟的銀行帳號。趕緊回電給 Marta 說，「我們的交易可能遭受詐騙，請趕快通知義大利銀行進行退匯止付，我也會請西班牙當地友人協助聯繫西班牙銀行凍結帳戶。」

Marta 急問 Carren，「這是怎麼一回事，Maria 指示我匯 7 萬歐元貨款至西班牙銀行，妳們沒有收到錢？貨物在義大利海關，那提單到底還能不能放行？」Carren 回覆說，「我稍後先請同事報警處理，至於提單放行部份，等我把來龍去脈搞清楚，會儘快給您回覆。」沒想到郵件詐騙血淋淋地發生在自己身上。太不齒詐騙集團的作為，Carren 憤恨交集心有不甘，試圖想挽救這一切，打電話回臺灣給凱舟經管 Stanley。

---

[4] 銀行為了保證付款的正確，解付行往往都很慎重地檢驗每筆匯款的真實性。

25 日凱舟緊急動員，全力截堵資金止付，Stanley 與 IT Yale 一同前往公司轄區的警察局報案，受理的員警說明「因發生地不在臺灣，僅能幫忙備案，請國外客戶儘快向當地銀行通報，並向警政機關報案。」報案後，Yale 也向中華電信申請調查，hiBox 服務專員向他表明，「中華電信內部主機後臺系統沒有被駭客入侵、病毒攻擊等異樣，駭客侵入管道應是藉由釣魚郵件的攻擊，竊得員工的帳號及密碼，駭入 maria@caware.com.tw 在 hiBox 的 Webmail，設定開啟轉信機制功能，藉此得知雙方對話內容。資安漏洞也有可能是客戶端，公司電腦私人上網行為、點選可疑連結及檔案等，都有可能造成電腦中毒，被駭客攻擊之風險。」專員隨即調出凱舟使用的 IP 範圍是 60.249.181.37~42，而登入 Maria 的Webmail 的IP 地址，則有來自香港跟土耳其。凱舟租用 hiBox 信箱的Webmail 功能默認，都是開啟的，一旦帳密洩漏，也等於門戶大開。建議取消「Webmail 收發信[5]」及「IMAP 郵件存取[6]」功能；Webmail 登入僅開放臺灣 IP，並限制僅由 IT 部門控制，來增加安全性。

另一方，Carren 的西班牙友人也回覆，「西班牙銀行表示貨款已經被轉匯至他國的帳戶。他並非當事者，銀行僅能告知資金流向，無權代辦理帳戶凍結。」26 日義大利客戶 Marta 回覆，「25 日是義大利解放日全國放假，今日聯繫銀行，被告知匯款已完成，無法進行止付。」

Carren 人在拉斯維加斯打天下，卻被天下打了一大嚇。公司電子郵件遭入侵，資訊安全出現問題造成財損，資安漏洞範圍到底有多大，不肖駭客是否還在暗處監控中，可能會波及其他重要客戶財損與合作合約，全面暫停出貨。盤點所有交易中的客戶，通知凱舟不會隨便更改銀行帳戶，即使有變更，一定會電話通知或者郵件加上電子簽章！報警似乎阻止不了這場資安災難，這恐怕損及公司與客戶之間的關係，該如何修復與全面防堵危機？現階段公司每個月支付 4 萬元雇用 IT 人員，但沒有自行處理資安的能力，事發緊急尋求外部資安顧問，費用約 30-35 萬/年，大勢所逼，成本得又要加上這一筆。

---

[5] Webmail 是透過網際網路，任何網頁流覽器（IE 或 Chrome），皆可收發電子郵件，使用者可以不必通過他們一般使用的上網終端的電子郵件軟體(例如 Outlook)，即能直接使用他們的郵件服務。

[6] IMAP 不論身在何處、可使用來自世界各地不同裝置(手機、電腦、朋友的電腦)，都能夠檢視存取電子郵件。使用 IMAP 存取或讀取電子郵件時，並非實際將郵件下載或儲存於您的電腦，而是從電子郵件服務中讀取。

肆、思對策合力防堵資安窘境

28 日 Carren 從拉斯維加斯抵台，隨即召開緊急資安會議，與各部門主管以及相關人一起商議對策。

經管 Stanley 提出他的意見，「近年資安事件頻傳，為避免遭受外部網路攻擊，許多大型企業及上市櫃公司都開始依循法規，建置信息安全管理架構。我們是中小企業，雖不受法規的限制與約束，不過在資通安全管控指引中，有涵蓋三大構面：策略面、管理面及技術面的內部控制措施(表 2)，或許有參考的價值。」

表 2：上市上櫃公司資通安全管控指引

策略	管理	技術
1.核心業務及其重要性 - 資通系統分級 - 資訊安全管理系統(ISMS) 2.資通安全政策及推動組織 - 資安政策及目標 3.專責人力及經費配置 - 資安/信息經費占經費比率 - 資安人力配置情形	4.資通系統磁片點及風險評估 5.資通系統或服務委外辦理之管理措施 6.資通安全維護計畫與實施情形之持續精進及績效管理機制 - 內部稽核及後續追蹤 - 資訊安全宣導課程(電子郵件社交工程演練) - 資通安全專業課程訓練(資安專責主管與人員)	7.資通安全防護及控制措施 - 實施八大安全性檢測 8.資通系統發展及維護安全 - 資通系統之防護需求與變更管制程式 9.資通安全事件通報應變及情資評估因應 - 情資分享機制 - 資安事件應變處置及通報作業程式 - 資安事件改善措施

資料來源：本研究整理

外部請來支援的資安莊顧問接著說，「凱舟的內網資安管理全靠端點的卡巴斯基防毒軟體，僅能管理網路通訊協定層的設定，無法管理到木馬、病毒等所屬的應用層。雖然阻斷外網的主動攻擊，但無法阻斷由內部發起的聯外攻擊行為，亦無法掌握各端點的防護狀況，像是中毒警示、病毒碼更新等，也較無法阻斷惡意軟體的平行擴散。大型企業每年編列 700 萬資安預算，來建立資訊安全管理架構，光是導入 ISO27001 資訊安全管理系統(ISMS)認證，依公司規模、驗證範圍（部門數、員工數、系統數等），至少要 7-9 個月，以及稽核時程等因素有所差異，花費 50～130 萬元不等，證書有效期為三年換證一次，每年須由協力廠商機構定期審查。」

Yale 經歷多天的重複查驗、掃毒，也無法防堵風險發生。自覺欠缺專業度，令他感到挫敗，回應著莊顧問所指出的內網安全問題點，「確實公司僅有家用防火牆設備跟防毒軟體來防護，已洽談網路安全服務業者趨勢科技、思科等，詢問相關的因應措施，他們可依公司規模客制化模組，提供風險評估，跨雲端、網路、裝置及端點的可視性資安平臺，掌握網路駭入的威脅，行動設備管理、數位身分認證、惡意軟體預防、建立零信任架構[7]等資安方案，公司需有專人管理。此外，提供企業 IT 人員防護產品與網路資安、最新威脅等培訓課程，依照選配計價，防護較完整，設備、系統建構價格約 150 萬上下，建置時間是3-6 個月。」

莊顧問建議，「從設備強化資安防禦能力方面，近年 ISP 業者除了提供網路連線以及企業郵件空間租用以外，也新增企業資安解決方案，像是中華電信的『資安鐵三角』方案(UTM 防火牆+SW 交換器+AP 無線基地台)，設備加系統服務月租費約$6,000~7,000/月，提供內外網防禦，在 SW 上隔離／攔阻問題主機(隔離 VLAN 虛擬網路)，並可用防火牆介面封鎖主機 IP，使用中文網路介面，視覺化的網路拓樸圖監控流量與統計分析。」

Carren 聽完後表示，「現階段全面禁止使用 Webmail 收取郵件、不可使用自攜裝置接收郵件或處理公務、嚴禁上班時用公家電腦處理私事；之後機密文件都需分級管理並加密、而且在存取或傳送時也要經過授權。最後，行政管理層一律配發筆電，內裝正版且定期更新的應用軟體。」發佈完政策後，Carren 接續再詢問，「之前可以遠距協同作業，我擔心資安事件之後過度嚴控，可能會陷入效率與安全的兩難狀態，導致內部簽核過程太冗長、出差同仁溝通又易受阻等，有無其他改善？」

莊顧問回覆說，「我們可以建立一個 eCaware 系統，即 EIP（Enterprise Information Portal）的概念，利用企業資訊入口網站，整合企業內外資訊的統一介面。對凱舟資安事件上，應該可以發揮小兵立大功的功效，短期建置以用戶管理、流程及許可權控管為主軸，利用選配模組，建置期間 2-3 個月，預估是 60 萬。」

[7] 零信任(ZTA)架構模式假定，在未驗證之前沒有一個連線、使用者或資產是值得信任的。意即以現有架構為基礎進行重建，決定好保護範圍，對使用者身份驗證、存取權限、檔案管理和影像備存，解決資料洩漏、竊取風險。

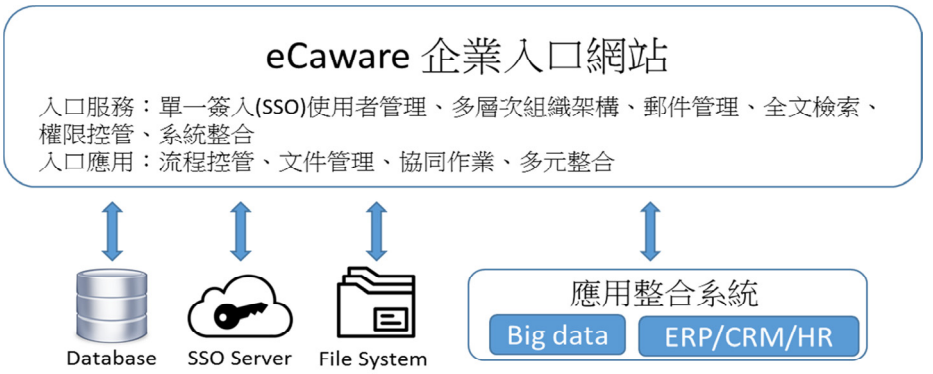

圖 4：eCaware 模組示意圖

資料來源：本研究整理

凱舟同仁面面相覷，Carren 疑惑表示，「公司目前有 ERP 進銷存系統，EIP 不就是提供員工服務像是打卡、訂便當、公告欄、知識管理、連結 ERP 等訊息傳遞的機制，是大型企業才會建置的奢侈品，如何在資安起作用呢？」莊顧問接著說明，「首先，eCaware 是企業組織架構與許可權對應，使用者單一簽入(SSO：Single Sign On)，員工可不受時間與地域限制的溝通，在外可透過 VPN[8] 連入。以公司配發的筆電做人機綁定，同仁憑 ID 個別取得密碼做 AD 認證[9]，具有密碼之隱蔽性。嚴謹的帳號密碼控管(例如，定期自動進行密碼生成，提醒更新密碼。可依部門設定，如郵件往來頻繁的業務部 1 月/次；其他部門 1 季/次)、依使用者權限登入限定的 IP，可存取工作所需的資訊，在伺服器保存郵件、修改紀錄。進入 eCaware 首頁資訊介面，可以針對企業各組織需求建公文、報表生成、連結 ERP，各系統之間不需要重登帳號與密碼認證，即可開啟流覽與作業，例如 HR 的出缺勤數據、各單位的 Flow 電子簽核系統，甚至管理階層最在意的生產排程、產能或財務資訊。未來，可視營運需求擴充 SRM、CRM 等功能，方便管理層或員工進行一頁式的管理，不僅可以區隔公司內外網，讓訪客、員工休息可以用外網連線，內網則獨立安全不受影響。」

此時，Carren 憂心的說著，「眼前的危機尚未度過，先別談未來，駭客將郵件地址從 0 換成 O、r n 改成 m，人眼都無法判別郵件真偽。」

---

[8] 虛擬私人網路（virtual private network，VPN）用戶可以遠端存取私人網路絡中可用的資源。

[9] Active Directory (AD) 是 Microsoft 目錄服務之一，作為 IT 營運的基礎建設，用於儲存使用者、使用者群組身分識別資訊的建議和預設技術，其中包含使用者認證的密碼編譯金鑰。讓 IT 人員在面對身分驗證與網域存取管理機制時可以更有效率。

莊顧問回應，「正好！eCaware 在技術面可建立 Email 管理機制，綁定員工個人的郵件，通知未讀郵件，利用大數據的概念，以程式碼判讀凱舟郵件備份資料庫(即白名單)。一旦發現有首次來往的郵件地址，會在郵件開啟前做一個確認與把關的動作，系統會自動跳出警告，提醒收件者確認此郵件是否安全(Y)，確認安全則收入 Outlook，以後不會跳出警告；反之則移至垃圾郵件，更進一步 IT 還可將騷擾郵件列入黑名單，回饋給中華電信請他們從源頭阻絕。另在教育面採上機訓練的方式，方便人資定期對全體員工進行資安教育訓練，請他們在系統裡聽課、看教學影片，再以線上測驗的方式，瞭解他們的吸收程度。資安行為列入年度考核基準、獎勵自主學習，既可提升員工資訊素養。」

面對 Stanley 所提出上市櫃公司的完整資安架構、Yale 提出的導入外部資安服務供應商方案，以及莊顧問建議的 eCaware 的企業入口網站，總經理 Carren 應該如何選擇呢？怎麼做才不會讓類似的事件再次發生？

伍、電郵詐騙是系統防護不足還是人員疏失？

聽取了 IT 的報告之後，Carren 隨即轉向業務主管 Judy 表示，「為了這件事，Marta 把她公司負責轉帳的財務人員給開除了，甚至懷疑我們有內鬼。營利事業登記證這麼重要機密文件，未經查證就寄出去，才會輕易落入跨國犯罪集團手中，成為順利提款的關鍵。」Judy 回應道，「我進來公司不久，接任主管職，Martech 是凱舟十多年的大客戶，往來最密切的商業夥伴之一。日常的熟悉感與信任，讓我卸下了警戒。過去在簽約時，客戶偶會要求提供營利事業登記證，我電腦裡有儲存掃描的 PDF 檔，當下不疑有他……。」身為管理階層，思慮低於正常水準，面對受害的公司及客戶，責任難辭其咎，也深怕公司會將全部損失歸咎於自己，面對Carren究責的眼神、客戶的質疑，辭職能解決問題嗎？

Carren 接著問了請公傷假[10]剛復工的 Maria，「駭客用你的郵件發信那麼多次，公司裡那麼多人，連客戶郵件地址跟以往不一樣，你居然都不知道？最近是不是有預覽或開啟不明郵件、點選連結及下載附檔？」Maria 感到無辜、罪惡感又難以擺脫，身心俱疲回答道，「公傷期間在家休息，突然被告知公司遭受跨國郵件詐騙，我很震驚也很自責。自己盡心盡力，跟往常做的事情一樣，一夕之間卻成為眾矢之的。Yale 花了好幾天盤問我，也清查電腦，郵件寄件備份也沒有發現什麼，我真的無法分辨什麼是釣魚郵件……。」

[10] 因執行職務或上下班途中發生危險，有醫囑必須休養或療治，而無法出勤上班。

事件發生後，Carren 經歷了人性的黑暗面，Carren 認為自己與 Marta 都是受害者，以為她會跟自己同仇敵愾、共同處理，結果卻是落井下石的局面。一面處理詐騙，一面安撫客戶，始終覺得一肚子火，無法與客戶取得共識。

陸、問題討論

一、 凱舟遭受國際駭客的攻擊和詐騙，整起事件經過哪些流程？
二、 為什麼這些手法，會讓雙方落入陷阱之中？
三、 BEC 事件造成什麼影響？出貨與否在財務損失和關係破裂的權衡下，Carren 應該怎麼做？
四、 BEC 攻擊對凱舟造成的影響甚鉅，應如何改善資安與防範？

教學手冊

壹、個案概要與核心議題

根據內政部警政署統計，2021 年商務電子郵件詐騙金額已逾新臺幣 2 億元[11]。企業在進行國際交易，高度依賴資訊科技所帶來的便利性，沒料到卻成為詐騙集團覬覦的目標。

本個案公司凱舟濾材為典型以製造外銷為基礎的中小企業。數位浪潮襲卷而至，資安漏洞被視為是企業數位技術的痛點，其中電郵詐騙更被不法人士認定是投報率最好的形式。駭客用了技術與非技術性的方法，使凱舟與客戶經歷的財務與非財務面的損害。第一階段，讓學生知道變臉詐騙攻擊或稱為商務電子郵件入侵(Business Email Compromise，簡稱 BEC)的始末。

為有效防堵 BEC 攻擊，學者 Cassandra 等人(2020)投入相關研究，提出技術與非技術的 BEC 解決方案。第二階段，藉由凱舟評估數位技術導入「eCaware」系統，築起公司資安護城河的過程，加上人員資安教育訓練、與利害關係人等建立暢通且有效的溝通管道，協助老師引導學生，當資源有限時，如何適切地組合有效解決方案，創造管理效率極大化。

[11] 內政部警政署 (2021 年 7 月 20 日)，「歹徒透過「竄改商務電子郵件」進行詐騙橫行 慎防是類詐騙手法」，臺灣經貿網，(取得日期：2021 年 5 月 12 日)，[available at https://info.taiwantrade.com/biznews/fraud-2383161.html]。

本個案在數位轉型的管理意涵是，在於企業主苦心經營賺的錢，卻因資安詐騙而人財兩失，在緊迫時間與資源下須解決痛點，導入數位工具，杜絕管理破口。此舉亦將凱舟全體推向數位治理的層面，一展科技管理的雄心，體現思維與態度的質變。

貳、教學對象與適用課程

大專院校商管科系，尤其是資訊管理與企業管理學系、EMBA 學生，藉由凱舟個案，使其理解「商務電子郵件」溝通工具，所引發資訊安全的問題以及解決方案。關於資通資訊安全控管策略在政府政策、研究領域、法規遵循等方面，皆針對大型企業與機構擬定方針，較少著墨在資源有限的中小企業。本個案可借鏡中小企業資安改善對策參考。

適用課程：資訊管理、資訊安全風險管理、數位轉型。

參、教學所需要的背景資料與理論觀點探討

一、什麼是 BEC？

BEC 又稱變臉詐騙，原本稱為 Man-in-the-Email 詐騙，2013 年開始，由於郵件伺服器代管服務業發展、電子商務迅速普及，這類資安災難在全球蔓延，為企業帶來嚴重威脅。2015 年美國網路犯罪申訴中心(IC3)和聯邦調查局 FBI 公開聲明，將 BEC(Business Email Compromise，商務電子郵件入侵)定義為針對與外國供應商合作企業或經常進行匯款支付企業的精密騙局[12]。BEC 案例金額與受害人數，每年以 110%的速度成長，2016~2019 年三年間，共 16 萬起案件，累計的損失金額高達 262 億美元，全球超過 2 萬家企業受害，每次事件平均損失金額為 140,000 美元[13]。

(一)BEC 攻擊的步驟與特徵

[12] Trend Labs (2016 年 2 月 2 日)，「認識變臉詐騙/BEC- (Business Email Compromise) 商務電子郵件詐騙與防禦之道」，資安趨勢部落格，(取得日期：2021 年 5 月 23 日)，[available at https://blog.trendmicro.com.tw/?p=16295]。

[13] Jessie Cai (2020 年 3 月 18 日)，「BEC 詐騙真的有賺頭？解析詐騙集團成本與獲利」，數位時代，(取得日期：2021 年 5 月 23 日)，[available at https://meet.bnext.com.tw/blog/view/19668]。

當犯罪者冒充員工、供應商或其他受信任的相關人員，來獲取資金、帳號、存取碼或其他敏感資訊時，就會發生BEC詐騙(Jakobsson, 2016; Zweighaft, 2017)。發生 BEC 事件，通常企業早就被駭客入侵一段時間，因此，網路犯罪者才會知道雙方公司之間的交易採購，或人員異動情形，再伺機以假冒電子郵件要求變更匯款。步驟流程如下：

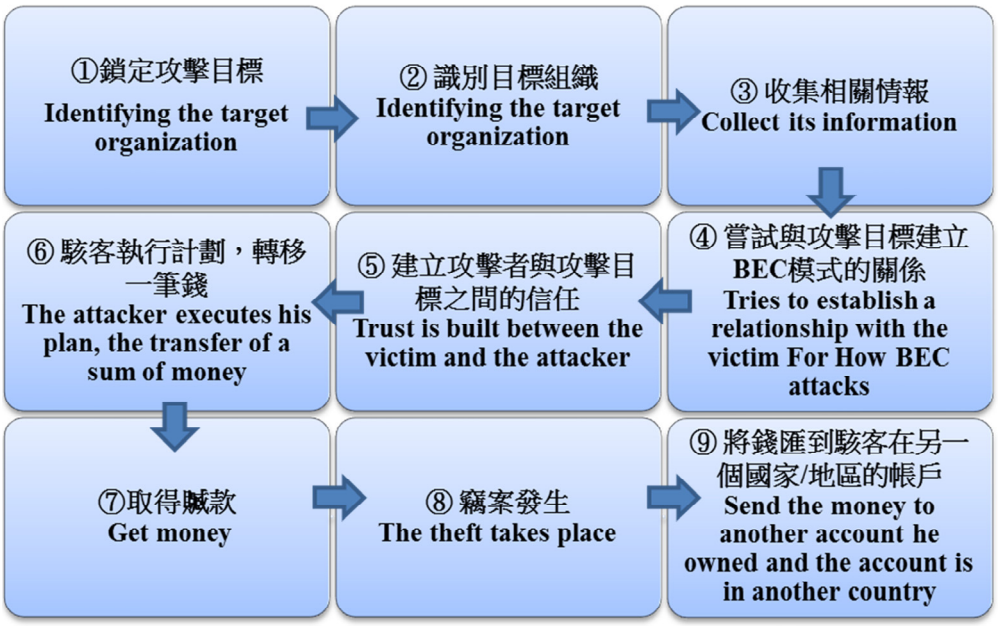

圖 5：實施 BEC 攻擊的步驟流程圖
(Flow diagram of steps to implement BEC attacks.)
資料來源：Business email compromise (BEC) attacks. Al-Musib et al. (2021)

①鎖定攻擊目標

駭客先傳送一封釣魚(phishing)郵件，內容常以熱門議題，名人八卦、各式好康，以及工作的發票、匯款單、程式更新等五花八門的主旨來引誘。不疑有他的用戶點選後，內含惡意 HTML 附件，蠕蟲(WORM_NUWAR.YH)、後門或木馬程式，騙取使用者輸入郵件帳號、密碼或憑證，便藉此管道進入使用者電腦，在不知不覺中變更其電腦設定，成為被駭客鎖定的目標。

②識別目標群組織

駭客在竊取相關人員的電子郵件(Account take over)之後，會開始進行確認該目標所屬的組織與部門職位。

③收集相關情報

駭客各方收集攻擊所需的資訊，通常會花半年左右的時間，從往來的商業郵件、公司網站或者相關報導去瞭解：攻擊目標的公司文化、人員之間的關係、互動方式、稱呼，以及用語措辭的習慣。企業高階主管更迭，對公司業務不熟悉，也常是駭客鎖定攻擊的目標。

④嘗試與攻擊目標建立 BEC 模式的關係

駭客會試圖與該組織或與組織相關，具有財務帳戶的受害者建立關係。直接利用被盜的電子郵件帳號來發信；或是與個人或組織極其相似之電子郵件地址跟域名，僅有相當細微的變化，眼睛無法輕易分別，魚目混珠試圖欺騙收件人。

⑤建立攻擊者與攻擊目標之間的信任

詐騙者可能也會趁公司高階主管出差，無法取得連系時，自稱高階主管（CFO、CEO、CTO 等）、董事、律師、高級官員或其他客戶、經銷商、供應商等，具「權威性」身分的犯罪手法。同時製作逼真的電子郵件，在郵件的收件人副本中，也有其他的員工。過程約持續一周，來取信受害者。

⑥駭客執行計畫，轉移一筆錢

僅用電子郵件進行溝通，聲稱感冒、在開會、飛機上或電話/語音/視頻不能正常工作，聲稱將要預付的款項「重要」，涉及敏感性、或要求即時和保密。轉匯至海外帳戶的金額通常是在合理範圍內，避免引起懷疑。

⑦取得贓款

目前各國針對洗錢防制，銀行開戶提款需出示相關公司證明文件。詐騙者為順利達成目標，事前會要求員工，特別是人資、財務提供未來攻擊所需的情報，例如，公司文件、高階主管身分識別資訊或憑證，能夠用來訂制對企業的特定攻擊。

⑧竊案發生

受害者向警方報案。

⑨將錢匯到駭客在另一個國家/地區的帳戶

把贓款再轉走至詐騙者在其他國家預設的人頭帳戶。

（二）社交工程(social engineering)

BEC 攻擊之所以會成功，是駭客有效的利用社交工程技巧(Cross et al., 2020)，來操弄人類先天具有的情感。例如合乎常理或好奇心的釣魚郵件，引誘員工開啟、點擊流覽或者下載惡意檔案。接著再以取信關係人的方式，在被攻擊目標的系統中站穩腳，意圖使員工採取網路罪犯所期待的行動，以便讓他們的詭計得逞。

同時，BEC 犯罪者知道員工都想做好份內工作，在上司面前有好的表現，利用這點，最常見且有效的組合就是製造權威性與緊迫性，假冒公司高層身分，要求員工完成他們的任務，通常是轉移資金(Jakobsson, 2016)。製造「緊迫感」突然最後一分鐘、接近下班或放假的前一天，指示更改收款人的匯款帳號，使員工無法理性思考，降低質疑指示的可能性。

二、BEC 爲什麼會破壞信任？

BEC 操弄人與人、組織與組織之間信任關係，使交易產生負面與非預期的結果。成功的供應鏈績效，植基於夥伴間高度的信任與強烈的承諾上(吳志明、朱素玥、方文昌，2006)，信任是對交易的另一方的可靠性與正直有信心(Morgan & Hunt, 1994)，也就是說廠商相信另一公司會採取對該廠商有高度利益的結果而行動。然而 BEC 破壞了交易活動中，所有關係人的期望，對是否能順利完成交易產生不確定性，會降低彼此的信任感。

企業遭 BEC 詐騙，損害可能超過實際的財務損失。從個人經歷詐騙的研究中得知，受害者會產生非經濟性的傷害，包括健康、情緒、失業、關係破裂，極端的情況下還可能會有自殺的傾向(Button et al., 2014; Rebovich et al., 2000)，組織環境的員工或者管理層可能也會經歷其中部分的影響。

三、防範 BEC 的措施

BEC 攻擊，犯罪者仰賴的通常不是複雜的技術，更多是社交工程手法有效的使用。BEC 攻擊者多半只花 35 美元，即可從網路購得後門程式，找到目標企業、以及其員工背景資料。比起其他的網路攻擊，BEC 低成本高獲益，是近三年美國網路犯罪總損失金額之冠。BEC 詐騙猖獗，一般企業該如何防範呢？學者們在研究中提出技術性與非技術性的解決方案(Cross et al.,2020 ; Al-Musib et al., 2021)：

在技術性解決方案可分為，資訊硬體設備，在每個終端設備的前面，利用

防火牆與交換器等，建構反惡意軟體與內網端點安全系統。軟體是指可用來防禦的資訊系統與應用程式，作業用的應用軟體應該要定期更新版本。在登入企業系統時，應強化身分驗證機制，自動定期更新且採用高強度的密碼、登錄以及修改紀錄應要保存 90 天。在電子郵件系統安全防護方面，採用電子郵件數位簽章，禁用 POP、IMAP、SMTP，使用機器學習分析電子郵件地址或內容，自動跳出顯示警告信號(即黑白名單)以及對國際 IP 登錄等可疑行為發出警告。

BEC 不光是攻擊資安軟硬體系統防護上技術的不足，也利用了人性的弱點。非技術性解決方案可以有效對應駭客使用的社交工程手法。為避免人員誤入 BEC 陷阱，企業應持續員工資安教育訓練，傳授 BEC 流程(社交工程演練)，提升員工、關係人等的資安意識。制訂資安政策，關於付款建立一致和安全的流程、治理程序。採用雙因素認證(Two-factor Authentication，2FA)，針對電子郵件更改銀行帳號的請求，應打電話給財務人員，驗證所有付款的合法性。商業電子郵件往來時，仔細檢查郵件地址與域名，隨時保持警覺心；加密郵件中不要提供憑證或密碼，應以電話或其他管道另行通知(Myojin & Babaguchi, 2020)。

肆、問題引導與教學計畫

一、開場破冰(10 分鐘/累計 10 分鐘)

建議課程開始，藉學生自身或周遭的詐騙經驗，引發對個案議題討論的熱度：

(一)自己或者身邊的人曾經遇過詐騙的請舉手。

(二)詐騙集團用什麼手法？引誘上當成功的關鍵因素是什麼？

此時教師可以藉由學生的分享，開始分類被詐騙的對象，是屬於個人還是組織，比較個人與組織詐騙手法的異同。例如，在個人詐騙方面，犯罪者會製造較多情緒等心理因素的手法，合乎常理、同情心、好奇心、恐懼以及貪婪等，使受害者落入犯罪者設計的情境當中；而組織詐騙是非情緒性，僅簡單的呼籲受害者做好份內的工作，設計合乎常理具有說服力的背景。

同樣的都會冒充身分，利用緊迫性的技巧，使受害者無暇思考要求的合理、合法性，降低質疑要求的可能性。上當的受害者通常都沒有再透過其他管道，例如撥打對方電話進行查證。

二、問題討論

(一)凱舟遭受國際駭客的攻擊和詐欺，整起事件經過哪些流程？(30 分鐘/累計 40 分鐘)

教師可在白板上畫出九宮格(圖 5 實施 BEC 攻擊的步驟流程圖)，引導學生依序填出駭客對凱舟實施 BEC 攻擊的詐騙流程圖，再針對每個步驟分析駭客縝密的手法與 BEC 特徵。

① Maria 點擊了釣魚郵件/連結,遭駭客列為攻擊目標

一開始，駭客利用了 Microsoft 應用程式更新為主旨的釣魚郵件，引誘凱舟業務 Maria 上鉤。駭客設計了合乎常理的理由，使 Maria 不疑有它點選後，出現假的 Microsoft 登入頁面，以騙取 Maria 輸入郵箱帳號及密碼。犯罪集團獲得了這組帳密，Maria 成為被鎖定攻擊的目標。

②確認 Maria 所屬組織，以及其職務

攻擊者隨即以 Maria 這組憑證，從國外的 IP 登入，成功接管其電子郵件帳號(Account take over)，並且修改郵件設定(簡體字介面、轉信機制)，開始監看 Maria 往來的信件。接著確認 Maria 所屬的公司組織—凱舟是專注外銷市場的中小企業，國際貿易頻繁。Maria 在組織中的職務是業務，常以電子郵件聯繫客戶訂單、出貨、通知匯款交易之重要居間者。

③收集凱舟公司、關係人等的情報

駭客花了近 6 個月的時間，從 Maria 與郵件往來人員之間的互動方式、網際網路的公開材料(公司網站或報導)、社群媒體(LinkedIn/FB)來收集凱舟濾材的組織架構、文化、關係人等資訊。如此一來可更好的掌握 Maria 與凱舟組織人員、客戶之間的關係，郵件中的稱呼、語言以及措辭的使用，藉以製作更具說服力、高度複雜的電子郵件，提升 BEC 成功率。

④BEC 攻擊者試圖與付款方的受害者 Marta 建立關係

職務、組織、關係人確認，攻擊所需的情報逐漸收集完成。當駭客從 Maria 的往來郵件中發現，凱舟與義大利客戶 Martech 公司正要進行 7 萬歐元交易。於是便竊用 Maria 電子郵件信箱，以銀行稽核凱舟帳戶，這看似合理的理由，企圖與擁有財務帳戶的受害者即付款方 Marta 建立關係。

⑤攻擊者多日來佯裝 Maria 身份，以逼真的匯款變更通知，與 Marta 對話，取信于客戶

同時，駭客製作逼真的電子郵件，為了讓建立關係的資訊看起來是真實的，假冒 Maria 名義寄出的郵件收件人副本中，看起來也有其他相關人員，但有部分是極為相似之電子郵件地址跟域名(表 1 真假電子郵件地址對比清單)，僅有相當細微的變化，眼睛無法輕易分別，企圖魚目混珠欺騙收件人。這個過程持續一周，直到和 Marta、關係人等之間建立信任：Marta 請 Maria 提供新的匯款帳號等相關訊息。

⑥要求將貨款轉移至西班牙的銀行帳戶

接著，攻擊者執行 BEC 的目標，向 Marta 提出將貨款 7 萬歐元轉移到海外，即指定的西班牙銀行帳戶。通常要求移轉的金額會是合理的範圍，不會超過貨款，避免引起懷疑。

⑦誤導 Judy 提供公司營登等文件，順利取款

Marta 匯款至西班牙銀行的帳戶，是駭客用凱舟濾材公司英文名稱開的戶，需要凱舟的營利事業登記證與提單副本(B/L)才能順利提款。Judy 甫上任，對公司業務流程不熟悉，加上凱舟總經理 Carren 至拉斯維加斯出差，在飛機上、會議中或者時差，無法直接聯繫進行確認。Judy 未經申請，便擅自將公司機密文件傳送出去，讓駭客順利取得贓款。

⑧報警，竊案成立

從 15 日匯款，經過 10 天，直到 24 日義大利客戶 Marta 按耐不住，打電話給凱舟總經理 Carren 確認後，才發現這場精心的騙局，雙方都報警竊案成立。

⑨贓款被轉走至其他國家的人頭帳戶

此時駭客已經從西班牙的凱舟帳戶將錢轉至駭客其他國家的人頭帳戶，再也追不回。

(二)為什麼這些手法，會讓雙方落入陷阱之中？（20 分鐘/累計 60 分鐘）

以個案受害者的角度換位思考，請學生針對下列 3 個問題問答，增加討論的有趣度：

- 如果你是 Maria，收到信，你會更新 Microsoft 的應用程式嗎？
- 如果你是 Marta，收到信，你會把錢匯到西班牙嗎？
- 如果你是 Judy，收到信，你會把公司文件給客戶嗎？

1. 技術性攻擊

商務電子郵件入侵(BEC)，駭客善於操控各種人性與組織的弱點，引誘 Maria 個人情感面產生合乎常理、想做好份內工作，有積極的表現(Jakobsson, 2016)，對工作熱忱，即使回到家，用私人電腦開啟 Webmail 收信工作。駭客以應用程式更新的主旨做為釣餌，在釣魚(phishing)郵件中夾帶的連結，進入假頁面，藉此截取 Maria 的 Webmail 帳密，進行長期接管與監控。收件被駭客設定轉信，造成 Maria 郵件頻頻被退信，冒名發信後，還會刪除寄件備份，以免被 Maria 發現。

2. 非技術性攻擊

駭客竊用 Maria 的電子郵件帳號，在收集情報階段，早已熟稔攻擊目標的互動方式，模擬過去郵件中的稱呼、語言以及措辭。Marta 憑藉著 10 多年與凱舟良好的交易紀錄，彼此存在著深厚的信任關係。即使在交易的最後一刻，突然被郵件通知，銀行稽核凱舟帳戶，提出更改匯款帳號至西班牙。凱舟在歐美有許多客戶，多一個西班牙銀行帳戶看似合乎常理。交易金額合理，加上信任關係，讓 Marta 不會起疑心。

業務主管 Judy 亦同，在 Marta 匯款至西班牙後，犯罪者因缺乏凱舟的營利事業登記證及提單副本(B/L)，暫時拿不到贓款。意圖向凱舟業務請求公司文件，為了降低 Judy 質疑該要求的可能性，便誤導凱舟內部人員：銀行新政策是貨款遲遲不到帳的合理解釋，營造出只要凱舟提供公司登記證以及提單副本(B/L)，就可以拿到貨款的假像。Marta 是凱舟的老客戶，具有身分上的權威性，凱舟也無制訂公司機密文件管理程序。總經理 Carren 出差中請示不便，同時 Judy 感受到時間的壓力，種種讓 Judy 無法理性思考 Marta 的要求，可能會帶來的風險。為了盡速完成收款工作，讓客戶可以順利取貨，該請求成為具有說服力的合理背景。

(三)BEC 事件造成什麼影響？出貨與否在財務損失和關係破裂的權衡下，Carren 應該怎麼做？（20 分鐘/累計 80 分鐘）

1. 凱舟和客戶 Martech 的損失

（1）經濟性損失

單筆交易遭到協力廠商惡意的破壞，短期最明顯的是財務損失，Martech 方面雖然貨款匯出了，但貨款被詐騙，是否能依約收到貨物未明；凱舟方面是貨出了，收不到貨款。

（2）非經濟性損失

長期面向來看，凱舟與 Martech 之間的商業關係與信任已遭破壞。Martech 基於商業誠信，急於出貨給客戶，原本整個供應鏈的績效，建立在夥伴間高度的信任與強烈的承諾上(吳志明、朱素玥、方文昌，2006)。BEC 事件發生，使凱舟與 Martech 的交易產生負面與非預期的結果。凱舟是否能順利完成交易產生不確定性，造成 Marta 對 Carren 是否會依過去的承諾，採取對 Martech 有利的行動失去信心。同理，Carren 也對 Marta 抱持著相同的期待，希望 Martech 也能採取對凱舟有利的行動，例如承擔部分貨款，減少凱舟的損失。BEC 破壞了交易活動中，所有關係人的期望，事件發生初期雙方無法達成共識。Marta 裁撤 Martech 公司出錯的財務人員，甚至懷疑凱舟有內鬼。業務主管 Judy 與業務經理 Maria 也免不了被究責，員工也是企業的無形資產，員工情緒、關係破裂會對組織績效造成影響。產線出貨大亂，一干人員遭波及，商譽減損客戶流失等非經濟性損失的成本是無法估算的。

2. Carren 應該怎麼做？

像凱舟遭遇詐騙，沒有收到客戶的貨款，跟客戶的出貨協議該如何履行權利與義務？此時可以請同學進行投票，Carren 該不該出貨給 Martech？分析完後，再問學生是否有無改變想法。

網路駭客入侵，扮演當事一方製造原有買賣雙方之誤會，趁機居中牟利。雖 Martech 應負起未向凱舟落實覆核制(Dual Approvals)，即確認匯款帳號更改一事之責任。但凱舟也未向 Martech 確認，便提供公司營利事業登記予駭客成功提款。Carren 為了長久營運，作為決策者面臨兩難，該不該出貨如何衡量利弊，從財務與信任等指標，考慮合適的決策方案：

表 3：出貨利弊分析

決策問題：是否放行提單	財務		信任	
	分析	選擇	分析	選擇
是	1. Martech有貨賣，有收入可能會分擔損失 2. Martech不分擔損失，但後續交易可能有議價空間 (凱舟收到錢的機率0-100%)	√	Martech心存感激，重建信任，繼續往來	√
否	客製品無法轉售 (收到錢的機率0%)		Martech沒貨賣，無法重建信任，失去客戶	

資料來源：本研究整理

小結：由凱舟個案可知，BEC 發生，無關情誼深厚，關係破壞殆盡。資安事件影響層面複雜，在信賴基礎被破壞的情況下，Carren 除了展現投入資安的決心，更要努力與 Marta 協商。從(表 3)財務的構面來看，Carren 如果選擇放行提單出貨，可能會有機會，可以追求更好的利益，不放行提單不出貨，僅有壞處，收到錢的機率是 0%；從信任的構面來看，Carren 如果認列損失，選擇如期如約完成交易，提升完成交易的確定性，使客戶願意重新建立信任關係，有機會贏回客戶的心，不放行提單不出貨，會造成 Martech 財務與信譽的損失，流失客戶。

（四）BEC 攻擊對凱舟造成的影響甚鉅，應如何改善資安與防範？（30 分鐘/累計 110 分鐘）

透過討論問題一跟二，已經帶領學生找出駭客利用 BEC 攻擊凱舟的步驟，與駭客慣用的套路。對此學者們(Cross et al.,2020；Al-Musib et al., 2021)建議可以尋求技術性與非技術性的方式來防堵。

1. 凱舟該如何防止成爲被駭客鎖定的目標，電子郵件被接管？

總經理 Carren 為避免人員在業務流程的疏失，決心從外部導入數位技術進行變革。凱舟的內網資安管理全靠卡巴斯基防毒軟體，雖能阻斷外網的主動攻擊，但無法掌握每個終端設備的防護狀況。在技術性解決方案的硬體防禦方面，可利用防火牆與交換器等，建構反惡意軟體與內網端點安全系統。Carren 也規定不可使用自攜裝置接收郵件或處理公務，並使用公司配發的筆電。軟體防禦方面，公司筆電購買正版作業用應用軟體，定期更新版本。公司入口網 eCaware 區隔公司內外網，登入系統時，用戶單一簽入(SSO：Single Sign On)功能，強化身分驗證機制。憑員工 ID 做 AD 認

證的人機綁定，自動提醒，定期更新且採用高強度的密碼、登錄以及修改紀錄應要保存 90 天。Maria 屬業務部門，一個月更新一次密碼，就算又不小心被破解，也僅有一個月時間被監控。

在電子郵件系統安全防護方面，雖然凱舟取消使用 hiBox Webmail 收取郵件，由管理者關閉 POP、IMAP、SMTP、國外 IP 登入等功能。Maria 仍可在家、在外透過 VPN 連入 eCaware，收發郵件。使用機器學習分析凱舟的電子郵件地址或內容，自動跳出顯示警告信號(即黑白名單)以及對國際 IP 登錄等可疑行為發出警告，可避免人眼把關，看走眼逃脫具高度風險的郵件。

即便有技術性解決方案，可以過濾所有相似度極高的陌生郵件，但無法阻擋像 Maria 這樣無法分辨什麼是釣魚郵件的個人行為。在非技術性解決方案可透過持續的員工資安教育訓練，傳授 BEC 流程(社交工程演練)，提升資安意識。建立賞罰機制，資安行為列入年度考核基準、獎勵自主學習，既可提升員工資訊素養。

2. 凱舟該如何防止將貨款轉移至海外銀行帳戶？

駭客以社交工程手法，日常的熟悉感與信任，誤導了 Marta 的判斷。凱舟可透過非技術性手段積極對策，業務應告知所有客戶，凱舟不會隨便更改銀行帳戶，即使有變更，郵件、匯款帳號會加上防偽的電子簽章，也一定會以電話再通知。重複提醒付款方在匯款之前，隨時保持警覺心，仔細檢查電子郵件地址與域名。關於付款建立一致和安全的流程、治理程序，採用雙因素認證（Two-factor Authentication，2FA），針對電子郵件更改銀行帳號的請求，打電話給財務人員，驗證所有付款的合法性。意識、培訓、重複，是挫敗 BEC 網路攻擊的重要因素(Zweighaft, 2017)。

3. 凱舟該如何防止將公司機密文件傳送出去？

凱舟應先制訂流程與資安政策，機密資料需分級管理並加密，加密郵件中不要提供憑證或密碼，應電話或其他管道另行通知(Myojin & Babaguchi, 2020)。如此一來，可以透過 eCaware 的使用者權限與組織架構對應功能，依使用者權限登入限定的 IP，存取工作所需的資訊。許可權外的資料存取或傳送，都需經過在系統上申請，主管的電子簽章授權。可避免主管出差或者新進人員，對業務不熟悉而影響資訊安全。並在伺服器保存郵件、修改紀錄，作為後續追蹤溯源。

小結：除了評估使用的技術是否能達到防禦效果之外，技術的使用(use of technologies)要考慮財務面的前提下才能進行轉變，財務面既是轉變的驅動力，也是約束力(Matt et al. 2015)。與大型企業每年 700 萬的資安投入相比，凱舟每年投入不到 5 萬，凱舟系中小企業，尋找兼顧成本與效率的解決方案，以成本最小化，取得效率與利益最佳的組合。

除了考慮上述技術與成本兩點，資安漏洞的範圍是否會波及其他重要客戶造成財損。凱舟全面暫停公司所有出貨，並盤點交易中的業務，在危機處理上有其時效性的限制，科技系統的導入所要花費的建置時間也是考慮的要素。

不管駭客是藉由哪個管道入侵，Carren 都要致力展現帶領團隊翻轉資安的決心，並說服 Marta 以及其他客戶通力合作，提供安全的環境，確保利害關係人等，在安全、風險可控下進行交易，重建彼此的信賴。

伍、後記（10 分鐘/累計 120 分鐘）

一、「凱舟 01」月會

「凱舟 01」月會，各部門的一級或二級主管與會，Carren 開場致詞，「在 BEC 事件之後，Judy 跟 Maria 相繼離職，Martech 訂單量有減少趨勢。為有效降低人為因素的影響，更堅定我司仰賴數位管理，堅以捍衛資安的決心，這也是我將此次月會命名為凱舟 01 的原因。與其被詐騙，還不如把錢用在大家合力提升資安與數位能力的獎勵上。針對各部門在 eCaware 使用的痛點與營運面數位管理，持續採用 PDCA，不斷地修改程式和評估新軟體與資源導入，因應客戶需求，強化競爭力。」

二、導入 eCaware 的效益

經管 Stanley 並向眾人報告，「導入 eCaware 在資安管理作為前後對比(表 4)，除此之外，編列預算注入經費，使 eCaware 成為員工每日工作儀表板，介接原有的生產、業務管理如 FLOW、SFT、CRM、ERP 等相關系統，無須多次重複登入帳密。依部門流程執行無紙化管理，ISO 表單、管理辦法、每日產出的管理報表與資料，儲存成為重要資料。各單位主管們可即時追蹤公司動態、業務/生產/研發各種績效，即時溝通，快速處理與決策。另外，在這次疫情期間布達防疫措施、宣導規定，第一時間也能掌握員工體溫及健康狀態，是遠距工

作的行動辦公室。偕同人資部門執行內部教育訓練，公司整體資安素養大幅提升。系統技術面提示初次往來的郵件，同仁們不會再淪為郵件詐騙的翻版，不必人工一一核對每一封郵件。對可疑郵件警覺性提高，能妥善處理信件異常、陌生來信等，避免不少假詢問、真釣魚的機會。電腦中毒事件銳減，從 2019 年 43 件，2020 年 26 件，至 2021 年的 16 件。」

IT Yale 回饋，「確實是，處理中毒處理變少，可以投入更多時間，收集各部門在數位系統使用上的回饋，為了幫助同仁們工作更加順暢，常與莊顧問研討如何延伸 eCaware 功能，也開始涉略軟體發展的領域。」

Stanley 接著說：「過去我們生產大眾化產品，現在行銷業務部收到各產業領域委託開發客制化產品的需求，會同技術研發部經常需要與不同地區的客戶、供應商透過 eCaware 共同參與協作。接下來將開放 eCaware 的專案功能，讓各部門員工可即時交換工作內容，提高部門間合作交流，方便主管與顧客追蹤個別與整體研發專案的進度。同時也可以保留研發紀錄做好知識管理，即便由其他人接手也容易看得懂，增加其可用性及管理效率。為了因應將來改版或擴充功能，要考慮系統整合相容性、移轉成本與員工適應性的問題，建議公司應該要培養自有的軟體開發人員。」

表 4：eCaware 導入資安管理作爲前後對比

資訊安全項目	導入前	導入後	管理作為
流程控管	未定義流程	監控流程	分析流程，優化營運
單一簽入(SSO：Single Sign On)	電腦開機輸入使用者帳密	進入eCaware內網輸入員工帳密，執行AD認證	區隔內外網，保障工作平台的安全性
首頁資訊區塊管理	公司內部訊息通過Email公告	一頁式管理，可讀取內部公告，資訊不漏接	建立內部良好溝通管道
密碼變更控制	未定期變更	系統統一亂數編配密碼,具有時效性及保密性	由系統設定密碼變更周期及設定,取代人為控制
資料防偽	未控管	系統內建選項	文件加密及電子簽章防止變造
Email安全性	未控管	系統連結郵件備份過濾陌生信件	騷擾郵件列入黑名單，自源頭阻絕
VPN(遠端控制權限)	由主管口頭准予開放	於電子簽核系統申請，人機綁定，執行AD認證	控管使用權限及存取記錄
申請用印/機敏性資料取用	由保管人員給予,未有控管機制	利用電子簽核系統送出申請單核簽後准予使用	提升使用印章/證件等之安全性,並留有完整電子申請記錄
資料匣權限/程式權限	由主管口頭准予開放	依權限順利的登入系統，並依權限看到不同的資訊	組織架構與人員帳號同步，深入個人化服務

資料來源：本研究整理

結語

Carren 感到欣慰，在數位跌倒，再從數位站起來，歷程 2 年資安事件下的產物 eCaware 似乎帶來意外的價值創造，特別是打破部門與公司藩籬，讓相關人員可以登入系統瞭解專案進度，同時保留完整的研發記錄，這是凱舟內部知識管理重要的一步。當然系統還可依公司持續壯大來擴充功能性，eCaware 帶來的便利、安全性，也讓凱舟營運加添想像空間。未來如果在顧客端與供應商端進行整合，讓他們參與研發與生產的過程，對於凱舟所提供給顧客的價值可以更上一層。

參考文獻

吳志明、朱素玥、方文昌，2006，「供應鏈關係中信任與承諾影響因素之研究-交易成本及社會交換理論觀點」，資訊管理學報，13 卷 S 期：91~118。(Wu, C. M., Chu, S. Y., and Fang, W. C., 2006, "The Study of Trust and Commitment Influence Factors in Supply Chain Relationships-Transaction Cost and Social Exchange Theories Perspectives," **Journal of Information Management**, Vol. 13, No. S, 91-118.)

Al-Musib, N. S., Al-Serhani, F. M., Humayun, H., and Jhanjhi, N. Z., 2021, "Business Email Compromise (BEC) Attacks," **Proceedings of Materials Today, Selection and Peer-review under Responsibility of the Scientific Committee of the International Virtual Conference on Sustainable Materials (IVCSM-2k20).**

Button, M., McNaugton, N. C., Kerr, J., and Owen, R., 2014, "Online Frauds: Learning from Victims why They Fall for These Scams," **Australian and New Zealand Journal of Criminology**, Vol. 47, No. 3, 391-408.

Cross, C. and Rosalie G., 2020, "Exploiting Trust for Financial Gain: An Overview of Business Email Compromise (BEC) Fraud," **Journal of Financial Crime**, Vol. 27, No. 3, 871-884.

Jakobsson, M., 2016, "Case Study: Business Email Compromise" in Jakobsson, M. (Ed.) **Understanding Social Engineering Based Scams**, First Edition, New York: Springer, 115-122.

Matt, C., Thomas H., and Alexander B., 2015, "Digital Transformation Strategies," **Business & Information Systems Engineering**, Vol. 57, No. 5, 339-343.

Morgan, R. M. and Hunt, S. D., 1994, "The Commitment-trust Theory of Relationship Marketing," **Journal of Marketing**, Vol. 58, No. 3, 20-38.

Rebovich, D., Layne, J., Jiandani, J., and Hage, S., 2000, **The National Public Survey on White Collar Crime**, 1st, Morgantown, WV: National White Collar Crime Center.

Myojin, S. and Babaguchi, N., 2020, "A Logical Consideration on Fraudulent Email Communication," **Artificial Life and Robotics**, Vol. 25, No. 3, 475-481.

Zweighaft, D., 2017, "Business Email Compromise and Executive Impersonation: Are Financial Institutions Exposed?" **Journal of Investment Compliance**, Vol. 18, No. 1, 1-7.

作者簡介

張敏華

國立中山大學企業管理學系 DBA 博士生。凱舟濾材股份有限公司創辦人，科技部審查通過核准進駐科學園區精準健康產業專區的資格。

E-mail: carrenchang@caware.com.tw

黃子佳

國立中山大學企業管理學系博士候選人。台灣集廣科技有限公司總經理，研究興趣主要包括動態競爭、企業管理個案撰寫等。研究著作曾發表於管理評論 2020 管理個案特刊。

E-mail: jiajia1491@gmail.com

戴佑真

國立中山大學行銷傳播管理所碩士。智策慧行銷顧問股份有限公司國際行銷顧問，研究興趣主要包括行銷傳播、社會文化與企業管理個案撰寫等。研究著作曾發表於管理評論 2020 管理個案特刊。

E-mail: youjen125@hotmail.com