資安事件後的企業數位鑑識決策模式

林敬皇
成功大學 電通所
gbox@crypto.ee.ncku.edu.tw

賴溪松
崑山科技大學 資訊工程系
citool@mail.ksu.edu.tw

摘要

數位鑑識被視為解決電腦與網路犯罪的方案之一，但除了犯罪調查者外，企業組織也試著利用數位鑑識來調查內部資訊安全事件及民事求償的個案。透過在資訊安全事件處理時，利用數位鑑識的方法保存事件的證據，以追蹤犯罪者或破壞者，並藉以提出求償的訴訟。我們建構一事後的企業數位鑑識決策模式，來輔助企業組織在面對內部的破壞、民事的資安事件時，如何評估與考量是否在事件處理過程中進行數位鑑識工作，避免更多的鑑識資源耗費在無價值的個案中，並促使企業組織在安全防護或犯罪調查上能更有效率。

關鍵詞：Cost-Benefit Model、Digital Forensic、Decision Model

一、前言

資訊安全事件可能為來自內部的破壞、民事或刑事的犯罪事件。執法機關對於刑事的犯罪事件，進行追查犯罪者是不計代價的。以企業的角度來看，除了處理內部的破壞及民事的資安事件外，也想要找出犯罪者與破壞者加以求償，以弭補因資安事件造成的損失。但企業資源有限，並非所有的資訊安全事件發生後，皆有能力與資源來進行追查或求償的工作，因此必需選擇有益的方案，以降低資訊安全事件所帶來的損失。

數位鑑識被視為解決電腦與網路犯罪的方案之一[14]，但除了犯罪調查者外，企業組織也試著利用數位鑑識來調查內部資訊安全事件及民事求償的個案。透過在資訊安全事件處理時，利用數位鑑識的方法保存事件的證據，以追蹤犯罪者或破壞者，並藉以提出求償的訴訟。影響企業組織找出犯罪者與破壞者加以求償的因素有很多，包含事件的種類、造成的損失與復原的成本、追蹤到犯罪者或破壞者的可能及資訊安全政策與規範等。企業組織可能因智財權的損失而傾向提出損害賠償告訴，也因為害怕事件曝光，可能影響商譽或造成客戶流失，而選擇吸收因資訊安全事件所導致的損失。這些因素是複雜的，並可能影響最後的資訊安全事件處理的決策與方向，故企業要如何評估與考量是否在事件處理過程中進行數位鑑識工作，以避免更多的鑑識資源耗費在無價值的個案中，是企業對於資訊安全防護投資的重要課題之一。本文提出一成本分析模式，用以提供企業組織是否進行追查犯罪者與破壞者，並加以求償的決策參考依據，以避免企業再資訊安全事件中造成無謂的損失。

我們所發展的成本模式，除作為事件處理時是否進行數位鑑識決策的參考依據外，亦可用來決定求償的最低成本與金額。同時解釋為什麼發生在企業內部的資安事件往往都不願曝光或與犯罪者對簿公堂的原因。

本文於第二節討論事件與數位鑑識成本所應涵蓋的範圍。第三節探討如何概算出可能的成本並建立一成本分析模式。第四節分析數位鑑識的可能效益。第五節中討論影響企業數位鑑識決策的因素及事後的企業數位鑑識決策模式，最後為結論與未來可能進一步探討與分析的議題。

二、事件處理與數位鑑識成本

依事件發生的前後來看，我們可將其分類為事前、事中及事後等階段。數位鑑識大都類歸為事後階段的分析處理，但愈來愈多的趨勢顯示，在事中階段的緊急處置動作，若未能保存相關的數位證據，則未來進行鑑識分析與追查犯罪者將更為困難，因此進行數位鑑識時，事中及事後階段的處理都需要投入相當的成本。本節說明事件處理、數位鑑識及當事件發生時，企業如何計算投入事件處理與數位鑑識的成本與效益。

(一)資訊安全事件處理

事件處理的目的是在事件發現後，進行有效的因應措施，以減少損失、維持營運持續運作或快速的復原。並於事後追查事件發生的原因，以避免相同事件再度發生[4]。

事件處理是由事件應變小組(Incident Response Teams, IRTs)來執行，事件應變小組包含處理事件應變及分配相關的資源用於減少損失與復原。在文獻[1,7,9,10]已討論如何建立事件應變小組處理事件發生後的相關事務。

資安事件發生後，企業必需付出額外的成本，已達到快速復原，這些成本包含處理事件所需付出的人力、時間、軟硬體設備及復原所需要的資源。由事件的處理來看，主要包含成本如下：

(1) **緊急處理成本**：進行事件的緊急處理或處置等行動所衍生之成本。如：事件應變小組人力、備源系統運作等。

(2) **損害成本**：事件所造成的損害。如：營業中斷、商譽或聲譽損失等。

(3) **復原成本**：復原過程中所需要的成本。如：軟體安裝設定、人力及資料重建等。

若為了保存相關的數位證據，則在事中的處理時，必須同時進行可能的數位鑑識工作。進行這些工作所衍生的成本則列為緊急處理成本及復原成本中，說明如下：

(1) 在保存證據與對事件緊急處理中，可能會有衝突之處，如：為保存證據，需將硬體設備封存，但事件緊急處理則可能必須將硬體設備重新設定後上線。所以需要投入額外的成本，應取得兩者間的平衡；即在進行事件緊急處理時，同時保存相關證據。

(2) 由於數位鑑識與相關的調查工作，往往曠日費時，但復原的工作卻是相當急迫的，如：需將設備復原以利正常的營運，但數位鑑識進行卻需保留設備事發後的原始狀態，以利分析，故需要投入額外的成本來進行。

基於上述，我們可以定義事件的應變及緊急處置為事中階段所進行，而數位鑑識與相關的調查工作則為事後階段所進行的。故企業決策者在進行企業數位鑑識是否執行決策時，有事中及事後兩個時間點可以進行。本文主要的時間點為焦距在事後的成本分析與決策。

(二)數位鑑識

數位鑑識[5]是使用資訊技術，用以蒐集、保護、分析、粹取、及解釋資訊安全事件過程中所遺留在電子媒體中的數位證據的科學。其目的是保留數位證據的完整性，及建構資訊安全事件發生的過程，以作為資訊安全事件處理及司法單位調查、判決之依據[6]。

要使數位證據能做為法庭上審理時參考的依據，企業進行數位鑑識時所使用的方法到數位證據在犯罪本身的證明能力及法律規範，則需要滿足下列條件：

(1) 擷取與分析時必須原始證據不被竄改，且採用合法的程序。

(2) 擷取與分析時所使用的方法及工具需經驗證。

(3) 數位證據要能夠證明事件(犯罪事實)原因與過程以做為認定犯罪事實之基礎。

不同的個案類型，進行數位鑑識所蒐集的數位證據標的亦不相同，如：企業內員工竊取商業機密文件，直接的證據為所竊取的商業機密文件；散佈毀謗訊息的事件，欲蒐集的證據則為訊息發佈與犯罪者的關連。因此，數位鑑識必須發展不同的方法或程序以符合各類型個案的不同需求，如：Abstraction Layers methodology[2] 及 Hierarchical, Objectives-Based Framework[11]。

數位鑑識的好處是協助企業處理資訊安全事件的同時，找出破壞者與犯罪者，並對其提出損害賠償。除藉以減少損失外，尚可提升外在的聲譽與企業形象。然而，數位鑑識的工作是複雜且需要專業的人力來進行數位證據的蒐證工作，因此成本相對較事件處理來得高。從數位鑑識人員到提出訴訟的所有過程，均可能須額外投入許多的資源。進行數位鑑識成本主要包含如下：

(1) 數位鑑識人力成本：數位鑑識蒐證與分析，甚至報告的相關人員人力成本，不同的團隊成員可能依專業而收取不同的人力費用。如：磁碟分析人員、破密人員等。

(2) 進行鑑識設備(工具)成本：數位鑑識蒐證與分析時所使用的相關設備，可能需要租借或購買所衍生之成本。如：分析工作站硬體及軟體等。

(3) 訴訟成本：提出告訴或要求損害賠償的相關成本，如：律師費等。

(三)成本效益分析

成本效益分析是個體經濟學與管理會計學領域中用以說明企業進行投資決策的主要理論依據之一。當企業進行投資決策時，若計算投入的成本遠小於回收的效益時，表示此項投資具有額外收益，故該項投資會被進行。相同的，我們可以借用成本效益分析的方法來看企業是否投入資源進行事件處理與數位鑑識之決策。

最早進行安全事件的處理之成本效益分析為 I-CAMP (Incident Cost Analysis Modeling Project)，I-CAMP 是一個早期由美國「十大」的十所大學(Big Ten Universities)所發展出來的成本效益分析模型，應用於安全事件成本評估。I-CAMP 所使用的成本模式是較為直接的與容易依循(follow)的，包含安全事件所造成的停工時間、使用的工具成本、人力成本及事件所造成的其他損失。I-CAMP 適合用來評估事件後的損失成本與可能的效益，但是許多時候，I-CAMP 並非有效的評估方法，如：研究人員，停工時間本來就不易計算，在估計事件損失的人力成本上，可能會低估或高估。

在商業的領域中，企業透過更為複雜的現金流(Cash Flow, CF)方法評估投資，以減低所遭受的投資風險。內部報酬率(Internal Rate of Return, IRR)與淨現值(Net Present Value, NPV)是最常用來評估是否採用該項投資的主要決策方法之一。內部報酬率是指將不同時期投入的投資成本換算成現值之總和恰巧等於期初投資成本的折現，即淨現值 (NPV) 剛好為 0 之折現率。

$$NPV = \frac{CF_1}{(1+IRR)} + \frac{CF_2}{(1+IRR)^2} + \frac{CF_3}{(1+IRR)^3} + \ldots + \frac{CF_n}{(1+IRR)^n} - CF_0 = 0$$

其中 $\frac{CF_i}{(1+IRR)^i}$ 表示為第 i 其投入的投資成本折現值，CF_0 表示期初投資成本的折現值。

故當企業評估對事件處理與數位鑑識的投資計畫時，IRR 大於投資計畫的資金成本時，表示企業對投資計畫滿足所得到的報酬率，故企業會將資金投入對事件處理與數位鑑識的投資計畫。反之，IRR 小於投資計畫的資金成本時，企業應拒絕此一投資計畫。

Gordon 與 Loeb[9]也利用類似 IRR 與 NPV 的方法，簡單地計算投資在資訊安全資產的報酬(return on investment, ROI)。DARPA-funded project 則發展一個類似 ROI 的數學模式來計算投入成本與所減少的潛在風險。

成本效益分析透過不同的形式展現及計算，其最終目的是確保所投入的成本小於回收所得的效益，即效益大於成本。除 I-CAMP project 外，目前尚未有對於事件處理所投入的成本或投資進行類似的成本或效益分析之模式。原因是在事件處理或數位鑑識的效益不易估計，所涉及的變數與不確定性多，特別是效益不易分析與計算。故本文試著分析事件處理或數位鑑識的成本與企業決策考量的相關變數，透過成本效益分析的觀點，建構分析企業在安全事件後是否投入成本進行數位鑑識工作之計算模型。

三、成本分析模式

成本的評估與計算是決策的重要依據之一。資訊安全事件後，對於損害的調查需要投入相當的資源，包含人力與軟、硬體設備，如：調查人員、重新安裝的電腦硬體、應用軟體等。企業在進行數位鑑識調查事件的同時，也需投入成本，這些成本包含：人力成本、投入設備的成本及因事件所致的損失與費用等成本。如下圖 1 所示。

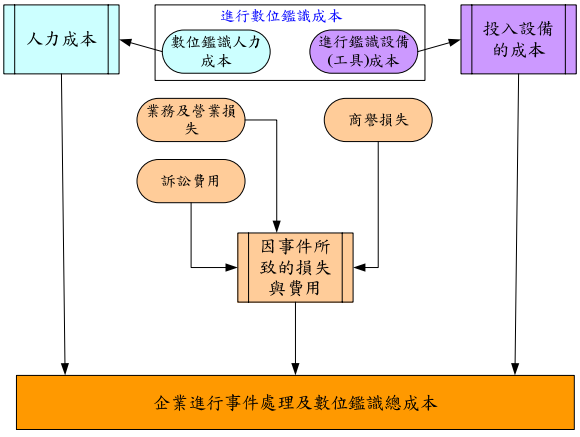

圖 1 企業進行事件處理數位鑑識成本

(一) 人力成本

人力成本為事後鑑識進行時所投入的人力成本。進行數位鑑識時，可能需要額外的人力甚至聘用外部的專家來進行，不論由內部或外部的人員進行，都必須付出相當的薪酬，此為數位鑑識人力成本。

數位鑑識人力成本＝Σ薪資(含加班費)*時數

(二) 投入設備的成本

數位鑑識為了保存、分析及在法庭上展示相關的數位證據，需要適當或對應的工具，以促使數位證據能夠在法庭上被認可為判決的依據。對於這些工具及設備的投入成本，為鑑識設備(工具)成本。這些成本可能單純以使用或租用的天數成本作為計算，亦可能以整批取得的成本作為計算，並在進行完數位鑑識工作後處分或分年攤提折舊。

鑑識設備(工具)成本＝進行數位鑑識所需設備運作成本（*天數）

(三) 因事件所致的損失與費用

資訊安全事件的發生，為企業與組織帶來了損失，這些損失包含：有形的及無形的資產損失，如：營業中斷、停工的損失及電腦軟、硬體設備的損耗及商譽等。有形的資產損失較容易估計與量化，但無形的資產損失，如：商譽等，則不易量化。故因事件發生或進行處理到事後的鑑識及訴訟所致的損失與費用與無形的資產損失應加入為成本的一部份。

因事件所致的損失與費用＝Σ（業務及營業損失＋商譽損失＋訴訟費用）

(1) 業務及營業損失：

業務及營業損失是當安全事件發生後所造成的營運損失，以營運中斷天數作為估計。該項損失的估計依不同的行業或個別業務，可利用前六個月的每日平均營收或前年度的同一時期的每日平均營收做為

估計在營運中斷期間每日營收金額，並依據此一金額計算安全事件發生後所造成的營運損失。

每日營收＝Average(前六個月) 或 Average(前年同一季)

業務及營業損失＝每日營收*天數

(2) 商譽損失：

無形的損失與估計是較難以量化的，特別是商譽、信用等級等損失，依一般公認會計原則，商譽可按照行業習慣或個別業務分別認列，最常使用的方法有二：

一為以當年度或去年度一年的超額盈利來估計商譽的價值。超額盈利的計算方法為總市值與淨資產總額（資產減去負債後的餘額）之差額[13]。

另一種商譽的價值估計，以平均超額盈利來估計商譽的價值。

超額盈利的計算方法，是把平均應稅盈利(即過去三年的應稅盈利的簡單平均數，但假如盈利趨升／跌，則取加權平均數)減去相同年度於已運用資本的固定比率獲利回報 [12]。如：在 2001、2002、2003 年的應課稅盈為 1,788,217 元、1,700,873 元及 1,749,573 元，合計：5,238,663 元。每年平均盈利 1,746,221 元。資產淨值 2001、2002、2003 年分別為 1,857,255 元、2,283,562 元及 2,858,324 元，合計:6,999,141 元，平均為 2,333,047 元，以 10%穫利為 233,304 元來看。商譽應為：1,746,221 元－233,304 元＝1,512,917 元。

因此，在無形的損失估計時，利用估計事發當時及處理期間所造成的獲利下跌情況及未來獲利能力的調整，如：獲利回報從 10%降為 9%等，即可量化無形的損失。

商譽可經由會計原則來加以計算，但尚有許多無形的資產可能無法精經量化，可採用相同的方式，估計事發當時及處理期間所造成的獲利下跌情況及未來獲利能力的調整，來反映在商譽中。

商譽及其他損害成本＝事前的商譽估計－事後的商譽估計

(3) 訴訟費用：

數位鑑識工作後，為了使因資安事件的損失能夠有所補償，企業對於所提出的訴訟，需要聘請律師或律師團。訴訟進行期間，審理相關的規費及證人出庭等費用，亦為整體訴訟成本中的一環。

訴訟成本＝律師訴訟費用＋訴訟規費

進行成本分析可作為企業數位鑑識決策的重要參考之一，當事件發生後，企業可以依此一成本分析模式概算所需的人力成本、設備物資成本及因事件所造成的相關損失成本等，作為企業數位鑑識決策的依據。

依所發展的成本分析可以在事件發生後將事件復原或求償所需的成本計算出來，但影響企業數位鑑識決策仍有許多其他的因素。

四、數位鑑識可能效益

影響企業數位鑑識決策的因素很多，最主要的部份仍脫離不了進行數位鑑識的成本及可能的帶來的效益。

數位鑑識所帶來的可能效益有二：一為透過蒐集與分析將事件損害的證據及造成損害的破壞者及駭客找出。二為在法庭上提供可被接受的數位證據，供法院作為損害賠償判定之依據。依此兩點分析，企業欲在事件發生後，尋求破壞者及駭客來分攤損害或保險金賠償。成功找到犯罪者的機率及求償成功機率是首先需要進行評估的。

(1) 成功找到犯罪者的機率(Probability of seized the suspect)

即進行數位鑑識後可能找到犯罪者、破壞者及駭客的機率，這樣的機率並非絕對。在應變處理時，可以先依事件的類型，如：駭客入侵、內部資料竊取等類型進行

分類。內部資料竊取之事件，由於大多有跡可循，可能較有機會找到犯罪者、破壞者。外部的駭客，許多時候是經由跳板進行入侵，若非在國境內則大多無法找到犯罪者或破壞者。因此對於成功找到犯罪者的機率估算，僅能利用在事件應變所得之分析記錄，來加以推估可能之機率為何。事前的紀錄與稽核措施愈為完備，則成功找到內部的犯罪者及破壞者機率愈高。反之，外部的入侵者及事前的紀錄與稽核措施缺乏，則成功找到犯罪者及破壞者機率愈低。

(2) 求償成功機率（Probability of Getting Indemnity）

除了保險求償的個案外，就算成功找到犯罪者、破壞者及駭客，也不一定能夠有足夠的證據，達到求償的目的。因此求償成功機率可從初估在數位鑑識的預估成果及同類型個案的先前判例來著手進行。預期數位鑑識所得的成果，為具體、直接與有力的證據，足以獲得勝訴，及同類型個案的先前判例多為成功求償，則求償成功機會較大。反之，則求償成功的機率小。

成功找到犯罪者的機率及求償成功機率是難以定義明確的，但可透過事件的種類、數位鑑識預期的成果及同類型個案的先前判例來加以概算。效益的評估尚包含可得的賠償金額及其他利益，可得的賠償金額為判決後，所獲得的補償金或保險公司所給予的損害賠償金。賠償金額的多寡大多以損失為主，可能為損失的全部或比例，但需考量成功找到犯罪者的機率及求償成功機率，若成功找到犯罪者的機率及求償成功機率較低，則賠償金額不論多寡，都不可能實現。分析如下表 1。

表 1 損害賠償金額估計

		成功找到犯罪者的機率	
		高	低
求償成功機率	高	可獲得賠償金額	保險個案：可獲得賠償金額
	低	證據不足 犯罪動機不足以起訴	獲得賠償金額機率低

在事件過後，若經數位鑑識並進行求償工作，有助於提升獲利能力，則依此計算可能的利得為何，如：提升客戶的信賴、獲利上升 10%，所增加的營收，則可能為企業帶來其他利益。但還是有許多無形效益是無法量化的，如：對內部組織稽核制度的提升、企業形象的肯定及成為社會公益與教育的個案等。數位鑑識進行後的效益估算，受到許多因素的影響，許多的因素是無法進行量化的評估，僅能依比例來進行預估，並決定可能的效益。

五、企業數位鑑識決策模式

除了上述成本的估計及數位鑑識可能效益外，影響企業於事件發生後是否進行數位鑑識工作，尚有許多其他的因素，特別是欲將數位鑑識所得的數位證據作為求償或興訟的依據時，企業可能面臨更多的變數及不確定性，尤其在犯罪者不知為誰或關係企業形象與未來業務推展的情況下，企業將可能選擇不進行任何的數位鑑識工作或求償工作，而選擇將事件所產生的成本由內部吸收。舉例來說，駭客入侵，導致銀行系統當機的事件，銀行可能寧願選擇將成本由內部吸收，而不願提出求償。因為一旦求償，可能導致銀行客戶對該銀行失去信心，進而影響未來業務推展。

但亦有可能企業內部不計一切代價，在事件後進行數位鑑識工作，試圖找出犯罪者加以求償。如：離職員工入侵系統將商業機密帶往競爭對手，這關係企業的存亡，故企業會選擇不計成本，對其進行求償動作。

最後影響企業數位鑑識決策因素，則為比較難以加以估計與計算的因素，包

含：其他無形或間接利益的提升及企業決策者的社會責任等。不同的個案類型，亦可能影響企業執行數位鑑識的決策。

綜論以上，我們可以更近一步整理出企業在資安事件後，進行數位鑑識決策時，主要的考量因素有：企業形象及商譽、所得的效益及預計投入的成本等三項。

企業的決策者，應追求企業利益的極大化，所以在資訊安全事件後，企業形象及商譽為首要的考量因素。當企業形象及商譽受損嚴重，甚至危害企業未來的獲利能力時，企業會不計成本找出犯罪者加以求償。因此，當所得的效益減去預計投入的數位鑑識成本後，比較與企業形象及商譽的損失即為本文所提的企業數位鑑識決策模式。

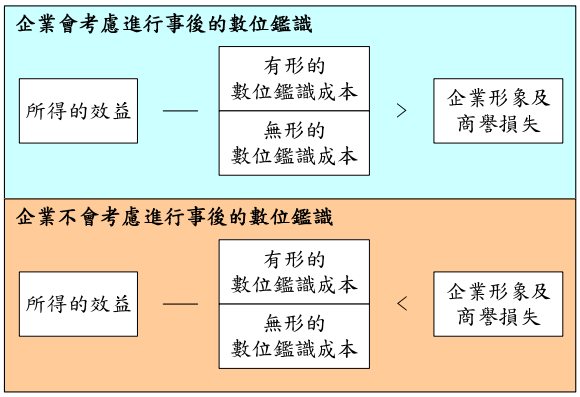

圖 2 企業數位鑑識決策模式

在我們的企業數位鑑識決策模式型中，企業進行數位鑑識的成本，可依第三節成本分析估算出來作為訴訟時求償的金額。所得的效益則可依第四節數位鑑識可能效益方式進行評估與估算，企業對於數位鑑識決策有三個可能的情況：

(1) 效益大於企業形象及商譽的損失：

企業進行數位鑑識所得的效益減去總成本大於企業形象及商譽的損失，表示企業進行數位鑑識將有助於獲得其他利益，則企業於執行數位鑑識工作可獲額外之利益，故大部分的企業應該選擇執行數位鑑識工作，找出破壞者及犯罪者進行求償。

但此類情況尚可能受到資訊不對稱或企業決策者擔當不足而有所影響。當資訊不對稱時，決策者容易誤判誤認為效益大於成本，而驟下決策，導致需投入其他成本來符合其效益。再者，企業決策者擔當不足，可能仍裹足不前，不敢冒然地進行鑑識及求償工作，以致未能取得額外之利益。常見的個案有：內部員工所引發的入侵或侵權、情節重大的事件，如：捲款或盜用公款等。

(2) 效益小於企業形象及商譽的損失：

進行數位鑑識的總成本大於效益，則表示企業可能需花費額外的成本，故依一般經濟法則來看，企業應避免進行數鑑識的工作，僅進行事件後的復原與重建，降低事件對營運的衝擊與支出的額外成本。

目前企業遭受到的許多資訊安全事件，如：駭客入侵、病毒等，因不易抓到犯罪者與可能獲得賠償機率低，故所得的效益遠小於成本及企業形象及商譽的損失，因此，大多選擇隱而不報。

但當個案的結果可能影響未來企業的存續或企業形象時，企業的決策者可能不計代價，一定要在事後的鑑識分析或訴訟中取得勝利，則亦可能選擇進行數位鑑識。常見的個案有：涉及公益的刑事案件、病毒感染、外部的駭客入侵及或影響多數人權益的事件，如：詐欺等。

(3) 效益等於企業形象及商譽的損失：

企業進行數位鑑識的成本等於其所產生的效益，則企業不進行數位鑑識都一樣，但是此類情況在企業若選擇不進行數位鑑識時，企業形象及商譽是存在損失的。

故此一情況與「效益小於企業形象及商譽的損失」相同。

六、結論與未來工作

對企業而言，用以支援營業的任何費用皆能視為投資，如投入機器設備的改善，以增加產品良率、投資廣告，以增加產品銷售、將產品送檢以增加產品在市場

的競爭力等。這些投資當然需要具有一定的效益或回饋，否則企業不會考量進行投資。因此企業對於資訊安全的努力，也可視為是一種投資行為，若非能夠有益於企業，則這樣的投資就不值得企業投入金錢或資源。同樣的，資安事件的處理及後續的鑑識工作也可視為企業所進行的投資，若該項投資無助於企業獲利，依一般的經濟法則，該項投資在企業內部就應該被否決掉而不可能會進行。

在資訊安全事件後，企業是否願意進行數位鑑識或求償，並找出事件發生的可能原因，而非僅有將受損的系統復原，掩蓋事件的痕跡。重要的考量為企業從進行數位鑑識或求償的過程中能否有適當的利得。本研究所建構的企業數位鑑識決策模式，除幫助企業了解數位鑑識的所有成本外，亦可作為在資訊安全事件後，是否進行數位鑑識及提出求償之決策依據。

我們主要貢獻為發展應用於數位鑑識決策之成本分析模式，並從事件發生後的成本估算可計算提出求償之金額與保險償付損失之金額。資訊安全事件在企業內部發生時，常常是隱而不報的，依成本效益分析的觀點來看，公開後的事件可能打擊企業的商譽或進一步影響其獲利能力，使得企業形象及商譽的損失大增，這也可以解釋為什麼許多的企業在事件後不公開的原因。

未來的研究可能有二：一為對於數位鑑識決策的時間點之不同，成本與效益的計算應不盡相同，所進行的決策分析模式也應不同，可分析及研究找出在不同時間點的決策對於資安事件處理及後續數位鑑識對於企業的影響。其二，探討對於不同個案成本估算細部的因素，及進行成功找到犯罪者的機率與求償成功機率的概算方法，使企業能夠運用此一成本效益分析模式，更為精確地計算成本與效益，以進行事發後的處理與鑑識投資決策。

七、參考文獻

[1]. A Framework for Incident Response,Information Security Team, DePaul University, Chicago, Dec 2002.

[2]. Brian Carrier, Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers, International Journal of Digital Evidence winter 2003, Volume 1, Issue 4.

[3]. Chris prosise, kevin mandia, Incident response & computer forensics, second edition, McGraw-Hill,New York,Nov 2004.

[4]. David Theunissen, Corporate Incident Handling Guidelines, Sans InfoSec Reading Room, Nov 2001 http://www.sans.org/rr/incident/corp_guide.php

[5]. Digital Forensic Research Workshop, A Road Map for Digital Forensic Research, August 7-8, 2001.

[6]. Eoghan Casey, Handbook of Computer Crime Investigation, 2002, ACADEMIC PRESS.

[7]. RFC 2350, Expectations for Computer Security Incident Response, http://www.faqs.org/rfcs/rfc2350.html

[8]. L.A. Gordon, and M.P. Loeb, Return on information security investments: Myths vs. realities. Strategic Finance Magazine, Nov 2002 http://www.strategicfinancemag.com/.

[9]. Guidelines and Recommendations for Security Incident Processing Working Group (GRIP), IETF.

[10]. Moira J. West-Brown, DonStikvoort, K.

Klaus-Peter, Handbook for Computer Security Incident Response Teams (CSIRTs), CERT/CC, DEC 1998.

[11]. L.B. Nicole, J.G Clark, A Hierarchical, Objectives-Based Framework for the Digital Investigations Process, Digital Forensics Research Workshop (DFRWS), Baltimore, Maryland, August 2004.

[12]. Statement of Financial Accounting Standards No.34 , Accounting Research and development Foundation,Jan,13 2005.

[13]. Summary of Statement 142, Goodwill and Other Intangible Assets, Financial Accounting Standards Board, FASB, December 15, 2001

[14]. Warren G. Kruse II and Jay G. Heiser, Computer forensics-Incident Response Essentials, Addison-Wesley corporation, 2002.