

國立政治大學

商管專業學院

碩士學位論文

以使用者中心概念，發掘企業創新來源？  
-以趨勢科技為例

Discover the source of corporate innovation by adopting  
user centric design methodology?

A study of Trend Micro Technology

指導教授：蕭瑞麟博士

研究生：趙伯鈞

中華民國九十八年七月廿三日

## 誌謝

### 運氣

我自認非天資聰穎或苦讀上進的標準學生，但從國中到大學升學皆躲過聯考的茶毒，利用機會多多體驗不同的人生歷練。在加拿大交換學生一年的時間裡，讓我決定在取得工作經歷後攻讀 MBA，同時對於自主學習有了更深切的體認。

隨著社會對於 MBA 需求的轉變，我得以進入政大商學院的窄門，並且和來自不同產業的同學與學養深厚的教授群一起學習。

上天同時贈與我的禮物，便是百年難得一見的金融海嘯，當全球各國政府與企業慌亂於解決連鎖性危機的同時，我卻得此奢侈機會靜心於指南山腳下，吸收新思維同時精進自己的能力。

### 緣分

與蕭老師結緣，起源於畢業後第一份在新加坡的工作，巧妙的緣分讓我們在五年後以不同的身份且在不同的地點重聚。

選擇學習質性研究的人，總是帶著些許的叛逆性格，想要與眾不同，更想要利用獨特的方法找到問題的根源，而這樣的特性讓我在整個研究過程中，吃盡苦頭亦備受挫折。

然而，論文研究主題的確立以及後續研究發展的架構，竟意外地與過去大學專業，或是免除聯考茶毒後，習得的人生歷練相連結，以致於在後續的田野調查期間，常常遭遇山窮水盡的沮喪，但最後卻是柳暗花明又一村的驚喜。

也因為蕭老師的鼓勵，讓我得以認識許多在學術領域不斷精進的學長姐與默默支持我們的行政團隊，為嚴肅且緊湊的研究生生活，增添許多歡笑與美好的回憶。

### 努力

回首 MBA 過程所遭遇的壓力與挑戰，雖然辛苦卻是滿足與甜蜜的收穫！畢竟，在決定結束工作重返校園後，每一個決定都代表背後的機會成本與風險抉擇，課堂間談笑風生的互動討論，往往是數十小時辛苦研讀的成果，蕭老師思辯的訓練方式，也一再撕裂我制式的思維想法，企圖移去教條式訓練的遺毒，而政大商學院緊湊卻範圍廣闊的訓練系統，能否滿足眾人期待與自己當初設定的目標，如同芒刺在背地警惕著我，持續創造局部優勢，拉近與既定目標的距離。

### 衷心感謝

我深信貧困與動亂的環境，是對於年輕人一輩子最大的祝福，家人給予我滿滿的關懷與鼓勵，是我面臨疑惑與挫折的避風港，女朋友的寬容與支持，讓我心無旁騖地鑽研學習，Hilti 公司的全額學習補助與定期回饋機制，幫助我檢視學習成效與實務需求的差異度，周遭許多朋友與長輩的支持，才得以成就我今日的學習成果，再此感謝各位對於伯鈞求學歷程中，具體且意義重大的支持。

2010 年於國立政治大學

## 摘要

什麼是創新的來源，許多人會認為創新來自於更好的產品功能或是更高階的設計概念。然而，也有人會認為創新來自於使用者。

如果創新來自於使用者，那麼我們是否可以要求他們描述自己的需要，便可以知道如何創造新的產品或服務呢？

從上述例子我們可以推論，使用者不一定明白知道自己真正的需要，若沒有完善的輔佐機制，使用者無法成為產品/服務創新的來源。

本研究發現，深入瞭解使用者的情境脈絡，可以發現新的創新來源。為了分析使用者的情境脈絡如何影響到組織對於資訊安全的需求，本研究調查六個來自不同產業的個案，並檢驗不同使用者的情境脈絡，如何影響到該組織對與資安的看法與行為。

事實上，個案的田野調查真實地呈現了如何將使用者的”洞見”轉化成產品/服務創新的最佳來源。來自五個不同產業的個案不但展現了大相逕庭的資安痛點，同時也廣泛地觸及了五個在未來具有高度發展潛力的領域，資安相關人員所關心的資安議題。

本研究強調，當我們試著瞭解使用者在不同產業處理資安議題時，深入地探索與思考使用者所處的情境脈絡時，我們一定會發掘到許多產品/服務創新的機會，以及相對應的組織管理議題。

## ***Abstract***

*What are the sources of innovation? Many people would consider better technical functions or superior industrial designs as innovations. Currently, more people would argue that innovative ideas come from users. Therefore, if we ask users to describe their needs, we will know how to innovate our products or services. But, users' inputs might not always be right because they might not know what they really want.*

*Our research suggests that ideas of innovation may better be inspired by user's local practices. To analyze how local practices may influence an organisation's security requirements, this paper presents five case studies and examines the contextual details affecting the expectations of different organizations.*

*Indeed, this field study illustrates how customers' insights could become a rich source of product/service innovation. It not only underscores the security pain points in each firm, but also exposes broader security issues in five different market segments.*

*The findings indicate that when we come to appreciate how users make sense of computer security in their actual business situations, we are able to identify viable ideas for innovation in products, services and organization management.*

## 目錄

<b>第壹章 緒論</b> .....	<b>8</b>
第一節 研究背景與動機.....	9
第二節 研究目的.....	11
第三節 研究問題.....	12
第四節 趨勢科技介紹.....	14
第五節 研究架構說明.....	17
<b>第貳章 文獻探討與理論基礎</b> .....	<b>19</b>
第一節 以使用者為創新來源的文獻探討.....	19
第二節 領先使用者創新導向的迷思與驗證.....	21
第三節 領先使用者脈絡與痛點研究.....	24
第四節 強化領先使用者理論與實務研究貢獻.....	25
<b>第參章 研究方法與設計</b> .....	<b>27</b>
第一節 研究方法說明.....	27
第二節 研究流程.....	28
第三節 資料蒐集.....	31
第四節 資料分析.....	35
第五節 分析單元選擇.....	37
<b>第肆章 個案研究發現</b> .....	<b>38</b>
第一節 S 電腦資訊中心.....	38
產業背景.....	38
現有資安產品與服務.....	38
資安痛點.....	39
創新解決方案.....	42
以 S 電腦全球資訊中心為例.....	42
個案歸納.....	44
第二節 S 金控電腦中心.....	45
產業背景.....	45
現有資安產品與服務.....	46
資安痛點.....	46
創新解決方案.....	50
在 S 金控案例.....	50
個案歸納.....	52

第三節 X BEAUTY 美妝購物網站.....	53
產業背景.....	53
現有資安產品與服務.....	54
資安痛點.....	54
創新解決方案.....	56
X Beauty 網路商店案例.....	56
個案歸納.....	58
第四節 X 縣政府資訊中心.....	59
產業背景.....	59
現有資安產品/服務.....	60
資安痛點.....	61
創新解決方案.....	64
P 縣政府資訊中心案例.....	64
個案歸納.....	65
第五節 L 網絡科技個案.....	66
產業背景.....	66
現有資安產品與服務.....	67
資安痛點.....	67
創新解決方案.....	70
L 網絡科技案例.....	70
個案歸納.....	71
第六節 本章結論.....	72
<b>第五章 研究結果分析與討論.....</b>	<b>74</b>
第一節 學理貢獻.....	74
第二節 實務貢獻.....	76
<b>第陸章 結論與建議.....</b>	<b>80</b>
第一節 研究結論.....	80
第二節 研究限制.....	80
第三節 研究建議.....	81
<b>參考文獻.....</b>	<b>82</b>
一· 中文部分.....	82
二· 英文部分.....	82

## 表目錄

表 1	全球資訊安全市場產品營收與市佔率 .....	9
表 2	全球資訊安全市場廠商營收與市佔率 .....	16
表 3	創新的來源，理論整理 .....	20
表 4	領先使用者研究方法與順序 .....	21
表 5	五個產業創新產品來自於領先使用者貢獻的比例 .....	22
表 6	研究領先使用者可能產生的缺點與風險 .....	23
表 7	研究設計階段訪談人員名單 .....	32
表 8	個案資料彙集階段訪談人員名單 .....	33
表 9	個案資料彙集階段訪談人員名單 .....	34
表 10	個案一歸納整理 .....	44
表 11	個案二歸納整理 .....	52
表 12	個案三歸納整理 .....	58
表 13	個案四歸納整理 .....	65
表 14	個案五歸納整理 .....	71
表 15	五個產業個案歸納整理 .....	79

## 圖目錄

圖 1	亞洲資安市場 2005-2010 年成長預估 .....	10
圖 2	本研究與 VON HIPPEL 領先使用者理論之架構差異 .....	26
圖 3	本研究架構概念圖 .....	30

## 第壹章 緒論

知識經濟時代的來臨，顛覆許多國際企業的營運與競爭模式，小企業憑藉著日新月異的網路科技與技術突破，將創新的商品或服務，如同病毒般擴散傳遞至世界的每個角落。

大型企業過去善於利用長時間累積的有形資產（土地，機器設備，人力）排除新競爭者加入市場，但知識經濟環境下所產生的創新產品與服務，卻給了數以萬計的創業家，一個更公平的立足點，得以和長期壟斷市場的國際巨人，肉搏競爭分出一個高下。

小蝦米如何利用創新思維打倒巨人的故事，過去已在不同類型的產業中被驗證，而不斷遭受創新觀念挑戰的產業領導者，最關心的議題便是如何利用現有企業資源，發掘有效的創新來源，持續不斷地提供創新服務來維持利潤與競爭力。創新的來源隨著產業與組織特性，有著多樣的作法與不同的想法，同產業的競爭者也易於模仿同業的作法，而達到類似的成效。

因此，如果企業決定持續地探索新的創新來源，並追根究底地研究創新來源的成因與未來發展潛力，無異是深化了企業本身對創新管理的競爭力，相較於對手的惡意競爭模仿，持續開發創新來源的企業，必定能以更具差異化與貼心的服務，滿足目標市場客戶。

產品使用者在創新領域中扮演著越來越吃重的份量，但使用者在產品開發或企業營運過程中應該具備的功能與角色，仍有許多爭論與實驗的空間，其主要的原因便是多數使用者不瞭解自己真正的需求，或是開發者無法瞭解使用者的情境需求，並成功地轉化為商業化的產品。

本研究採用質性研究方式探討如何發現企業新的創新來源，並藉由深入的個案田野調查資料，呈現使用者在操作產品時所處的情境脈絡，幫助產品研發與經營者在瞭解使用者情境脈絡後，發掘未被滿足的需求與創新機會，開發更多創新且滿足使用者需求的商品/服務。



## 第一節 研究背景與動機

過去三十年間，資訊安全產業隨著個人電腦的逐漸普及與網際網路的快速擴展，發展出專業定位明確且上下游分工密切的國際性產業，除了重量級的專業廠商引領資安產業的產品與服務發展，資安產業未來的成長性與發展的多樣性，目前仍持續吸引許多不同領域的廠商，搶食這塊蓬勃發展的市場大餅。

Gartner Group 在 2006 年估計全球資安市場規模已達到 65 億美金，年平均成長率約在 15% 左右<sup>1</sup>，而 IDC 針對亞洲資安市場 2005-2010 的年成長預估，受亞洲強勁的經濟發展，推估未來每年的複合成長率達到 18% 以上的水準<sup>2</sup>。

因商業快速發展而衍生的蓬勃資安需求自然吸引了最優秀的人才與世界級企業研發最先進創新的資安技術與產品，但各家廠商相互競爭或模仿所推出的資安產品/服務，卻讓使用客戶感覺到，『不同品牌的資安產品似乎沒有太大的差異。』

表 1 全球資訊安全市場產品營收與市佔率

資料來源：Gartner Group Dataquest, 2006

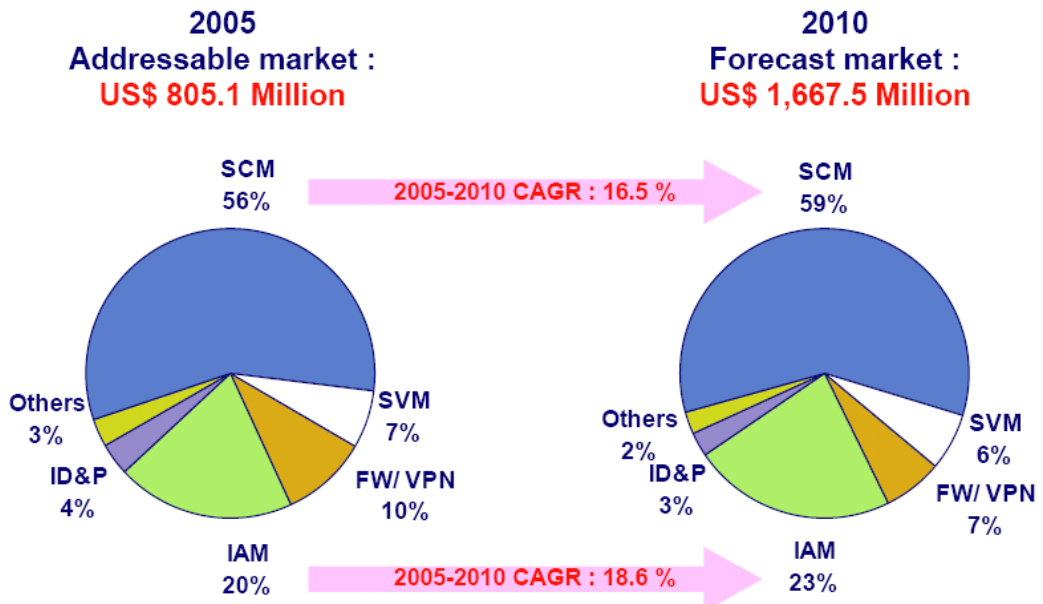
Total Security Software Revenue, Worldwide, 2005 (Millions of Dollars)					
	Revenue 2004	Revenue 2005	Market Share 2004	Market Share 2005	Growth 2004-2005
Symantec	2,077.9	2,381.6	32.2%	32.2%	14.6%
Others	1,609.1	1,891.6	25.0%	25.6%	17.6%
McAfee	816.3	918.1	12.7%	12.4%	12.5%
Trend Micro	550.8	630.0	8.5%	8.5%	14.4%
CA	398.2	438.2	6.2%	5.9%	10.1%
IBM	280.5	299.0	4.4%	4.0%	6.6%
RSA Security	232.4	222.0	3.6%	3.0%	-4.5%
Sun Microsystems	148.1	209.6	2.3%	2.8%	41.5%
Websense	111.9	148.6	1.7%	2.0%	32.9%
Novell	116.1	131.5	1.8%	1.8%	13.2%
Panda Software	105.0	130.0	1.6%	1.8%	23.8%
<b>Total</b>	<b>6,446.3</b>	<b>7,400.2</b>	<b>100.0%</b>	<b>100.0%</b>	<b>14.8%</b>

Source: Gartner Dataquest (July 2006)

由上表分析資安市場主要的收益來源，超過五成來自安裝於電腦主機的防毒軟體，而針對電腦主機端的防毒功能，不論是個人家庭用途或是企業專業用途，各大資安品牌皆提供琳瑯滿目的掃毒功能，藉由不斷推陳出新的軟體版本，搭配著免費試用方案或是不同的管道提供給所有的電腦使用者。

<sup>1</sup> Gartner Group Dataquest, 2006

<sup>2</sup> IDC APeJ Security Software Tracker, 1Q 2006



Source: IDC APeJ Security Software Tracker, 1Q 2006

圖 1 亞洲資安市場 2005-2010 年成長預估

資料來源：IDC APeJ Security Software Tracker, 1Q 2006

照理說，如果資安產品的研發速度與產品多樣選擇像手機產業一般，每一季甚至每個月都有新的版本上市，則客戶應該非常高興，因為客戶可以根據不同的組織特性或是功能特點來選購符合自己期望的資安產品，但在資安廠商不斷提供客戶更多且更創新的產品戰爭中，我們卻發現一群對資安產品越來越不滿的客戶，這股不滿的情緒甚至隨著時間增加而越來越強烈。

資安廠商也很苦悶，因為結合全球最優異的研發團隊，並且採用最新技術打造一套創新且功能強大的產品，資安業者不但期待商品推出後可以帶來豐厚的收益，打造破百萬美金的全球資安商機，更期待新功能的推出，可以改寫資安市場的遊戲規則，將競爭對手遠遠拋之在後，甚至將其自市場中淘汰。

然而，真實的結果卻是越來越大規模的資源投入產品研發，獲得卻是越來越少的利潤與越來越短的產品生命週期，伴隨著越來越多變的客戶抱怨與改善需求。

在瞬息萬變的資安產業，研發團隊費盡心力將最新防毒功能搭載到最新版的資安產品中，卻得不到市場與客戶的正面肯定，而客戶總是不斷在學習新增的功能，卻新產品卻無法保證降低業務營運可能發生的資安風險。

使用者的需求，如何在產品研發階段即導入，使其成為一重要的創新來源，而研發團隊如何瞭解客戶在使用產品時所處的脈絡情境，發現未被滿足的需求與可能改進的空間，使研發資源得以有效的使用並提昇產品未來上市的成功機率。企業若能成功將使用者需求轉化為產品開發方向，顧客對產品的滿意度是否能大幅改進？

而針對使用者需求開發的資安產品，能否像 I-pod 或 NetBook 一般，在快速成長的資安市場中，發光發亮？以上原因，都強化了筆者研究的動機。

## 第二節 研究目的

回顧很多產業的產品/服務研發歷程，初期皆由偏重技術或功能的大眾生產導向，演變成中後期分眾的顧客導向。

電腦、通訊、家電、運動用品...等無一不是；而且並不以工業產品為限，縱為服務性商品，如汽車租賃、金融服務...等產業的商品開發，也漸由大眾導向進入分眾導向。

由供應者的生產概念進入使用者的設計概念，由大眾演變成分眾的共同理由，是各分眾的需求逐漸產生並與大眾需求不盡相同；廠商的競爭面也必須由技術或功能研發，改為分眾的區分標準和各分眾需求的探索，再由技術的創新演化成服務的創新。

資安產品市場，是否也會有相同或類似的發展軌跡呢？如果答案是肯定的，資安廠商應該在產品創新甚或競爭策略上如何思考呢？

**Eric Von Hippel(1988)** 提出在快速變動產業中，藉由分析領先使用者的需求，發現企業新的創新來源，檢驗現有產品改善的空間與未來產品的創新方向。

筆者研究現今資安產業的產品研發模式，往往著重於技術端的創新突破而忽略了使用者操作產品/服務時所面對的情境脈絡，在性質上，現有資安產品偏重於技術模式或採用較狹隘的創新來源，因此隨著使用者需求的分眾化及快速變化，以此模式開發的資安產品/服務，似乎越來越難以滿足多變的市場需求？

產品開發過程中若能有效地將使用者情境脈絡，導入不同研發階段做為產品創新的有效來源，而各領先使用者族群中所呈現的的情境脈絡，分別衍生出哪些不同的產品與服務創新機會？

使用電腦教室進程式教學的老師與學生操作的電腦，或是券商營業員每日進行金融商品下單的電腦，對於資安的需求以及操作電腦過程中可能產生的風險，兩者的需求有何異同之處？又有哪些層面仍須加強改進？

以使用者為產品創新來源的設計導向，可否藉由深入地瞭解與分析情境脈絡，研發出高顧客滿意的產品/服務，最後提升市場佔有率呢？

### 第三節 研究問題

以領先使用者作為產品/服務研發創新的來源，經由學術界長時間的研究與產業界的驗證後，發展出『焦點小組』、『個案訪談』、『問卷調查』甚至『資料探勘』等從領先使用者蒐集並分析資料的方式。

許多新產品的研發過程中也大量採用使用者的意見作為創新的依據，但最終仍面臨失敗的結局。為什麼在分析並採用大量的使用者資料後，仍然無法打造符合市場需求的成功產品呢？

本研究假設多數的領先使用者不一定能清楚地陳述自己的期望與需求，某些領先使用者或許能描述自己的需要，卻忽略的使用時的情境脈絡。

如果使用者無法明確說明產品/服務需求，且當時的情境脈絡也缺乏清楚地分析，則產品開發過程中雖然規劃採用使用者的意見為重要根據，但受限於使用者

不具備清楚描述需求的能力與模糊的情境脈絡分析，仍然造成採用使用者想法的研發結果乏善可陳。

組織對於資訊安全的需求與具體作法實為一個高度複雜且牽涉範圍廣且深的議題，一般組織的使用者往往會受限於對資安技術的認知，產業環境的客觀限制以及擔任職務的本位主義，而無法詳細陳述對於產品/服務的創新需求與改進空間。

而分析多種組織因不同結構或產業特性而衍生出的資安需求，若組織的使用者無法提供一完整且具深度的說明時，便需要靠著深入且高互動性的田野調查，瞭解並記錄使用者對資安議題的想法與具體作法，同時學習不同的產業特性與環境限制後，整理歸納出不同組織使用者獨特的資安脈絡，藉由發掘資安脈絡追溯痛點，最後體認痛點的成因與影響層面，最後找到產品創新的新來源與現有產品/服務改善的方向。

本研究藉由探討領先使用者對於資安議題的情境脈絡，然後從情境脈絡中找出痛點，則產品研發過程才能藉由解讀資安痛點中，發掘更多隱藏在不同產業中的情境知識與脈絡，若能成功地將不同產業隱含的資安痛點解碼成新產品/服務的賣點，創新產品便可有效地與競爭品牌做出差異化策略，大幅提昇產品/服務在客戶的識別度與滿意度，同時擴大與競爭對手的差異。

### 對理論的貢獻

Eric Von Hippel(1988)強調觀察領先使用者的需求與作法，但要經歷怎樣的過程與機制，才能發現新的創新來源？

本研究假設瞭解領先使用者情境脈絡，分析痛點，找尋創新機會來源，對於領先使用者的資料蒐集與分析方法，可否找出更多隱藏在不同情境脈絡中的訊息？

## 對實務的貢獻

資安廠商對「研發資源投資的效益愈來愈差」之事實及成因，已有愈來愈多的瞭解，但對於合理的解決方案卻仍在摸索之中，如何有效地呈現不同群組的資安領先使用者情境脈絡，並在產品研發流程中產生互動，成為新一代的資安產品創新來源。

切入的角度，除了採用使用者導向的基本觀念外，更重要的是避開本位主義所產生的盲點與既有立場，正確挖掘與分析不同領先使用者的資安痛點，並成功地轉變未來研發的方向。

## 第四節 趨勢科技介紹

趨勢科技在1988年成立於美國加州，成立之初，以個人電腦病毒防治的大眾化套裝軟體為主要的利基市場。特別的是，1992年趨勢科技即赴日本開拓市場，後來，趨勢科技沒有在台灣尋求股票上市，反而在1998年於日本東京成為首家股票在日本上櫃的台灣軟體廠商，也成為台灣第一家股票上櫃的軟體公司。<sup>3</sup>

自從2000年以來，趨勢科技的產品多次獲選國家精品獎，並多次蟬聯由外貿協會與Interbrand所頒發的台灣國際品牌價值第一的榮譽。

## 個案公司組織型態演進整理與回顧

趨勢科技共有近4000名員工，分佈在台灣，中國，亞洲，日本，紐澳，美加地區，中南美地區，歐洲地區，超過30個國家與市場設有營運據點，年營收約為400億台幣。

---

<sup>3</sup> 2009/01/31，以策略與業理論觀點，探討持續創新與競爭優勢建構的挑戰：以趨勢科技為個案，張一中

## 趨勢科技產品線與創新演進

如果回顧趨勢科技自1988年以來的產品與技術的歷史，可以發現幾個特色：

- 趨勢科技由低階的消費者型電腦防毒軟體產品PC-Cilin起家。不過，歷經幾次重大的技術突破，與目標市場的轉移，現在的趨勢科技是以企業（大型與中小型企業）的一般型防制電腦病毒的軟體產品（非客製化型的產品）為主。

技術的範疇，也一直聚焦在與個人電腦，網路病毒防制相關領域。一直要到2000年之後，才開始往周邊不同的技術領域發展。不過即使如此，基本上，以產業界的術語來說，趨勢科技的技術是一直集中在所謂 Content Security 的範疇之內。

- 另一方面，趨勢科技的公司經營模式，基本上也一直是以電腦軟體產品，『產品導向』、『產品銷售』的邏輯來運作的。因此，為了能在競爭中勝出，趨勢科技的高階主管一直十分重視產品技術的領先性，即所謂的利基型的定位，以技術的優異性與差異性為競爭的賣點。此外，眾多的產品線，彼此的關連與整合性似乎並不明顯。

如果對照同樣是在軟體業的微軟公司的產品線，趨勢科技的產品比較像是各自單一的特定功能產品。趨勢科技即使有包裹式（Suite）的銷售方式，但是，產品與產品之間並沒有完整的系統整合與技術平台的構造存在。

- 趨勢科技的產品與技術研發，在整個1990年代，基本上都非常集中專注在『電腦病毒-防制的領域』。鮮少跨入其他因為網際網路而衍生的其他需求。例如：趨勢科技專注於電子郵件病毒，一直到2003年才進入垃圾郵件防制。又例如，以網路進行資料窺侯的間諜軟體（Spyware）資料外洩保全等等，也是一直到2005年之後才涉入。

相較於趨勢科技的主要競爭廠商，如Symantec與McAfee公司，趨勢科技的對外併購的策略與次數，都是相對比較不積極的。這在技術快速變遷的資訊軟體業界，是十分特別的。雖然也因此在公司財務上相對比較好，但是，在對先進技術的取得與領先的時間上，是相對處於追趕的位置的。

表 2 全球資訊安全市場廠商營收與市佔率

資料來源：Gartner Group Dataquest, 2006 年

附錄.表- 2 全前資訊安全市場廠商營收與市佔率。資料來源：Gartner Group Dataquest，2006 年

Total Security Software Revenue, Worldwide, 2005 (Millions of Dollars)					
	Revenue 2004	Revenue 2005	Market Share 2004	Market Share 2005	Growth 2004-2005
Symantec	2,077.9	2,381.6	32.2%	32.2%	14.6%
Others	1,609.1	1,891.6	25.0%	25.6%	17.6%
McAfee	816.3	918.1	12.7%	12.4%	12.5%
Trend Micro	550.8	630.0	8.5%	8.5%	14.4%
CA	398.2	438.2	6.2%	5.9%	10.1%
IBM	280.5	299.0	4.4%	4.0%	6.6%
RSA Security	232.4	222.0	3.6%	3.0%	-4.5%
Sun Microsystems	148.1	209.6	2.3%	2.8%	41.5%
Websense	111.9	148.6	1.7%	2.0%	32.9%
Novell	116.1	131.5	1.8%	1.8%	13.2%
Panda Software	105.0	130.0	1.6%	1.8%	23.8%
<b>Total</b>	<b>6,446.3</b>	<b>7,400.2</b>	<b>100.0%</b>	<b>100.0%</b>	<b>14.8%</b>

Source: Gartner Dataquest (July 2006)

- 由上圖，可清楚看出 2004 年開始，全球的資訊安全軟體產業以 Symantec，McAfee 與趨勢科技為領先群。以營收與市場佔有率而言，位居首位的 Symantec 的營收是趨勢科技的三倍以上，它是該產業中的第一名，而趨勢科技與 McAfee 則分別居第三與第二位，雙方的差距並不很大。但是，即使是趨勢科技與 McAfee 合併，仍然比不上第一名的 Symantec。持平而論，趨勢科技即使是在領先群內，在經營的規模上，仍然與產業的龍頭有相當大的差距。

而在趨勢科技之後，仍有像是 IBM，Computer Associate，Novell 等等知名的公司在虎視眈眈，利基型（Niche）的公司，例如：RSA security，Websense，也在其專長的產品區塊，（RSA 專長是資料加解密，Websense 則專長於資安 Appliance）建立堅強的市場堡壘。



## 第五節 研究架構說明

本研究論文的寫作論述結構，依序一共分為以下的六大章節，各章的內容重點整理如下：

### 第一章

本章內容在於說明本研究的相關背景，和個人選擇此研究題目的動機。同時，本章也說明進行此研究時，筆者心中所預設的研究目的，以及希望尋求解答或是尋求解釋的研究問題。

### 第二章

在文獻探討部分，本研究針對 Eric Von Hippel (1988) 的『創新的來源』為研究架構，深入瞭解領先使用者 (Lead User) 的資安情境脈絡，研究當領先使用者情境脈絡融入產品研發設計流程中，對使用者，組織與產品帶來的影響，可否幫助企業發現新的創新來源？藉由 Eric Von Hippel (1988) 對領先使用者的研究要點，來形成本研究的主要觀點，以作為本研究的研究方法設計，與研究個案分析探討時的理論基礎。

### 第三章

本章內容在於說明，本研究所選定的研究策略與方法（質性研究，田野調查法）。以及如何規劃接著進行的研究步驟，與工作流程。同時，依照文獻整理與回顧的結果，說明所設計的研究架構與研究構面。接著說明研究設計的方式，與資料收集，資料分析所使用的方法。本章希望藉由清楚說明，所遵循的社會科學研究方法，間接向讀者保證本研究的產出品質，同時在本章的最後，則以說明可能的研究限制作為結尾。

## 第四章

本研究的研究發現，藉由五個來自於不同產業的個案，瞭解領先使用者的情境脈絡與發掘痛點找尋產品創新來源，將重要關鍵事件或是活動依序展開，然後再輔以相關的事件，或是關鍵人物，對於該事件的訪談重點整理，以呈現該事件對於資安創新來源的影響與反思。

## 第五章

本章內容在於讓第四章所整理的個案內容，與第二章的文獻理論及第三章研究方法中所設定的研究構面進行『對話』。筆者應用第二章所整理的研究文獻論點，與第三章設計的研究架構與構面，對第四章收集的個案資料進行分析與論證。

## 第六章

本章是本研究論述的尾聲，因此本章的內容在於提出本研究的研究結論總結，包括本研究之發現及其對資安管理創新機會的貢獻、以及對未來實務與理論研究的建議等。

## 第貳章 文獻探討與理論基礎

### 第一節 以使用者為創新來源的文獻探討

Eric Von Hippel 於 1988 年提出以使用者為核心，發掘產品/服務創新來源的觀念<sup>4</sup>，顛覆了過去工業生產導向時代，創新來自於新技術的研發或是生產工具的改良。

若以使用者角度重新定義創新，創新不再是產品本身新增的功能或是外觀設計上的改變，而是如何掌握使用者需求，設計出符合市場/使用者期待的產品/服務。

隨著現實環境與商業競爭快速變遷，生產者的創新研發能力已經趕不上市場因環境演變衍生對創新的需求速度，如何發掘使用者在現實環境中遭遇的問題以及未被滿足的需求，在 Von Hippel 提出『創新的來源(Source of Innovation)』後，成為日後學界研究的重點。

不同於其他學者對於使用者 (User) 的研究，Von Hippel 強調研究領先使用者 (Lead User) 才能掌握真正關鍵創新來源。<sup>5</sup>無論是專業工業品 (如，電路板設計系統，圖書館管理系統) 或是一般家用品市場 (如：登山腳踏車，洗髮精)，觀察領先使用者對於新產品需求的洞察力 (Insight) 以及解決現有問題的能力和技巧，皆可以成為產業/服務差異化競爭，最佳的創新來源。<sup>6</sup>

Von Hippel (1988) 強調，領先使用者因為處於趨勢的前端 (Front of the trend)，所以比研發者更瞭解實際的需求，因此研究領先使用者不僅可以有效改善現有產品缺點，大幅增加生產力外，也降低了未來產品研發創新過程試誤的成本與潛在風險。

---

<sup>4</sup> Eric Von Hippel, Lead User Analyses for the Development of New Industrial Products, May, 1988.

<sup>5</sup> Von Hippel, E. 1988. *The Sources of Innovation*. New York University Press, Oxford.

<sup>6</sup> Von Hippel, E. 2007. Horizontal innovation networks--by and for users. *Industrial & Corporate Change* 16(2) 293-315.

表 3 創新的來源，理論整理

資料來源：Eric Von Hippel，1988

<b>Eric Von Hippel，The source of Innovation. (1988)</b>	
<b>研究發現</b>	在許多快速變動的產業或領域，領先使用者因長期浸淫於工作環境中，對於新產品/服務的創新過程，提出獨到的見解與作法，成為該領域主要的創新來源。
<b>為什麼是領先使用者</b>	<ul style="list-style-type: none"> <li>➤ 位於產業趨勢前端，相較於一般使用者，具備敏銳的想法。</li> <li>➤ 期待成為現有產品/服務改善後，最大的獲益者。</li> <li>➤ 因不滿足於現狀，故參與研發或親自動手實驗。</li> </ul>
<b>創新來源</b>	<ul style="list-style-type: none"> <li>➤ 對產品/服務的建議與想法 (Insight)</li> <li>➤ 面對與處理問題的能力與技巧(Problem Solving Skill)</li> </ul>
<b>創新產生的效益與影響</b>	<ul style="list-style-type: none"> <li>➤ 發現產品問題，大幅提昇產品/服務生產力。</li> <li>➤ 以使用者為導向，成為多種產業的產品/服務創新來源。</li> </ul>
<b>衍生的作法</b>	<ul style="list-style-type: none"> <li>➤ 焦點團體，問卷調查，電話訪問，資料探勘。</li> </ul>

## 第二節 領先使用者創新導向的迷思與驗證

研究領先使用者需求而成功發現新的創新來源雖然在多個領域證實為有效的模式，Von Hippel(2002) 亦在研究中說明對於領先使用者的研究方式與步驟<sup>7</sup>，我們是否可以推論，所有的新產品研發過程，只要選擇使用者導向，並採用領先使用者的研究方式，則所有產業設計出來的各式商品便可以完全滿足市場的需求呢？

表 4 領先使用者研究方法與順序

資料來源：Eric Von Hippel,1988

- 
1. 訂立領先使用者指標 (Specify Lead User Indicators)
  2. 確定領先使用者組群 (Identify Lead User Group)
  3. 提供觀念/產品給領先使用者 (Generate Concept/Product with Lead Users)
  4. 測試領先使用者的想法/產品 (Test Lead User Concept/Product).
- 

若深入瞭解採用領先使用者研究，成功將其需求轉成商品化的產業，如：登山腳踏車，戶外運動用品，電腦主機板設計軟體，圖書館管理系統等，為什麼採用使用者開發商品的成功比率（% of Developing and building innovation for own use）平均約在 10-35%，沒有達到 100%的成功率呢？

---

<sup>7</sup> Von Hippel, E. 2007. Horizontal innovation networks--by and for users. *Industrial & Corporate Change* **16**(2) 293-315.

表 5 五個產業創新產品來自於領先使用者貢獻的比例

資料來源：Eric Von Hippel, 2002

創新領域	樣本數量	來自於領先使用者貢獻的比例(%)	這些創新用戶是領先使用者？
<b>工業用商品</b>			
印刷電路板 開發軟體	136 個使用者出席 PC-CAD 座談會	24.3%	是
管線懸掛設備	管線懸掛設備安裝 公司 74 家	36%	N/A
圖書館 資訊系統	102 間澳洲圖書館採 用電腦化資訊系統	26%	是
<b>消費性商品</b>			
戶外消費性 商品	戶外商品郵購目錄 訂戶 153 人	9.8%	是
極限運動設備	專家使用者 197 人	37.8%	是
登山 自行車設備	專家使用者 291 人	19.1%	是

由上表可知，雖然領先使用者對於創新有獨到的見解，但受限於自身的能力或客觀的環境限制，根據領先使用者為創新來源的產品開發過程，仍然有許多需要加強與改善的地方。

領先使用者要如何將自己對於產品改善的空間或是創新的機會，完整地表達讓研發團隊瞭解？有多少比例的領先使用者，同時兼具多種能力呢？

在整理歸納領先使用者需求的過程，有哪些重要的訊息或需求，是領先使用者根本不熟悉也無法表達的領域？若忽略了這部分需求，市場對於新產品的接受度，是否埋下了不確定的風險？

研發團隊在蒐集大量的使用者資訊後，能否確實地轉化使用者需求，成為創

新的產品/服務特點？而使用者是否對於研發團隊抱著太高的期望，以致於在研發過程中提供太多高難度或是不切實際的想法？

領先使用者的需求，是否與主流市場需求一致？要經過什麼篩選與檢驗的機制，才能確保領先使用者的需求滿足主流市場對創新的期待？

從研究『採用使用者開發商品的比率』平均約在 10-35%之間，我們推論需要持續改善研究使用者意見的方法，並推測若錯誤地採納使用者意見，可能產生的風險可能性，整理如下表。

表 6 研究領先使用者可能產生的缺點與風險

資料來源：本研究整理

研究領先使用者	優點	缺點或限制	風險
蒐集	<ul style="list-style-type: none"> <li>➢ 改善現有產品缺失，增加生產力</li> <li>➢ 降低新產品研發風險與成本。</li> </ul>	<ul style="list-style-type: none"> <li>➢ 使用者不瞭解真正需要或無法清楚描述需求。</li> <li>➢ 使用者需求過於天馬行空。</li> </ul>	<ul style="list-style-type: none"> <li>➢ 市場接受度低</li> <li>➢ 產品差異度低</li> <li>➢ 與現有產品/服務差距過大。</li> </ul>
建議或想法			
觀察解決			
問題技巧			

從 Von Hippel (1988) 的理論與實驗中可瞭解，研究領先使用者成為新的創新來源，且此種創新方式可為不同產業開發新產品/服務的創新來源。

然而，研究領先使用者的洞察力與解決問題技巧，卻不能保證開發成功的創新產品/服務，我們可否從領先使用者中，找尋到其他的線索或研究方法，藉由新的觀察點分析領先使用者的需求，這是本篇研究對於領先使用者提出的貢獻。

### 第三節 領先使用者脈絡與痛點研究

如果蒐集領先使用者的意見與觀察問題解決技巧，仍然有許多需要改善的空間，那麼我們可以用什麼不同的機制，讓關鍵的資料不至於流失？並從關鍵資料裡分析出許多寶貴的資訊？

而不同的觀察角度或資料蒐集方式，又會讓我們產生哪些不一樣的想法，而這些想法是否可以讓我們對領先使用者扮演創新來源的角色，產生不同的解釋與作用呢？本研究希望藉由不同的方式，研究領先使用者對於創新來源的貢獻。

#### ➤ 研究使用者情境脈絡，彌補使用者因無法描述真實需求而產生的盲點

使用者在分析本身需求時，常常會因表達的能力、自身的盲點、外部環境限制等因素，以致於在描述產品創新需求過程，產生『失真』的狀況。

而產品研發人員，在經歷各部門無數次的往返互動與長時間的開發過程，重要資訊也容易被『稀釋或扭曲』，而誤解對使用者需求的瞭解。

本研究希望藉由深入的田野調查，發現領先使用者的工作脈絡，讓研發人員完整地理解使用者的工作脈絡情境，使得重要的脈絡訊息不至於流失或扭曲。

#### ➤ 從脈絡中找尋痛點，發掘問題相關性與創新可能性

藉由瞭解領先使用者工作脈絡後，發掘目前遭遇的挑戰或是工作瓶頸，即本研究所謂之『痛點』，從解決領先使用者的痛點發現創新的來源，不僅讓研發人員更深入地了解不同痛點的相關性與隱藏資訊，為解決痛點而衍生出的解決方案，更能刺激許多創新想法的產生。



#### 第四節 強化領先使用者理論與實務研究貢獻

Von Hippel 強調蒐集領先使用者意見與觀察使用者的問題解決技巧，即可成為創新的來源，但觀察相關領域產品研發的表現，導入領先使用者想法成功推行至市場的比率，僅在 10%-35% 之間。<sup>8</sup>

本研究假設，**觀察領先使用者的情境脈絡發掘痛點**，藉由分析痛點讓使用者的需求可以更具體地呈現，不但刺激研發人員發現其他創新機會，藉此提高以使用者導向的產品成功上市的比率。希望研究發現能同時對理論與學術，提出建議與貢獻：

##### 對理論的貢獻

觀察領先使用者痛點，保留重要脈絡資訊並維持其真實度與完整性。

##### 對實務的貢獻

如何進入田野，挖掘領先使用者痛點，並將完整脈絡情境資訊導入產品研發過程。

瞭解使用者情境後，並將脈絡資訊導入研發流程，導入前與導入後對於研發團隊，產品設計與使用者的影響？

---

<sup>8</sup> Von Hippel, E. 2007. Horizontal innovation networks--by and for users.

# 產品/服務創新計畫

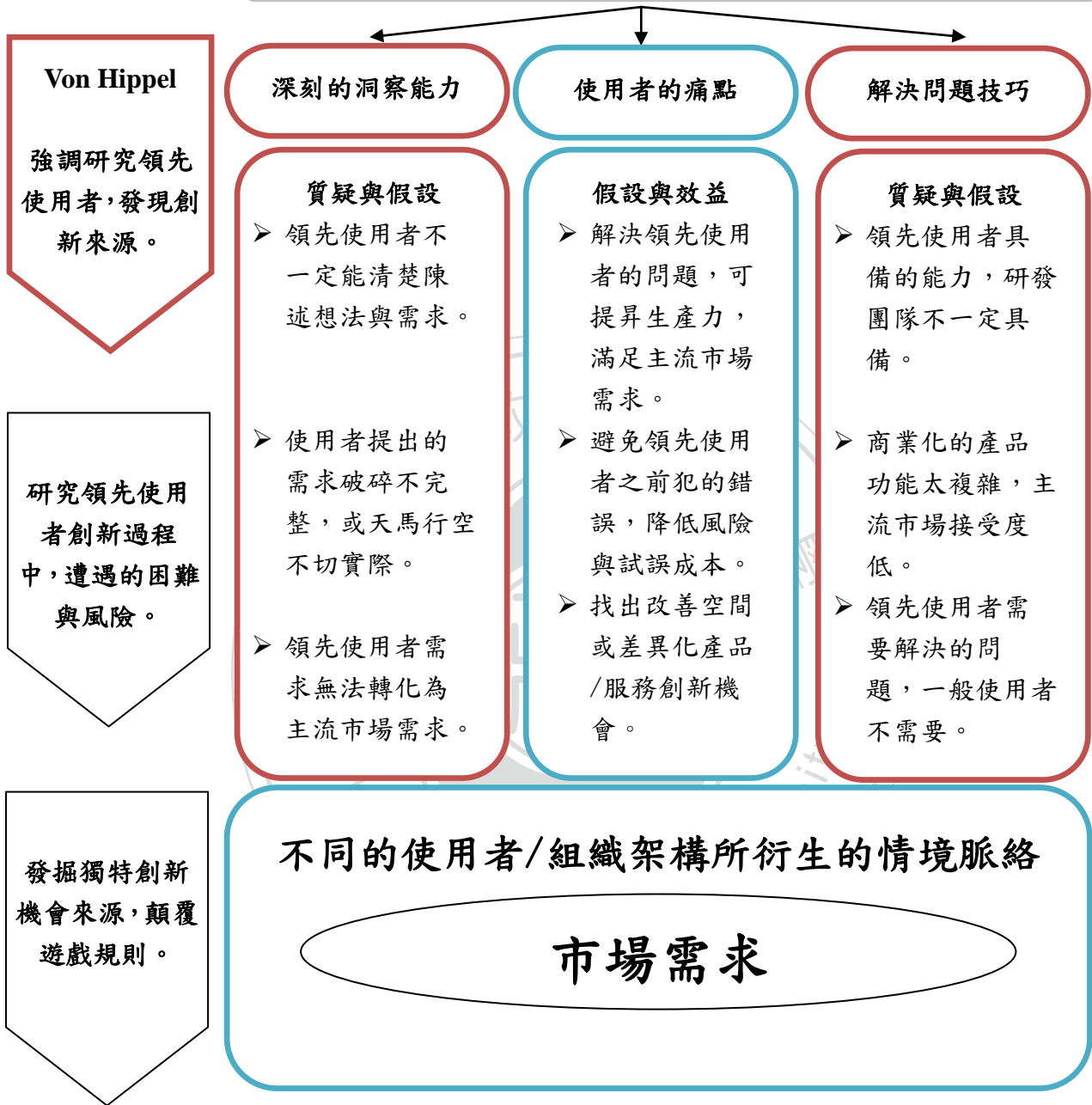


圖 2 本研究與 VON HIPPEL 領先使用者理論之架構差異

資料來源：本研究整理

## 第參章 研究方法與設計

### 第一節 研究方法說明

說明研究架構的三個層次，產業，企業與產業個案。

首先，為何選擇資訊安全產業，研究以領先使用者為創新的來源？

接著，趨勢科技將創新導入開發過程中，面臨什麼樣的挑戰與壓力？

最後，說明為何採質性研究法，以及如何以田野調查方式呈現領先使用者脈絡？

#### 1. 資安產業變化快速且需求複雜，創新來源多為技術導向

根據 Von Hippel 的研究 (1988)<sup>9</sup>，產品特徵與需求越簡單，研發團隊便能輕鬆地瞭解領先使用者對於產品/服務創新的需求。但資安產品/服務的需求設計，因涉及企業各部門，上下游廠商，主管機關限制與科技演變等多種因素，使得資安廠商無法明確掌握消費者需求，導致新產品推出的時間越來越快，但被客戶接受的比率卻越來越低的現象。

因此，研究資安產業領先使用者的需求，根據研究發現設計符合市場需求的創新產品，可幫助資安產業將大量研發資源聚焦在對的問題且滿足消費者真正需要。

#### 2. 趨勢產品與服務尚待整合，台灣為研發部門主要據點

利用研發部門高度集中在台灣的特性，研究台灣不同產業對資安的需求，即時將研究發現與研發團隊互動，也因為地域的便利性，針對個案所產生的疑問與後續研究，提供正確且完備的支援。

藉由瞭解領先使用者需求而產生新的創新來源，將可有效地幫助趨勢科技整合未來產品與服務的研發方向，在未來更有系統地將創新政策，轉為使用者導向。

---

<sup>9</sup> Von Hippel, E. 1988. *The Sources of Innovation*. New York University Press, Oxford.

### 3. 發掘痛點與脈絡，檢視問題本質與創新機會

目前多數組織尚未發展完整的權責職務與標準作業程序處理資安議題，不同產業作法差異甚大，資安工作者多從資安事件中學取經驗教訓，而企業資安政策亦不願公諸於世，因此需採用質化研究法，深入調查資安對於不同組織的價值與衍生的政策。

企業資安需求是高度與工作情境連結，且牽涉到許多外部因素影響的議題，而以領先使用者角度研究資安需求，便需要採用田野調查法，瞭解使用者日常場所處的情境環境與對於突發事件的應變反應，經由質性研究者的分析整理，將領先使用者的情境脈絡有條理的呈現，並發掘連使用者也可能忽略的需求與創新機會。

#### 第二節 研究流程

本研究時間自2008年9月到2009年6月為止，依照時間順序分類，可將研究階段分成『研究設計階段』（2008年09月-12月），『個案資料彙集階段』（2009年01月-04月）與『個案歸納分析階段』（2009年04月-05月）。

在『研究設計階段』，本研究彙整自2008年四月起，政大科管所博士生於趨勢科技台灣分公司進行田野調查時，與趨勢科技各部門32名員工的訪談紀錄，目的是要瞭解趨勢科技於資安產業的定位以及其產品服務所涵蓋範圍。

同時間，筆者研讀國內外『資安管理』、『以使用者為創新來源』以及『資安政策與企業組織和員工互動』之文獻，以求建立後續個案訪談之理論架構與研究問題。

在『個案資料彙集階段』，筆者初期研究台灣某金控資訊中心多起電腦中毒事件，嘗試建立病毒攻防戰史與資安病歷表，藉由回溯資安危機處理事件，理解工作脈絡，並學習金融產業針對資安風險而衍生的組織架構及實務作法，並試圖從使用者角度，找尋金融業資安痛點並深究當時情境脈絡。

後期訪談個案擴及高科技製造業，政府部門，電子商務與網路遊戲等多產

業，試圖從訪談過程中瞭解因產業差異而衍生出不同的工作脈絡，並從脈絡中分析整理該產業的資安痛點。

在『個案歸納分析階段』，研究團隊與趨勢科技內部來自研發，技術支援，行銷，客服與業務部門的資深主管進行個案討論，並根據不同背景成員進行編組，分組討論不同產業工作脈絡而衍生的痛點，並於當日提出趨勢的創新解決方案以及未來可應用的潛力產業。並於會後一個月內，獲得該組與會人員，針對未來產品/服務創新計畫，更詳細的執行規劃與說明。



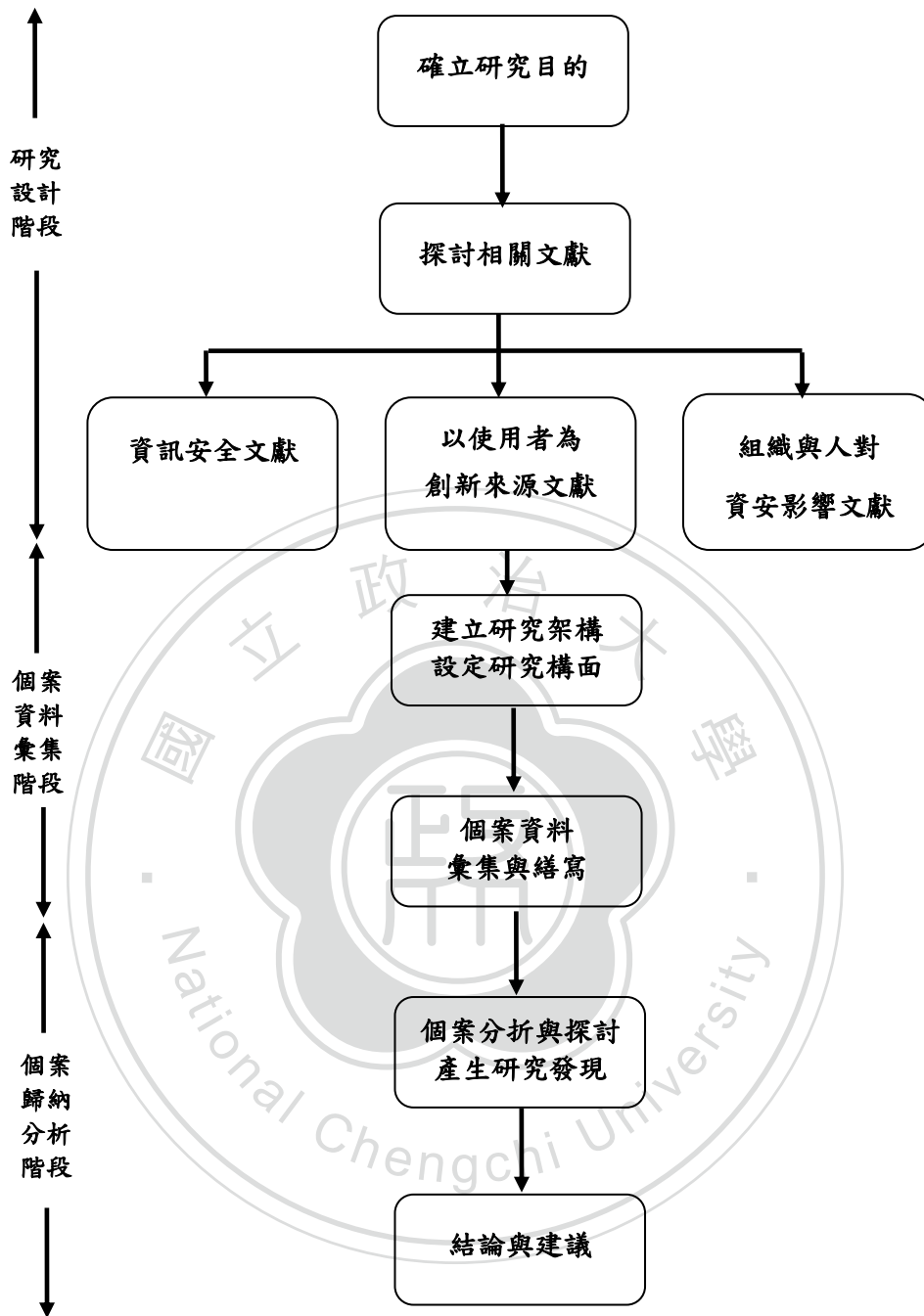


圖 3 本研究架構概念圖

資料來源：本研究整理

### 第三節 資料蒐集

由於本研究採取質性研究的「田野調查法」，因此資料的彙集首先是著重在於盡可能地，詳細地取得所觀察個案事件的全貌，並客觀地陳述與展示。因此，藉由個案訪談，觀察所研究的組織與相關資安議題，並且親聆主要事件關鍵的當事人的敘述與其觀點，剖析個案的事件現象。

原本規劃由趨勢科技推薦訪談的個案，竟因資安議題涉及公司營運機密且若不甚外洩將導致傷害公司形象或影響股價表現而予以婉拒。

後來成功訪談十個以上個案，多動用私人管道或校友網絡，遂使訪談順利進行，也因禍得福地使得訪談對象的組合，包含負責企業資訊安全的最高負責人，中階幹部與基層業務執行人員。

除了在訪談過程中累積了不同產業各階層資安相關人員，對於資安議題的想法與因為產業特性而衍生的作法，也因為研究過程中與趨勢科技保持密切的互動，使得資料蒐集過程中產生的疑點得以獲得解答，也幫助釐清確定各階段的研究議題與方向。

資料依照性質分類，包括「初級資料」和「次級資料」二個來源，分述如下：

#### 初級資料

初級資料主要都是來自與個案中事件關鍵的當事人，就個案的事件進行深度訪談，做為本研究解說與推導因果邏輯關係時，所依據之最主要的資料來源。

#### 次級資料

本論文的次級資料彙集，以相關的時事報導與評論為資訊蒐集之依據。資料來源方面包含：個案廠商（趨勢科技）在台灣之網站資訊；美國CSO-Online（資安官網站）、報導資安個案雜誌；如：資安人雜誌、CNet電子報以及網路上搜尋之有關資料，例如「聯合知識庫」「Google News」（新聞等最新動態）、與專業報章雜誌。

表 7 研究設計階段訪談人員名單

資料來源：本研究整理

研究設計階段（2008年09月-12月）			
受訪者單位	職稱	訪談時間	地點
趨勢科技	專案經理，V	2008/09/25，14:30-17:00	大安區
趨勢科技	協理，B	2008/09/30，10:00-11:30	大安區
某金控資訊中心	經理，T	2008/10/15，13:30-16:00	內湖區
某金控資訊中心	專案經理，K	2008/10/17，17:00-19:00	內湖區
某金控資訊中心	資訊長，T	2008/10/20，19:00-00:30	文山區
某金控資訊中心	資訊長，E	2008/10/27，13:30-16:00	文山區
某金控資訊中心	襄理，H	2008/10/30，14:00-16:30	內湖區
某國際軟體廠商	顧問經理，J	2008/11/01，14:00-15:00	信義區
某金控資訊中心	資安官，H	2008/11/11，13:00-16:30	內湖區
某金融監控單位	資安組長，L	2008/11/28，10:30-12:00	內湖區
某金控風險管理處	電腦稽核，I	2008/12/08，13:00-14:30	信義區
某金控資訊中心	資安官，H	2008/12/15，13:00-16:30	內湖區

在研究設計階段，主要目標有三：

- 第一， 瞭解趨勢科技特性並熟悉其產品與服務涵蓋範圍。
- 第二， 閱讀相關文獻，建立研究架構
- 第三， 針對單一金控資訊中心，以病毒攻防戰役模式回溯資安事件情境脈絡，並熟悉金融產業的資安組織權責架構與產業生態。

研究設計階段的面談資安相關人員，可分為三種階層，

- 第一， 基層網管人員，主要訪談組織內資安應變機制與回溯事件發生情境脈絡，與該產業最頻繁發生的資安事件類型與災害控制作法。
- 第二， 中階部門主管，研究資安與不同部門牽連的範圍與互動關係，監管機關對資安的要求規範，以及因應產業發展，資安未來的機會與挑戰？



第三，高階資安負責人，資安對於企業風險管理可能產生之影響與威脅，以及資安在企業營運中，扮演的策略性角色？

表 8 個案資料彙集階段訪談人員名單

資料來源：本研究整理

個案資料彙集階段（2009年01月-04月）			
受訪者單位	職稱	訪談時間	地點
某資安雜誌	主編，K 編輯總監，P	2009/02/09，13:00-14:45	內湖區
某軟體資料庫廠商	業務副總，M	2009/02/11，09:30-11:00	內湖區
某電腦OEM廠商	資訊經理，H	2009/02/12，10:30-12:00	內湖區
某美妝網站	總經理，V	2009/02/12，17:30-19:00	內湖區
某縣政府資訊中心	中心主任，Y	2009/02/13，10:00-12:00	信義區
某品牌電腦資訊中心	資訊長，T	2009/02/20，16:00-18:30	北投區
某外商資訊部門	資訊長，J	2009/03/08，13:30-15:00	信義區
某傳產石化製造業	總經理，W	2009/03/10，09:30-11:00	大安區
某券商資訊中心	經理，E 協理，P	2009/03/10，13:30-14:30	大安區
某資訊系統整合廠商	資深處長，K	2009/03/15，13:30-16:00	內湖區
某金控資訊中心	資訊長，E 技術經理，K	2009/03/23，10:00-12:30	松山區
某線上遊戲廠商	董事長，C	2009/04/02，16:00-18:30	萬華區

在個案資料彙集階段，主要目標有三：

- 第一， 金融產業以外，訪談積極導入資安的領先使用者，如高科技製造業，醫療生技產業，網路遊戲產業，電子商務產業。
- 第二， 分析不同產業所衍生的痛點與情境脈絡，並以學理架構驗證個案發現。
- 第三， 與趨勢科技檢驗個案發現，澄清個案疑點並鎖定具創新潛力的機會點。

表 9 個案資料彙集階段訪談人員名單

資料來源：本研究整理

個案歸納分析階段（2009年04月-05月）			
受訪者單位	職稱	訪談時間	地點
趨勢科技	Customer Insight 團隊	2009/04/16，13:30-17:30	大安區
趨勢科技	研發部 協理	2009/05/18，14:00-15:30	大安區

在個案個案歸納分析階段，主要目標有三：

- 第一， 結合學理與實務發現，分析訪談對象情境脈絡後，以個案型態呈現痛點，並尋求可產生龐大商機的創新來源。
- 第二， 組織趨勢科技內部來自研發，技術支援，客戶服務，產品行銷以及業務部門的資深主管，以混成編組方式研究分配之個案，在清楚瞭解使用者情境脈絡與痛點後，團隊需規劃一創新且高可行性的解決方案。
- 第三， 一個月內，蒐集趨勢科技整合內部人員所提出之更詳細解決方案，依照解決方案之可行性與未來市場潛力，針對領先使用者制訂下階段產品創新研發規劃以及未來學術研究發展方向。

#### 第四節 資料分析

若根據 Von Hippel(1988)<sup>10</sup>的理論，觀察『領先使用者的洞見或想法』與研究『領先使用者解決問題的技巧』，便可找到新的創新來源與機會。

然而，從本研究超過二十場針對領先使用者的訪談過程中，我們卻發現若僅憑理論找尋創新的來源，卻可能因為不熟悉當時的情境脈絡，而產生以下的誤判。

- **不同產業於訪談過程中，對於同樣的問題，竟有相似的反應與看法，但背後原因與邏輯卻差距甚遠**

不同產業如何配合產業環境與特性，建立一套完善的資安機制？金融產業與高科技製造業的資訊長皆異口同聲地認為，即使採用最先進的資安硬體與軟體技術，仍然無法建立嚴密的資安機制，唯有落實對員工的『資訊安全教育訓練』，才算是理想的資安防範體系。

高科技製造業資訊長對於落實員工資安訓練想法的解讀是，因為集團各部門與分公司設置於全球各地，即使投注天文數字於資安保護上，也無法防範有心人士的入侵，而內部員工資安意識的建立，才能有效地保障研發團隊的心血結晶並且獲得客戶的信賴。

然而，金融產業的資訊長對於資安教育訓練的落實，主要來自於主管機關將資安教育列為優先查核指標，資安教育若無法貫徹落實，則會被列為重點觀察對象。

金控架構旗下各單位皆會處理到客戶部分的重要資訊，資安教育在此成為一個警惕與恐嚇的工具，若違反資安內規不僅工作不保，亦可能牽涉法律責任。

金融與高科技產業雖然皆同意教育訓練對於資訊安全的重要性，但其背後的原因與衍生的作法，卻是大相逕庭。

---

<sup>10</sup> Lead User Analyses for the Development of New Industrial Products, May, 1988.

同樣的狀況，也發生在電子商務產業與政府機關對於『營運效率』的看法。

電子商務產業與政府機關的資安負責人強調，資安可以有效地提升營運效能與效率，但是電子商務執行長的原因來自於完善的資安防範使得員工安心地上班，不用擔心重要資料被破壞，而花心神在備份資料或重灌系統上，而員工把時間專注在對的企業活動上，公司效能自然因為完善的資安防護而得以提升。

不過，政府機關效能的提升卻是因為資安監控了所有電腦的作業活動，使得非公務的電腦作業活動無所遁形，藉由嚇阻而激發了效能。另一方面資安品質的改善提昇人民對政府的信心，也幫助政府在推動許多網路業務時，因為資安的助力而大幅改善業務推動的效率。

- **不同產業針對發生相似資安事件，竟有相同的反應機制與作法，但其背後的限制與環境，亦是天差地遠。**

在研究網路遊戲產業以及金融產業對於『電腦病毒攻擊的應變措施』時，網管人員的標準作法便是『拔掉電腦網路線，格式化所有資料，重灌電腦』..，這看似簡單的回應作法，在背後支持這解決方案的原因卻大不相同。

網路遊戲產業將關鍵資訊（如，遊戲開發原件）保護於 Linux 作業系統，不同於一般業務作業電腦需使用的 Windows 系統，異質的作業環境系統確保病毒無法蔓延，將傷害控制在最小的範圍內。

因此，當電腦因中毒當機，『重灌』變成了多次經驗後的最佳良方。

金融產業花費重金投資異地備援系統與大型主機(MainFrame)設備，協助資安人員在短時間內控制病毒的傳播速度，網管人員選擇切斷中毒電腦所屬的網域，並對於該網域的電腦全部進行重灌，系統重灌後再將同步備援儲存的資料，寫入原來的中毒電腦，即可將電腦病毒的傷害降到最低。

從上述訪談資料發現，單純就理論觀點，歸納不同產業領先使用者的意見或問題解決的技巧，而忽略使用者所處的情境脈絡與產業特性，創新的結果可能產生偏差，甚至完全不符合使用者預期，而本篇研究的產業個案，是否可藉由深入瞭解使用者脈絡資料找出痛點，發掘不同的創新來源呢？

## 第五節 分析單元選擇

下一章（第肆章）的研究發現，希望探討不同的分析單元，以個案的形式呈現不同產業因其獨有的情境脈絡而衍生的資安議題，並從使用者的角度來瞭解，該產業最擔心的資安議題如何帶來新的創新機會？

分析單元分別來自五個不同產業，他們對於資安的看法與現有的作法，皆可以反應資安在該產業扮演的角色以及面對的挑戰。

**個案一**，來自電腦製造業，二十年前創立於台灣隨後發展至全球五大洲，業務範圍涵蓋品牌與代工領域，本個案可以連結高科技產業全球化過程中，經營自有品牌或代工產品所潛藏的資安挑戰。

**個案二**，金融產業，在金控總部下包含了證券，銀行，投信，保險等不同事業體，並積極設立國外分行，進行海外佈局與網路業務，本個案呈現台灣金融產業因開放競爭而走向業務轉型過程中，典型的金融產業資安問題。

**個案三**，電子商務產業，個案公司規模約為 20 多人，代表著台灣佔九成以上比例，接近百萬家的中小企業，當廠商期望為客戶提供更即時且方便的網路服務時，可能面臨的資安風險為何？

**個案四**，某縣政府資訊中心，公家機關儲存大量人民機敏資料，舉凡稅務、地政、警政與出入境資訊等，當地方政府每年以少少的預算和有限的人力保管如此龐大且機敏的資訊時，可能遭遇的瓶頸與障礙是？

**個案五**，網路遊戲產業，宅經濟的發燒讓線上遊戲公司一炮而紅，善用網路特性衍生的社群網站如 FaceBook，MySpace，MSN 等更是時下年輕人瘋狂沈溺的活動，但其中因電腦病毒或駭客攻擊所帶來的資安風險，卻仍然讓該產業的資安人員感到頭痛萬分？

## 第肆章 個案研究發現

### 第一節 S 電腦資訊中心

#### 產業背景

S 電腦成立於1980年代，公司成立初期以優異的技術生產製造品質精良的主機板，受到國際市場的青睞，同時也奠定了S電腦國際化的基礎，目前全世界每三片主機板就有一個是由S電腦公司所生產。

S電腦的產品包含桌上型電腦，筆記型電腦或是手持行動裝置，其工業設計能力也屢次得到國際設計大獎，除了替IBM、HP或Dell等國際大廠代工生產外，也經營自有品牌，2008年集團營收接近新台幣八千億元，全球員工人數近七千人。

S電腦在2008年將公司切割為「品牌」和「代工」兩個集團，另以P集團負責電腦產品相關代工事業體，S電腦則將主力放在品牌，集團總部設於台北，負責掌控全球五大洲分公司的營運。

S電腦的全球資訊中心團隊約為四百人，負責支援全球各分公司的日常營運活動，並協助研發部門設計縝密的監控系統，保護重要的研發結晶不至於外洩，在工廠生產端也要每日過濾來往的下游協力廠商，防範因不小心的人為疏失，可能對於S電腦集團造成傷害。

#### 現有資安產品與服務

受創辦人亦為工程背景影響，重要的事情就應該盡全力做到最好。

因此，資訊中心很早便開始內部的資安規劃，在2001年建立了完整的資安政策與災難發生時的應變措施，亦搭配行政院資訊安全通訊小組的計畫，利用政府的專案補助經費，成功地導入ISO認證機制。

在歷經數次全球性的病毒攻擊事件後（例：Code Red 病毒），資訊中心特別成立專職的資安小組，組員共三人，全天三班制24小時監控集團內的資訊安全。

資安小組負責的範圍包含員工的往來信件，產品研發的相關資料，防止網路駭客惡意攻擊的防入侵程式等，歷年來皆以計畫性且專款專用的預算方式，重點性地強化 S 集團的資安需求。

## 資安痛點

以 S 全球電腦中心四百人以上的編制，以及全天候監控的資安小組，可說是該產業的資安典範，然而面對來自全球分公司，上下游材料商與經銷商，以及全球對 S 電腦產品有興趣的企業與客戶，S 電腦的資訊長，每天總是戰戰兢兢地在八點前便抵達辦公室，對於如此龐大的集團日夜無休地營運過程中，到底可能產生什麼令資訊長睡不著覺的問題呢？

## 商業機密被盜是第一大危機

代工訂單仍為 S 集團重要業務，其關鍵客戶包括 Apple（生產 iPod、Powerbook、iBook 等產品）與 HP，IBM，Dell 等大廠。

在接單初期，牽涉到 S 集團研發部門與國外客戶密集地針對產品規格進行觀念上的溝通與確認，在協同設計（Collaboration Design）的過程中，客戶最關心的是新產品生產規格是否會被商業間諜竊取，而產品雛形相關資料的保密性更影響到未來上市的成敗。

為了達到滴水不漏的效果，OEM 客戶會嚴格檢查 S 集團的資安等級，從產品研發設計部門到生產工廠，甚至包含負責接單的業務與訂貨的採購部門。

資安的檢查可分為定期或是不定期抽查，若有資訊外洩可能性，客戶會毫不留情、馬上轉單，甚至立即取消下一筆訂單以及未來合作機會。

因此，資訊中心全員無不上緊發條，將 S 集團資安防範設為策略性工作，就是害怕產生任何的商業機密外洩。

換言之，資安防護可能是 S 電腦集團可以勝出其他代工廠商，贏得訂單的競爭力。

不過，S電腦集團的資安經理對趨勢科技的信心並不高，認為趨勢只是一家低階的防毒軟體公司，不是一家資安專業服務企業。

### **最怕病毒潛入生產過程**

S電腦集團最怕員工使用手持無線上網設備（Mobile device），目前許多3G手機使用全天候上網吃到飽的方案，往往成為集團內資安的死角。

若員工使用的私人設備無意間上到惡意網站，或在收發電子郵件時感染病毒，或因隨身儲存裝備攜入病毒，在沒有掃毒的動作下又將隨身碟接到生產線上的電腦，便很有可能造成整個廠區電腦中毒，相對也造成生產線上的新產品，在製造過程中，因為生產線電腦中毒因而也遭到污染的危機。

過去希捷硬碟（Seagate）便因此損失慘重。希捷員工私人的隨身碟在無意間受到病毒感染，將生產資料灌到硬碟時，使整個生產線產品中毒。

所以客戶拿到產品時，軟硬體系統又被感染病毒。希捷不僅要負擔產品召回同時更換新品的成本，更要賠償客戶因重要資料損毀而產生的連帶損失。

### **企業網站於全球五大洲遭受攻擊**

S電腦集團全球網站有六大語言版本，由各國區域總部分別管理。但是集團內各部門若要更新網站上的資訊，並非交由資訊中心的人員統一進行企業網站資料的維護與更新，而是讓各部門或是區域總部的網站管理人員修改網站資料。

在S集團企業網站中，上萬篇網頁內容、文字、圖形、檔案與應徵者投遞履歷等工作均分散進行。也因此，駭客有機會找到網站的弱點，並植入病毒或外掛程式到網頁中。

不知情的使用者包括：想要瞭解S集團產品的一般消費者、想要採購商品的企業用戶、提供貨料的上游廠商等等，往往因點選網頁後而造成自己的電腦中毒。

更令資訊中心苦惱的是，用戶由網站上下載驅動程式時，常常連病毒一起下載，許多客戶在不知情的狀況下，反而造成對自己更大的傷害。S電腦集團常常



會接到顧客的申訴，因此要負連帶責任。

S電腦集團全球網站中每日的超過上萬人的點擊率，以及頻繁的產品相關資料與驅動程式下載，使得資訊中心每日須防範多達上千次的惡意入侵。

顧客或是S電腦的業務向資訊中心反映中毒事件後，資訊中心卻常常苦於無法診斷出駭客是由何管道進入？如何防護網站藏毒問題，是資訊長的第三大困擾。

公司全球網站為S電腦集團的企業形象，屢屢中毒事件若被媒體披露，或是網友因為自己的電腦遭受波及，在網路上大吐苦水，不但使過去投注龐大心力建立的資安績效化為流水，更有損S公司過去多年在國際上打造的專業形象

也因此，資訊中心倍受管理高層責備，並且無辜地成為S電腦集團形象受損的眾矢之的。在無法統整各國網站的狀況下，資訊中心目前僅能針對自家網站，進行弱點防禦與掃毒偵測。

## 創新解決方案

以 S 電腦全球資訊中心為例，我們可以看到幾個『服務創新』機會：

第一，

OEM 客戶會因產品的類型與訂單金額不同，要求 S 集團提供不同等級的資安檢驗標準，雖然資訊中心已經通過 ISO 認證以及多項資安能力檢定，但仍無法使這些國際級客戶放心，確定 S 集團已達到滴水不漏的防範能力，而客戶對於資安標準的不放心，使得資訊中心人員疲於奔命於滿足不同客戶的要求，業務人員也分神擔心，因為資安問題可能造成客戶的臨時抽單。

資訊中心迫切需要一個公正的資安檢驗機制，可以讓客戶放心。而趨勢科技是否領先其他資安產業競爭對手，深入瞭解高科技製造業在研發生產中的每一個環節，並針對每個環節可能產生的資安風險，研發出一套專屬於高科技製造業的資安防毒創新解決方案，則成為一個可以深入研究的服務創新機會。

第二，

趨勢科技可以重新包裝現有產品，推出「網站防駭攻擊」解決方案，協助資訊中心建立入侵防護網，一旦駭客侵入，資訊中心馬上可以偵測到侵入點並做防衛措施。

當駭客竄改網頁資料時，資訊中心能立刻偵查出什麼資料遭受竄改。另外，駭客掛網或對下載程式放毒時，資訊中心也可以馬上祭出反制措施。

第三，

S 集團在分散式系統的全球環境下，要如何利用有限的人力，把資安問題的每一個角落都照顧的無微不至？

以資安小組三班制全天候監控的工作模式下，每個時間也僅有一個人負責維持 S 集團全球的資安監控，而趨勢科技在瞭解同樣類型公司的資安人員工作模式後，能否在產品設計的初期，便考慮未來使用者在操作產品的情境與方便性，幫助資安人員在有限人力卻瞬息萬變的情境中，可以更有效率地利用手中的資安軟

體防範駭客惡意的入侵？

然而，根據S集團資安人員的說法，趨勢科技現有的產品組合，無法提供給跨國企業的資訊總部一套有效率的中央控管防毒機制，因為趨勢產品設計的著眼點是給企業的單一部門，或者一個台灣分公司的規模，最多七、八百人。

對S集團資訊中心來說，選購一套趨勢科技的防毒商品是不夠的，必須要買30套才能應付目前營運的需求，但是買產品是小錢，後續維持產品正常營運所需耗費的資源管理才是大錢。

Cisco的產品比較能滿足S集團電腦中心的需求，因為Cisco考量到跨國公司在現實環境營運時的需求，因此將『集中管理系統』列為提供給這類型客戶必要的產品功能，所以很多大型公司可能會覺得趨勢科技目前提供的產品服務不夠完善，這是因為趨勢科技研發的產品並非針對大公司，而這無異限制了趨勢科技在這類型市場發展的空間。

以S集團對於資安的需求，Cisco的產品只要兩套便能抵過趨勢科技30套產品所提供的效能，雖然兩套的金額遠比趨勢科技30套的價格高出許多，但在S集團資訊中心的眼中，付出較高的『價格』購買Cisco的產品卻能夠產生比趨勢科技更高的『價值』，這也說明了如果研發團隊在設計的過程中不能考量客戶的使用情境與實際應用需要，縱使提出再多的創新功能於新一代的產品上，客戶也無法從新產品中體認其應有的價值。

## 個案歸納

在瞭解產業資安情境脈絡後，根據使用者痛點所發現的創新來源與方向

表 10 個案一歸納整理

資料來源：本研究整理

個案產業	跨國S電腦集團全球資訊中心（高科技製造業）
現有資安 產品/服務	<ul style="list-style-type: none"> <li>● 個人電腦防毒軟體</li> <li>● 伺服器與防火牆管理軟體</li> </ul>
情境脈絡	<ul style="list-style-type: none"> <li>● 公司員工多為工程師背景，實事求是且目標導向。</li> <li>● 資訊中心400人支援全球分公司近7000人的資訊需求</li> <li>● 三人資安小組輪班監控資安事件</li> <li>● 各大事業群散落世界各地，資安防範從員工教育訓練做起</li> </ul>
資安痛點	<ul style="list-style-type: none"> <li>● 商業機密外洩，客戶轉移訂單</li> <li>● 員工缺乏資安觀念，生產線感染電腦病毒</li> <li>● 全球網站連番遭駭，傷害企業形象</li> </ul>
創新 解決方案	<ul style="list-style-type: none"> <li>● 供應鏈產業資安解決方案，符合研發流程與使用者需求</li> <li>● 資安防護水準檢驗服務，提供具公信力的評價機制</li> <li>● 重新包裝現有產品，強化全球網站弱點防護能力</li> <li>● 產品設計，應符合跨國企業講求高效能與管理方便的要求</li> </ul>

## 第二節 S 金控電腦中心

### 產業背景

S金控於2002年在台灣證券交易所掛牌上市，資本額約為新台幣700億元，淨值超過900億台幣，總市值更高達1200億元，為台灣最積極佈局全球的金融機構。

S金控在洛杉磯、香港、澳門、北京、上海、越南、倫敦設有分支機構或辦事處，並於美國加州擁有全資銀行『小S銀行』。

S金控於執行長下設經營委員會，負責公司營運相關決策與協調，金控總部設置會計處、行政處、公共事務處、資訊處、作業處、風險管理處、人力資源處、財務處、法令遵循總處及研究總處。

由於銀行保存著許多客戶的重要資訊，因此除了資訊處負責保護所有資料的安全外，另由風險管理處設計一套監控機制，確保若資料不慎外洩時，將可能產生的風險危機降到最低。

資訊處權力龐大，約有300人，辦公地點佔據了十個樓層，並與金控總部獨立分開，為的就是要確保其資料的隱密性與安全性。

不同於多數銀行採用的IBM大型主機（MainFrame）架構，S金控在新一代銀行核心系統（Core Banking，存款、放款、外匯會計資料與客戶檔案）規劃完全採用微軟的開放式環境架構，為的就是藉由微軟環境系統所提供的彈性（Flexibility），應用系統多樣性（Availability）以及與顧客的親近性（Accessibility），滿足S金控各事業群擴張與全球佈局的要求。

S金控主要使用趨勢科技防毒產品，卻仍不願簽訂服務合約。

## 現有資安產品與服務

資安產品/服務的預算，約佔資訊處每年 3-4 億預算的 4%-5% 左右，並且依照銀行每年的業務發展規劃，逐年編列相關的資安產品/服務採購計畫。

金融產業可以說是台灣最重視資訊安全的產業，不僅因為銀行業務的資料事涉機密而提高了防範措施，主管機關於近期通過的『個人資料保護法』，對於個人資料洩密的加重處罰條款，使得銀行資安負責人員莫不緊繃神經地觀察任何可能的風吹草動。

資訊處採用的資安產品，可根據下列不同屬性而產生不同分類：  
依來源分類，可以分為內部人員自行開發與外部廠商購買。  
依類型分別，可分為資安的硬體設備，以及安裝於電腦內部的各類型資安軟體。  
以使用的地點分類，可分為使用於分行內部的個人電腦(PC)與伺服器(Server)，或是於資訊總部使用的小型電腦(Mini Computer)或是大型主機(MainFrame)

由於採用的資安產品/服務包羅萬象，使得所有資安廠商莫不將金融產業視為資安市場的最重要一塊大餅，趨勢科技亦在金融產業的個人電腦防毒軟體市場中，擁有三成以上的佔有率。

## 資安痛點

E 先生是 S 金控副總經理同時兼任資訊中心資訊長，根據他對資安事件的經驗，他最害怕在一早清晨六點起床後，聽到公務手機響起的鈴聲。

每天早上八點前，資訊中心會對所有的系統進行測試，確保金控旗下各事業群開始營業前，所有的系統安全無恙。

而如果在清晨一大早接到公司的電話，或是在八點整的一剎那聽到電話鈴聲響起，資訊長的心便涼了一大半，接電話前，腦袋裡想著盡是各種可能的突發事件畫面。

回顧過去經歷大大小小的資安事件，資訊長緩緩說出他印象最深刻的回憶。

## 防毒反應太慢

S金控對趨勢科技的服務不完全是正面的評價，因此仍在猶豫是否要增加趨勢的採購預算。

主要原因是2008年六月初，某分行因為行員使用電腦不慎中毒，而擴散至該分行的所有電腦系統，以致於連續三天分行電腦系統無法與總行的電腦進行即時同步資料處理，所有客戶的交易紀錄，必須先以人工的方式在分行建檔後，等到下班再一筆一筆地輸入至總行系統。

發現分行電腦中毒的第一時刻，資訊處網管人員便馬上將分行內部網域進行分隔控管，以控制中毒範圍不會繼續蔓延。

同時，資訊處人員透過電話與趨勢技術部門人員嘗試診斷問題，趨勢工程師先要求資訊處人員，對於分行內所有的電腦進行全面掃毒，並要求分行每台電腦掃毒後的系統紀錄，傳回趨勢技術部門分析，才能得知究竟癱瘓電腦的是何方神聖？

當時一名在現場處理電腦中毒事件的資訊處技術經理 T 回憶：「一台一台電腦掃毒並收集資訊的過程枯燥並且非常沒有效率，我們只能利用分行下班後，全部的資訊處人員連夜加班到分行進行掃毒，而電腦內建的掃毒程式竟然無法自動執行全面系統掃毒的功能，實在是非常不人性化」。

而趨勢在接收到掃毒資料的三天後，才確認分行的電腦遭受到「僵屍病毒」的攻擊。

僵屍病毒的威力是讓電腦成為任人擺佈的「殭屍」(Zombie)，主要的原理是駭客將受害者電腦植入遙控程式，以用來傳播垃圾郵件、進行網路詐欺、散播病毒甚至阻擋防毒攻擊，因此這些受控制的網絡系統，稱為殭屍網路(Zombie networks)。

然而，即便確認電腦遭受到「僵屍病毒」的攻擊，但在嘗試過多種不同的掃毒方法後，仍未解決分行電腦中的僵屍病毒。

事發一個禮拜後，不耐於時間流逝所造成的有形與無形損失，S金控資安人員決定將分行電腦內所有系統進行重灌，結束此次資安事件。

資訊處人員表示，趨勢科技的反應時間超過銀行對於資安緊急處理標準作業規範可以忍耐的範圍。

在經過類似的經驗教訓後，往後只要發生資安事件，他們大多傾向自行解決，就怕因為趨勢科技太慢的回應，而產生更大的損失。

目前已經購買的防毒產品也只是當作買保險，因為在資安事件發生時，無法產生立即的遏止效果。

資訊長擔心即使提高資安預算，在資安問題發生時，仍然無法獲得預期的服務水準，而配合防毒廠商進行一連串的掃毒作業，在歷經漫長的等待卻得到毫無幫助的解答，但資安事件期間若再次被惡意人士入侵得逞，若消息被媒體披露而導致公司股價因此受影響，這責任應該由資訊長來承擔，還是由防毒廠商來負責呢？

### **銀行防毒有專業**

趨勢科技人員雖然具有處理電腦病毒之能力，但因為對於銀行各部門業務與作業程序的不瞭解，往往無法根據銀行業務處理關鍵程序，對症下藥。

這就像是剛從醫學院畢業的年輕醫生，雖然習得了一身學理上的知識，但卻無法像有經驗的老醫生一般，觀察病人的行為或是日常作息，便能推斷病灶的成因，甚至在瞭解病人的心態與生活條件後，給予符合患者需求的處方與療程。

而金融產業對於資安的需要，就像是一群擁有明確固定行為的病患，許多資安的問題，往往不是突發的事故，而是經過一定時間醞釀而衍生的問題，但面對金融產業的電腦中毒問題或其他資安事件，趨勢科技人員往往花費許多時間在銀行覺得無關痛癢的問題上，而浪費許多寶貴的時間與機會，也讓資訊處人員對於趨勢的專業產生懷疑。

金融產業的資安工作，與其他產業有何不同呢？



以每天負責接待客戶的分行據點為例，負責不同業務的行員，在電腦操作功能有一定的權限，不同的行為因而衍生出不同的問題。

好的療程必須建立在對於使用者情境的瞭解，方能達到立竿見影的療效，同時產生藥到病除的效果。

外匯部門行員的電腦僅與總行主機相連，查詢最新的外幣匯率報價，這類型的電腦因為沒有連線到網際網路的能力，不太可能經由電子郵件或瀏覽網站中毒，但如果不小心將隱藏病毒的隨身碟連接至外匯部的電腦，便可能讓分行與總行間的連線受到感染。

負責貴賓理財或是基金業務的行員，常常需要使用網路連結到國內外各大財經網站，提供客戶最新的市場動態與投資建議。這類型的使用者最容易因為連結到惡意的釣魚網站使得電腦安全產生漏洞，或因為使用電子郵件中毒，或客戶重要交易資料於傳輸中被攔截解密，產生高風險的資安問題。

信用貸款部門的行員無須使用網際網路(Internet)進行日常業務，但卻需要使用區域網路 (Intranet) 調閱不同分行間，客戶的交易與擔保資料，而這類型的行員往往在『資料夾分享』未設定防範措施，而讓業務機密資料，暴露於無管轄的高度風險環境中。

由於趨勢的防毒工程師不了解銀行的業務內涵，在診斷時可能花費許多時間進行例行的掃毒措施，(如檢查電子郵件或全面掃毒檔案)，卻忽略該行員的業務範圍所衍生的特定資安問題，再加上每次到現場處理的工程師都不是同一個人，以致於先前處理資安事件的經驗無法累積，往往錯失了有效制止病毒蔓延的先機。

### **缺乏客製化服務通報**

趨勢科技每週會定期發佈最新的病毒通報，有時候碰到特殊危急事件，通報的頻率可能會達到一天多次的狀態。

為什麼會有這麼高的頻率？主要是因為病毒通報記載著全球各地最新產生

的病毒或資安事件，卻未分析簡化成不同產業或使用者所應該知道的訊息。

S金控資訊處的資安人員常常淹沒在一大堆的病毒通報中，卻不知如何反應？資訊處技術經理 T 回應說，『病毒通報裡每個病毒似乎都是來勢洶洶，每台電腦都有被攻擊的可能，以全球目前每天都產生近一百個新病毒的速度來說，我光是處理病毒通報就不用作其他的事情了！』

銀行最忌諱有「狼來了」的虛驚，因為擔心假警報會引發金管會（金融監督管理委員會）的處分、股東的反彈、客戶的不信任。

為了避免接二連三的病毒通報引起S金控內部一陣虛驚，T 經理選擇接收病毒通報但『被動地』對內部成員發佈訊息。

然而，回想當初分行真正受到僵屍病毒侵擾時，卻總是無法獲得趨勢的通報與支援。而且，趨勢的病毒通報裡沒有提到解決的辦法，也反應資安人員面對現有病毒通報的無奈與不滿。

## 創新解決方案

在 S 金控案例，我們可以看到幾個『服務創新』機會。  
第一，

趨勢如何對銀行客戶的產業知識有深入的了解？

去客戶端之前，趨勢的技術服務人員對於客戶的環境跟現狀了解嗎？相關產業基本知識有嗎？趨勢目前尚未幫客戶建立資安病歷表，也沒有完整的工具讓工程師為銀行客戶快速診斷。趨勢只有一套SIP工具，但這樣的工具足以應付眼前的棘手問題嗎？

金融業是個值得開發的市場，但趨勢科技要知道怎麼用產品與服務來滿足客戶需求才是關鍵。然而，這需要趨勢對金融產業相關知識了解，才能看到創新機會的來源；同時，這也是趨勢未來產品發展的規劃重點。

例如，趨勢科技可以效法戴爾電腦的服務模式，為銀行關鍵客戶配駐專屬技

術專家，長期建立對該銀行的了解。如此，在發生資安事件時，這些資安專家便可以快速地進入狀況，爭取解毒第一時效。

第二，

趨勢科技也可以針對銀行客戶開設「金融資安教育」，除了增進行員對病毒的處置外，也可提供政府金管會對銀行的資安稽查重點。

關於產品的研發，趨勢科技如何能弄清楚銀行的應用情境？趨勢科技如何能知道銀行最常被侵入的病毒是什麼？

S金控雖然在國內有著嚴密的資安控管，但其國外分行（OBU，Offshore Banking Unit），如洛杉磯、香港、澳門、北京、上海、越南、倫敦等地的資安控管卻是最大的死角。針對台灣金融產業在國外分行的資安控管，趨勢科技若能提出境外資安管控的方案（Security Offshoring），應該會受到金融界的矚目。

總之，趨勢科技在金融產業擁有近三成左右的佔有率。但可惜的是，趨勢科技在過去並未建立起對銀行防毒的領域知識（Domain knowledge）。不過，這也是趨勢的創新契機。

若趨勢科技能分析銀行業最常發生的病毒，縮小搜尋範圍，針對銀行業提供病毒通報，並提供解毒方法，應可以獲得銀行業客戶的青睞。而且，建立銀行業解毒的專業度時，趨勢科技也才可以在最短的時間內，用最省力的方式解決問題。

此外，趨勢科技也可以開發「預防病毒」方法（Preventive maintenance），透過分析使用者上網行為，協助銀行儘速找到病毒攻擊的脆弱點（Vulnerability analysis）

## 個案歸納

在瞭解產業資安情境脈絡後，根據領先使用者痛點所發現的創新來源與方向

表 11 個案二歸納整理

資料來源：本研究整理

個案產業	S金控總部資訊處（金融產業）
現有資安產品/服務	<ul style="list-style-type: none"> <li>● 個人電腦防毒軟體</li> <li>● 郵件/檔案/網頁伺服器防毒軟體</li> <li>● 電話專人即時技術支援服務</li> </ul>
情境脈絡	<ul style="list-style-type: none"> <li>● 金融產業因競爭而壓低營運成本，走向開放式系統環境</li> <li>● 不同屬性業務，操作不同系統與權限，產生相異資安問題</li> <li>● 網路興起，業務發展要求快速靈活，資安須兼顧安全與效率</li> <li>● 特許產業，政府管控嚴格，客戶的信賴是最寶貴的資產</li> </ul>
資安痛點	<ul style="list-style-type: none"> <li>● 防毒速度太慢，不符合金融業對資安管控的要求</li> <li>● 防毒廠商不瞭解金融專業，錯失防毒寶貴時機</li> <li>● 未經客製化的病毒通報，無法改善客戶反應能力</li> </ul>
創新解決方案	<ul style="list-style-type: none"> <li>● 成立團隊深入熟悉金融產業，設計金融產業整體解決方案</li> <li>● 協助業者進行資安教育訓練，建立有效資安防制架構</li> <li>● 建立客戶專屬資安病歷，針對突發事件快速掌握問題點</li> <li>● 提昇業者境外資訊管控能力。</li> </ul>

### 第三節 X Beauty 美妝購物網站

#### 產業背景

「X Beauty」是一家網路商店，西元2000年成立時以賣面膜起家，當初看準了網路無時差、無國界且高隱密的特性，業務迅速擴大至美妝、女性內衣、女用雜貨等領域。

公司僅有二十餘人卻創造出數億的業績，藉由電子商務平台提供精準且跨國界的服務，因此造福了許多在歐美、紐澳地區的華人，之後出國再也不用大包小包地扛著瓶瓶罐罐的化妝保養品。

有了像 X Beauty 這類的專業B2C網路購物網站，原本繁瑣的採購過程就在幾下滑鼠的點選與信用卡交易機制中被完成。

空氣對人類生存的重要性，就像 X Beauty這類型的購物網站對於網路的絕對依賴，從採購人員與供應商的業務往來，到業務行銷人員將最新商品資訊公布於網站銷售，到消費者瀏覽網站下單後的資訊確認，接著物流人員憑藉資料庫中的訂單資訊安排出貨，到最後財務人員與銀行和供應商核對業績收入與往來貨款。

公司內所有員工都身兼數職，利用網路與不同的對象進行複雜的溝通與業務執行，而總經理 V 先生除了身負公司營運成敗責任外，在清一色皆為女性員工的網路美妝公司中，常常要負責處理許多因電腦而衍生的『高科技』問題。

對「X Beauty」這類網路商店來說，所有人的工作皆需要依靠網路與電腦資料庫，因此網路穩定性與交易資料的安全性，便成為網路公司能否正常營運的關鍵問題？因為一旦電腦中毒，所有的員工的業務便瞬間停擺。

## 現有資安產品與服務

早期，「X Beauty」使用隨機附贈的防毒軟體。然而，不同廠牌的軟體亦造成公司管理的不便，該公司總經理 V 先生在2008年找趨勢科技推薦經銷商，從此全面統一公司的防毒軟體。

## 資安痛點

V 先生當初時常出差在外，卻經常接到員工因為防毒軟體到期通知，員工要求協助續約的問題，在根據自己過去使用趨勢防毒軟體的經驗，決定全公司統一採用趨勢科技的防毒軟體，有些電腦仍可使用其他品牌的防毒軟體，也在 V 先生的決定下一併更換。

在與趨勢客服中心聯絡後，趨勢根據 X Beauty 的使用需求，安排了地區經銷商為 X Beauty 進行全面轉換趨勢防毒軟體的服務。轉換成趨勢商品後，果然再也沒有員工因為防毒軟體陸續到期，擔心電腦資料受病毒攻擊而影響到工作進度的問題，但他卻沒想到全面整合的防毒軟體，在之後差點讓他的公司營運產生意想不到的大問題。

## 續約造成資安空窗

就在一年之後，V先生收到趨勢科技寄來的電子郵件，通知他使用合約即將在十多天內到期，請於期限前完成續約動作。

V先生隨即點選了郵件提供的網站進行續約，但網站卻要求V先生填入詳細的使用者資訊以及相關電腦的作業系統版本資訊與其他的硬體設備資訊，這樣的續約過程讓V先生感到非常的頭痛，因此決定讓經銷商來處理續約的問題。

V先生致電請經銷商過來處理，但是經銷商卻遲遲不來。就在合約即將到期的前三天，忍無可忍的V先生決定直接打電話給趨勢科技客服部，希望趨勢能夠立即解決他的燃眉之急。

V先生本以為只要報出自己公司的大名，趨勢的客服人員便能夠像信用卡客服中心一樣，調閱出自己詳細的消費資訊，然後迅速地解決這煩人的續約問題。

但電話那端的客服人員不但找不到 X Beauty 購買趨勢產品的資訊，倒是又問了一堆讓V先生不知該如何回答的問題？（例：服務你的經銷商是誰？他為什麼沒有服務您呢？您需要買趨勢的什麼產品呢？）

在致電趨勢客服中心後，發覺竟然找不到自己的消費紀錄，而經銷商似乎忙著照顧比 X Beauty 更重要的客戶時，V先生已經做好最壞的打算，從此再也不使用趨勢科技的產品/服務。一直到合約到期當天，經銷商終於前來處理，而且在不到一小時內便完成所有軟體的更新。

當V先生回想起經銷商以及趨勢科技的服務態度時，搖頭表示：「就算是對趨勢科技的產品再有信心，但人的感受就是不舒服。」漫長繁瑣的續約過程，問題一再無法解決。

再加上美妝網站的員工多為不熟悉電腦運作的女性職員，軟體不斷到期的訊息影響到員工的工作情緒，深怕在處理訂單時電腦突然中毒。

續約軟體介面的瑕疵造成 X Beauty 資安空窗期，這都是因為續約手續繁雜，客服作業缺失。

V先生想起這事件就生氣，提到若趨勢科技想走客戶導向、以客為尊（Customer centric）的方式，就應該設計一個「One click」功能來整合所有的續約服務工作。

### 經銷商開天窗

V先生開玩笑地說：「幾十分鐘的服務就可以賺十幾萬塊，這麼好的生意居然還要我主動聯絡經銷商？」

經銷商為何會如此被動的處理續約服務？這會不會是偶發事件而已？

或者，其中是否存在趨勢科技的通路政策的問題？或是業務部門與經銷商之間的溝通機制出現問題，還是經銷商選擇不夠謹慎？

## 緩慢回應的客服中心

了解客戶行為是客服的第一大重點。電子商務公司的資安防護不可間斷，一旦間斷就沒有生意可做。

因此，企業延續能力（Business continuity）是此類公司之營運首務。前面提到資安空窗期會使電子商務營運失靈、業務量流失、客戶資料被盜等重大損失。客服人員若是對這類客戶不了解，無法給予即時服務，不但客戶會流失，企業形象也會受損。

趨勢科技如何讓客服人員立即回應客戶的續約問題，是服務創新要思考的議題。

此外，趨勢科技只有在週一到週五的上班時間客服中心才運作，對電子商務全天候無國界不中斷的營運模式，趨勢科技提供的支援服務就像是遠水救不了近火，只希望客戶能夠自求多福。

## 創新解決方案

**X Beauty 網路商店案例**，可以觀察到三個創新契機。

第一，

趨勢科技在客戶服務上可以參考醫院的「急診室模式」，提供最即時有效的服務。在客服前線，除了選用非常有經驗的客服人員，幫助客戶在初診過程中快速辨認資安事件的類型與嚴重度，更應該將目前的資安客服模式，設計成支援客戶的營運模式，這不僅可以即時處理續約或防毒服務，更可以建立客戶的信心。

第二，

針對網路商店提供一套中小企業的資安防護合約也許是一項潛在商機，雖然這類型的客戶並非趨勢科技的主要收入來源，但若能深入地瞭解中小企業對於資安的需求而設計出符合市場期望的商品，點點螞蟻亦可成雄兵！

趨勢科技目前只提供遠端監控服務給頂級客戶（如：跨國企業或金融產業）。



試想，如果將遠端監控技術於產品研發初期時，便制訂為基本的產品/軟體功能，在未來產品到期時，客服中心服務人員便可以藉由此產品功能，來協助顧客續約、安裝新軟體或進行遠端的資安防護例行作業。

第三，

趨勢科技可以重新檢討經銷商機制與通路政策，分析到底是哪一個環節出了問題。這也許是一個服務供應鏈的創新議題，這個問題到底誰才能幫上忙？是研發，還是客服，還是技術支援(Technical Support)？

趨勢目前的服務分成四等級：白金、金、銀、銅。有跟趨勢科技簽約PSP (Premium Support Program，加值服務合約)的客戶會獲得一組專屬的電話號碼，擁有此電話號碼才可以獲得趨勢24小時不中斷的技術服務支援。

其他客戶則是讓經銷商服務，所以中小企業打的電話，並不是技術支援接手；因為他們不是PSP，所以負責服務的只是單純處理續約的人員，而這些續約人員或許因為沒有具備基本的技術背景或產業知識，以致於在電話另一端的客戶，於續約過程中感到非常的不便與繁瑣。

X Beauty 的案例提供了許多對於中小企業涉及電子商務的線索，讓我們思考怎麼滿足潛在客戶的需求並鞏固市佔率，如何把後續的服務做好。

## 個案歸納

在瞭解產業資安情境脈絡後，根據使用者痛點所發現的創新來源與方向

表 12 個案三歸納整理

資料來源：本研究整理

個案產業	X Beauty 電子商務網站 (電子商務產業)
現有資安 產品/服務	<ul style="list-style-type: none"> <li>● 個人電腦防毒軟體</li> <li>● 伺服器與防火牆防毒軟體</li> </ul>
情境脈絡	<ul style="list-style-type: none"> <li>● 24小時不間斷營運，關鍵資訊儲存與業務溝通皆依賴網路</li> <li>● 員工分飾多角，無專職資安或技術人員</li> <li>● 業務潛力小，地區經銷商素質不均</li> <li>● 客戶選擇網路消費，不僅買方便，同時買的是對網站的信任</li> </ul>
資安痛點	<ul style="list-style-type: none"> <li>● 產品續約造成資安空窗期</li> <li>● 回應緩慢的經銷服務系統</li> <li>● 找不到客戶檔案資料的顧客服務中心</li> </ul>
創新 解決方案	<ul style="list-style-type: none"> <li>● 建立One Click的續約機制與完整客戶資料的建檔管理</li> <li>● 重新檢討地區經銷商獎勵與教育訓練政策</li> <li>● 客服中心營運應改為急診室模式，深入瞭解中小企業需要</li> </ul>

## 第四節 X 縣政府資訊中心

### 產業背景

P 縣政府資訊中心最重要的任務在統整 P 縣府各部門資訊業務發展，並協助 P 縣機關行政流程再造，是一典型的地方政府組織。以資訊中心目前約30名的人力編制，需要支援縣轄範圍內鄉、鎮、市約五百多個行政單位，共計約5萬多名公務人員的資訊需求。

相較於直轄市資訊中心動輒擁有十倍以上的資源但卻服務比 P 縣政府資訊中心還要少的人數，資訊中心主任 Y 先生在任內無時無刻都在思索如何將每一分錢花在刀口上。

若能夠了解該中心的資安運作實務，將有助於推廣資安服務到台灣各縣市政府。進一步，本案也有助於了解其它地方政府或中央機關在推行資安政策時的資安痛點。

此外，P 縣政府資訊中心目前為台灣地方政府資訊化的典範型組織，行政院研考會歷年來所舉辦的資安金盾獎，P 縣政府資訊中心皆榜上有名，同時成為其他縣級資訊中心在學習資安實務推廣過程中，爭相拜訪請教的對象，也因此 P 縣資訊中心於縣內各部門推行資安政策所遭遇的挑戰困難，應可作為發現創新來源的最佳參考。

## 現有資安產品/服務

中心 Y 主任一開始便道破了身為政府部門資訊首長推動業務的難點：

『資訊中心在政府機關裡面向來是吃力不討好的工作，因為受到台灣選舉文化的影響，砸在資訊建設的投資，倒不如把錢花在籠絡樁腳的地方建設上，如果因為不小心花錯了錢而輸了選舉，誰會記得你在任內對縣政資訊建設的貢獻呢？』

然而，在歷經 911 事件後，卻開啟了資安政策推動的另一扇門。

在 911 爆炸事件後，紐約證券交易所僅在三天內便恢復正常運作，當時也受創的機場航空系統與美國國防部五角大廈也在一個禮拜內恢復所有的正常運作，這樣迅速的災後重建能力，讓當時的 P 縣縣長感到非常的驚訝與佩服。

而縣長反問資訊中心 Y 主任，若類似的災難事件若重創 P 縣，資訊中心需要幾天才能恢復全縣行政機關的正常運轉呢？以當時 P 縣資訊中心全年不超過五百萬預算的規模，（五百多個行政單位皆添購一台新電腦都不夠），Y 主任很誠實地向縣長報告：『快的話至少要一個月，不過很多資料因為缺乏管理與備份，可能從此再也救不回來，因此無法保證 P 縣在歷經大規模災難事件後，可以在短時間內提供人民行政服務。』

這個消息啟發當時 P 縣長意識到資訊安全的重要性，因此展開了全面性的風險評估。他希望建立一套完善的資訊安全反應機制，目標是預防 P 縣在遭遇重大災害後，能迅速恢復縣政運作，而為了確保政策落實執行，由副縣長擔任召集人的『資安推動委員會』，定期檢核每一階段的目標是否依照規劃完成，並在三年內將資安預算比例提升至 P 縣年度預算的 5%-5.5%。

因為 911 的轉捩點，讓身處冷衙門的資訊中心大力推行資安政策，從保護機敏資料的『資料異地備援計畫』切入，再逐步推展至各部門行政資訊系統的整合，最後大力推動 E 政府計畫以提昇行政效率，而這一連串的改革方案皆奠定於紮實的資安防護基礎，也因此讓 P 縣的全年度資訊預算由開始的 500 萬元，實施三年後達到三億元的規模，並將原本散落在各鄉、鎮、市上百個各自獨立的電腦資

料庫與行政系統，統一由新設立的電腦中心統一管控。

## 資安痛點

今天的 P 縣資訊中心，設置於遠端監控、具有獨立發電且恆溫保護的專業電腦機房內，所有人員的進出皆有嚴密的管制並錄影存查。

在接待其他縣政府資訊中心人員的來訪，並接受大家投以羨慕欽佩羨慕的眼光時，Y 主任回想當初與資訊中心同仁徹夜加班，以一人當十人用，筚路藍縷的過程。

## 鄉鎮資訊分散、控管不易

過去，P 縣與其他縣市政府一樣，受限於預算分屬於不同地方行政單位編列，因此資訊系統的建置與管理大多為分散模式。在此情況下，各鄉、鎮、市公所電腦是否交由專業人員管理，關於縣民重要敏感的資料，是否受到嚴密與完善的保護，這一切的狀況皆無法得知。

同時，員工可以於公務時間上網，利用公家機關資源下載非法軟體影片或濫用私人電子郵件，縣政府資訊中心在分散式架構下是很難監控的。但在公務人員『多一事不如少一事』的心態下，很少有人提出現有問題的解決方案，以免破壞了部門之間的和諧氣氛。

P 縣資訊中心，藉著 911 事件的契機與縣長的大力支持，在經過長期內部協調後，終於將地方政府資訊，例如戶政、民政、地政、教育、稅務、警政等資料，由分散的處室轉換到中央電腦系統以便控管，單一控管的好處就是將原本鬆散在外的弱點，集中到一個嚴密的銅牆鐵壁內保護，避免駭客找到落單的弱點進行攻擊，這便是資訊長所提倡的「大水庫理論」。

集中式管理架構讓所有處室的資訊流通管道，皆由單一出口進出，統一管制，減少駭客的分段點進擊，以便大幅提升資安層級。

不過，大水庫管理模式卻加深了中央監控人員的負擔與責任，雖然資安預算

可藉由集中分配模式得到更高的效益，但同時也增加因發生資安事件而遭到其他部門群起圍攻的風險。

據資訊長聲稱，全台灣只有P縣做到中央資安管控，其它縣市的政府單位都隨時面臨資安風險而不自知。

### 網路犯罪 (cyber-crime) 難防堵

在推動資安政策青黃不接的階段，曾發生替代役男於 P 縣的某鄉公所，利用該單位的電腦，每日下載大量的色情影片與盜版電影，甚至利用鄉公所的燒錄設備，將影片燒成光碟後於網路販賣，獲取高額不法的報酬。

該名替代役男因為具有資訊科技背景，知道單一電腦高流量的狀態必定會引起相關單位的注意，但他利用公家機關資訊架構分散控管，難以精確掌握使用者行為的特點，使用同事的帳號登入公用的業務查詢電腦。

後來，調查局根據電腦IP位置，確認下載電腦來自於 P 縣某鄉公所，因此調查局人員帶著證據衝進資訊中心要抓人，Y 資訊長看到調查人員蒐集的資料後瞭解，因為資安控管不實而讓不法之徒有機可趁，若此害群之馬無法在最短時間內被逮捕，則其行為將使全縣行政單位過去對於資安政策的努力瞬時化為泡影，而這樣的事件也驚動了當初大力支持推動資安政策的縣長。

資訊中心花了很多時間追查電腦的登錄使用記錄 (log)，受當初決心推動資安而導入的『單一簽入統一密碼 (SSO, Single Sign On)』的幫助，資訊中心得以根據登錄記錄並比照案發當時排班記錄表，將可疑人數縮小到一定範圍，然後再針對員工背景跟嫌疑人員進行比對分析，才找出這位替代役男。

若非其中央資安控管模式，在系統中保留所有進出記錄資訊，要追查出嫌犯的機會就不高。

Y資訊長表示，若防毒公司能夠提供網路使用行為分析的軟體，那說不定可以在未犯罪前就找到嫌犯，使資安防護更加完備。

## 資安是政策的延伸

近年來行政院研考會大力推行E-Government（電子化政府）計畫，要求各政府機關落實資訊化服務，也因此，資訊安全便成為電子化政府的首要隱憂。

因為，原本鎖在鐵櫃裡面的資訊，現在全面 E 化提供民眾查詢，但這些 E 化資料若沒有嚴密的保護與監控，若被有心人士盜取甚至竄改資料，那麼因為政府機關資安漏洞而產生的損失與擴及的範圍將難以想像。

而近日媒體多次披露，民眾交給地方政府的資料常被盜取，因此多數民眾不願意將私人資料交付政府保管，如果政府的資訊服務信用程度下降，那麼「電子化政府」的美意與方便也就成為了空談的口號。

P 縣政府資訊中心在完成了集中式控管模式，將縣府部門的資訊交換限制在單一嚴密的管道進行，因此大幅提昇資安的品質於防範能力，所以贏得了多數縣民的信任。

與直轄市比較推動E 化服務的成效，直轄市一年僅能推廣7項電子化服務，但是 P 縣則可推廣至30 項。

同時因為推動多項E 化服務產生的經濟規模使得處理每項E化服務的成本得以下降，因此雖然擁有較少的行政資源，卻可以完成比直轄市更高品質的服務水準。

在成功推動多項電子化便民措施後，不僅大幅省去民眾的交通時間、降低社會成本，也方便各處室追蹤民眾申請案與抱怨事件，因此大幅提昇民眾對縣政府的滿意度。

## 創新解決方案

**P 縣政府資訊中心**案例，可以讓我們省思四個問題。

第一，

除了P縣政府以外，其他縣市資訊仍採分散式管理，缺乏專業網管人員與相關資安軟硬體設備。趨勢科技是否能提出不同的產品或服務方案，滿足此缺口？

第二，

公家機關普遍缺乏資安專業，對網路犯罪毫無防護力。因此，當未來資安問題越來越嚴重時，地方政府勢必要提高資安預算。對此，趨勢科技又應該如何因應？

第三，

縣政府對電子郵件濫用、節約用電（提醒員工晚上要關機）、上班時間瀏覽不法網頁等資安內控問題感到頭痛，趨勢科技又可以提供怎樣的服務或產品？

第四，

由客戶立場來看，在分散環境中，縣政府無法預防犯罪，勢必要委外。這種委外不只是服務，還可能需要派一組人來協助內部架構的改善。趨勢如何訓練經銷夥伴是一條路，而趨勢可以思考的另外一條路是，能不能設立專責單位為縣政府管資安？

McAfee為了商機，還去併購一家顧問公司，可見這是一個很大的商機。

那麼對於P縣以外的鄉鎮中心呢？有這樣的痛不只有一個吧？

因此，業務部門可以提供包裹式的服務加產品。例如，趨勢可以利用遠端控管服務，去替縣市政府那三、五個人管理五、六千台電腦的資安問題。

此外，除了台灣省20多個縣市政府公部門外，還有中央部會如立法院、監察院、中央銀行、外交部、內政部等單位也是潛在客戶。



## 個案歸納

在瞭解產業資安情境脈絡後，根據領先使用者痛點所發現的創新來源與方向

表 13 個案四歸納整理

資料來源：本研究整理

個案產業	P縣政府資訊中心（政府部門，公領域）
現有資安產品/服務	<ul style="list-style-type: none"> <li>● 個人電腦防毒軟體</li> <li>● 郵件/檔案/網頁伺服器防毒軟體</li> <li>● 單一簽入（SSO,Single Sign On）統一密碼管理系統</li> </ul>
情境脈絡	<ul style="list-style-type: none"> <li>● 年度預算拮据，專款專用缺乏彈性</li> <li>● 公務人員，『多一事不如少一事』的怕事心態</li> <li>● 部門內資安人員多為兼職性質，缺乏專業資安訓練</li> <li>● 鬆散的安控機制卻掌管許多人民重要敏感的資料</li> </ul>
資安痛點	<ul style="list-style-type: none"> <li>● 鄉鎮市公所幅遠廣大，落實資安控管不易</li> <li>● 內賊難防，網路犯罪舉證困難</li> <li>● 資安建設為推動E化政府的基礎</li> </ul>
創新解決方案	<ul style="list-style-type: none"> <li>● 針對公領域預算特性，協助政府機關規劃資安逐步導入方案</li> <li>● 依據機敏資料特性，整合趨勢現有產品，設計符合政府機構人力配置的資安解決方案</li> <li>● 提供專業資安委外服務，同時強化公部門資安教育訓練</li> </ul>

## 第五節 L 網絡科技個案

### 產業背景

L網絡科技可以算是台灣第一家自製研發並成功經營線上遊戲（OnLine Game）的本土公司，相較於許多台灣遊戲公司主要代理韓國線上遊戲，L公司在十年前便投下重金與清大研發團隊打造『多人即時線上遊戲（MMOG，Massively Multiplayer Online Game）』所需要的核心軟體原件，並且利用此核心原件開發出多套膾炙人口的線上遊戲，同時也將遊戲開發工具商品化，轉售給同為線上遊戲產業的對手。

為了培育台灣線上遊戲產業的專業研發人才，L公司不僅無條件地捐贈國內大學院校網路多媒體系所使用其自製研發的3D物件顯像遊戲引擎（3D Object Rendering engine），每年更與資策會合作開班授課，希望更有系統地訓練出大量的遊戲軟體人才。

L公司位於台北的研發團隊約有250人，包含研發遊戲主題與角色的企畫部門，設計遊戲場景與主角造型的美術部門，確保數萬名玩家於即時網路環境中仍能順利運行的技術部門，以及負責處理突發事件的遊戲關主（GM，Game Master）。

研發團隊為求玩家能夠獲得最好的遊戲功能與即時的互動效果，因此在自行架設的Linux環境內，進行所有遊戲的研發，測試以及正式上線營運。

在掌握台灣市場玩家遊戲風格與累積成熟的研發能力後，L公司預計在未來每1-2年皆要推出一套新的線上遊戲，並藉由授權的方式將廣受歡迎的線上遊戲，推展至國際華人市場。

L公司主要收入來自遊戲玩家於便利商店購買遊戲點數的費用，以及在遊戲過程中，玩家為求更高深的魔力或更強大的武器，購買寶物所產生的利潤。

L公司線上遊戲採用集中式主機管理架構，搭配Linux環境管制資訊入口，再

加上遊戲主機(Linux)與電腦玩家(Windows)所使用的電腦作業系統不同，因此比較沒有一般的資安問題，就算玩家的電腦中毒，也不會感染到其他使用者。

可是，雷爵的資安痛點卻是很另類的。分析雷爵的案例有助於了解遊戲公司與科技平台類組織（例如電子市集、電視購物台）的資安需求。

## 現有資安產品與服務

電腦遊戲的開始雖然可以追溯至 1970 年代，但因網路發展而帶動的線上遊戲產業不過是近十年的光景，在一個非常年輕且仍然快速成長的產業裡，廠商因為不同的營運模式而衍生出相異的資安需求，使得目前線上遊戲產業的資安作法，尚未有一個普遍被業界採納的作法。各家遊戲廠商憑藉著對風險的認知與應變能力，規劃自己本身對於資安防護的要求。

以 L 公司來說，因為董事長從小到大便是玩遊戲出身，因此從產品研發架構如何反制網路資安問題，便有獨到的見解與防禦機制。

但是，為防範網路世界多變的風險，L 科技特別聘請過去即是惡名昭彰的網路駭客，擔任線上遊戲資安的守門員。這三位過去經常以攻破別人網站或系統為榮的駭客，如今嘗試著以過來人的心態，解讀覬覦網路遊戲世界財寶的新興駭客。

## 資安痛點

不同於一般產業發生資安事件，公司因為機密資料被盜或損毀而產生嚴重的損失，網路世界裡的受害者反倒是遊戲的玩家，因為防護檢驗機制出現漏洞，而讓某些玩家得到不當的利益，造成遊戲不公平競爭的情況發生，L 公司要如何在虛擬的網路世界裡，以最短的時間內找到犯罪的根源，並根據線索一次根除犯罪集團卻不傷及無辜，變成了資安人員與駭客之間的鬥智大戰了。

## 外掛機器人

專業玩家會鑽遊戲的漏洞以便快速練功，提高自己的點數和戰鬥力。資深玩

家常會在遊戲中插入外掛程式，以軟體機器人在遊戲中繼續收集寶物。所以即使玩家在睡覺，程式仍然會自動收集寶物，藉此累積玩家的戰鬥力。

但是，外掛程式的使用容易造成遊戲的不公平競爭。

若被其他遊戲會員發現，他們就不再信任L公司的線上遊戲平台，遊戲的銷售便會大受影響。

另外，也有玩家會買一些特殊器材，如飆速鍵盤，約為一般鍵盤四倍頻率（註：超速鍵盤按一下，約為一般鍵盤按四下）。

玩家用超速鍵盤是要加快寶物收集速度，或在格鬥時能夠進行「秒殺」。

「秒殺」即一秒內殺完，因為超速鍵盤會使人物移動的速度加快，更會使攻擊反應的能力加快。L公司的資安人員最討厭此類機器人外掛程式（也算是一種入侵）。

當資安人員由遊戲玩家登錄的系統記錄察覺有異狀時（例如，有玩家24小時都不下線），資安人員便會從系統端丟訊息測試玩家的反應，一旦察知是機器人時，資安人員會以軟體程式干擾，讓機器人速度變得很慢，讓違法玩家知難而退。

## 間諜與洗錢

依據慣例，遊戲在正式上線前會進行幾個階段的測試活動。

電玩公司首先會提供一般玩家試玩期（公測），檢驗系統在數萬人上線時最大的承載能力。

接著，邀請專業的玩家上線測試（封測），以測試遊戲的完備度。

最後，在產品上市初期利用免付費的宣傳方式吸引大批玩家上線試玩（免費試玩），一方面達到增加曝光率的效果，同時也在進行最後的系統功能檢驗。

從遊戲進行測試到正式收費前的期間，因為許多系統功能尚未到位，也因此產生許多資安的死角，而惡意的電玩間諜便會趁著安全機制尚未完備期間，刺探系統弱點。

其目的有二；這群不速之客要的是遊戲的資料演算法則（Algorithm），並

試著截取傳輸封包內容 (Package)，以得知遊戲關鍵資訊的存放位置與編碼方式。電玩間諜在得知演算法則後，便可以了解整個遊戲架構，仿製到自己的程式中。

或者，遊戲間諜也可以由封包內容找出遊戲的弱點，複製寶物。

電玩間諜以廉價出售寶物給玩家，使遊戲人物增強「魔攻」（如魔法功力）或「物攻」（如寶劍）的威力。

這些寶物（軟體）在黑市可以獲取豐厚的利潤，L公司也很難查出哪些寶物是正牌的，那些又是來自黑市的。

有些電玩間諜也會利用系統弱點，瞬間累積遊戲的金錢數，然後透過電玩貨幣匯兌，洗錢獲取暴利（例如，魔幣或天幣等熱門電玩貨幣都有兌換真實貨幣的匯率行情）。

## 帳號竊賊

L公司雖然有完備的資安防護，聘請駭客擔任遊戲的資安人員，但是多數電玩公司的資安防範並不是很完善，而電腦玩家對於個人資料保護的警戒心，更是參差不齊。

例如，有些粗心的玩家的帳號和密碼是一樣的，有些玩家的密碼則是用自己的小名。更嚴重的是，大多數玩家會使用同一套帳號與密碼，來玩遍國內各大電玩遊戲。

熟知遊戲玩家行為的駭客，便可以針對資安防護能力較差的遊戲進行攻擊，在成功盜取其他遊戲廠商的會員資料庫後，便可以藉由程式不斷地測試 L 公司的遊戲帳號。

若成功登入遊戲後，更堂而皇之地將被受害玩家帳號內的寶物洗劫一空。更惡劣的竊賊在賣光寶物後，便直接將受害玩家帳號註銷。

L 公司是否應該要負擔受害玩家的損失，常常成為難解的爭議？

## 創新解決方案

**L 網絡科技案例**，我們可以看到幾個『服務創新』機會。

本案使我們更加了解資安問題與產業特性有很高的關聯性。過去的資安需求統計往往過於廣泛，而忽略產業脈絡。

電玩產業的需求不在防毒，而是在維護遊戲平台的公平性、防止黑市洗錢以及防範帳號竊賊。趨勢科技面對這種另類資安問題，要如何依產業特性為L公司設計一套產品與服務呢？

其實，趨勢早知道線上遊戲產業有特殊資安問題，凡是像遊戲產業這樣特定族群的應用，以及藏有個人資訊的組織，例如MySpace、Blogger、Yahoo、Google、Facebook、Plurk等，都是潛在客戶。

從社群這個角度來看，這案子就有意思多了。對於這種社群組織的創新點可以由兩個方向來看。

第一，

由產品來說，網路社群含有大量Web2.0的資安漏洞，像是Facebook就允許使用端在其系統架構上面寫程式，這就會牽扯到資安問題。

目前趨勢跟eBay有這樣類似的合作，但是市面上尚未有相關的解決方案。

第二，

從服務方面，由網路社群後台的資安架構來看，也許趨勢就可能有機會。目前McAfee已經提供類似服務，但是尚不完整；例如定期為客戶掃描網頁，例如，賽門鐵克前一陣子就提出類似網路社群資安服務包下了新加坡國防單位政府所有的訂單。

趨勢能否為線上遊戲產業，設計出一套符合該產業脈絡需求的解決方案呢？

## 個案歸納

在瞭解產業資安情境脈絡後，根據使用者痛點所發現的創新來源與方向

表 14 個案五歸納整理

資料來源：本研究整理

個案產業	線上遊戲科技公司（網路社群產業）
現有資安 產品/服務	<ul style="list-style-type: none"> <li>● MIS技術人員負責Linux環境穩定性</li> <li>● 具備駭客經驗人員擔任電玩遊戲的監督者</li> </ul>
情境脈絡	<ul style="list-style-type: none"> <li>● 遊戲為新興產業，各家資安防範措施不一樣</li> <li>● 遊戲玩家為資安受害者，寶物與金幣為歹徒覬覦目標</li> <li>● 網路世界難辨善惡，資安爆發必須立刻處理以免傷害擴大</li> </ul>
資安痛點	<ul style="list-style-type: none"> <li>● 外掛機器人影響遊戲公平性</li> <li>● 遊戲駭客刺探系統弱點，獲取不法高額暴利</li> <li>● 其他廠商未落實資安防護，L公司反遭池魚之殃。</li> </ul>
創新 解決方案	<ul style="list-style-type: none"> <li>● 除產品功能外，應搭配顧問公司由服務面著手，多方面解決遊戲產業資安問題。</li> <li>● 針對網路社群發展，設想未來可以發生的問題，預先設計於新產品研發功能中。</li> <li>● 成立專責小組，研究線上遊戲與網路社群產業之共同性，提出符合該產業需求之整合方案。</li> </ul>

## 第六節 本章結論

本章以趨勢科技為例，研究防毒軟體/服務在五個截然不同的產業中，因為產品研發過程忽略考慮使用者情境脈絡，而產生許多使用者抱怨或降低整體工作效率的事件。

不同個案的研究發現也指出，研發過程若僅強調技術創新而忽略使用者情境脈絡，則新產品不僅無法滿足市場需求，反而將白白浪費寶貴的研發資源。

本節針對研究領先使用者痛點對產品研發結果的影響，提出四點分析與建議，並於第五章『研究結果分析與討論』，提出學理與實務上的研究貢獻。

### 一、 客戶抱怨來自於研發團隊忽略使用者情境脈絡

數個個案於訪談中皆表達在操作防毒軟體過程中的不滿與挫折，歸納主要的原因來自研發過程中，忽略以使用者角度來設計產品，因為研發團隊單純地以為增加新功能/新技術的方式便可以獲得使用者的青睞，卻忽略新產品/新技術在不同的脈絡環境下，可能面臨的限制與反彈。

若趨勢科技有系統地整理使用者的建議與抱怨，應可發現許多改善空間與創新的想法，這不僅可以大幅改善顧客抱怨，亦可從顧客身上學到許多寶貴的經驗。

很可惜的是，或許是受到科技產業快速變化的影響，趨勢科技並沒有靜下心來研究使用者對於產品的抱怨。

又或許因為研發團隊本身的驕傲或盲點，使得他們忽略考量不同情境脈絡下，對於不同產業資安人員的重要性。

### 二、 如何傾聽使用者需求，發掘技術創新以外的創新來源

研究使用者需求尋找創新來源，就像在尋寶過程中，戴上不同顏色的眼鏡，透過不同鏡片的折射功率，發現平常環境中也隱藏著關鍵的創新線索。

資安事件本來就是多個領域交錯糾結的複雜議題，許多使用者對於資安的理解與需求也如霧裡看花般，越看越模糊。

為了設計出創新且真正符合客戶需要的產品，趨勢科技應該學習從使用者的



情境脈絡，瞭解資安事件發生的原委，並以專業防毒廠商的角色，清楚地抓出使用者真實的需要，並排除許多陷阱與煙霧彈，藉由充分瞭解使用者情境，設計出連使用者都想不到的創新產品/服務。

### 三、 解讀領先使用者資安痛點，使研發資源得以發揮最大功效

每個領先使用者在創新嘗試過程中，必定付出了可觀的學習成本，因此衍生出現有的行為模式與獨到的觀點。如果領先使用者的每一個動作都包含著大量的試誤經驗與脈絡知識，研發團隊在研究領先使用者痛點過程中，要如何審慎地解讀每一個動作與眼神，蘊含的限制與關連性？

就像剝洋蔥般，如何順著洋蔥的紋理脈絡剝皮，才不會劃破表皮組織，防止辛辣刺激的汁液噴出，剝皮的人不會淚流滿面？

研究脈絡，發現痛點，才能讓隱藏在層層保護的資安議題現形，也因此可以將有限的研發資源，投注在尚未被滿足的需求上。

### 四、 將現有研發流程與創新來源密切接合，預知市場需求發展方向

創新來源若是多樣性的，彼此要如何配合產生新的火花？應該要設計怎樣的機制，使得領先使用者的需求與研發團隊的資源，不因彼此的距離或時間而產生差距？如果領先使用者對創新的需求可以透過某種機制與研發團隊密切互動，則使用者可以因分享經驗與想法而獲得有保障的創新產品/服務，企業也因充分掌握市場變化，而推出比競爭者更差異化或客製化的產品/服務。

## 第五章 研究結果分析與討論

### 第一節 學理貢獻

#### 對使用者導向理論（UCD，User Centric Design）有何貢獻

本研究於緒論中說明，當企業無法再利用技術創新滿足市場的需求，或是一味講求技術創新而忽略了使用者的情境脈絡，將會導致使用者對於產品的抱怨反彈，最後企業會因為無法提供真正的創新商品，面臨被市場淘汰的結局。

企業在處理使用者對於產品/服務日新月異的需求，如何以使用者意見轉為新產品的創新來源（UCD），反倒是幫助企業在競爭市場中，提供差異化服務的最佳助力。

使用者不僅可以對現有產品提供建議，更可以藉由不同的方法，收集使用者對於未來需求的想法，而多種不同的資訊來源將可以支撐許多創新產品的研發方向。

本研究從個案訪談中發現，經由詳實的田野調查方法收集使用者情境脈絡，並彙整使用者對目前資安產品的建議，以及未來可能衍生的需求，可以幫助研發團隊在設計新產品時，不需倚靠創新的技術，單純地藉由瞭解使用者的情境脈絡，也能找出許多產品/服務創新的機會。

例如，資安產品功能的整合或改良，現有服務的流程創新，或是相同的技術應用在不同領域，也可以產生許多新的價值與市場機會。

因此，即使在凡事講求新技術/新功能的資訊安全產業，在產品研發創新的過程中，仍然能夠藉由以使用者為導向的方式，找到許多好的創新來源。

#### 為何要研究領先使用者，對於創新有何關鍵影響？

從訪談個案中發現，領先使用者勇於挑戰現實環境的不合理條件並嘗試與傳統不同的作法，因而累積許多寶貴的試誤經驗，以及對於許多議題有著獨到的解讀方式。

在研究過程中發現，尋找資安創新來源的崎嶇過程中，領先使用者的意見有

效地剔除了許多無用不可行的想法，而對於具有發展潛力的想法，領先使用者亦能提出許多獨到的洞見與作法，

相較於一般使用者，領先使用者具備更積極的態度，因而能夠動員更多的資源來刺激創新想法，在面對失敗的情境下，亦能系統性地學習失敗的原因。

然而，領先使用者並非群聚在一起或是有著明顯的標示說明他們的身份，在研究使用者需求過程中，『找尋』具代表性且足量的領先使用者反而成為最困難的挑戰。

本研究在不同產業中嘗試以相同的訪談架構研究多間組織，若發現不同訪談對象對於相同議題竟產生相異的看法，便可利用此差異點，確認在該產業領先使用者的特徵與線索，藉由此方式尋找到領先使用者並進行訪談，方能避免因為一般使用者直觀的想法，對研究的結果產生偏差。

#### **觀察領先使用者的痛點，對於 Von Hippel 的理論有何貢獻與差異？**

痛點就是無法解決的問題，或需要付出相當高的代價才可能解決的難題，企業要充分利用現有資源與創意才可能解決使用者痛點，因此痛點的解決方案蘊藏相當高的創新成分，換句話說：『痛度越高，創新的價值越高。』使用者亦願意付出高額的代價去解除現有的痛苦。

Von Hippel 理論強調，領先使用者對需求的洞見或問題解決的技巧是創新的最佳來源。

但此創新來源卻可能因為時間的轉移或不同的個人立場而產生差異，如果研發團隊根據此方式推出產品/服務時，經過時間的落差，市場或許不再需要此產品或是已經產生其他的替代方案。

由解決痛點而產生的創新方案，卻因為痛點的累積並非短時間內可解決，痛點亦為瞭解使用者脈絡與情境限制的最佳切入點，因而針對痛點設計的解決方案可以滿足市場的真正需求，同時也符合使用者的情境脈絡限制。

## 第二節 實務貢獻

### 對於資安產業的貢獻與建議

目前資安產品創新模式主要是由新技術的創新帶動新的消費需求，而這些新技術或新功能選擇，卻決定於一群關在研究室的研發人員。

當研發團隊選擇將艱深的技術或忽略使用者情境的功能，設計成新一代的產品，我們可以把這類型的產品視為創新嗎？這些產品的功能是否真的能發揮功用，並產生預期的價值呢？

經過個案訪談，我們學習到產品因為忽略情境脈絡而產生的抱怨？目前擔任資安產品研發的工程師團隊是否有能力將這些研究發現，轉化為新的研發方向呢？

如果競爭對手早一步發掘使用者的需求，並搶先推出新產品搶佔市場，但是我們仍然堅持原本的研發模式，我們仍然可以保持競爭優勢而不被市場淘汰嗎？

本個案的證據顯示，當研發團隊清楚瞭解到使用者脈絡與痛點後，讓他們對於產品的創新方向，有著不同的作法與更深度的認知。

那麼我們應該怎樣有系統地採將使用者意見導入研發流程，讓創新的來源容納更多的聲音，同時讓研發團隊在考量新技術創新的過程中，可以更清楚地瞭解使用者在實際操作時，面臨的情境限制，並且在未來創新研發的目標，亦能針對使用者痛點去解決，才能產生最大的價值。

### 在引進資安產品/服務時，應該考量哪些因素？

從訪談中發現，不同產業對於資安的需求與作法有著極大的差距，有人因為不瞭解自己所處的風險與針對災難的反應能力，因此投下大筆的資源卻換不到預期的效果。

換句話說，以採購資安產品/服務為例，首先需要瞭解自己的需要，才能夠在最後找到最符合自己需要的產品，別人使用滿意的商品若不能與自己的情境脈絡配合，真正使用起來也會綁手綁腳，同時產生許多不必要的資源浪費。

而在選擇廠商時，評鑑廠商的專業度不單單僅是產品本身，而是廠商能否充分瞭解我們產業的情境脈絡，以及隱藏的風險限制。

為客戶設計出符合需求的客製化商品/服務。

### **趨勢在學習使用者痛點後，產生哪些改變與給予趨勢的建議？**

當不同產業使用者的情境脈絡，以個案分析討論的方式，與趨勢科技來自於不同部門的資深人員互動後，產生了三個不同的影響：

第一，

不同產業個案連結了趨勢各部門人員的專長，因為不同趨勢人負責的業務與客戶產生不同的連結點（例：客服人員解答客戶問題，但業務人員推銷產品），而個案研究的形式幫助不同趨勢人對於個案產業有著更完整的瞭解，因此也產生了更深入的解讀。

趨勢各部門人員，過去從未有此機會學習不同客戶的需求以及其背後的情境資訊，因此在過去對於顧客提出的抱怨和疑問，往往想不出比較具建議性的看法。

然而，在瞭解個案情境後，與不同的趨勢人進行腦力激盪，因而產生了彼此間的綜效，而綜效的產生便是新的創新來源。

如果部門間共同解決使用者的痛點能夠產生如此龐大的綜效，趨勢在未來是否善用團隊綜效，轉為未來產品創新的來源呢？

第二，

觀察趨勢不同部門間綜效的形成過程，不同部門的趨勢人亦藏著許多對創新資安產品/服務有著獨特想法的領先使用者，如何這不同的創新洞見有系統地整合起來，滿足目前產業使用者的痛點，是趨勢科技下一步可以開始進行的規劃。

另外，台灣使用者的痛點，在其他國家是否有不同的解決方法或是創新的機會點？如果其他國家，也普遍存在著像台灣使用者一樣的痛點？那這是不是一個極具創新潛力的市場呢？那麼趨勢科技要利用何種機制，有系統地去調查某個創新市場是否存在，以及如何設計出滿足新市場的創新產品/服務？

第三，

當使用者的痛點經由各部門腦力激盪產生的綜效，在跨國的營運平台上獲得了創新的解決方案，趨勢科技要如何將這樣的組織創新模式與創新精神複製下去，讓所有的趨勢人學習到找尋創新的方法，並帶著這個方法與不同背景的人驗證想法，同時早競爭對手一步將創新轉化為商業產品/服務，並將這種持續創新的能力，內化為組織每個成員的記憶與能力。



下表整理五個產業使用者痛點與不同趨勢人的創新想法，歸納整理未來趨勢科技可能的作法。

表 15 五個產業個案歸納整理

資料來源：本研究整理

個案產業	資安痛點	創新發展方向
電腦集團資訊中心	<ul style="list-style-type: none"> <li>● 商業機密外洩，客戶轉移訂單</li> <li>● 員工缺乏資安觀念，生產線感染電腦病毒</li> <li>● 全球網站連番遭駭，傷害企業形象</li> </ul>	<p>產品重組</p> <p>例：全套網站防護系統</p> <p>技術創新</p> <p>例：高效能的掃毒軟體</p>
金控總部資訊處	<ul style="list-style-type: none"> <li>● 防毒速度太慢，不符合金融業資安的要求</li> <li>● 防毒廠商不瞭解金融專業，錯失寶貴時機</li> <li>● 未經客製化的病毒通報</li> </ul>	<p>服務創新</p> <p>例：客戶資安履歷建檔</p> <p>組織重組</p> <p>例：培育金融產業專家</p>
網路美妝網站	<ul style="list-style-type: none"> <li>● 產品續約造成資安空窗期</li> <li>● 回應緩慢的經銷服務系統</li> <li>● 找不到客戶檔案資料的顧客服務中心</li> </ul>	<p>產品重組</p> <p>例：遠端簡易續約模式</p> <p>服務創新</p> <p>例：24H 急診室客服模式</p>
縣府資訊中心	<ul style="list-style-type: none"> <li>● 鄉鎮市公所幅遠廣大，落實資安控管不易</li> <li>● 內賊難防，網路犯罪舉證困難</li> <li>● 資安建設為推動E化政府的基礎</li> </ul>	<p>服務創新</p> <p>例：資安架構規劃服務</p> <p>公職人員資安訓練</p>
線上遊戲公司	<ul style="list-style-type: none"> <li>● 外掛機器人影響遊戲公平性</li> <li>● 遊戲駭客刺探系統弱點，獲取高額暴利</li> <li>● 其他廠商未落實資安，自己反遭池魚之殃</li> </ul>	<p>技術創新</p> <p>例：雲端運算解決方案</p> <p>服務創新</p> <p>例：網站安全評價機制</p>

## 第陸章 結論與建議

### 第一節 研究結論

成功的企業有效率地整合資源與技術，滿足不同市場特有的需求，並深入瞭解不同客戶的情境脈絡，領先競爭對手提供給客戶預料之外的創新服務/產品。

若企業的創新的來源是單一受限，且無法隨著外在需求環境改變而即時反應，在日趨競爭的現實環境下，失去靈活創新能力的企業終將被消費者淘汰。

資安產業在過去因過份強調技術研發創新而忽略對於使用者情境脈絡的瞭解，當不同的使用者，因為身處的產業環境劇烈改變，因而衍生的根據不同產業情境的資安需求？過去強調技術創新的資安產品，能否滿足現今多變的使用者需求？

本研究證明藉由分析不同使用者情境脈絡發現資安痛點，解決不同產業使用者的資安痛點，便能發現許多創新的來源與無窮的商機。若能掌握持續發現新來源的能力，便能領先競爭者推出更多符合市場需求的產品/服務，不僅有效提高客戶滿意度，也強化企業的競爭力。

以使用者為中心的創新來源，已逐漸取代單純依賴科技研發或改量生產設備的技術創新模式，在每個企業階將創新視為核心競爭力的年代，不僅要用心做出好產業，也要清楚瞭解服務顧客的情境脈絡與痛點，唯有參考多方不同的思維與作法後，才能持續發現無窮潛力的創新來源。

### 第二節 研究限制

本研究是以個案研究法為研究的方法與策略，由於研究方法論，以及受限於有限的時間與資源之下，所彙集的資料素材，勢必將面臨以下幾項困難與研究的限制：

第一，

本研究之主要資料的取得來源，乃以產業人士的深入訪談，與次級公開的文



獻資料為輔。不可避免地，受訪者所提供的觀點，或是情報，有可能受到報喜不報憂的扭曲，或是受訪者可能隱藏部份屬於營業的機密，或是公司內部的敏感資訊，使事實描述的部分在正確性上略有瑕疵。

第二，

本研究係選擇以質性分析的方式進行研究，難免會因為夾帶個人主觀認知判斷，而影響了推論結果，產生推論上的偏差或是誤解。

第三，

本研究依據資料來源，雖涵蓋個案訪談、會議資料與多樣來源的次級資料。但是因為商業機密考量，或因單一公司個案的侷限性。的確可能影響推論結果的週延性，造成難免的偏差或是失誤。

第四，

本研究之主題與問題，在理論上所整理「以使用者為創新來源」理論範疇，與所選定的研究構面，做一探討。難免在深入性、完整性、與嚴謹程度上有所欠缺。然而，本研究對於以領先使用者為產品研發創新導向的產業實證個案之彙整研究，仍然具備相當之學術與實務價值。

### **第三節 研究建議**

領先使用者的痛點若順利與研發創新流程結合，在未來的合作計畫中，應該從哪一個產業，對雙方彼此可以產生最大的互惠效果？在產業的選擇上，應該選擇目前規模最大的金融產業，或是選擇目前看似仍在發展中，但卻後勢可期的網路社群產業呢？

為了有系統地將使用者導向轉為商業需求，趨勢科技應該組成怎樣的團隊來瞭解不同產業的使用者需求呢？何種公平互惠的機制，才可以保障雙方在合作過程中不會受到傷害，同時分享開發的結果？

趨勢科技在導入使用者為創新來源後，在未來的經營模式與研發模式上，可能產生什麼新的作法？相較於同為資安產業的競爭對手，趨勢的競爭優勢為何？

## 參考文獻

### 一． 中文部分

1. 行政院金融監督管理委員會，本國銀行業務檢查手冊，民 93 年。
2. 資策會 MIC，金融業資訊安全運用與需求分析，民 95 年。
3. 蕭瑞麟，「不用數字的研究」，培生出版，民 95 年。
4. 吳宣諭，電腦病毒特性與病毒/防毒廠商研究，民 97 年。
5. 張一中，以策略興業理論觀點，探討持續創新與競爭優勢建構的挑戰：以趨勢科技為個案，民 98 年。
6. PCHome，希捷硬盤被爆內含病毒專收集網游密碼，民 98 年。
7. 遊天鴻，資訊保安與 ISO 27001 資訊保安全管理體系，SGS，民 98 年。

### 二． 英文部分

1. IDC, 2007. Upcoming Trends and Evolution of IT Security Solution Market
2. Ernst & Young, 2004. Global Information Security Survey 2004
3. Von Hippel, E. 1988. *The Sources of Innovation*. New York University Press, Oxford.
4. Von Hippel, E. 1998. Lead User Analyses for the Development of New Industrial Products, *Management Science*, Vol. 34, No. 5.
5. Von Hippel, E. 2007. Horizontal innovation networks--by and for users. *Industrial & Corporate Change* 16(2) 293-315.
6. Ruey-Lin Hsiao, 2009. Customer Insights: Innovating Information Security Services through Users' Local Practices