結合安全測試與異常偵測之防範架構降低電子商務安全風險

賴森堂　　羅翊萱
實踐大學資訊科技與管理學系
stlai@mail.usc.edu.tw

摘要

在網際網路的年代，日常的各種活動都與網路適度結合，商業的各種交易活動更是需要網路的服務，凡是透過網際網路進行的商業交易行為都統稱電子商務(Electric Commerce)。電子商務具備網路的優勢，在各式各樣商業行為與活動中，確實提昇許多的效益，不過，卻也隱含了許多急需改善的問題和缺失，其中又以交易與個人資料安全對於組織及利害關係人的影響最大。本文針對電子商務安全相關議題進行討論，且探究與剖析電子商務的例行性安全測試與異常事件偵測作業，進而提出一套結合安全測試與異常偵測兩層式之電子商務安全防範架構(EC Security Prevention Scheme, ECSPS)，定期的例行性弱點掃描及滲透測試找出電子商務安全的漏洞及缺失，再搭配安全事件偵測作業即時阻斷安全事件的衝擊減少損失擴大，以有效降低電子商務安全風險。

關鍵詞：電子商務、安全測試、安全事件、安全防範架構、ECSPS

Abstract

In the network and digital age, the high efficiency and high profit activities have to incorporate with the internet. E-commerce is an important system in the internet fever. However, the network intrusion, malicious users, virus attack and system security vulnerabilities have continued to threaten the operation of the e-commerce, making e-commerce security encounter serious test. In order to avoid security flaws and defects of the system caused user significant loss, how to improve e-commerce security has become a topic worthy of further exploration. Combining security test procedure and exception detection procedure, in this paper proposes an E-Commerce Security Prevention Scheme (ECSPS). Applying ECSPS, no security event before, routine security test procedure can identify security vulnerability and defect, and develop repair operations. Security event occurred, abnormal detection procedure can quickly detect and identify event, develop security defects revision step, and recover e-commerce system normally operation. Two-layer security prevention scheme can effectively enhance e-commerce security and concretely reduce e-commerce security risk.

Keywords: e-commerce, security test, exception detection, security event, ECSPS

1. 緒論

在網際網路與數位化的年代，促使各種追求高效率與高效益的活動都必須與網際網路適當的結合，如此才能在網路熱潮下提昇其競爭力以延續其生存空間，商業的各項行為與活動一直都是追求高效益與高利潤的先驅，因此，配合網際網路而改變的各種商業行為與活動，更是積極且快速的被開發與推動，凡是透過網路進行的商業活動都統稱電子商務(Electric Commerce; EC)[4, 5]，依據研究調查機構 eMarketer 的調查數據顯示，全球電子商務銷售首度超越 1 兆美元，且預估 2013 年電子商務銷售將成長至 1.3 兆美元，其中亞太區銷售額將超越北美[1]。而根據「新網路時代電子商務發展計畫」之調查顯示，2011 年我國 B2C 市場規模為新台幣 3,226 億元，預測至 2013 年可望達到新台幣 4,781 億元[8]。不過，Gartner 的研究報告指出，由於消費者擔心安全上的問題，使得電子商務的銷售額因而短少 20 億美元之多[15]。從以上的研究報告中，可以得知電子商務銷售額將持續的成長，而影響銷售額成長的關鍵因素就是電子商務的安全性。

電子商務具備了網路的優勢，在各式各樣商業行為與活動中，提昇許多的效益與競爭力，不過，卻也隱含了許多急需改善的問題和缺失，包括執行效率、網路交易安全、系統運作的特性及配合環境調整與異動的維護能力等問題，所涉及的因素非常多，其中又以交易資訊與個人資料的安全對於組織及利害關係人的影響最大，其衝擊已經超越功能與效能的需求，電子商務安全性是一項必須重視的議題。電子商務出現的安全漏洞或缺失幾乎都非主動被發現的，反之大部份異常事件屬於被告知後才發現的，因此，一旦查覺系統被入侵或資料外洩等事件，對組織所造成的損失以及對用戶所形成的衝擊，是難以評估與預期的，即使後續採取耗費人力與成本的修補作業或改善措施，也無法有效彌補，為此本文針對如何以安全防範措施有效提昇電子商務系統的安全性進行探討，且以「預防重於治療」的觀念，於電子商務安全事件發生前後，主動測試與偵測電子商務的安全缺失，以安全防範為基礎，提昇電子商務安全性。

電子商務系統除了必須搭配複雜的網路環境及更新頻繁的硬體設施外，還要協助運作中的各項

任務能夠滿足組織與用戶所提出的各項需求，另外為了協助企業/組織達成永續經營的目標，電子商務系統應該具備可以持續改善、高擴充能力、高完整性及高安全性等基本特質，其中又以高安全性的基本特質是各種商業交易活動或行為必須重視且加強的關鍵項目。本文針對電子商務的安全相關議題進行探討，且探究與剖析電子商務的例行性安全測試與異常安全事件偵測作業，進而提出一套結合安全測試與異常偵測兩層面之電子商務安全防範架構(EC Security Prevention Scheme, ECSPS)，在安全事件發生前後，即時標示出安全漏洞與缺失，適時進行安全缺失調整與改善措施，具體降低電子商務的安全風險，有效提昇電子商務安全性。本文共分成五節，第二節將探討電子商務系統的安全議題及其特質。找出運作中電子商務的安全漏洞是改善電子商務安全性的首要步驟，第三節從例行性安全測試與異常安全事件偵測作業兩個層面探討電子商務的安全性。安全測試與異常偵測是防範電子商務安全風險的必要步驟，第四節將提出一套結合安全測試與異常偵測兩層面之電子商務安全防範架構(ECSPS)。第五節將彙整電子商務安全防範程序在降低電子商務安全風險的貢獻，且針對本主題作個結論。

2. 電子商務安全之重要性

網路的熱潮改變了商業交易方式，為電子商務系統帶來許多商機，卻也隱含了難以預期的安全危機。

2.1 電子商務安全相關議題

凡是利用網路進行的商業活動或交易行為都稱為電子商務(EC)，電子商務的各項活動或行為都會涉及關鍵的個人資料與交易資訊，這些重要的資訊成為電子商務安全性的一大隱憂。根據 104 市調中心對於網路購物的安全性及影響調查的結果顯示，有 84%的民眾，擔心使用網路購物而導致「個人資料外洩」(如圖 1 所示)，也有 42%的民眾發生過「個資外洩」或遇到「詐騙事件」[7]。而近年來，個資外洩以及交易安全的問題更是越來越頻繁，從 2011 年日本 Sony 公司的 PlayStation Network 遭駭客入侵竊走 7,700 萬筆 PS3, Qriocity 音樂隨選服務使用者的個人資料[9]，及南韓線上業者 SK Communications 維運的 Nate.com 入口網站、CyWorld 部落格網站遭駭客入侵造成約 3,500 萬會員個資外洩 [11]，到 2012 年 3 月美國線上交易付款服務公司 Global Payments 遭駭客入侵恐致上千萬筆 Visa、萬事達、美國運通與 Discover 持卡人的個資外洩甚至遭人盜刷[10]等安全事件。因此，各大公司無不採取各種方法以避免客戶個人資料因駭客入侵而外洩。其中，除了透過防火牆(Firewall)、網路偵防系統(Intrusion Detection and Prevention, IDP)等硬體設備加強網路安全防護外[2]，還應該採取弱點掃描工具與滲透測試技術檢測軟體系統與應用程式的安全漏洞與缺失，以降低被駭客入侵的風險。

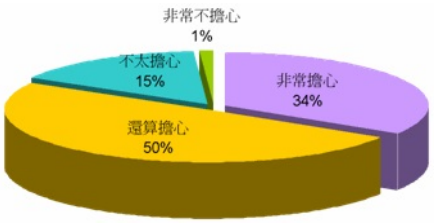

圖 1 84%的民眾擔心網路購物個人資料外洩
***資料來源：104 市調中心**

2.2 電子商務應具備的安全項目

當單位或組織規劃的電子商務系統未能關注安全上的議題時，不但會讓使用者對於該單位或組織所提供的系統產生安全上的質疑，還會大幅降低對於該單位或組織的信任度與系統的使用意願。因此，電子商務系統必須在開發前，就擬訂一套完善的安全需求，以強化系統的安全性 [3, 5, 13, 14]。Holcombe 認為任何電子商務系統都必須滿足四個安全需求[16](如圖 2)：

(1) 授權(Authorization)：對於電子商務驗證完成的使用者，必須確認該使用者的功能權限。
(2) 完整性(Integrity)：在電子商務資料交換的過程中，必須確保資訊不會遭到變更或篡改，以確定資訊內容的完整性。
(3) 隱私性(Privacy)：在電子商務資料交換的過程中，必須避免未經授權人員的接觸及參與，以善加保護用戶的個人資料與交易資訊。
(4) 不可否認性(Non-Reputation)：各種電子商務的交易行為中，均能夠具體證明且記錄交易雙方都已經確實收到對方的交換資訊，以達到不可否認性。

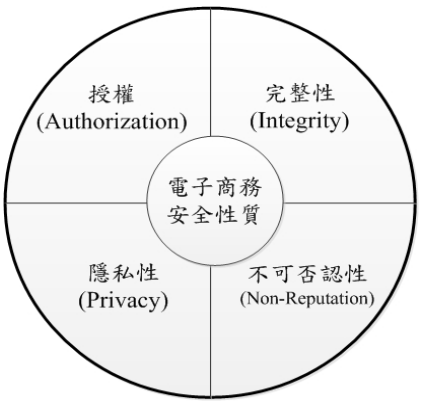

圖 2 Holcombe 電子商務四項不可分割的安全性質

Web App 系統的安全問題受到許多國際性團體與組織(SANS(安全訓練、認證與研究機構)，OWASP (開放 Web App 安全計畫，Open Web Application Security Project)的重視，陸續公佈 Web App 的關鍵安全漏洞與弱點：SANS Top-20 Security Risks [19] 與 OWASP Top 10 [16]，以協助降低電子商務軟體的安全風險。根據 SANS Top-20 Security Risks，OWASP Top 10 以及 Holcombe 提出之電子商務系統不可分割的四項安全需求[13]，將安全缺失與漏洞分為五種類型：

(1) 授與之權限之缺失：電子商務系統的維運人員必須規範明確的權限，系統無法掌控人員使用權限，將造成嚴重的安全缺失與漏洞。
(2) 完整性之缺失：當電子商務系統運作過程中，必須確保資訊或資料不會遭受到變更或篡改，以確定資訊內容的完整性，系統無法確保資料完整性，將是一項關鍵的安全缺失與漏洞。
(3) 隱私性之缺失：用戶個人資料與交易資訊是系統一項重要隱私，系統必須有能力保護用戶個人資料與交易資訊，當發生個人資料與交易資訊外洩，將形成嚴重的安全事件。
(4) 不可否認性之缺失：電子商務的交易行為中，當發生交易糾紛時，系統必須詳細記載交易行為的各項資料，且有能力分析且判斷交易行為的執行細節，以達到不可否認性，否則，將形成交易糾紛的安全事件。
(5) 入侵與攻擊手法之缺失：入侵與攻擊手法五花八門且持續創新，像是無線網路的入侵手法(封包竊聽、中間人攔截、拒絕存取、偽冒基地台攻擊…等)或是網路釣魚等，系統無法防範入侵與攻擊手法，將形成難以預期的安全事件。。

3. 安全測試與異常偵測

電子商務的安全性應該從例行性安全測試與異常事件偵測作業兩個層面進行探討。

3.1 例行性安全測試作業

電子商務系統必須擬訂一套例行性的安全測試作業以確保電子商務能夠在安全的環境中正常運作，安全測試作業大致分成弱點掃描與滲透測試兩種方式[6, 17]：

(1) 弱點掃描(Vulnerability Scan)：屬於系統內部安全漏洞與缺失的檢測作業，可交由電子商務軟體系統維護人員執行，至少應該半年執行一次，利用弱點掃描工具的協助找出電子商務軟體系統的安全漏洞與缺失，再由維護人員進行後續的修補作業，免費或開放原始碼的掃描工具包括 NetCat, NIKTO, Paros Proxy 等。由於弱點掃描只能針對程式碼可能存在的安全缺失與漏洞進行檢視，無法達成全面性的安全環境測試作業，能夠處理的範圍與改善的能力較為有限，此外免費的弱點掃描工具出現誤判率過高的狀況，也造成安全漏洞修補人員的一大困擾。為了彌補弱點掃描的缺陷，滲透測試成為安全防範措施不可缺少的重要作業[6]。
(2) 滲透測試(Penetration Test)：是一項正式的安全漏洞與缺失的檢測作業，它是模擬惡意攻擊者的攻擊手法，來去評估整個系統的安全性，而滲透測試一般都委託顧問公司且由專業人員來執行，測試的時間與檢視項目的多寡有關，且至少需要五個工作天以上，完成的滲透測試報告，除了詳述測試的執行過程外，最重要的是完整記錄發現的安全漏洞與缺失，若經費預算之許可，更可以交由顧問公司協助企業或組織進行後續的安全改善措施[6]。

使用弱點掃描及滲透測試等檢測作業，或多或少還是會有小部分的漏洞與缺失是沒辦法找出來的，所以，最後還需依靠人工針對所列舉出來的電子商務安全清單一一去做審核的工作。Racquel 針對電子商務的安全性提出了人工檢視的清單，其目的是幫助企業或組織提供一個安全且可靠的環境給使用該電子商務軟體系統的客戶，使企業或組織的系統與網站的信任度能夠提升[18]。最後，將弱點掃描、滲透測試及人工檢視針對其特性整理如下表(如表 2)。

表 1 安全測試方法相關特性比較表

測試方法 / 特性	弱點掃描	滲透測試	人工檢視
執行頻率	三個月或半年	半年或一年	依需求
執行時間	短	長	長
成本	低	高	中等
執行人員	維護人員	專業技術人員	維護人員
改善方式	自行改善	顧問公司協助完成	自行改善

3.2 異常安全偵測作業

安全測試作業可以有效提昇電子商務系統的安全性，卻無法保證系統不會被駭客或惡意使用者的入侵，更無法確認系統本身不會發生例外的安全事件，因此必須規劃一套安全事件的偵測作業，即時發現安全事件且阻止事件與損失的擴大。安全事件的偵測作業可以廣泛蒐集各種資訊安全事件的發生原因，透過歷史資料與數據制定出安全事件的判斷法則，以下為本文整理的六項安全事件判斷法則：

(1) 存取量異常：系統用戶的個人資料出現超出正常的存取現象。
(2) Log 檔異常：資料庫存取的 Log 檔出現不正確、不完整或不一致等異常現象。

(3) 交易行為異常：客戶在特定期間的交易行為出現數量過多或金融龐大的異常現象。
(4) 非法使用者：系統於運作過程中，發現非法使用者進行資料存取或竄改的異常現象。
(5) 銀行通報：信用卡發卡銀行以緊急訊息通報客特定客戶信用卡止付。
(6) 客戶通報：客戶透過相關管道告知，存放在系統的個人資料已遭竊取或竄改的現象。

這些法則具有高度的調整彈性，可以依實際的安全事件發生狀況進行新增、修訂或調整，能夠即早發現難以避免的安全事件，就可以減少事件帶來的嚴重衝擊，也可以大幅降低，因客戶個人資料外洩所造成的損失，更可以有效提高用戶對於企業或組織的信賴度。

4. 安全防範架構與運作流程

本節以例行性的安全測試與異常事件偵測作業提出一套電子商務安全防範架構，且從運作流程說明安全防範架構如何降低電子商務安全風險。

4.1 安全防範架構

企業或組織對於電子商務個人資料與交易資訊的隱私，必須規劃一套完善的安全防範措施以善盡保護個人資料與交易資訊的安全。電子商務的安全防範措施可以從兩個層面進行強化，第一層面為安全事件未發生前的測試與修補作業，網路與資訊相關設備日新月異，不斷有新的技術或產品被推出，電子商務系統必須配合這些新的技術或產品持續的調整與精進，以滿足市場的需求。此外駭客與惡意使用者的入侵手法與資訊竊取技術也不斷翻新，促使電子商務系統必須擬訂一套例行性的安全測試作業，在安全事件未發生前，識別出系統因調整與精進所導入的安全漏洞與缺失，或是翻新入侵手法與竊取技術所衍生的安全風險，例行性的安全測試作應該於 3 至 6 個月至少執行一次弱點掃描，6 至 12 個月至少進行一次滲透測試，及時找出安全漏洞與缺失，以協助後續的修補與改善作業。

第二層面為安全事件發生後的偵測與補救作業，電子商務屬於持續運作中的資訊系統，因此任何時段都有可能出現異常的安全事件，一旦發生安全事件，不僅將危及系統的正常運作，更可能波及客戶個人資料與交易活動細部資訊等重要隱私，因此，電子商務系統必須擬訂一套異常事件偵測與補救作業，此項作業屬於持續運作中的程序，在安全事件發生後，能夠透過安全偵測主動且及時得知事件發生，且依事件情節的輕重進行後續補救措施，以有效減低安全事件所造成的各項損失。

結合第一層面安全測試與修補作業，及第二層面安全事件偵測與補救作業，我們稱此安全防範措施為電子商務安全防範架構 (EC Security Prevention Scheme, ECSPS)，在安全事件未發生前，識別出系統的安全漏洞與缺失，適時找出安全漏洞與缺失，以進行後續的修補與改善作業。在安全事件發生後，主動且及時發現安全異常事件，且依安全事件情節的輕重進行後續補救措施，以有效降低安全事件造成的擴大衝擊。

4.2 ECSPS 運作流程

ECSPS 的第一層面必須制訂一套例行性安全測試程序，透過例行性的弱點掃描、滲透測試及人工檢視等方法找出電子商務系統的安全漏洞或缺失，在安全事件未發生前，即針對系統安全漏洞或缺失進行修補及改善作業，可有效降低駭客入侵、惡意使用者或系統異常等安全事件。例行性安全測試程序包括四個作業階段(參閱圖 3 所示)，說明如下：

(1) 測試規劃階段：
- 廣泛蒐集且分析現今 Web App 可能出現的安全漏洞與缺失，及駭客任入侵與新攻擊的手法。
- 針對行性安全測試作業擬訂一套完善的測試計畫。

(2) 測試執行階段：
- 規劃且設計安全測試的相關個案。
- 依據測試計畫執行安全測試且標示系統出現的各種安全漏洞與缺失。

(3) 問題識別階段：
- 剖析標示出的各種安全漏洞與缺失，且刪除誤判的項目。
- 依據確認後的安全漏洞與缺失，判斷系統受影響的功能與模組。

(4) 修補作業階段：
- 修補確認後的安全漏洞與缺失。
- 評估安全漏洞與缺失的修補作業。

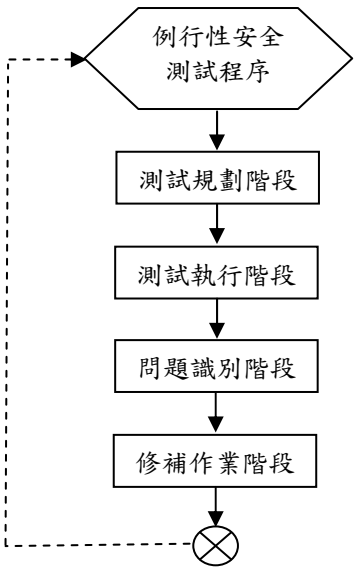

圖 3 例行性安全測試程序作業流程圖

第二層面是擬訂一套異常事件偵測程序，持續且即時的監測各種可能的安全異常事件，一旦發現資訊安全的異常狀況，經過進一步確認後，必須立即進行採取行動阻止安全事件的擴大，以有效減少安全事件的衝擊與損失，最後再針對系統的安全漏洞或缺失提出修補與改善措施，盡快恢復電子商務系統的正常運作。安全事件偵測程序包括五個作業階段(參閱圖 4 所示)，說明如下：

(1) 事件偵測階段：
- 在電子商務運作過程中，持續監控所有的交易行為與資料傳輸等活動。
- 依據事先擬訂的法則判斷方法，識別可能出現的安全事件。

(2) 事件確認階段：
- 深入分析可能出現的安全事件，進一步確定真正的安全事件。
- 剖析安全事件嚴重性，了解事件對用戶個人資料的影響程度及對系統的影響範圍。

(3) 暫停運作階段：
- 依據安全事件的嚴重性，決定停止某些功能的運作或暫時停止整個電子商務系統的運作，以減少的影響成範圍。

(4) 事件識別階段：
- 識別出安全事件發生的原因，且針對安全漏洞與缺失擬定與規劃安全事件修補與電子商務系統復原策略。
- 完整記錄安全事件發生的時間、原因、如何發現、受損的範圍及修補與復原策略。

(5) 修補恢復階段：
- 依策略修補造成電子商務安全事件的安全漏洞與缺失。
- 盡快恢復電子商務系統的正常運作。

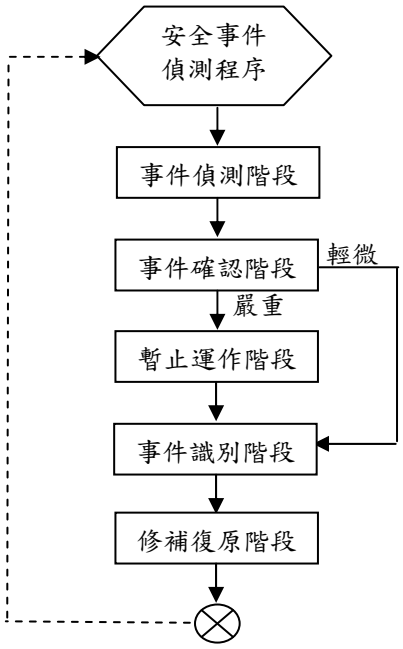

圖 4 安全事件偵測程序作業流程圖

為了具體且有效的降低電子商務系統個人資料與交易資訊的安全風險，本文規劃兩層面的安全防範架構，結合例行性安全測試程序與異常安全事件偵測程序 (參閱圖 5 所示)，例行性安全測試程序主要目的是標示潛在的安全漏洞與缺失，在未發生安全事件前，即針對電子商務安全漏洞與缺失進行修補與改善作業，大幅降低異常安全事件發生率。大部份電子商務異常事件屬於被告知後才發現的，因此，安全事件經常對組織與用戶造成重大的損失，異常安全事件偵測程序主要目的是即時偵測異常事件，且針對異常安全事件發生後，採取適時的補救措施，以降低安全事件的擴大與損失。

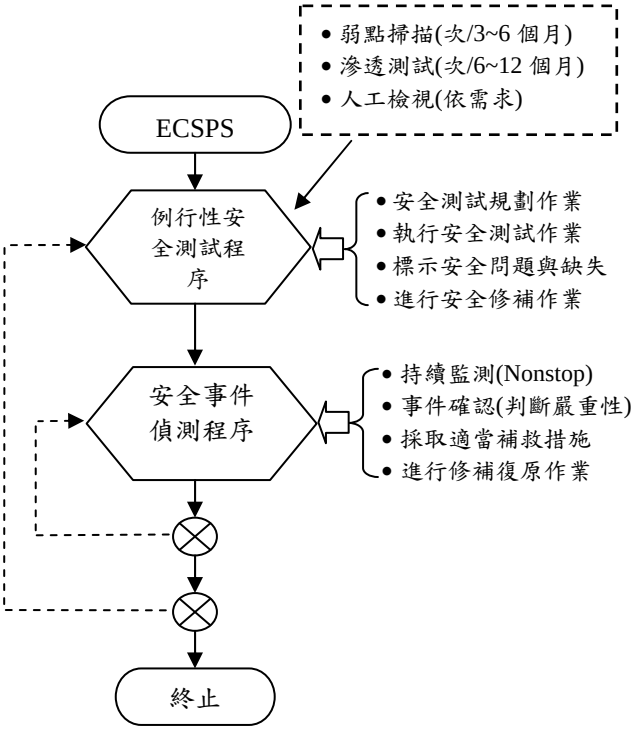

圖 5 電子商務安全防範架構運作流程圖

4.3 ECSPS 之優勢

駭客與惡意使用者入侵手法與技術持續成長，系統調整與精進過程中，因為人員的疏忽，經常造成系統本身的安全漏洞與缺失，這是電子商務系統必須面臨的問題，例行性的安全測試程序可以有效標示安全漏洞與缺失，增強電子商務的安全性，異常事件偵測程序可以即將發現異常安全事件，有效降低電子商務衝擊與損失，進而提昇個人資料與交易資訊的安全性。ECSPS 三項優勢說明如下：

- 安全事件發生前：例行性的安全測試程序可以針對事件發生前的安全漏洞與缺失，進行識別與確認，且及時提出漏洞修補與缺失改善作業。
- 安全事件發生後：異常事件偵測程序可以即時發現異常安全事件，且判斷事件的狀況，進而

採取後續的補救與強化作業。

- 降低安全風險：兩層面的安全程序可以達到互補效果，強化相互程序的漏洞與缺失判斷能力，以有效降低電子商務安全風險。

5 結論

在網際網路的年代，促使電子商務的應用範圍越來越廣泛，電子商務系統的交易行為及金額更是逐年持續增加，人們的日常生活幾乎無法擺脫電子商務的應用範疇，也因此電子商務的安全性成為一項值得深入探討與重視的議題。電子商務系統應具備可以持續改善、高擴充能力、高完整性及高安全性等基本特質，其中又以高安全性的基本特質是各種電子商務活動或行為必須重視且加強的關鍵項目。本文結合安全測試作業與異常偵測作業，提出一套電子商務安全防範架構 (EC Security Prevention Scheme, ECSPS)，在安全事件未發生前，識別出系統的安全漏洞與缺失，適時找出安全漏洞與缺失，以進行後續的修補與改善作業。在安全事件發生後，主動且及時發現事件，且依事件情節的輕重進行後續補救措施，以有效降低安全事件的風險。兩層面的安全防範架構，可以有效降低電子商務安全風險。ECSPS 具備的三項優勢為：

- 例行性的安全測試程序在安全事件發生前，及時提出漏洞修補與缺失改善作業，以降低安全事件發生率。
- 異常事件偵測程序可以即時發現異常安全事件，進而採取後續的補救與強化作業，以減輕安全事件的衝擊與損失。。
- 漏洞與缺失的判斷及安全事件的確認，可以強化兩安全程序對問題的識別能力，以達到互補效果。

參考文獻

[1] 李思萱，全球電子商務銷售首度超越 1 兆美元，預測 2013 亞太區銷售超越北美，2013/02/07-DIGITIMES，中文網。(http://www.digitimes.com.tw/tw/dt/n/shwnws.asp)

[2] 黃于珊，[觀點] 惡魔藏在細節中-- 個資外洩的四大漏洞，2012/08/14- 網路資訊雜誌 (http://news.networkmagazine.com.tw/magazine/2012/08/14/42204/)

[3] 陳政龍，軟體開發之資訊安全管理問題探討，資通安全專論，2008 年 4 月。

[4] 梁定澎主編，電子商務理論與實務，華泰文化事業公司，2000 年 5 月。

[5] 賴森堂，“電子商務軟體品質量測模式”，企業管理學報，第 53 期，53-72 頁，國立臺北大學企業管理學系，2002 年 6 月。

[6] 賴森堂，“以弱點掃描結合修補函數提昇 Web App 安全品質”，電腦稽核，第 25 期，158-168 頁，2012 年 1 月。

[7] 八成民眾，擔心網路購物遇到【詐騙事件】，104 市調中心，2010 年 04 月。(http://www.104survey.com/faces/newportal/viewPointCtx.xhtml;jsessionid=70AFB339F7F99D2503FBD40CBF199DD4.syyweb202?researchId=254)

[8] 我國電子商務發展狀況，2012 中華民國電子商務年鑑，2011 年 10 月。(http://ecommercetaiwan.blogspot.tw/2012/10/blog-post_29.html)。

[9] SONY 又出包 已逾 1 億人個資外洩，2011/05/04-自由時報電子報。(http://www.libertytimes.com.tw/2011/new/may/4/today-int10.htm)

[10] Visa、萬事達卡遭駭 台灣百張信用卡遭殃、已通知換卡，2012/03/31-NOWnews 今日新聞網。(http://www.nownews.com/2012/03/31/320-2800410.htm#ixzz2ZTZOAQFe)

[11] M. Bishop, Computer Security: Art and Science, Addison-Wesley, 2003

[12] D. Evans and D. Larochelle, “Improving Security Using Extensible Lightweight Static Analysis,” IEEE Software, January/February, pp.42-51, 2002.

[13] C. Holcombe, Advanced Guide to eCommerce, LitLangs Publishing, 2007.

[14] G. McGraw, “Software Security”, IEEE Security & Privacy, vol. 2, no.2, 2004, pp. 80–83.

[15] E. Schuman, Gartner: $2 Billion in E-Commerce Sales Lost Because of Security Fears, 2006/11/27-pcmag (http://www.pcmag.com/article2/0,2817,2064021,00.asp)

[16] OWASP Top 10 (https://www.owasp.org/index.php/Top_10_2013-Table_of_Contents)

[17] Penetration Testing vs. Vulnerability Scanning (http://www.tns.com/PenTestvsVScan.asp)

[18] Racquel, 15 Point e-Commerce Security Checklist,2013/3(https://www.swipehq.com/blog/post/15-point-e-commerce-security-checklist/1395)

[19] SANS Top-20 Security Risks (http://www.sans.org/critical-security-controls/)(2013)