供應鏈資訊安全風險因素之研究

徐淑如
國立嘉義大學資訊管理學系
slhsu@mail.ncyu.edu.tw

董和昇
國立嘉義大學資訊管理學系
hsdoong@mail.ncyu.edu.tw

宋品慧
國立嘉義大學資訊管理學系
s0981500@mail.ncyu.edu.tw

摘要

資訊系統的運作攸關供應鏈的正常營運與利益，隨著企業對交易夥伴間依賴度的增加，提高企業間資訊系統連結的緊密程度，企業資訊的風險也隨之提升，使得資訊安全成為供應鏈管理不可忽視的重要議題。

目前有關供應鏈資訊安全風險管理議題的研究仍不多見，在管控風險時，辨識風險因素為首要步驟。針對供應鏈之資訊安全，本研究採取調查法，藉由語意變數問卷與模糊德爾菲法彙總問卷資料，提出45項具有共識之關鍵風險因素，提供決策者控管供應鏈資訊安全之參考。

關鍵字：供應鏈、資訊安全、風險管理、模糊德爾菲

壹、緒論

資訊科技(Information Technology, IT)的進步為供應鏈管理提供有效的支持，藉由IT快速傳輸即時訊息、分析資料、整合資訊，供應鏈得以有效的降低庫存、快速回應市場的需求(Jiang and Yang, 2007)。隨著經營環境從企業對企業的競爭轉變為供應鏈對供應鏈的競爭，使得企業獲利日益受交易夥伴合作的程度所影響(Lee et al., 2003; Cooper and Slagmulder, 2004)。然而根據Baker et al. (2007)針對企業資訊安全（以下簡稱資安）的調查發現，隨著交易夥伴間依賴度的增加，企業資安風險也隨之提高，顯示資安風險的程度及多樣性與企業間資訊系統連結的緊密程度有關(Sutton et al., 2008)。

根據Smith et al. (2008)的觀點，供應鏈資安風險為因供應鏈成員（供應商、客戶或資訊服務承包商）造成組織資訊正確性(correct)、可用性(availability)或機密性(confidentiality)損害的情況。有關供應鏈資安的影響，以Dartmouth與Virginia大學一項針對煉油廠的研究為例，若煉油廠的監控與資料採集(Supervisory Control and Data Acquisition, SCADA)系統失效，基於安全考量立刻關閉生產作業，估計停工10天，將影響美國10%汽油供應，造成供應體系4.05億美元的損失(Symantec Corporation, 2008)，顯示維繫供應鏈各環節資訊安全的重要性。

風險管理的目標是在風險造成損害之前，針對各項風險來源，建立一個平衡、整合性的策略，並監督、控制這些策略的執行(Rook, 1984)。Giunipero and Eltantawy (2004)表示風險管理是透過確認潛在的損失與瞭解損失的發生率和嚴重性，處理不確定性因素的問題。風險評估的目的即在於衡量風險項影響的輕重，以確認具有風險性的資產，進而建立正確的程序以保護風險性資產(Ree and Allen, 2008)。目前主要的風險評估方法可分為量化與質化二類，其中量化是一種客觀標準與比較基

礎，可避免主觀意識產生的偏差，依據分析的結果，選擇重大威脅項目作為優先控管的對象。

在風險評估過程中，決策者常須將重要性或威脅程度等定性資料轉換為定量等級，此過程中須使用精確的數值或尺度，較不符合人類模糊認知的特質(Zadeh, 1965)。此外，一般以李克特式量表與語意差別量表問卷多採明確的等距數值(crisp interval value)量化語意措詞，往往無法真正反映受測者語意表達的差異性及不確定性（徐村和、朱國明與詹惠君，1999）。針對這種情況，Bowles and Pelaez (1995)、Guimaraes and Lapa (2004)、Tay and Lim (2006)等學者建議可應用模糊理論(Fuzzy Theory)使用語意(linguistic)變數進行衡量，以評估風險威脅所屬的語意項。

經由前述說明可知，風險管理對供應鏈資安的重要性，然而回顧目前供應鏈資安的研究，除了 Sutton et al. (2008)探討企業間電子商務的風險因素外，少有研究針對供應鏈資訊安全的威脅因素，提供較完整的考量(Baker et al., 2007; Faisal et al., 2007; Smith et al., 2007; Smith et al., 2008)。據此，本研究以 Sutton et al. (2008)提出的企業間電子商務風險因素、規範企業資訊安全的國際標準 ISO 27001 及供應鏈風險規範 ISO 28000 為基礎，發展影響供應鏈資訊安全之風險項，選擇製造業從事供應鏈資訊業務主管為對象，發放語意變數問卷調查，之後採取模糊德爾菲法進行回收問卷分析，以萃取出具有共識的供應鏈資安關鍵風險項目。

貳、文獻探討

一、供應鏈資安風險管理

隨著市場全球化，企業愈需相互合作，增加供應鏈的整合性，以改善供應體系效率與有效性(Baker et al., 2007)。為提昇供應鏈的整體價值，運用 IT 管理公司間複雜的資訊流成為重要的策略，藉由 IT 的應用與連結，降低公司或夥伴間採購與銷售成本、增加服務水準，移除組織資產與流程障礙(Biehl, 2005)。雖然 IT 可為供應夥伴協同合作激發更高的價值，另一方面，Smith et al. (2007)發現隨著供應鏈協同夥伴數目、IT 系統整合層級與資訊分享範圍的增加，組織遭受資安事件的機會也顯著的攀升。

Faisal et al. (2007)定義供應鏈資訊風險為因資訊不正確、不完整或非法使用，導致供應鏈遭受損失之情況；Smith et al. (2007)認為供應鏈資安風險係指因組織、供應鏈網路或外部環境的威脅引發 IT 弱點，造成供應鏈的基礎設施或結構資源效率不佳或中斷；Smith et al. (2008) 則表示供應鏈資安風險係指因供應鏈夥伴，導致組織遭受資安事件，造成財務性與非財務性損失，例如：資訊系統故障或安全漏洞能危害整體網路作業，造成立即性銷售損失、增加緊急服務與復原資料成本，及長期的商譽損失(Faisal et al., 2007)。供應鏈資安風險所涉及因素相當廣泛，例如：ISO28000 針對供應鏈資安議題提出七項要素；優質企業(Authorized Economic Operator, AEO)針對資訊交換、運用與保密、資訊技術安全、安全訓練、事故預防與處理，及評量與改善提出一套見解 （陳慧儀，2010）；ISO 27001 (2005)針對組織的資訊安全風險，分別就安全政策、組織、資產管理、人力資源安全、實體與安全環境、資訊與作業管理、存取控制、資訊系統獲取、開發與維護、資安事故管理與營運持續管理的資安層面共 11 個控制面，制定 133 項風

險項目；Sutton et al. (2008) 針對 B2B 電子商務風險，就科技、使用者應用與商業三項風險層面歸納出 49 項風險項目。

二、模糊理論

1. 模糊理論

對於風險項的評估，傳統上多是將定性的語言轉換成定量的數值，再透過效用函數評估造成系統失效風險的大小，作為改善優先順序的依據。雖有定性轉換為定量的等級，但人類的想法、推論或感知具有相當程度的模糊性，因此評估過程中使用精確的數量方法與機率數學無法完全符合人類的思考邏輯及解決較複雜的問題(Zadeh, 1965)，使分析人員可能面臨難以正確評分的情況。

模糊集合理論(Fuzzy Set Theory)是針對現實環境中不明確與模糊性的資料，使用模糊變數與有系統的模糊運算，將觀察所得的不明確資料轉換成可運用的資訊(Pillay and Wang, 2002)。為使風險分析的執行更穩定與可靠，許多學者建議可應用模糊理論於評估風險項，藉由語意(Linguistic)變數進行衡量，將各項決策因子由非明確的語意項轉換成計量數值，反映風險項的優先順序(Bowles and Pelaez, 1995; Sankar and Prabhu, 2001; Pillay and Wang, 2003; Guimaraes and Lapa, 2004; Sharma et al., 2005; Tay and Lim, 2006; Sharma et al., 2007)。相較於傳統的計量方法，納入模糊理論輔助風險分析具有以下優點：（1）進行風險評估時，所收集的數值資料、定性資料、含糊或不嚴密的資訊都可用於風險評估，並可使用一致的方法彙整處理；（2）特定風險項可以透過語意變數直接衡量其重要性，評估風險項所屬的風險層級(Bowles and Pelaez (1995)；（3）允許專家使用其判斷、經驗與知識，以使用更具彈性與可靠的評量方法(Sharma et al., 2007)。

2. 歸屬函數

模糊理論允許存在屬於與不屬於之間的中介狀態，使用模糊集表示集合，模糊集是收集一領域之資訊元素，該領域的邊界是不明確與模糊難辨的，可藉由歸屬函數指定區間，領域的任何元素皆介於 0 至 1 的區間內，所分配的值即為歸屬度，其指定該元素於模糊集中的隸屬程度(Wang et al., 2009)，描述元素和集合之間的關係，將語意或口語化的敘述轉換成模糊集合，再透過一系列有系統的模糊運算，將語意或口語化的敘述轉換成可運用的資訊。歸屬函數的建立可藉由與專家討論，歸納出各語意變數的意涵，語意變數是將人類自然語言中使用的語詞、片語所視為變數，以處理不明確或模糊的資料，透過可用的詞組（如：極低、低、中、高與極高）表示對某項準則或偏好的評估，表達歸屬函數中各尺度的隸屬程度。歸屬函數可用圖形方式表達，藉由圖表可以了解各數值等級所屬的語意變數，與各數值等級占各個語意變數的比例，在各類歸屬函數中，三角形函數與梯形函數因運算簡單且易於瞭解而最常被採用(Bowles and Pelaez, 1995; Sharma et al., 2005)。

3. 解模糊

解模糊(Defuzzification)目的是將已模糊評估的結果，轉換為一明確分級數值的過程(Bowles and Pelaez, 1995; Sankar and Prabhu, 2001; Sharma et al., 2005)，以表示

輸入的資料如何歸屬至語意術語中(Sharma et al., 2007)。

三、模糊德爾菲

Hwang & Lin (1987)、徐村和（1998）與陳昭宏（2001）等學者指出，傳統德爾菲可能會產生下列的缺點：(1）為使專家意見趨於一致，必須反覆進行問卷調查，既耗時亦增加成本；(2）隨著問卷調查次數的增加，使得問卷回收率降低；(3）傳統德爾菲中的一致性，指專家意見落於專家評定值的中位數及中間 50%的意見範圍，但此範圍隱含模糊性，並無法確定真正的落點為何，故傳統德爾菲未將模糊性納入考量；(4）在彙整專家意見時，可能因先入為主的觀念，易造成系統性削弱專家正確意見，或是抑制不同的想法。

基於上述傳統德爾菲的問題，有學者提出將模糊理論的概念導入德爾菲中，如：Murry et al.（1985）使用模糊語意變數，用以解決德爾菲調查的模糊性問題，惟其並未提出具體的計算，因此，學者們陸續提出一些解決的方法，包括最大值-最小值法(Max-Min)、模糊積分(Fuzzy Integration)、三角模糊數、以及雙三角模糊數之模糊德爾菲等（李孟訓與郭羽真，2008）。

參、研究方法

承先前所述，本研究定義供應鏈資安風險係指因供應鏈成員造成組織資訊正確性、可用性或機密性損害之情況。針對威脅供應鏈資安之風險因素，首先是以 Sutton et al. (2008)、ISO 27001 與 ISO 28000 定義之風險項目為基礎，結合五種語意變數與模糊函數發展風險因素問卷(非常不同意(0,0,3)、不同意(0,2.5,5)、普通(3,5,7)、同意(5,7.5,10) 與非常同意 (7,10,10)（Chen and Hwang, 1992; Chen and Chiou, 1999)，問卷以具有供應鏈資安業務經驗者為調查對象，針對 2010 年中華徵信所五千大企業排名資料庫的 2698 間製造公司，隨機抽取 1000 間公司之資訊部門主管發放問卷，問卷以五項語意變數進行衡量，回收問卷基於模糊德爾菲(Hwang & Lin, 1987; 徐村和, 1998; 陳昭宏, 2001)，利用「雙三角模糊數法」整合各問卷結果，並藉由「灰色地帶檢定法」檢驗專家意見是否達到收斂，並求算填答者的共識程度值，進行步驟如下：

1. 每位填答者分別評估每個風險項目語意，每個語意項對應至一三角模糊數區間值。此區間數之最小值，表示此填答者對該風險項目重要性分數的「最低認知值」；而此區間數之最大值，則表示此填答者對該項風險重要性分數的「最高認知值」。
2. 對所有填答者給予每一項風險項目 i 的「最低認知值」與「最高認知值」進行分析，將落於 2 倍標準差以外的極端值剔除後，求出未被剔除的「最低認知值中之最小值C_L^i、幾何平均值C_M^i、最大值C_U^i與「最高認知值」中的最小值O_L^i、幾何平均值O_M^i、最大值O_U^i。
3. 經由上述步驟，可建立每一個風險項目 i 的「最低認知值」三角模糊數$C^i=(C_L^i,C_M^i,C_U^i)$及「最高認知值」三角模糊數$O^i=(O_L^i,O_M^i,O_U^i)$。
4. 檢定填答者的共識程度

（1） 無灰色地帶：若$C_U^i \le O_L^I$，即雙三角模糊數無重疊現象，表示各填答者區間值有共識區段。此評估項目 i 的「威脅度共識值」G^i等於C_M^i與O_M^i的算術平均數，其運算式為：

$$G^i = (C_M^i + O_M^i)/2$$

（2） 有灰色地帶存在：但填答者的意見相差微小，若$C_U^i > O_L^i$，表示雙三角模糊數有重疊現象，且當模糊關係之灰色地帶$Z^i = C_U^i - O_L^i$，小於填答者們對該風險項「高重要性認知」與「低重要性認知」的幾何平均值之區間範圍$M^i = O_M^i - C_M^i$時，顯示各填答者的意見區間值，雖產生模糊區段，但是給予極端值意見者，並沒有與其他填答者的意見相差甚大，故並無導致意見分歧發散。此時風險項目i的「威脅度共識值」G^i等於雙三角模糊數的模糊關係之灰色地帶。之後以交集（min）運算產生模糊集合$F^i(\chi_j)$，並求出該模糊集合數之最大隸屬值$\mu_{F^i}(\chi_j)$，其公式為：

$$F^i(\chi_j) - \{\int_x \{\min[C^i(\chi_j), O^i(\chi_j)]\} dx\}$$

$$G^i = \{\chi_j \mid \max u_{F^i}(\chi_j)\}$$

（3） 有灰色地帶存在，但填答者間意見相差大，若$C_U^i > O_L^i$，表示雙三角模糊數有重疊現象，且當模糊關係之灰色地帶$Z^i = C_U^i - O_L^i$，大於填答者對該評估項目「高重要性認知」與「低重要性認知」的幾何平均值之區間範圍$M^i = O_M^i - C_M^i$時，則表示各填答者的意見區間值，產生了無共識的模糊區段，意即給予極端值意見的填答者，與其他人的意見相差過大，導致意見分歧發散，此時，將未達共識收斂之風險項剔除。

經由上述步驟計算出填答者對風險項 i 之「威脅度共識值」G^i，數值愈高者，代表威脅程度愈高（李孟訓與郭羽真，2008）。

肆、資料分析

本研究共回收 86 份問卷，扣除資料不全或填答者非供應鏈資安業務相關者，獲得有效問卷 76 份，依據前一節模糊德爾菲的分析流程，計算每項風險項是否達成共識以及「威脅度共識值」G^i。資料分析結果如表 1 所示，歸納之 45 項風險皆具威脅度共識值，其中雙三角模糊數若無模糊灰色地帶，其「威脅度共識值」G^i相對於有灰色地帶項目高，數值越高者代表填答者認知該風險項威脅度越高。

分析結果以「未建立完善的資訊處理與儲存程序，以防止資訊被交易夥伴與承包商不當揭露或誤用」、「未根據存取控制政策，限制交易夥伴與承包商對系統功能之存取」、「對於交易夥伴或承包商存取公司的資訊設備時，未完善確認可能發生的風險」、「未能與交易夥伴或承包商建立完整的資訊交換程序和控制措施，無法確保資訊交換的安全性」、「無法確保電子商務中透過網路進行資訊傳輸的安全，無法防止遭詐欺行為、合約爭議及資訊遭揭露或竄改」、「無法確保線上交易資訊的安全，防止訊息遭竄改、揭露、複製與回覆」、「無法確保交易夥伴或承包商通行碼遵循資訊安全政策操作」、「交易夥伴或承包商管理服務前，未完整鑑別風險並制定適當控制措施，並與交易夥伴或承包商協議後併入合約」、「未完善發展各項政策、流程與標準，以授權與管制交易夥伴與承包商的遠端服務」、「未進行完善的密鑰管理，以適當地支援組織間傳遞資料時加密技術的使用」、「當交易夥伴變更交易內容時，未對相關風險再次進行完整性評估」、「管理階層未定期執行完整的正式程序，審查交易夥伴與承包商使用者存取權限」、與「針對交易夥伴提交的服務、報告和紀錄未定期進行監督、檢閱與稽核」等 13 項風險項具有較高的共識度，數值依序為 7.34、7.27、7.23、7.21、7.11、6.95、6.88、6.88、6.87、

6.85、6.84、6.76 與 6.59，且各項目重要性最高認知值與最低認知值未有交集情況，表示填答者對該部份風險項之最高認知值與最低認知值已達共識，各項目的「威脅度共識值」G^i 約介於 6.59 至 7.34 之間。其餘32項風險項之重要性最高認知值與最低認知值雖有交集，但尚未到達差異過大，並存在「威脅度共識值」G^i，各項目威脅度共識值約介於 5.81 至 6.18 之間。

表 1 供應鏈資訊安全風險項資料分析結果

供應鏈資訊安全風險項	最低威脅度認知三角模糊數 (O_L^i, O_M^i, O_U^i)			最高威脅度認知三角模糊數 (C_L^i, C_M^i, C_U^i)			G^i
1. 未建立完善的資訊處理與儲存程序，以防止資訊被交易夥伴與承包商不當揭露或誤用。	3	5.21	7	7	9.47	10	7.34
2. 未根據存取控制政策，限制交易夥伴與承包商對系統功能之存取。	3	5.16	7	7	9.38	10	7.27
3. 對於交易夥伴或承包商存取公司的資訊設備時，未完善確認可能發生的風險。	3	5.05	7	7	9.40	10	7.23
4. 未能與交易夥伴或承包商建立完整的資訊交換程序和控制措施，無法確保資訊交換的安全性。	3	5.04	7	7	9.38	10	7.21
5. 無法確保電子商務中透過網路進行資訊傳輸的安全，無法防止遭詐欺行為、合約爭議及資訊遭揭露或竄改。	3	4.97	7	7	9.25	10	7.11
6. 無法確保線上交易資訊的安全，防止訊息遭竄改、揭露、複製與回覆。	3	4.87	7	7	9.03	10	6.95
7. 無法確保交易夥伴或承包商通行碼遵循資訊安全政策操作。	3	4.75	7	7	9.02	10	6.88
8. 交易夥伴或承包商管理服務前，未完整鑑別風險並制定適當控制措施，並與交易夥伴或承包商協議後併入合約。	3	4.67	7	7	9.10	10	6.88
9. 未完善發展各項政策、流程與標準，以授權與管制交易夥伴與承包商的遠端服務。	3	4.69	7	7	9.06	10	6.87
10. 未進行完善的密鑰管理，以適當地支援組織間傳遞資料時加密技術的使用。	3	4.69	7	7	9.00	10	6.85
11. 當交易夥伴變更交易內容時，未對相關風險再次進行完整性評估。	3	4.63	7	7	9.05	10	6.84
12. 管理階層未定期執行完整的正式程序，審查交易夥伴與承包商使用者存取權限。	3	4.59	7	7	8.94	10	6.76
13. 針對交易夥伴提交的服務、報告和紀錄未定期進行監督、檢閱與稽核。	3	4.36	7	7	8.83	10	6.59

供應鏈資訊安全風險項	最低威脅度認知三角模糊數 (O_L^i, O_M^i, O_U^i)			最高威脅度認知三角模糊數 (C_L^i, C_M^i, C_U^i)			G^i
14. 未使用密碼控制措施保護交易夥伴與承包商重要資訊。	0	4.38	7	5	8.81	10	6.18
15. 未與交易夥伴及承包商定期舉辦跨組織管理會報，協調組織間資訊安全控制措施的執行。	0	4.02	7	5	8.58	10	6.09
16. 無法完善控制遠端系統過濾不合法的存取。	0	3.86	7	5	8.69	10	6.08
17. 未完善保護可公開使用系統中資訊的完整性，以防止未經授權的竄改行為。	0	3.74	7	5	8.60	10	6.05
18. 所有交易夥伴與承包商使用者未具有專屬的通行碼，以便追蹤責任歸屬。	0	3.74	7	5	8.57	10	6.05
19. 未能完整區分交易夥伴與承包商之職務與責任範圍，以降低資訊或服務未經授權的修改或誤用之機會。	0	3.67	7	5	8.62	10	6.04
20. 未要求交易夥伴與承包商使用者使用通行碼。	0	3.77	7	5	8.50	10	6.04
21. 未完善保護儲存裝置，無法防止未經授權之交易夥伴與承包商存取、誤用或毀損。	0	3.61	7	5	8.66	10	6.04
22. 無法完善控管交易夥伴與承包商使用者電腦服務之存取路徑。	0	3.64	7	5	8.59	10	6.03
23. 對於交易夥伴或承包商存取公司的資訊設備時，未實施適當的控制措施。	0	3.68	7	5	8.52	10	6.03
24. 未對交易夥伴或承包商尚可公開進出區域（無須授權仍可進入之地點）進行全面性控制，防止不當存取。	0	3.60	7	5	8.57	10	6.02
25. 組織將所有或部份資訊系統、網路、桌上電腦環境等之管理及控制工作委外時，其安全要求未於雙方合約中提出並獲雙方同意。	0	3.70	7	5	8.44	10	6.02
26. 公司與交易夥伴或承包商之聘雇契約條款中，未規範其資訊安全責任。	0	3.58	7	5	8.53	10	6.02
27. 未完整鑑定與未定期審查組織機密協議，該協議能反映組織資訊保護的要求。	0	3.63	7	5	8.41	10	6.01
28. 無法確保設備皆妥善安置，降低來自交易夥伴或承包商未經授權之存取機會。	0	3.52	7	5	8.51	10	6.00
29. 交易夥伴或承包商進入公司內存取資訊或是資產資料前，未確認用戶身份。	0	3.53	7	5	8.46	10	6.00
30. 交易夥伴或承包商未注意並主動報告與本組織相關系統之已發現或疑似的安全弱點。	0	3.48	7	5	8.50	10	6.00

供應鏈資訊安全風險項	最低威脅度認知三角模糊數 (O_L^i, O_M^i, O_U^i)			最高威脅度認知三角模糊數 (C_L^i, C_M^i, C_U^i)			G^i
31. 未區隔公司網路並有效控制不同交易夥伴與承包商使用者的資訊服務。	0	3.50	7	5	8.45	10	5.99
32. 資安事故發生後，未依據相關法律的規定追蹤交易夥伴與承包商活動，蒐集與保留證據，並未以符合法律規定的形式提交相關司法單位。	0	3.44	7	5	8.36	10	5.97
33. 當聘雇關係終止時，未移除交易夥伴或承包商對資訊和資訊處理設施的存取許可。	0	3.47	7	5	8.31	10	5.97
34. 交易夥伴間未簽署資料保密協定。	0	3.43	7	5	8.31	10	5.96
35. 公司未完善建立交易夥伴與承包商違反資訊安全政策及程序的懲處流程。	0	3.34	7	5	8.31	10	5.95
36. 未能與交易夥伴或承包商建立完整的資料或軟體更新協議，重要協議皆未訂有正式的合約。	0	3.28	7	5	8.33	10	5.95
37. 當結束聘雇關係時，交易夥伴或承包商未歸還所使用之組織資產。	0	3.27	7	5	8.25	10	5.93
38. 交易夥伴或承包商使用者連線能力能跨越共享網路的範圍，未能符合存取控管政策。	0	3.18	7	5	8.22	10	5.92
39. 管理者未要求交易夥伴與承包商確實依照公司既定的程序，實行資訊安全之責任。	0	2.97	7	5	8.19	10	5.88
40. 交易夥伴與承包商使用者可存取未經授權的資訊服務。	0	3.07	7	5	8.10	10	5.88
41. 交易夥伴或承包商管理階層未能全力支持組織間資訊安全相關計畫。	0	3.08	7	5	7.98	10	5.86
42. 未採取完善的控制措施以保護軟體開發委外工作的資訊安全。	0	2.97	7	5	8.05	10	5.86
43. 對於交易夥伴可使用之系統，組織未對交易夥伴使用者提供系統的教育訓練。	0	3.02	7	5	7.94	10	5.85
44. 違反公司資訊安全政策及程序的交易夥伴或承包商，無法依規定予以懲處。	0	2.83	7	5	7.88	10	5.82
45. 承包商在申請工作時未進行背景調查。	0	2.86	7	5	7.84	10	5.81

伍、結論與建議

本研究以 Sutton et al. (2008)提出企業間電子商務風險因素與規範企業資訊安全的國際標準 ISO27001 及供應鏈風險規範 ISO28000 為基礎，使用供應鏈資安風險為因供應鏈成員（供應商、客戶或資訊服務承包商）造成組織資訊正確性(correct)、可用(availability)或機密性(confidentiality)損

害之情況，歸納出 45 項風險項，採取問卷調查法，應用語意變數衡量問項，蒐集具有實際管理供應鏈資訊業務經驗主管的意見，問卷資料模糊德爾菲進行彙總與分析。

分析結果顯示45項風險項的重要性皆達到共識收斂，其中又以「未建立完善的資訊處理與儲存程序，以防止資訊被交易夥伴與承包商不當揭露或誤用」、「未根據存取控制政策，限制交易夥伴與承包商對系統功能之存取」、「對於交易夥伴或承包商存取公司的資訊設備時，未完善確認可能發生的風險」、「未能與交易夥伴或承包商建立完整的資訊交換程序和控制措施，無法確保資訊交換的安全性」、「無法確保電子商務中透過網路進行資訊傳輸的安全，無法防止遭詐欺行為、合約爭議及資訊遭揭露或竄改」、「無法確保線上交易資訊的安全，防止訊息遭竄改、揭露、複製與回覆」、「無法確保交易夥伴或承包商通行碼遵循資訊安全政策操作」、「交易夥伴或承包商管理服務前，未完整鑑別風險並制定適當控制措施，並與交易夥伴或承包商協議後併入合約」、「未完善發展各項政策、流程與標準，以授權與管制交易夥伴與承包商的遠端服務」、「未進行完善的密鑰管理，以適當地支援組織間傳遞資料時加密技術的使用」、「當交易夥伴變更交易內容時，未對相關風險再次進行完整性評估」、「管理階層未定期執行完整的正式程序，審查交易夥伴與承包商使用者存取權限」、與「針對交易夥伴提交的服務、報告和紀錄未定期進行監督、檢閱與稽核」等 13 項風險項有較高的威脅度認知。所驗證之風險項目可作為組織辨識供應鏈資安風險來源之參考。

參考文獻

[1] 李孟訓與郭羽真，從價值鏈的觀點探討建構農業生物科技園區關鍵成功因素-以屏東農業生技園區為例，中小企業發展季刊，2008，第 7 期，第 17-48 頁。

[2] 徐村和，模糊德菲層級分析法，模糊系統學刊，1998，第 4 卷第 1 期，第 59-72 頁。

[3] 徐村和、朱國明與詹惠君，廣告業服務接觸與顧客行為意圖關係之研究—模糊語意尺度之應用，東吳經濟商學學報，1999，第 26 期，第 1-25 頁。

[4] 張淙筆，資訊系統開發專案風險評估方法之研究，國立嘉義大學資訊管理研究所碩士論文，2010。

[5] 陳慧儀，ISO 28000 應用於供應鏈安全管理之探討，東吳大學資訊管理研究所碩士論文，2010。

[6] 陳昭宏，亞太港埠競爭力與核心能力指標之研究，運輸學刊，2001，第 13 卷第 1 期，第 1-25 頁。

[7] Baker, W.H., Smith, G.H., and Watson, K.J., “Information Security Risk in the E-Supply Chain,” IGI Global, 2007, pp.142-161.

[8] Biehl, M., “Selecting Internal and External Supply Chain Functionality: The Case of ERP Systems Versus Electronic Marketplaces,” *Journal of*

Enterprise Information Management, 2005, Vol. 18, No. 4, pp. 441 – 457.

[9] Bowles, J.B. and Pelaez, C.E., "Fuzzy Logic Prioritization of Failures in a System Failure Mode, Effects and Criticality Analysis," *Reliability Engineering and System Safety*, 1995, Vol. 50, No.2, pp. 303-213.

[10] Chen, L.H. and Chiou, Y.W., "A Fuzzy Credit-Rating Approach for Commercial Loans: A Taiwan Case," *Omega*, 1999, Vol. 27, No. 4, pp. 407-419.

[11] Chen, S.J. and Hwang, C.L., "Fuzzy Multiple Attribute Decision Making Methods and Applications", Springer-Verlag, New York, 1992.

[12] Cooper, R. and Slagmulder, R., "Interorganizational Cost Management and Relational Context," *Accounting Organizations and Society*, 2004, Vol. 29, No. 1, pp. 1-26.

[13] Faisal, M.N., Banwet, D.K. and Shankar, R., "Information Risks Management in Supply Chain: An Assessment and Mitigation Framework," *Journal of Enterprise Information Management*, 2007, Vol. 20, No. 6, pp.677-699.

[14] Giunipero, L.C. and Eltantawy, R.A.," Securing the Upstream Supply Chain: A Risk Management Approach" *International Journal of Physical Distribution and Logistics Management*, 2004, Vol. 34, No. 9, pp. 698-713.

[15] Guimaraes, A.C.F. and Lapa, C.M.F., "Fuzzy FMEA Applied to PWR Chemical and Volume Control System", *Progress in Nuclear Energy*, 2004, Vol. 44, No.3, pp. 191-213.

[16] Hwang, C. L. and Lin, M. J., "Group Decision Marking Under Multiple Criteria: Methods and Applications," Springer-Verlag, New York, 1987.

[17] ISO 27001:2005, "Information Technology - Security Techniques - Information Security Management Systems – Requirements," on http://www.securitycn.net/img/uploadimg/20070924/183844756.pdf, access on 2010/4/12.

[18] Jiang, H. and Yang J., "Information Technology Support System of Supply Chain Management," *Proceedings of the 11th WSEAS International Conference on APPLIED MATHEMATICS*, 2007, pp. 138-142.

[19] Lee, S.C., Pak, B.Y. and Lee, H.G., "Business Value of B2B Electronic Commerce: The Critical Role of

Inter-Firm Collaboration," *Electronic Commerce Research and Applications*, 2003, Vol. 2, No. 4, pp. 350-361.

[20] Murry, T. J., Pipino, L. L. and Gigch, J. P., 1985, "A Pilot Study of Fuzzy Set Modification of Delphi," *Human Systems Management*, Vol. 5, No. 1, pp.: 76-80.

[21] Pillay, A. and Wang, J., "Modified Failure Mode and Effects Analysis Using Approximate Reasoning," *Reliability Engineering and System Safety*, 2003, Vol.79, No. 1, pp. 69-85.

[22] Ree, J. and Allen, J., "The State of Risk Assessment Practices in Information Security: An Exploratory Investigation," *Journal of Organizational Computing and Electronic Commerce*, 2008, Vol. 18, No. 4, pp. 255 – 277.

[23] Rook, P.S., Software Reliability Handbook, Crown, American, 1984.

[24] Sankar, N.R. and Prabhu, B.S., "Application of Fuzzy Logic to Matrix FMECA," *Review of Progress in Quantitative Nondestructive Evaluation*, 2001, Vol. 557, No. 1, pp. 1987-1994.

[25] Sharma, R.K., Kumar, D., and Kumar, P., "Systematic Failure Mode Effect Analysis (FMEA) Using Fuzzy Linguistic Modeling," *International Journal of Quality and Reliability Management*, 2005, Vol.22, No. 9, pp. 986-1004.

[26] Sharma, P.K., Kumar, D. and Kumar, P., "Fuzzy Decision Support System (FDSS) for Conducting FMEA" *IE(I) Journal-MC*, 2007, Vol. 88, No. 3, pp. 39-44.

[27] Smith, G.E., Watson, K.J., Baker, W.H. and Pokorski, J.A., "A Critical Balance: Collaboration and Security in the IT-enabled Supply Chain," *International Journal of Production Research*, 2007, Vol. 45, No. 11, pp. 2595 – 2613.

[28] Smith, G.E., Watson, K.J. and Baker, W.H., "Perception and Reality: An Introspective Study on Supply Chain Information Security Risk," *Issues in Information Systems*, 2008, Vol. 9, No. 2, pp. 272-278.

[29] Sutton S.G., Khazanchi, D., Hampton, C. and Arnold, V., "Risk Analysis in Extended Enterprise Environments: Identification of Critical Risk Factors in B2B E-Commerce Relationships," *Journal of the Association for Information Systems*, 2008, Vol. 9, No. 3/4, pp. 151-174.

[30] Symantec Corporation, “IT Risk Management Report,” 2008, Vol. 2, on http://eval.symantec.com/mktginfo/enterprise/other_resources/b-it_risk_management_report_2_01-2008_12818026.en-us.pdf, access on 2010/8/16.

[31] Tay, K.M. and Lim, C.P., “Fuzzy FMEA with a Guided Rules Reduction System for Prioritization of Failures,” *International Journal of Quality and Reliability Management*, 2006, Vol. 23, No. 8, pp.1047-1066.

[32] Wang, Y.M., Chin, K.S., Poon, G.K.K. and Yang, Y.B., ”Risk Evaluation in Failure Mode and Effects Analysis Using Fuzzy Weighted Geometric Mean,” *Expert Systems with Applications*, 2009, Vol. 36, No. 2, pp. 1195 – 1207.

[33] Zadeh, L., “Fuzzy Sets,” *IEEE Information and Control*, 1965, Vol. 8, No. 3, pp. 338-353.