每朵閃亮的雲端背後都藏有一絲黑暗：淺談雲端運算,監控與資料安全風險

Every Silver Cloud Has a Dark Lining: A Primer on Cloud Computing, Regulatory and Data Security Risk

作者: **Carl Cadregari, CISA,**

is principal and practice lead in the Enterprise Risk Management Division of the Bonadio Group and also serves as chief information security director at one of the largest insurance companies in upstate New York (USA). Cadregari has more than 28 years of experience in IT and IS security architecture, deployment, project management, security by design and governance.

Alfonzo Cutaia, Esq., is an associate in the Information Technology & Internet Law Practice Group of Hodgson Russ LLP and focuses on patent practice. Before joining Hodgson Russ, Cutaia served as an intellectual property assistant for the Office of Science, Technology Transfer and Economic Outreach at the University at Buffalo (USA).

譯者: 徐立群, 國立成功大學會計學系,教授

由於經濟環境與法規政令的快速變動，企業需求將如同天氣一般善變。為了使組織能夠適應這種如同地表上天氣的風暴，組織需要變得更加敏捷。預算的限制、管理規範及法令遵循議題的增加，迫使組織尋找它們的日常需求是否有更好的替代性解決策略。

其中一個選擇便是：雲端運算。但雲端的運用對企業營運會造成怎樣的衝擊?又當雲端上高度敏感的商業及客戶資訊遺失時，所導致的可能罰款、制裁及訴訟，企業又該如何生存?

「雲端運算」是一個最近許多人都會遇到且感到困惑的學術用語，「雲端」一詞實際上是在 1990 年代由IT組織向電信產業借引而來的。它是一個廣意的概念而非一個實際技術。在最廣範的意義及學理中，雲端運算係指大規模集中的運算資源。透過集中運算資源，資訊、流程及軟體可以讓許多公司、使用者及服務藉由遠端方式各自獨立地操控雲端使用。透過新科技的使用，包含虛擬化，當需要額外的資源時，組織可以快速地準備新電腦資源。

諷刺地，集中化運算是一種原始的運算模型－當較低運算能力的「dumb terminal」(不處理資訊的終端機器)從遠端連接到集中式的大型電腦主機時，提供其處理能力。因此隨著時間的演進，當計算處理能力已不再昂貴，運算模型已演變為主從式架構(Client-Server)－一種主機端提供基本功能(例如檔案儲存、列印序列管理)而大部份的運算能力則存在於網路終端使用者之筆記型電腦與桌上型主機的運算架構。時至今日，以前無法達到的資料傳輸速度與充足的網路頻寬，因為網路的普及造成了資料傳輸以及運算需求的成本的降低，再加上雲端提供者具有較強運算能力的電腦，顯示整體運算環境的架構將重新回到更為集中化的運算模型。

雖然雲端運算仍處於發展初期，一些雲端概念卻已被廣泛地使用。企業的資料處理通常使用雲端運算及概念，像是應用主機，包括透過網路提供軟體服務的「軟體即服務」(Software as a Service, SaaS)及透過網路提供應用服務的「應用服務供應商」(application service providers, ASP)；虛擬化的儲存方式，包含雲端儲存及線上備份；資訊科技委外(IT outsourcing, ITO)；及企業流程委外(Business Process Outsourcing, BPO)，包含了服務支援、虛擬資料中心及主機資料中心委外等。儘管這些概念是如此熟悉，然而，集中化及分享式資

源所造成的潛在傷害可能會迅速地擴散，並且超過雲端運算用於商業範疇的層級。每個組織必須了解上述的風險，並在使用雲端作為解決方案時進行仔細地衡量，如此方能使組織藉由雲端運算帶來的效益達成企業經營目標，並且繼續成長茁壯。

The Silver Cloud—Measurable Savings
閃亮的雲端-可衡量的效益

使用雲端運算有許多的優點[1]。分享運算的特性及富有調整彈性的雲端提供者能夠讓客戶端快速及簡便的調整其系統規模以符合改變中的需求。如此作法可以避免在傳統式主從架構中，設計者經常需要設計高於預計的運算能力，以確保系統在尖峰負載狀態下仍能夠正常運作。此外，許多雲端基礎的系統也讓使用者能從任何網路瀏覽器存取資訊，即使是最新的智慧型手機、平板電腦平台，且為了最大化系統效能，每個使用者消耗的資源皆可以被有效地監控。

企業展開雲端基礎系統可以避免硬體上的資本支出以及軟體的資本化；小型企業也可能因雲端提供者具備的經濟規模，可調節昂貴資訊資源的支出費用，像是系統管理員聘用、備援基礎建設及多使用者的網路基礎建設等，並因此而獲得經濟效益。上述的效益將明顯地減少雲端的進入障礙，因基礎建設係由第三方所提供，不需一次買斷所有設備，且能夠避免一些極少發生的運算資源不足風險。

The Dark Lining of the Cloud
雲端的黑暗面

雲端運算的好處將會因為組織資訊的一些極端無法控制與無法預見的潛在風險或威脅所考驗，因此企業在移動資料進入雲端前，必須全盤地評估、了解及減輕所有的風險。

維持企業營運所需的資訊是一種有價的資產，有時候為無形的、有時候則否。為何企業所持有的資料與資訊對一家公司而言是有價值的？這些資料資訊對網路犯罪來說的價值有多高?駭客又可以用這些資訊做什麼? 如果這些資料被其他公司存取並竄改，對公司來說又會造成多大損失? 如果因雲端提供者的疏失而導致失去這些資訊或遭到未受權的存取，企業又該如何因應?若部份資料被變更，企業應如何知曉?如果資料外洩，則企業應採行的法律行動為何?

資訊安全弱點遭受攻擊以及資料損失實際上是經常發生的，在2010年，根據*DataBreaches.net*, 美國聯邦調查局(FBI)[2]，電腦資訊安全協會(CSI)[3]，以及其他許多類似組織都有追蹤這類事件，這些數以百計被報導的資安事件包含了幾億筆記錄，而這還不包含尚未被報導出來的部分。事實是沒有人會打開報紙或閱讀線上頭條卻不知道網路攻擊與網路犯罪是現實生活的一部分－像ALDI,[5] T.J.Maxx,[6] Heartland Payment Systems,[7] the US Veterans Administration,[8] Ben & Jerry's,[9] 與PETCO,[10]等等都是新的例子。因此，使用雲端提供者的服務，將顯著增加資安事件的風險，並且增加上述事件產生的所有成本，包含法律上的補救以及違法所產生的其他損失。然而，除了資安事件風險增加的成本外，決定影響範圍並且從資安事件中回復的成本也應該一併被納入採用雲端運算的考量中。

資料及資料的存取對於企業的繼續經營有著真實的價值，特別是對於企業所服務的客戶。有時候，更確實地說，資料對某些人來說的價值足以讓部份企業或即使是部份國家都想要去竊取、操作或執行其他危及這些資訊的動作。

資料對於網路犯罪者的價值直接取決於企業面對這些威脅的立場態度。攻擊者會衡量取得資訊的風險相對於他們所能獲得的報酬。當使用雲端運算時，上述問題將會變為：當集中的資料包含數以百計其他公司的資料時，這些公司將如何去面對其中一家企業所面臨的資安威脅？顯而易見的事實是，一家企業對於放置於雲端中的資料所處得資訊環境是絕對沒有直接控制權的，此外，服務級別協議(service level agreements, SLAs)也無法幫上什麼忙，因為雲端提供者可能只採取了極

少的措施來替客戶確保安全性、可用性或回應時間。

大部份的SLAs使用許多時間與篇幅於切割(carve-out)以及最佳防護(best-effort hedges)，但這些行動並不能對企業擁有者提供具體的保證，特別是提供者在法律規範下應負擔的責任。當雲端運算進行時，資料必需被覆核，至少需定義並回應由雲端安全聯盟(Cloud Security Alliance)[11]所提出的6個核心問題：

1、若資產被廣泛地公開以及廣泛地散佈，企業將遭受怎樣的損害？
2、若雲端提供者的員工可以存取企業的資產，企業將遭受怎樣的損害？
3、若企業流程或系統功能可以被外部人員操作，企業將遭受怎樣的損害？
4、若企業流程或系統功能提供的結果是錯誤的，企業將遭受怎樣的損害？
5、若資訊/資料有不可預期的變更，企業將遭受怎樣的損害？
6、若企業資產在一段期間中無法使用，企業將遭受怎樣的損害？

雲端的法規遵循

為了維持下列法案與標準的遵循：美國聯邦資訊安全性管理法案(FISMA)； 美國醫療保險流通與責任法案 (HIPAA)；美國經濟與臨床健康資訊科技(HITECH) 法案；美國金融服務業現代化法案(GLBA)；支付卡產業資料安全標準(PCI DSS)；美國家庭教育權利和隱私法案(FERPA)；美國兒童網際網路保護法案 (CIPA)；美國沙賓法案；美國聯邦法規(CMR)第201節；美國加州資料隱私法案 (SB) 1386；美國紐約國家信息安全違反通知法(NYISBNA)；美國聯邦條例法典FDA21 CFR11 (21CFR11)；及其他的資料安全準則，企業必需接受被稽核的要求並實際進行稽核行動。

因此，企業必需瞭解使用雲端運算後對於企業所應擔負的責任與法規遵循會造成怎樣的影響。一般來說，大部份的法令及遵循要求企業證明這些雲端提供者(或是ASP, SaaS 提供者及資訊委外廠商)至少要有相同或相似於企業內部對於主機系統的內部控制措施，以保護資料符合相關法令規範與法令遵循。因此，當組織為雲端基礎下由第三方提供運算處理、並且由第三方負責取得組織中隱私資訊(personally identifiable information, PII)的公開發行公司時，雲端提供者需要做什麼?企業需要做什麼?以及當資料遺失、遭受不適當存取或遭遇其他方面的危害時，將導致什麼問題產生?

資料遭受非法侵害的成本

在現今的世界，盜用資料、實體資產的竊取與損失，以及蓄意/非蓄意地違法行為經常性地在各種類型與規模的企業發生。最近由 Ponemon 研究機構所完成關於網路犯罪成本及頻率的研究，顯示每一間受查公司每個星期至少發生一件成功的網路犯罪，且管理這些網路攻擊的年成本超過美金三百八十萬元[12]。這個研究詳細地指出在大部份遭受到影響的商務範疇中產生的成本，包含網路犯罪偵查、規避、事件管理以及資產損失，但不包含不遵循法規導致的罰款、容易使實際成本加倍的制裁及訟訴等。一些最近發生且遭到課徵罰金的事件包含：

- **Rite Aid®**—US $1 百萬，違反HIPAA[13]。
- **The TJX Companies Inc. (of which T.J.Maxx is a part)**—US $40.9百萬，遺失信用卡資料[14]。
- **Health Net of NE**—US $250,000，損失硬碟[15]。
- **Six California (USA) hospitals**— 超過 US $790,000，係違反加州公共衛生局(CDPH)於私密資料的侵害[16]。

當雲端運算持續成長，代表它將會暴露或被利用於犯罪活動中，也因此將會更需要雲端鑑識(Cloud Forensics)的技術，而這也可以在任何資料非法侵害或任何相關網站中找到佐證，舉例而言：Cloutage.org在2010時，報導了322筆事件、其中有54筆資料遺失的發生係因雲端提供者遭駭客入侵或因雲端弱點被找到而導致[17]。

雲端的保證

使用雲端資源雖能對大多數的企業帶來極高的效益，但企業永遠必需關注伴隨而來的風險，並從稽核與法律社群中選用適當的資源與專業人員確保雲端的使用獲得一定程度保證，同時也需準備好回答下列的問題：

- **安全性：**
  - 靜態儲存資料及動態資料傳輸時將如何加密？
  - 如何保護資料免於非授權存取？
  - 資料將如何配置部屬？
  - 雲端提供者如何執行內部安全管理？包含以下三個面向：
    - 管理者控制
    - .實體控制
    - .邏輯控制
  - 當發生資料遭受非法侵害時，企業應有的權利及義務為何？(例如：稽核的權利、鑑識調查的能力)
  - 當遭受安全性侵害時，雲端提供者應告知使用者的報導義務為何? (例如遭受非法侵害的賠償)
  - 雲端提供者採取何種行動來預防攻擊行為？
  - 雲端提供者需要企業建置的保護措施為何？
  - 雲端提供者如何確實地對客戶展示及溝通安全程序？
  - 雲端提供者可以給予客戶執行安全驗證(如安全掃瞄或進行稽核)的能力有多少？
  - 當與法令有違背或發生衝突時，雲端提供者將如何處理？

- **遵循性**
  - 雲端提供者須符合什麼標準?
  - 再使用雲端前、正要改用雲端或已經採用雲端時，相關法令規章的遵循該如何被持續維持？
  - 該採用何種第三方認證標準文件(例如SAS 70、資訊系統認證（WebTrust）、資訊系統認證（SysTrust）等)來確認相關規範的遵循性？
  - 企業如何追蹤資料存放的實體位置並確保已遵循相關規範？(例如部份法令禁止資料存放於某些城市)?
  - 除了資料安全性，雲端提供者需提供給企業哪些文件用來確保維持法令規範的遵循，例如美國沙賓法案(US Sarbanes-Oxley Act)?
  - 企業是否已因應企業資料所需要的程度，準備足夠的內部控制與建立一定程度的規範遵循？
  - 當企業提供的內控與商業流程相關資訊達到何種程度時，將可能因此危害企業本身的營運？

- **可用性**
  - 多少正常運行時間是被保證的？
  - 是否有保證的服務等級?由誰監督是否達成?
  - 若保證的服務等級未滿足時，會有什麼賠償?
  - 現在所有服務都是透過網路存取，企業是否有足夠的頻寬分派給所有員工，以及雲端提供者是否有足夠的運算能力及頻寬用來服務企業的需求?
  - 雲端服務是否有可能因其他不相關的客戶的使用而導致中斷？ (例如硬碟中訊息傳遞(hard drive subpoena))
  - 如何在客戶間將彼此的資訊進行區隔?
  - 雲端提供者所提供的認證如何與可用性連結?
  - 服務中斷或問題所造成的企業損失，雲端提供者的責任、財務、合法性或其他相關項目，應達到何種等級?
  - 當企業有雲端基礎建設時，災害復原及企業永續經營計畫將如何訂定?

- **營運**
  - 企業如何監督雲端的負載及效能？
  - 雲端提供者如何確保費用是依據企業使用量公平地收取？
  - 什麼工具可以被用來監控雲端的安全性？

- **整體專案**
  - 誰是專案前已規畫事項的獨立稽核員？
  - 執行稽核的頻率為何？

上述的問題是當企業想仔細挑選雲端提供者時須被回應的基本問題。企業應針對科技、法令遵循性及企業內部溝通進行足夠深入的準備。在

所有的案例中，當雲端提供者針對上述問題有一個不確定或否定的答案時，便應該被嚴重地看待，畢竟即使僅有一個控制是不足的，也足以奪走所有企業的寶貴資料。

結論

當雲端運算持續演變為資訊處理、資料儲存及跨界通訊的主流，資料一致性是否被檢查以及已辨識的威脅是否緩和到與資料價值相同的程度將是關鍵的風險所在。

雲端運算的基礎建設價值是可被衡量的，在資料的可用性、顧客關係管理及硬體成本與資訊基礎建設的建置成本都可以有效地降低，但違反法律或遺失資料產生的潛在性主管機關罰款、民事訴訟或商譽損害的成本，卻更容易超過企業所省下的資源。

切記，對於企業而言，保護其資料的機密性、完整性與可用性，同時盡到符合法令規範的義務，並且避免在雲端上遭受損失，永遠是企業最重要的責任。

Endnotes

1 See the case studies published by Microsoft *(www.microsoft.com/en-us/cloud/tools-resources.aspx?CR_CC=200010704&WT.srch=1&WT.mc_id=A8A7CD18-DA39-4EEE-81FC-BA7440F28341&CR_SCC=200010704#casestudy) and the information provided from VMware (www.vmware.com/solutions/cloud-computing).*

2 The Federal Bureau of Investigation, "Internet Crime Trends—The Latest Report," USA, *www.fbi.gov/news/stories/2011/february/internet_022411/internet_022411.*

3 Computer Security Institute, *http://gocsi.com/sites/default/files/uploads/Surveyand%20webinar%20PR%202010.pdf*

4 See *www.bankinfosecurity.com, www.ftc.gov, www.first.org, www.cloudsecurityalliance.org and www.cloutage.org.*

5 ALDI, "ALDI Notifies Customers of Tampered Payment Card Terminals," press release, 1 October 2010,*www.aldifoods.com/us/media/company/company/Press_ Release.pdf*

6 Jewell, Mark; "TJX, Visa Reach $40.9M Settlement for Data Breach," USA Today, 30 November 2007,*www.usatoday.com/money/industries/retail/2007-11-30-tjx-visa-breach-settlement_N.htm*

7 McGlasson, Linda; "Heartland Payment Systems, Forcht Bank Discover Data Breaches," BankInfoSecurity.com, 21 January 2009, *www.bankinfosecurity.com/articles.php?art_id=1168*

8 Yen, Hope; "VA Agrees to Pay $20 Million to Veterans in 2006 Data Breach," Boston.com, 28 January 2009, *www.boston.com/news/nation/washington/articles/2009/01/28/va_agrees_to_pay_20_million_to_veterans_in_2006_data_breach*

9 See Open Security Foundation, http://datalossdb.org/incidents/3062-2-500-customers-names-and-addresses-exposed-on-the-web.

10 See Open Security Foundation, *http://datalossdb.org/incidents/30-up-to-500-000-credit-card-numbers-exposed.*

11 Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," USA, 2009,*www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf*

12 Ponemon, Dr. Larry; "Five Countries: Cost of Data Breach," Ponemon Institute LLC, revised 19 April 2010, *www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf*

13 Masters, Greg; "Rite Aid to Pay $1 Million Fine for HIPAA Violation," SC Magazine, 28 July 2010,*www.scmagazineus.com/rite-aid-to-pay-1-million-fine-for-hipaa-violation/article/175729*

14 Op cit, Jewell, Mark

15 Santalesa, Richard L.; "Health Net Agrees to $250,000 Fine and 'Corrective Action Plan' to Settle Loss of PHI," Information Law Group, 21 July 2010, *www.infolawgroup.com/2010/07/articles/hitech-1/health-net-agrees-to-250000-fine-and-corrective-action- plan-to-settle-loss-of-phi*

16 Hennessy-Fiske, Molly; "Six California Hospitals Fined for Medical Record Security Breaches," Los Angeles Times,19 November 2010, *http://latimesblogs.latimes.com/lanow/2010/11/hospital-fines.html*

17 See Open Security Foundation, *http://cloutage.org/incidents?reported_year=2010.*

Quality Statement:

This Work is translated into Chinese Traditional from the English language version of Volume 3, 2011 of the ISACA Journal articles by the Taiwan Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the ISACA. The Taiwan Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

品質聲明：

ISACA臺灣分會在ISACA總會的授權之下，摘錄ISACA Journal 2011,Volume 3中的文章進行翻譯。譯文的準確度及與原文的差異性則由臺灣分會獨立負責。

Disclaimer:

The ISACA Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the ISACA Journal.

Opinions expressed in the ISACA Journal represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. ISACA Journal does not attest to the originality of authors' content.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

免責聲明：

ISACA Journal係由ISACA出版。ISACA 為一服務資訊科技專業人士的自願性組織，其會員則有權獲得每年出版的ISACA Journal。

ISACA Journal收錄的文章及刊物僅代表作者與廣告商的意見，其意見可能與ISACA以及資訊科技治理機構與相關委員會之政策和官方聲明相左，也可能與作者的雇主或本刊編輯有所不同。ISACA Journal 則無法保證內容的原創性。

若為非商業用途之課堂教學，則允許教師免費複印單篇文章。若為其他用途之複製，重印或再版，則必須獲得ISACA的書面許可。如有需要，欲複印ISACA Journal 者需向Copyright Clearance Center(版權批准中心，地址：27 Congress St., Salem, MA 01970) 付費，每篇文章收取2.50元美金固定費用，每頁收取0.25美金。欲複印文章者則需支付CCC上述費用，並說明ISACA Journal 之ISSN 編碼(1526-7407)、文章之出版日期、卷號、起訖頁碼。除了個人使用或內部參考之外，其他未經ISACA或版權所有者許可之複製行為則嚴明禁止。