打造未來

IBM 2014 年 CISO 調查報告洞察

IBM

IBM Center for Applied Insights
ibm.com/ibmcai | ibmcai.com

未來變化多端弔詭難測。資安官面對此挑戰兢憂度日，芒刺在躬。他們奮力防範公司受到各種千變萬化的安全威脅，如今必須做好準備迎接不止是接踵而來的攻擊，而且還有更加複雜的攻擊者。

我們的報告係為調查如今資安官肩負的各類挑戰，以及針對管理這些不確定性因子可以採取的行動。

IT 世界中的「守護者」角色進退維谷。運算創新加速前進，衍生出各種令人印象深刻的全新技術，而且造就深遠影響，但通常也加諸了資安官的防禦職責。行動裝置、雲端技術和海量資料日益增長的力量雖令我們雀躍不已，但為了確保安全性，仍需專門投入同樣巨大的工作負載。這並未包括現有的挑戰，例如管理 IT 風險、應對監管法規與合規性要求以及建立高效能合作。

但這還不足以成功確保安全，僅在今年就已經發生了多少次資料洩漏或資訊安全故障的消息？即便 CISO 向企業一一道述各種威脅的重要性，他們的角色仍無法獲得足夠的重視。

IBM 應用洞察中心本系列研究的首次報告《2012 年 CISO 調查報告》中構建了三種資安官的原型——應對者 (Responder) 、保護者 (Protector) 和影響者 (Influencer) ——由此開始探索他們各自的特點。一年之後，《2013年 CISO 調查報告》中闡述明確的步驟說明資安官如何達到影響者的地位，並且介紹了在過渡時期如何為安全領導力設定了一種全新的標準。

研究簡介

為了深入理解資安官的當前形勢和未來發展藍圖，IBM 應用洞察中心攜手 IBM Security 部門，深入採訪了 138 名資安官，他們都是負責企業資訊安全事業的高級 IT 和業務主管。這些資安官有些冠以 CISO（資訊安全長）的職位名稱，但是鑒於企業組織結構各異，有些人則並未冠以此頭銜。其他受訪的資深主管還包括 CIO、IT 資安副總裁，以及資安總監。63% 的受訪企業設有 CISO 職位。參與者橫跨不同的行業，來自五個不同的國家。

2014年的《CISO 調查報告》評估了安全領導力的現狀以及資安官在未來三至五年內預計將會面臨的形勢。資安官正在處於轉型階段。受到外部攻擊威脅和自身企業需求的刺激，他們正轉型成為企業組織領導者的角色，專注於風險管理，並且採用了整合性與系統性的方法。

安全領導力演變的下一個階段是什麼？憑藉已然全面的佈局，資安官需要採取哪些行動才能鞏固自身的準備工作並且提升自己的遠見？

關鍵主題

1. 資安官職責的轉變與擴張
2. 外部威脅所產生的疑慮
3. 更多與外部合作的契機
4. 資安官應聚焦於現有的技術
5. 搖擺不定的政府政策

資安官職責的轉變與擴張

資安官及其企業已察覺自身職責正面臨巨大的轉變：82% 的受訪者表示在過去的三年間已經改變了原本對於安全性的看法。眾多企業不僅調整安全性原則細節，更重新思考其整體原則，藉以將日益漸增的資料、設備、使用者需求和各處與業務有關的整體安全重要性考慮在內。

同樣的，這也直接提高了 CISO 及其相關主管的權利。過去，眾多資安專業人員渴望成為企業決策性的影響者，今年 61% 的受訪者也將自己歸納為「影響者」。此外，64% 的受訪者在評定已記錄的企業安全性原則等級時都給予「極度成熟」的評價。這種轉變證明：更多在企業中深諳此一趨勢的資安官已日趨成熟。

這種不斷擴張的權力不僅是依據運算分析的需求，資安官還要利用自身的影響力管理更加詭譎多變的外部威脅以及應對企業內部更高預期的要求。而保護雲端、行動裝置等領域和新安全技術所涉及的廣泛範圍，造成盤根錯節的複雜情勢。CISO 不再只是安全技術的管理員，而是必須考量企業業務營運的決策者。資安官在獲得更大影響力的同時，也需將它運用到公司的廣泛目標並善理過程中每一步所會發生的風險。

獲得更多的影響力和支援

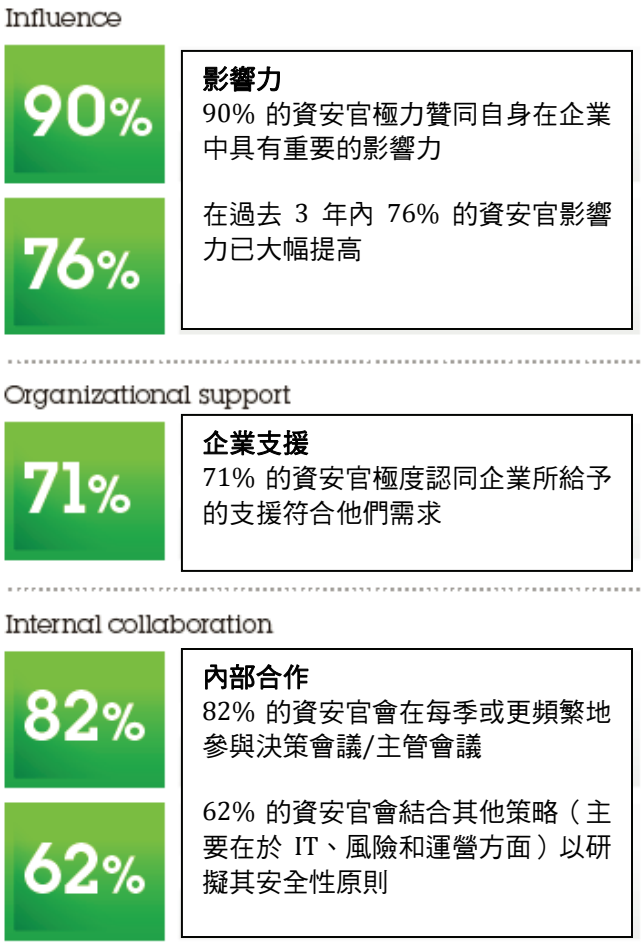


圖1. 資安官需要成熟發展和培養影響力，以此應對更具挑戰性的外部威脅挑戰。

CISO 觀點：肩負重任以應對更加嚴峻的挑戰

作者： Jonathan Klein
CISO ，Broadridge 金融解決方案公司

近年來，我作為 CISO 的職責不斷提高。在企業中的影響力更甚過往，必須定期與公司高層和其他資深主管開會。但因資安形勢日益複雜，蘊藏諸多嚴峻挑戰—因此我整體的職責和能力也必須同步提升。Broadridge 公司為金融機構提供豐富多樣的技術和服務。位其職，我們協助客戶維護其最具價值的資產之一，即客戶資訊。

眾多企業如今面臨最大的挑戰之一為匯集資訊安全技術與適切的業務流程。新技術通常旨在抵禦最新的安全威脅，但是若無適當與業務流程匯集，則會效果不彰。我與 Broadridge 公司的高層經過研討，將資安和風險考量因素整合至其業務決策的初期階段，並確保其技術不僅能夠保護自身的企業，且能促進業務流程和策略發展。

例如，企業中仍然存在諸多作為標準的封閉式資料。眾多企業往往期望能符合這些標準以確保敏感資料在整個數據週期內達到安全指標，而無需採取附加措施。這已被證明為一種危險的假設，許多受到高度關切的資料洩漏事件已經說明了這一點。在 Broadridge 公司，我們不僅符合標準的框架，更注重於確保資料的安全性。

IT 的消費化也產生其他併發現象。私人和專業人員所使用的設備和應用程式之間不再有明顯的區別。這往往導致最初設計於私人性質的技術逐漸公開化，造成大眾迅速採用所產生的安全性威脅。而大眾只聚焦在新的功能上，而非其安全性，這讓眾多企業難以快速採用這些新技術，同時還需評估其全面的安全性。

確保安全性為基本任務，並非最終目標，這將是 CISO 影響力不斷提升的關鍵要素。

外部威脅所產生的疑慮

鑒於進階持久性威脅、犯罪企業、具有國家背景的駭客、駭客活動家以及其它網路犯罪行為帶來的挑戰，是提高資安官成熟度和影響力的關鍵。資訊安全威脅迫在眉睫，許多企業對此挑戰無不感到憂心忡忡。接近 60% 的受訪資安官表示攻擊者的複雜程度已經超越了企業防禦的負荷程度。超過 80% 的資安官已經察覺到過去三年來不斷增長的外部威脅，並將此視為當前的首要任務。此外，外部威脅的未來趨勢不會減弱，正如半數的受訪資安官所言，它需要企業在未來的三至五年內投入最大的心力與之抗衡。

圖2. 資安官將會繼續聚焦於未來可預測的外部威脅，致力降低資安風險。

CISO 觀點：通過合作改進安全性原則

作者：John Taylor
英美煙草集團前 IT 安全部全球主管

外部合作為資安官提供有效考察市場與實踐的機會，並與同行攜手發展以利深入瞭解業界新興的合作模式。此外，更有助於將業界革新歸納為一套通用流程，以便在您於私有的環境內使用。在英國煙草集團，我們採用豐富彈性化的合作模式，包括正式和非正式的方法以確保架構充分有效運作的網路。

我們與業界同行、供應商、合作夥伴以及政府在內連結成最為堅實的合作關係。我們可以將團隊成員派遣到全球諮詢委員會，邀請專家加入討論，而且還可通過與各類專業人士共進餐點時獲得洞察，或者從中得知新興的挑戰或威脅。這觀點似乎有些矛盾，但處於維護隱私和保全資料越發困難的情況下，提高安全性的關鍵鎖匙在於提高開放性。

然而，必定有人會對加入或建構這樣的企業組織不屑一顧，因為許多人都會抵制這個目的並貶低其價值。我們需要支援更加有效的企業組織，並且確保它們可以全方位觀察各種潛在的資安風險。

提到共同合作以實現未來發展，有些企業組織需要獨有的專業人員，而其他組織則是需要由合作機構、終端供應商與合作夥伴來提供支援。CIO 還需要將更多廣泛的企業組織包括在內，而不能僅局限在資安官範圍內。當涉及到合作時，我們希望具豐富經驗的行業能在我們的生產過程中給予指導。銀行業一直以來不遺餘力地共用資訊（特別是威脅資訊），進而助於保護大量的私人資料和金融財產，創造其他行業渴求的模型。

如今不斷擴展的資安威脅表明我們無法全面保護所有領域。其他企業也面臨相同的挑戰，因此傾聽同行的觀點有助於改善我們保護敏感資料的策略。

更多與外部合作的契機

隨著企業的資訊安全警戒線不斷擴展、混合以及消失，資安官日益需要整體的安全生態系統，而不能僅局限在自身的企業範圍內。通過隔離實現保護的做法在現今環境下簡直是捨本逐末：62% 的資安官極為贊同以下觀點：由於與客戶、供應商以及合作夥伴頻繁的交流和聯繫，自身企業的安全等級也在不斷提升。儘管大範圍的網路互聯性驅動了現代企業的發展，但資安官還未充分實現與其他企業的合作。當前，只有 42% 的受訪企業為正式相關行業的安全性組織成員。然而，86% 的受訪者認為這些組織的必要性在未來三至五年內將會逐步提升。

圖3. 為了降低客戶、供應商與合作夥伴頻繁聯繫所致的風險，需要提供一種有保障的「安全生態系統」。

資安官應聚焦於現有的技術

接近半數的受訪者都將新安全技術列為三大計畫之一，這成為資安官最受矚目的領域。資安官對於既有的安全技術十拿九穩並認為這是他們的「基本技能」。超過 70% 的受訪者更表示自身的網路入侵防禦、先進惡意軟體檢測和網路漏洞掃描技術已經十分純熟。

然而，更新的技術領域（防止資料洩漏、雲端和行動裝置的安全性）則存在更多的不確定因子： 28% 的受訪者確定其中每一種技術都需要企業巨大的轉型或改善，而企業革新迫切性與高彈性的變化方式則列入清單的首要事項。

- **資料** – 72% 的資安官表示即時安全智慧分析對企業來說有著舉足輕重的地位。然而，資料分類和發現以及安全智慧分析等領域的成熟度較低，還需加以改善或者進行轉型。
- **雲端** – 雲端安全所受到的關切程度依然名列前茅，雲端消費雖已十分廣泛但將會持續增長。調查顯示 86% 的受訪者已採用雲端或者正在規劃雲端方案。在未來三至五年內，四分之三的資安官預計雲端安全預算將會增加或者大幅提高。
- **行動裝置**– 大多數的資安官表示他們不具備高效能的行動裝置管理方案。從成熟度來看，行動裝置和設備安全性在技術排名中敬陪末座。

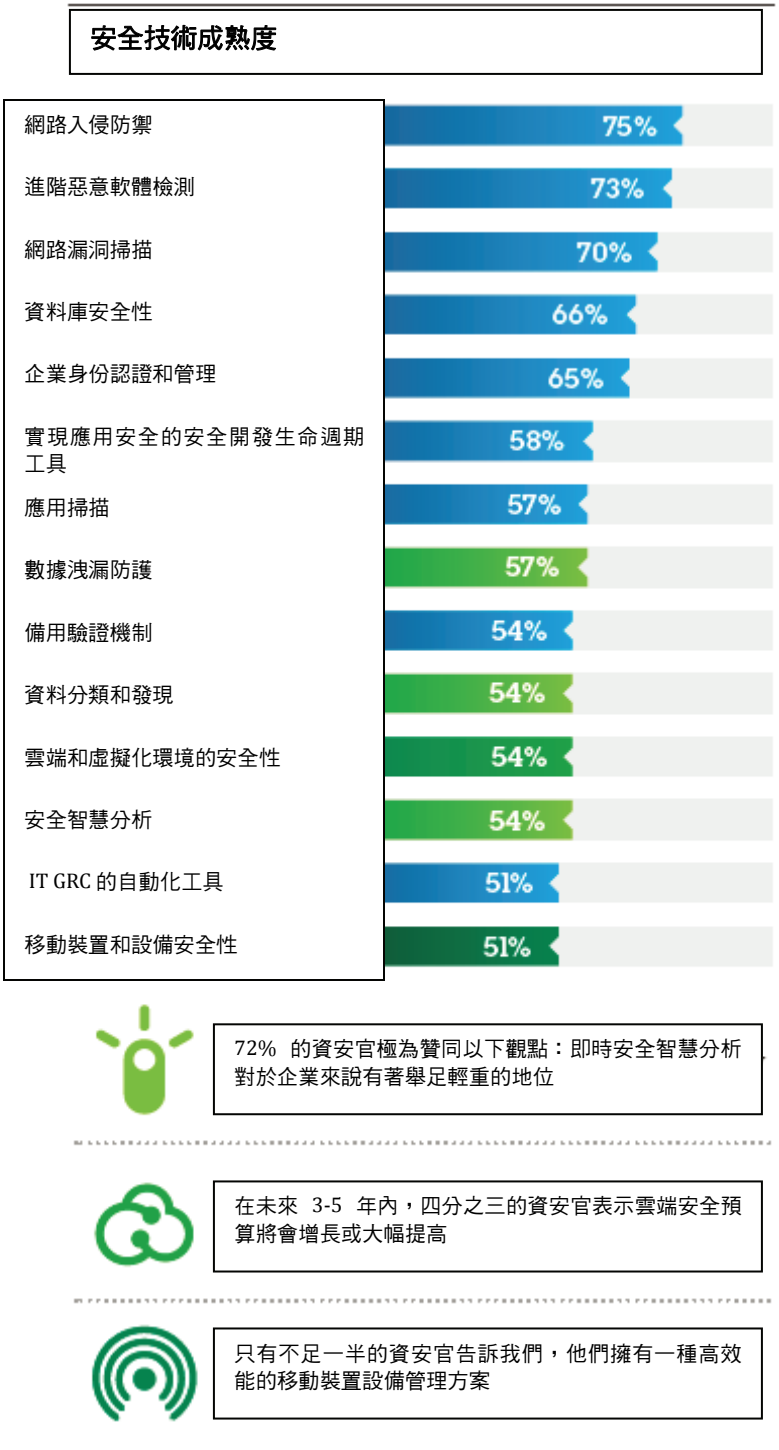


圖 4. 資安主管認為自己在諸多傳統領域中實屬技術純熟，卻在數據分析、雲端和行動裝置等新興領域中缺乏自信。

超過半數的受訪者表示，安全性革新方案日益增長的步伐讓企業無法保持同步發展，導致無法適時滿足其安全需求。受到部署、匯集和改善當前系統的壓力，令資安官難以發展進階技術。因此，在展望未來時，超過半數的受訪者無法設想到超越當前水準的其他安全功能。資安官依然需聚焦於現有的安全技術。

搖擺不定的政府政策

法規、標準與合規性都是所有資安風險主管日常處理的事務。我們從受訪者得知，這一領域將會成為打開希望之門的關鍵鎖匙，但實際上其發展策略尚有諸多變數。

大多數企業的安全願景取決於它的地理位置，因為各個國家的法規和標準不斷在改變。對於全球範圍內運營的企業，法規的多樣性將會成為眾多複雜問題的癥結。

CISO 觀點：降低複雜度，解決法律問題和隱私挑戰

作者：Jamie Giroux
MA XIMUS 公司安全審計副總裁

資訊安全的複雜性將會持續增長，這意味著未來的資安官需要推動簡潔的流程。提升安全技術與法律和隱私領域之間的溝通管道，或者匯集全面性的技術。如果無法瞭解企業內部所有的運作情況，涵括法律、隱私、合約以及協商層面，您便不能確保系統的安全性，並且協調這些各自獨立的部分。

市場和法律領域的多種潛在發展趨勢可能會為未來的資安官提供幫助。供應商服務和產品之間的高度相容性可以支援全方位的安全願景，而單一介面更是能顯示出全盤性的風險。儘管瞭解前端攻擊的位置極具價值，但能夠從伺服器到主機全面性地跟蹤攻擊，才是根本解決之道。如果您眾多的儀錶板和工具集無法統一運作，要實現上述目標謂為困難。

然而，大多數的契機掌握在立法者手中。美國最大的不足之處之一在於沒有一套全國性的標準，在全國範圍內需要平衡各方利益，這需要建立一套安全標準。當您為一家像 MA XIMUS 這樣的企業工作時，會涉及到它分布在各州多種行業的業務，而各州不同的法規往往為相互衝突的根源。

儘管部分資訊安全的未來願景掌握在我們的手中，但某部分發展還需視相關法規的符合程度而定。無論業務流程和相應的法規為何，資安官必須增進自身的技術，以便通過最簡單的方式來達到企業的資安需求。

無論位於何處，似乎都存在一些十分常見的問題：政府會成為阻礙還是會伸出援手？未來是否將會出現或多或少的合作和資安監管透明化？要如何在隱私權與不斷增長的安全性之間達到平衡？

- 超過四分之三的受訪者 (79%) 表示來自政府政策和行業標準的挑戰在過去三年來不斷增加。
- 法規和標準是需要企業投入最大精力予以應對的領域之一，其次為外部威脅。
- 60% 的受訪者無法確定政府是否會在全國範圍還是全球範圍內處理安全監管以及其透明度問題。
- 僅 22% 的受訪者認為政府將在未來三至五年內就對抗網路犯罪的全球性方案達成一致。

打造未來

資安官該採取哪些行動才能防止這些資安風險呢？資安官如何才能避免採取可能會阻礙業務發展的行動呢？他們採取什麼樣的行動才能讓企業對未知風險做好充分準備呢？我們認為資安官可以完成以下四項任務：

增強雲端、行動裝置和資料的安全性

採用傳統安全技術的企業之間存在著成熟度的差異，而這些技術會不斷發展至全新的領域。為了釋放資源致力於開發全新的領域，思考一下您企業的哪些功能足以成熟到實施委託、自動化或者外包業務。

- 企業廣泛運用雲端技術，並且投入大量資源確保其安全性。儘管人們對雲端技術有所擔憂，但它卻是現今企業不可或缺的利器。請確保您的企業充分利用雲端優勢，同時將風險降到最低。
- 行動裝置的安全性往往被忽略。隨著越來越多的裝置不斷互聯化，「物聯網」的願景也已實現，但卻導致盤根錯節的資安問題，唯有增強行動裝置的安全功能為上策。
- 縱使企業生成的資料數據不斷增加，切勿為此感到焦慮，請聚焦於您最關鍵的資產。改善您的方案，增強即時安全智慧和分析功能，以利抵禦不斷增長的外部威脅。

增強教育訓練和領導能力

在問及資安官未來三至五年內預計需要何種技術的訪談中得知：為企業提供培訓和教育訓練以及準備承擔更多的領導責任是最重要的部分。並需憑藉核心業務能力和完善技術知識來承擔日益漸增的職責影響力。

企業與外部合作的契機

由於客戶對企業持有豐富多樣的預期需求，供應商與合作夥伴的風險等級也隨之提升，資安官必須理解如何才能合理顧及他們的資訊生態系統，而不僅是保護他們的企業。這還需各方戮力同心，確定如何清楚明確地評估客戶與企業之間的安全性，即您如何在一個相互合作和廣泛的資訊生態系統中建立互信關係呢？鑒於只有 14% 的受訪者認為標準化的評估和認證資訊安全風險方案在未來三至五年內才能獲得廣泛運用，這要求顯得極為關鍵。如能達成便可將各行業組織作為重要的溝通橋樑。

規劃多種政府政策方案

由於政府是否會對網路安全採取行動存在太多變數，應規劃多種可能性方案。儘管能設想各國政府將會制定更加嚴格的安全標準和方針，以便直接協助企業，但此願景並不會立即實現。

確保您與隱私保密官 (CPO) 和諮詢顧問定期溝通，以深入瞭解可能產生的需求。72% 的受訪者表示客戶隱私日漸成為與企業主管經常談論的話題，然而只有 9% 的資安官將 CPO 視為在企業中的三大策略合作夥伴之一。此外，僅 14% 的受訪者將諮詢顧問列為其三大合作夥伴之一，並向他們採取綜合性方案，收集安全職能範圍以外的建議。

更具影響力的未來

可想而知，就資安官而言，不斷提升的資安風險對公司的安全保護策略更顯艱鉅。但 CISO 也不需對未來趨勢過度恐懼，應化其為提高安全等級的難得契機。在過去十年間不斷提升的威脅等級已鍛鍊出一批卓越的資安官，他們歷久彌新，引領企業向前邁進。通過瞭解業務流程中的資安風險並制定相應的解決措施，便能持續為企業的未來展望提供良好的環境。

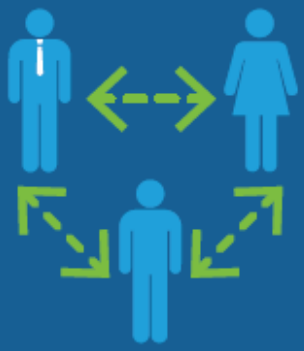
資安官目前可以採取諸多措施，為企業未來打造成功基石。

增強雲端、行動裝置和資料的安全性

資安官切勿仰賴未來技術以解決現有的問題，應當加強現今的安全技術，將差距降至最小。

增強教育訓練和領導能力

技術的增強縱然不可或缺，但純粹的業務能力將會提升資安官日漸增加的影響力。



企業與外部合作的契機

資安官應眾志成城，確定如何建立互信關係，並且清楚明確地評估資訊生態系統的安全性。

規劃多種政府政策方案

與隱私保密官和諮詢顧問定期交流，為資安官瞭解未來需求的關鍵。

作者簡介

Marc van Zadelhoff 是 IBM Security Systems 的全球策略、行銷和產品管理副總裁。在 IT 和安全領域的策略、風險投資、業務開發和市場行銷方面具有 20 多年的豐富經驗。Marc 與全球範圍內的客戶共同合作，為他們提供安全策略的建議，並且開發全新的技術，以便滿足客戶的需求。同時營運 IBM 安全諮詢委員會，管理 25 名頂級 CISO ，為 IBM 提供安全性組合產品的建議。在 IBM 荷蘭分公司出售之前，Marc 也是荷蘭高層團隊中的一員。以下聯繫方式為 Marc 的 LinkedIn 和電子郵件：
marc.vanzadelhoff@us.ibm.com.

Kristin Lovejoy 是 IBM Security 服務部門的總經理，負責 IBM 全球客戶的安全服務和專業安全服務的開發與管理。Kris 也曾擔任 IBM 資訊技術風險和全球 CISO 的副總裁，負責管理、監控並測試 IBM 的全球企業安全和恢復功能。如今，Kris 不但是眾多外部委員會和顧問小組的成員，還是位備受認可的安全、風險、合規性與監管方面的專家，並多次出現在 CNBC、NPR 和 WTOP 等電視節目中。以下聯繫方式為 Kris 的 LinkedIn 和電子郵件：
klovejoy@us.ibm.com.

David Jarvis 是 IBM 應用洞察中心研發團隊和相關事務經理，致力於新興策略與技術領域的業務。也是 IBM 眾多調查研究的合作作者之一，其中包含 2012 - 2014 IBM CISO 評估調查報告。除了職責以外的研發作業，David 還負責提供商業未來展望和革新問題的解決教學。以下聯繫方式為 David 的 LinkedIn 和電子郵件： djarvis@us.ibm.com.

其他參與者

Walker Harrison
Tanya Dhamija
Yana Krasnitskaya
Ellen Cornillon
Sue Ann Wright

台灣國際商業機器股份有限公司
台北市110松仁路7號3樓

2014 年 12 月

IBM應用洞察中心簡介

ibm.com/ibmcai | **ibmcai.com**

IBM應用洞察中心旨在介紹全新的思考、工作和領導方式。依據研究數據，該中心為企業主管提供實用的指南和案例以利實現企業轉型。

WGL03061-USEN-00