

北京CBD論壇開幕 京港綠色金融合作潛力巨大

【大公報訊】記者馬曉芳北京報導：2024北京CBD論壇於6月5日-7日在京舉行。記者從5日舉行的開幕式獲悉，北京CBD集聚了跨國公司114家，數量佔北京市一半，已發展成全球排名第七、中國排名第一的商務中心區。香港中華總商會會長蔡冠深在開幕式上表示，香港和北京CBD應加強綠色金融方面互動，推動更多北京品牌進駐香港，出海國際。作為商務板塊的首場活動，首屆北京CBD跨國公司大會吸引了眾多國際組織與商協會、超百家跨國公司地區總部負責人參會。大會上，聯合國開發計劃署與北京商務中心區管委會簽約，將探索開展零碳CBD實踐及建立綠色發展創新平台。

蔡冠深：期待企業善用香港平台上市

蔡冠深表示，香港是北京最重要經貿夥伴之一，也是北京吸引外資的重要渠道，香港在北京累計設立1萬8千多家企業，投資超過1350億美元，北京對香港累計投資也超過520億美元。他指出，香港

作為國際金融中心，能為北京CBD企業「走出去」擔當跳板和融資平台，「期待更多北京企業善用香港平台上市，持續深化擴大兩地金融市場互聯互通，促進金融人才雙向流動。」他認為，香港和北京CBD可以加強在綠色金融產品和配套服務方面的互動，推動更多北京企業到香港發行更多元化的綠色可持續金融產品。雙方還可探討全面建立招商合作機制，為海外企業拓展京津冀及其他內地市場提供支援，推動更多品牌進駐香港，出海國際。

記者了解到，北京CBD是首都對外開放的重要窗口，歷經20餘年發展，已成為全球排名第七、中國排名居首的商務中心區，現有外資企業超過1萬家，世界500強企業超過200家，聚集了全

球十大律師事務所、十強諮詢公司、十強人力資源公司等。「願與世界交朋友，交世界朋友」，北京市朝陽區委書記文獻在開幕式誠邀國內外企業落戶北京CBD，期待與各國企業共享機遇，共同發展。

在首屆北京CBD跨國公司大會上，聯合國開發計劃署與北京商務中心區管委會簽約，將探索開展零碳CBD實踐及建立綠色發展創新平台，提升區域可持續發展目標（SDGs）和綠色發展意識。新加坡國際仲裁中心和北京商務中心區管委會簽約，將共同向區內公司和投資者推廣國際仲裁以解決跨境爭議，雙方將交流關於國際仲裁最新發展信息和理念，商議現存及潛在合作渠道。



▲本屆北京CBD論壇打造北京首個利用市民碳普惠減排實現碳中和的國際論壇。

首設國際論壇 倡導綠色低碳生活

同時，本屆北京CBD論壇打造北京首個利用市民碳普惠減排實現碳中和的國際論壇。北京商務中心區管理委員會主任陳黛介紹，該論壇將通過使用北京市「綠色生活季」產生的市民碳普惠減排量，實現碳中和，並通過數字化手段減少論壇紙質材料使用，採用環保包裝小支飲用水等措施減少碳排放，積極倡導與會嘉賓選擇綠色出行，感受低碳生活。

據悉，近年來，北京CBD持續推進高質量發展。2023年CBD功能區稅收收入近1300億元（人民幣，下同），同比增長10%；新註冊企業超過12000家，同比增長超過20%。功能區稅收過億樓宇達145座，較上年同期增加14座；過10億樓宇20座，較上年同期增加1座；過100億樓宇1座，高品質樓宇貢獻突出。截至目前，CBD功能區跨國公司地區總部達到114家。

國安部：警惕雲端網攻 密件不得上網

公布「違規存儲」案例 指出境外間諜無孔不入

雲存儲作為一種新興網絡存儲技術，近年來，隨着網絡「雲」功能不斷普及，「雲端」數據成為境外間諜情報機關關注的重點。中國國家安全部5日發文指出，他們通過網絡攻擊、植入木馬等各種手段，試圖竊取中國敏感信息和涉密數據，給個人隱私和國家安全造成嚴重威脅。然而，一些單位和個人保密意識淡薄、僥倖心理作祟導致雲存儲失洩密，給境外間諜情報機關網絡竊密帶來可乘之機。國安部提醒，「雲」上存儲需脫密，「雲」端防護需加強，密件不得上網，確保國家秘密安全。

強化民眾保密意識：上傳留痕無法刪除

【大公報訊】記者趙一存北京報導：「某省直單位工作人員李某，利用自己的網盤私自保存機密級涉密資料」「某縣級機關工作人員楊某為方便工作，擅自將收集到的包括1份機密級文件、2份秘密級文件在內的大量文件資料上傳至某網盤，並回家下載使用」「某縣領導幹部方某，在未經保密審查的情況下，要求辦公室工作人員將包含1份秘密級文件在內的15份文件材料上傳到某網盤，並設置為分享模式，供有關人員瀏覽」……國安部介紹，近年來，國家保密行政管理部门公布多起違規雲存儲國家秘密的案例，相關責任人在未經保密審查的情況下，將涉密資料上傳至網絡，事後均依紀依法受到嚴肅問責處理。

應堅守「涉密不上網 上網不涉密」底線

國安部指出，上述案例反映出，使用者保密意識淡薄、僥倖心理作祟是導致雲存儲失洩密的重要原因。黨政機關和涉密單位工作人員應始終繃緊保密之弦，規範使用互聯網行為，嚴禁通過網絡、手機、雲盤等存儲、處理、傳輸、談論涉密及敏感信息，堅決防範失洩密事件發生，確保國家秘密安全。「『雲』端防護需加強。」國安部提醒，在日常工作中使用互聯網處理個人事務時，面對雲存儲賬戶易遭非法網絡攻擊等風險，需從操作層面加強相應安全防護。相關人員和單位應堅守「涉密不上網、上網不涉密」底線，嚴禁通過互聯網上傳、存儲、處理涉密信息。做好敏感信息保護。個人隱私或敏感信息，盡量不要上傳至雲端，如必須上傳，可將重要信息設置為「禁止分享」。敏感信息通過U盤、光盤等與外界有物理隔離的介質進行備份。

同時，要對網盤內容進行加密。對需要分享的雲存儲數據，設置「提取碼」和「分享時效」，減少信息洩露可能性。還要及時維護賬號密碼。將賬號與手機、微信、郵箱等綁定，每次登陸時通過動態驗證碼進入；設置較為複雜的密碼，並經常修改密碼，發現賬號異常時及時調整密碼。

此外，很多服務商為用戶提供將照片、通訊錄、數據等信息定期自動備份到雲端的功能，要慎重選擇「自動備份」這個功能，可通過手動方式，有選擇地對相關數據進行備份。而在網絡化、數字化、智能化時代，普通民眾和相關單位亦須提高保密意識，強化保密觀念，堅決維護國家網絡安全、數據安全。

在北京一家部委直屬單位工作的小陳坦言，自己感覺「後怕，萬一因為我導致國家秘密洩露，我都無法原諒自己。」小陳表示，今天回家第一件事就是檢查雲存儲內容，「設置密碼、設置提取碼、分類上傳，以後真是要好好學習保密的法律法規了。」

「現在才知道，只要上傳到雲端過，留下過痕跡，哪怕刪除也沒用。」河北石家莊的公司職員白先生坦言，保密的知識和保密的意識非常重要。



▲工作人員在中國聯通貴安數據中心對微模塊機房運行狀態進行巡檢。新華社

「雲」端防護 注意事項

嚴禁涉密信息上網

● 相關人員和單位應堅守「涉密不上網、上網不涉密」底線，嚴禁通過互聯網上傳、存儲、處理涉密信息，嚴守國家秘密和工作秘密。

做好敏感信息保護

● 個人隱私或敏感信息，盡量不要上傳至雲端，可將重要信息設置為「禁止分享」。敏感信息通過U盤、光盤等與外界有物理隔離的介質備份。

進行網盤內容加密

● 大多數雲存儲網盤都提供文件加密功能，對需要分享的雲存儲數據，設置「提取碼」和「分享時效」，減少信息洩露可能性。

及時維護賬號密碼

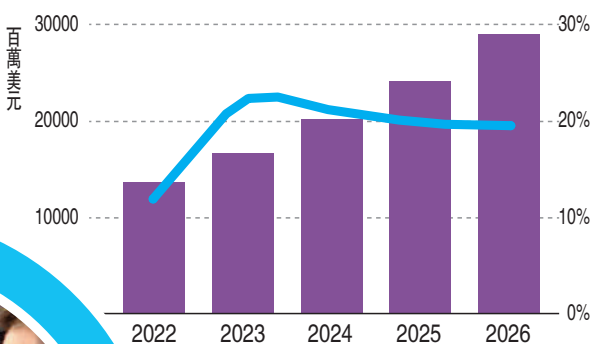
● 將賬號與手機、微信、郵箱等綁定，每次登陸時通過動態驗證碼進入；設置較為複雜的密碼，並經常修改。

謹慎選擇「自動備份」

● 很多服務商為用戶提供將照片、通訊錄、數據等信息自動備份到雲端的功能，應慎重選擇該功能，可通過手動方式，有選擇地備份數據。

大公報記者 趙一存整理

中國網絡安全市場 支出預測 (2022-2026)



▲與會者在2023中國互聯網大會的中國移動展台上了解雲電腦技術方案。新華社

國產量子計算機 攻守兼備

儲備技術

隨着全球開展「量子算術」競賽，現有「數據加密防線」缺口乍現，量子領域的「攻」與「守」成為業界一大焦點。早前，中國第三代自主超導量子計算機「本源悟空」成功裝備國內首個PQC「抗量子攻擊護盾」——PQC（Post Quantum Cryptography後量子密碼）混合加密方法。這將使「本源悟空」更好抵禦其他量子計算機的攻擊，確保運行數據安全。本源悟空「鑄盾」，意味着中國自主超導量子計算機可以「攻守兼備」，成為中國數據安全新技術應用的重要探索。

安徽省量子計算工程研究中心副主任賈猛漢介紹，「本源悟空」此次上載的PQC「抗量子攻擊護盾」由本源量子計算科技（合肥）有限公司研發，是內地首次實際應用，邁出攻守兼備新階段。新華社、中國科學報

曝光網攻手法

供應鏈攻擊：MOVEit Transfer數據盜竊

● 文件傳輸服務MOVEit的漏洞已經導致2706個組織遭到（勒索軟件）攻擊，超過9300萬人的個人數據被洩露。攻擊者可利用MOVEit Transfer服務器曝出的漏洞入侵並下載用戶存儲的數據。

間諜軟件攻擊：三角測量

● 卡巴斯安全研究人員鮑里斯·拉林(Boris Larin)披露了iPhone歷史上最複雜的間諜軟件攻擊——三角測量(Triangulation)的技術細節。該攻擊技術自2019年以來被用於監聽iPhone用戶。2023年6月俄羅斯政府首次曝光了大規模的iPhone後門活動，攻擊者利用三角測量攻擊感染了俄羅斯外交使團和數千名使館工作人員的iPhone。

醫療數據洩露：23andMe數據洩露

● 2023年10月基因檢測提供商23andMe遭遇撞庫攻擊，導致重大數據洩露，690萬用戶的數據被洩露。攻擊者試圖出售竊取的數據，但沒有買家接手，最終黑客在論壇上洩露了100萬德系猶太人和400萬英國居民的個人數據。其中包括550萬DNA尋親功能用戶和140萬家譜功能用戶。央視網

話你知

《商用密碼管理條例》

在保障網絡安全的各種手段和技術中，密碼是目前世界上公認的最有效、最可靠、最經濟的關鍵核心技術，相當於網絡安全DNA。商用密碼廣泛應用在金融、通信、公安、稅務等國民經濟發展和社會生產生活的眾多領域，用於保護數據交互和存儲安全。新修訂的《商用密碼管理條例》去年7月1

日起施行。條例明確，國家加強商用密碼人才培養，建立健全商用密碼人才發展體制機制和人才評價制度，鼓勵和支持密碼相關學科和專業建設，規範商用密碼社會化培訓，促進商用密碼人才交流，並鼓勵企業、社會團體和教育、科研機構等參與商用密碼國際標準化活動。央視網