標書少提網安 保密體系不全

專家總結三弊：業者缺統一認證 招標要求待提高 外判欠計分問責

特區政府部門近期接連出現網絡安全事故，有資訊保安專家指出，事件反映的不光是部門問題，更是資訊科技行業整體問題，凸顯行業三大弊病：全球有各類型網絡安全標準，但香港未有統一的資格認證，從業人員難免良莠不齊；以往招標合約對網絡安全、個人私隱的着墨不多，但隨着市民愈發關注私隱，標書必須提高對網絡安全的要求。他認為，香港資訊科技外判制度缺乏問責制，建議特區政府效法建造業外判制度設立計分制，使服務未符預期的承辦商日後難參與投標或中標，促使承辦商更重視網絡安全。特區政府資訊科技總監辦公室在回覆香港文匯報查詢時表示，政府目前有機制監察承辦商表現，有權暫停表現不達標的承辦商競投新的報價邀請，直至其表現有所改善（**見另稿**）。

◆香港文匯報記者 張弦、王儅鑽研

本身從事資訊科技的香港特區立法會議員吳傑莊向香港文匯報表示，資訊安全範疇廣泛，包括搭建系統、防火牆等，「有些大判會購買系統交付給政府，該系統會經過第三方測試，之後整個招標過程就通常不會再睇外判商或第三方有否符合國際標準或水平，而是看他們之前做過什麼項目、工程師有無通過國際認證考試等。」

或有部門不重視政府要求

在招標準則方面，他指出，政府部門一般會進行技術評分、價錢評分，並視乎部門實際情況決定有關評分的佔比，有些着重技術，有些更着重價錢。

部分資料外洩事故由部門內部運營過程中出現，但其實特區政府內部建議要求每一兩年委託第三方公司進行黑客攻擊系統測試，找出漏洞及需要改善的地方，相隔幾個月更需要更新系統，但近年發生多次的資料外洩事故，相信是部門不重視網絡安全導致。

近期事故外判非專攻數據處理

綜合資訊科技界的意見，近期的網絡安全事故反映香港資訊科技行業的普遍問題。「中港網絡安全協會」創會主席葉青陽指出，今次「出事」的外判承辦商，不少並非主力從事數據處理，他解釋資訊科技範疇廣闊，網絡安全是其中一範疇，需要專業

香港大學資訊保安及密碼學研究中心計算機科學系副教授鄒錦沛向香港文匯報表示，特區政府招標網絡服務商，標書上會列明要設計什麼系統、所需功能、需要的後續服務，參與招標的服務商必須提供合乎要求的資格，包括證書、業績、公司經營狀況等，只要符合所有要求，那麼價低者得無可厚非，畢竟要節約公帑。

明確安全級別與投入更多成本

「問題是政府的標書，有無列明所要求的網絡安全級別、內容。」鄒錦沛解釋，以往社會上對個人隱私、網絡安全方面欠缺足夠重視，而政府招標網絡服務商，也更重視所設計系統的功能性，可能對保密級別、網絡安全、個人隱私保護方面要求不足。

他說：「如果標書列明要做到一定保密級別，例如要進行反網絡滲透，以及個人隱私保護，那麼網絡服務商當然會按要求去做，以達到標書標準。如果沒要求，那麼就不會做這些額外設計，以節省成本。畢竟網絡安全除了系統設置會複雜很多，還需要定時測試，及時補足安全漏洞，需要額外的工作時數，亦需向政府收取相關費用。」

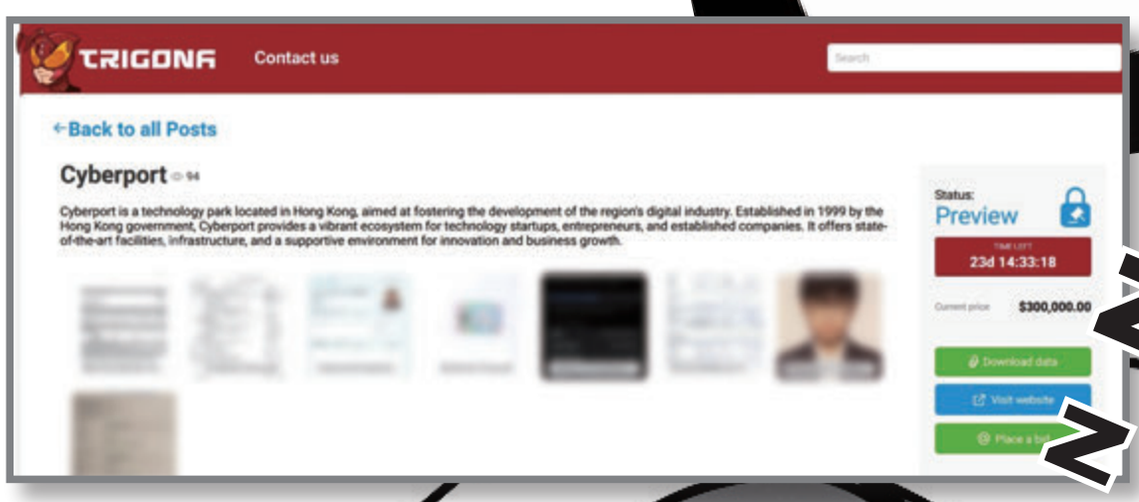
鄒錦沛建議特區政府全面檢視各政府部門的網絡安全，制定相應的安全級別，並向各部門網絡服務商諮詢，檢查並補足網絡安全漏洞。

資科辦：招標非純求價低 定期評核承辦商保障質量

香港文匯報訊（記者 費小燁）特區政府部門出現的網絡安全事故，部分涉及外判商，令人質疑外判在缺乏問責下質素良莠參差。特區政府資訊科技總監辦公室昨日在回覆香港文匯報查詢時表示，政府各部門在發展資訊科技系統時，會根據《政府物料供應及採購規例》，透過公平、公開及具競爭性的程序，採購物有所值的貨品和服務。在衡量採購是否物有所值時，採購部門會通盤考慮購買貨品和服務所投入的資源，是否取得最佳成效，而非單純追求「價低者得」。

在監管服務承辦商方面，資科辦表示，已發出「外判資訊科技項目管理執行指引」，以協助各部門改善管理及監督承辦商的工作。資科辦不評論個別情況，一般而言如承辦商的表現未能達到合約上列明的服務要求標準，部門會按個別合約訂明的條款適時採取行動。

由資科辦統籌、合約金額上限為2,000萬元的《優質資訊科技專業服務常備承辦協議》亦設有承辦商表現監察制度，就每份在該協議下所批出的合約，相關部門會每6個月及於合約完成後，評核承辦商的表現。協議下亦有機制暫停表現不達標的承辦商競投新的報價邀請，直至其表現有所改善。



▲去年8月，數碼港遭黑客入侵，黑客將資料上傳到網上販賣。 資料圖片

◀私隱署早前公布調查報告指，消委會在遭受黑客入侵的事件中有5項缺失，當中部分缺失甚至包括人為錯誤或疏忽因素。 設計圖片

議員：隱私遭洩難追責 促確立罰則與索償機制

香港文匯報訊（記者 張弦）香港的公私營機構近年不時發生網絡安全事故，或導致部分市民資料外洩，甚至令不法之徒有機可乘、設下騙局，導致資料持有人蒙受經濟損失。有立法會議員及網絡安全專家均認為，香港現行法例並沒有確立機構或公司的網絡保安責任，資料外洩的當事人只能透過民事訴訟向機構追討責任，但取證困難，往往徒然。對此，專家建議針對資料外洩建立罰則，以及引入責任制，加強保障受害者，例如制定民事索償機制。

民事追討失職機構成本過高

香港特區立法會議員吳傑莊表示，最近爆出的幾宗網絡安全事故，令資料當事人感到無奈，例如數碼港事故，有市民7年前的資料被暴露在網上，然而當事人若要追討損失，只能自掏腰包，透過民事訴訟方式向財團機構追討，「要證明資料被外洩，同時證明到因該個機構洩露其數據而導致損失，其間或需花不菲訟費。」

他認為有必要在法律上加強資料外洩罰則，以及制定民事索償機制。香港有鄰近地區規定，機構或企業一旦導致資料外洩，要承擔法律責任及定額賠償，例如新加坡、他認為這樣的做法令公司或部門在保護數據上投入更多資源，「若有明確的罰則，相信所有公司會重視。」舉例而言，美國有網絡安全保險，公司若已盡其責任保障資料，但仍被攻擊而洩露資料，可以通過保險賠償公司及受害者。

資安需設問責機制

同時，香港現行法例下機構或企業一旦導致資料外洩，只要依私隱專員公署要求進行修正或改善，就無須負上刑責，吳傑莊認為阻嚇力不足。例如有公司被查出做假賬，公司的會計師便有責任；樓宇出現意外，證明工程師有疏忽，亦會被追究，資訊安全方面亦應該有類似問責機制。

他舉例說，倘有網絡保安負責人檢視新開發系統後簽署確認，日後若發現有關系統存在重大網絡保安漏洞，負責人就要承擔責任，以提高阻嚇力，「可以分短中長期去做，否則頻繁出現資料外洩事故，對香港建立智慧城市沒有好處。」

「中港網絡安全協會」創會主席葉青陽指出，目前發生資料外洩的情況後，涉事機構或部門只須盡快通報私隱專員公署及受影響者，就沒有其他處罰，故建議在數據處理方面應該有處罰機制，「例如出現奪命工業意外，判頭可能會被判誤殺罪，網絡安全亦應該有類似的機制。」他又建議修訂法例，讓資料持有人循獨立的索償機制追討權益。

專家倡發牌規管 確保從業員質素

香港文匯報訊（記者 王儅）香港大學資訊保安及密碼學研究中心計算機科學系副教授鄒錦沛表示，外國有各類型網絡安全標準，香港目前從事網絡安全的專業人員，往往接受過不同的系統培訓，而香港並無統一的資格認證，也沒有發牌制度，建議特區政府引入資格認證制度，例如考核發牌等。

◆鄒錦沛倡議成立網絡安全人員學會。 港大圖片

鄒錦沛：招標未設有效扣分制度

他認為，引入資格認證制度可確保人員的質素，保障市民的私隱，「既然社會越來越重視隱私保護，重視網絡安全，也許政府需要全面考察各類型網絡安全標準，要考慮認可哪些標準，以及制定從業人員的專業資格。」

目前，特區政府資訊服務商的招標制度，未有對不合格承辦商實施扣分制，以及建立黑名單，以確保行業素質。鄒錦沛認為對曾引起網絡安全事故，或不負責的承辦商，特區政府應加以問責，「網絡安全人員需要有專業操守，只要接手維護一套系統，就必須確保系統正常運作，以及確保網絡安全。就如電梯維護，不能因為更換承辦商就將責任推卸係之前一手的問題，那會出人命的。」

鄒錦沛建議參照其他專業行業設立「網絡安全人員學會」，以明確專業資格標準，向業內人員實施考核發牌制度，以及紀律處分：「網絡安全是很專業的行業，有必要成立學會統一管理，中止行業亂象，提升整體行業水平，進而全面提升香港網絡安全，最大限度降低大規模洩密風險。」