Hong Kong’s Financial Cybersecurity Solutions at a Crossroads
香港金融網絡安全方案何去何從

The recent incident involving US tech firm CrowdStrike sent shockwaves through the global financial community. While many parts of the world floundered with their airports, hospitals, and banks suddenly unable to operate, computers across Mainland China and the organisations relying on them worked perfectly. This CrowdStrike incident brought to the forefront a crucial question: Why doesn’t Hong Kong, a global financial powerhouse, utilise more Mainland Chinese and home-grown cybersecurity systems?

最近涉及美國科技公司CrowdStrike的事件令全球金融界震驚。世界各地多處機場、醫院和銀行忽然停止運作，眾人不知所措之際，中國內地的電腦設備和使用這些設備的機構如常運作。這次CrowdStrike事件帶出了重要問題：為什麼香港這個環球金融重鎮沒有使用更多內地和本地開發的網絡安全系統？

In the wake of what may be the most expensive tech outage in history, Hong Kong finds itself at a critical juncture in its cybersecurity strategy, prompting Hong Kong's Digital Policy Office to call for a comprehensive plan to address potential worldwide computer system shutdowns. The answer to this question could have far-reaching implications for Hong Kong's banking and finance sector, as well as its position as an international financial hub.

The recent CrowdStrike outage serves as a stark reminder of the vulnerabilities inherent in relying heavily on foreign technology providers. On 19 July 2024, a serious bug in an update to CrowdStrike's Falcon Sensor software took down 8.5 million Microsoft Windows systems, many of which disrupted critical operations within the aviation, healthcare and banking sectors. The CrowdStrike outage impacted some of the largest and best-known international banks that operate in Hong Kong. For the banking sector, such outages can have catastrophic consequences, potentially disrupting trading activities, payment systems and customer services. The costs of this single outage are projected to be in the billions of US dollars.

The CrowdStrike incident should be a wake-up call. Hong Kong's financial institutions, like their global counterparts, have increasingly relied on complex cybersecurity solutions provided by international tech firms. These solutions supposedly offer cutting-edge protection against evolving cyber threats, but they also create an opaque dependency on external providers. The CrowdStrike incident highlights the potential risks associated with this dependency, particularly when it comes to critical infrastructure and sensitive financial data. And this is before the geopolitical risks of using US cybersecurity technology in Hong Kong, Macao and Mainland China are considered. On one side is the potential of "backdoors" (a means of bypassing an organisation's existing security systems), or the chance that a US vendor might suddenly stop supporting their technology. A number of overseas cybersecurity firms have already taken this step.

這次技術故障，可能是有史以來最昂貴的一次。經此一役，香港的網絡安全策略來到關鍵時刻，驅使香港數字政策辦公室呼籲制訂全盤計劃，應對全球電腦系統停運的可能。這問題的答案，對香港的銀行金融業，以至國際金融中心的地位可能有深遠影響。

最近CrowdStrike故障事件，正好提醒我們過度倚賴外國技術供應商有欠穩妥。2024年7月19日，CrowdStrike的Falcon Sensor軟件更新版有嚴重漏洞，導致850萬個微軟視窗系統故障，擾亂了航空、護理和銀行業的關鍵運作。是次故障影響了許多在香港營運的最大和最知名的國際銀行。這種故障可為銀行界帶來災難性後果，有可能干擾買賣活動、支付系統和客戶服務。這次單一故障的代價估計達數以十億美元。

> *“Hong Kong’s financial institutions, like their global counterparts, have increasingly relied on complex cybersecurity solutions provided by international tech firms.”*

The need for true multi-layered cybersecurity

In the wake of the CrowdStrike incident, Hong Kong’s Digital Policy Office’s call for a plan to tackle global computer system shutdowns is not just timely, but also essential. As a global financial centre, Hong Kong cannot afford to be caught off guard by system-wide failures, especially the failure incidents caused by problems stemming from a single overseas technology vendor. The CrowdStrike incident underscores the need for a more diversified approach to cybersecurity; one that, at a minimum, incorporates a mix of international, regional and local solutions. Most organisations in Hong Kong - even if they currently take a multi-layered approach to cybersecurity - install systems from several vendors which are still based on underlying overseas technology, which can be prone to the same vulnerabilities, bugs, and potentially, backdoors.

By not relying solely on a single technology provider, or geopolitical bloc, for cybersecurity solutions, Hong Kong’s financial institutions can mitigate the risks associated with provider-specific outages, vulnerabilities and backdoors. Such a multi-faceted approach, incorporating various technologies and providers, can create a far more robust defence against cybersecurity threats and system failures. At the same time, it would also significantly reduce the geopolitical risks posed by governments. It should be remembered that one of the largest ransomware attacks in history, the WannaCry ransomware attack in May 2017, was propagated using “EternalBlue,” an exploit developed by the United States National Security Agency (NSA) for Microsoft Windows systems.

Indeed, as far back as December 2013, Brad Smith, Microsoft’s EVP of Legal and Corporate Affairs, labelled the American Government as an “advanced persistent threat.” This is a term used in cybersecurity to describe a team of intruders

CrowdStrike事件應是一個提醒。與全球的金融機構一樣，香港的金融機構日益倚賴由國際科技公司提供的複雜網絡安全方案。面對持續演變的網絡威脅，這些方案應能提供最先進的保護，但也造成對外間供應商的倚賴。CrowdStrike事件突顯了這種倚賴的潛在風險，特別是涉及關鍵基礎設施和敏感財務資料時，風險尤大。在香港、澳門和內地使用美國的網絡安全技術，更要考慮地緣政治風險。一方面，方案設計可能有「後門」（即有方法繞過機構現有的安全系統）；另一方面，美國供應商可能突然停止提供技術支援。一些海外網絡安全公司已經採取了這一措施。

需要真正多層的網絡安全

CrowdStrike事件之後，香港數字政策辦公室呼籲制訂處理全球電腦系統停運的計劃；這呼籲不僅合時，也是必要之舉。作為環球金融中心，香港不能被廣泛系統故障殺個措手不及，承受尤其是由單一海外科技供應商的問題引起的事故。CrowdStrike事件突顯了有需要以多元化的方式處理網絡安全事宜，起碼應結合國際、地區和本地的方案。香港大部分機構即使已採用多層方案處理網絡安全，並安裝由多家供應商提供的系統，但其基礎技術仍主要來自海外，可能存在相同的弱點、漏洞或後門。

“與全球的金融機構一樣，香港的金融機構日益倚賴由國際科技公司提供的複雜網絡安全方案。”

that establishes an illicit and persistent presence on a network in order to steal highly sensitive confidential data. As cybersecurity crimes become more prevalent and sophisticated, it becomes increasingly important that Hong Kong’s financial institutions, and indeed all institutions, raise the level of focus on understanding and mitigating these risks. For example, multi-layered cybersecurity which relies on vendors which in turn all rely on one operating system, or one technology platform, or come from one geopolitical bloc, is not truly multi-layered.

The idea behind multi-layered cybersecurity is to reduce dependency and to remove a single point of failure. But if hidden in each layer is the same bug, the same vulnerability, or the same backdoor, then the risk of being successfully attacked has not been reduced at all. Instead, there will likely be a sense of false security permeating each organisation, which will render it even more vulnerable to becoming the next victim of a cyberattack. As global tensions rise, having access to diverse cybersecurity options could provide strategic advantages. Not just technological alignment, but cultural and linguistic alignment, is needed, which means that Mainland Chinese and home-grown cybersecurity solutions may be better tailored to the specific needs and nuances of the Chinese-speaking world.

要是不倚賴單一科技供應商或地緣政治板塊提供的網絡安全方案，香港的金融機構便可減少因個別供應商相關的故障、弱點和後門所引致的風險。這種結合不同技術和供應商的多層方式，可更穩妥地防範網絡安全威脅和系統故障，同時大大降低由政府引起的地緣政治風險。須知道歷來最大規模勒索軟件攻擊之一 - 2017年5月的WannaCry勒索軟件攻擊，就是透過“EternalBlue”傳播，而這正是由美國國家安全局針對微軟視窗系統而開發的漏洞利用程式。

的確，早在2013年12月，微軟的法律及機構事務執行副總裁Brad Smith已經指出，美國政府是「高級持續性威脅」。這是個網絡安全用語，指的是一組入侵者隱匿而持久地入侵電腦網絡，以盜取高度敏感的機密資料。網絡安全罪行日趨普遍和複雜，香港的金融機構以至所有機構都應更重視了解和減緩這些風險。例如，雖然多層網絡安全方案由多個供應商提供，但若這些供應商全都使用同一個運作系統、技術平台，或者來自同一地緣政治板塊，該方案便不是真正多層。

多層網絡安全方案的理念，是減低倚賴性，避免單一來源的故障。但若每層背後都有同一漏洞、弱點或後門，那麼遭成功攻擊的風險便並沒有減低，反而可能使機構會有安全的錯覺，使機構更容易成為網絡攻擊的下一個對象。環球局勢日趨緊張之際，採用多元的網絡安全方案可在策略上佔優。不僅要在技術層面保持一致，文化和語言上的一致性也有其必要，內地和本地開發的網絡安全方案可能更切合華語世界的特定需要，和考慮到有別於其他族群的細微之處。

Local cybersecurity platforms could also mean reduced costs and improved support

There are other clear advantages to leveraging local cybersecurity platforms. Costs, for example, can be significantly reduced. Overseas cybersecurity vendors are demonstrably charging a lot more for their various services, despite obvious quality control issues impacting their clients worldwide. It is not a problem unique to CrowdStrike; the list of cybersecurity vendors (including Fortinet, Cisco, Juniper, Netgear and Barracuda) that have been infiltrated by hackers and criminals to exploit critical vulnerabilities in their platforms is alarming. Yet organisations are projected to pay USD58 billion for cybersecurity from these vendors, while *Cybercrime Magazine* estimates that by 2025, cybercrime will cost the world USD10.5 trillion annually. In financial terms this could be considered a poor return on investment. Using local cybersecurity vendors, on the other hand, could provide long-term savings which could be realised through reduced dependency on expensive international solutions.

In addition to improving security and reducing costs, moving to local cybersecurity platforms also allows for vastly improved local support. There is a Chinese saying which

本地網絡安全平台成本較低和支援較佳

善用本地的網絡安全平台還有其他明顯的好處，例如可以大大降低成本。海外網絡安全供應商的多項服務收費顯然遠高於本地供應商，然而卻有明顯的質量控制問題，影響全球客戶。這問題並非CrowdStrike獨有，眾多網絡安全供應商（包括Fortinet、Cisco、Juniper、Netgear及Barracuda）均已被駭客及罪犯滲透，利用他們的平台上的關鍵弱點，情況令人擔憂。可是，估計各機構向這些供應商支付580億美元換取網絡安全服務，而據Cybercrime Magazine估計，到2025年，網絡犯罪每年會令全球損失105,000億美元。從財務的角度看，這方面的投資回報可說並不理想。另一方面，選用本地的網絡安全供應商可減少對昂貴外地方案的倚賴，長遠而言節省成本。

除了提升安全度和降低成本外，改用本地的網絡安全平台還可享受更佳的本地支援。俗語有云，遠水不能救近火。香港已經有世界級的安全業務中心方案，可以全年24小時隨時隨時為客戶提供支援。此外，本地供應商更能了解和處理香港獨有的網絡安全需要和法規要求。

> “By fostering local innovation, collaborating with regional partners and investing in talent development, the city is taking proactive steps to enhance its cybersecurity posture.”

is very apt: “Water which is far away, cannot save you from fire which is nearby.” World-class security operations centre solutions are already operating in Hong Kong that offer immediate support to clients around the clock, 365 days a year. Furthermore, local vendors are better positioned to understand and address Hong Kong’s unique cybersecurity needs and regulatory requirements. Hackers, scammers and criminals are now localising and customising cyberattacks to maximise their impact and effectiveness. In terms of protection, a local cybersecurity vendor is far more likely to be aware of the nuances of the local environment and marketplace, and as a result be able to offer effective solutions.

It is also not just a choice between global versus local cybersecurity vendors and services. Both can (and should) be measured against respected international standards. For example, a Managed Cybersecurity Service Provider running a Security Operations Centre 24/7/365, should be properly certified against Quality Management (ISO 9001), IT Management (ISO 20000), IT Security Management (ISO 27001) and Risk Management (ISO 31000), and audited standards, overseen by a primary consultant such as SGS Switzerland or TÜV Germany. The Payment Card Industry Data

駭客、騙徒和罪犯正逐漸本地化，精心設計符合本地情況的網絡攻擊，達到最大影響和最佳效果。從保障的角度看，本地的網絡安全供應商更能了解本地環境和市場的細微差異，從而提供更有效的方案。

在作考慮和決策時，也不僅是外地和本地網絡安全供應商和服務之間的考慮。不管是外地還是本地供應商，都應以認可的國際標準來衡量。例如，營運24/7/365的安全業務中心的網絡安全服務供應商便應取得質量管理(ISO 9001)、資訊科技管理(ISO 20000)、資訊科技安全管理(ISO 27001)、風險管理(ISO 31000)和審核標準等方面的認證，並由主要顧問如瑞士SGS或德國TÜV等監督。假如機構業務牽涉Visa、MasterCard和American Express的運作，那麼符合支付卡行業資料安全標準也至關重要。有了這些認證，加上內地日益獲公認的認證，本地銀行和金融機構便可左右逢源。香港開發的網絡安全技術已取得全球專利，並在世界各地獲取超過170個行業、媒體和政府獎項；Network Box善用這些技術，現正為超過2,500家機構提供網絡安全服務。

Security Standard is also critical if an organisation needs to comply with Visa, MasterCard and American Express. With such certifications, as well as increasingly recognised certifications from Mainland China itself, local banks and financial institutions can enjoy the best of both worlds. Leveraging world class cybersecurity technology developed in Hong Kong, which have achieved global patents and won over 170 industry, media and governmental awards across the world, Network Box is currently protecting more than 2,500 organisations.

The future of cybersecurity is already here

The recent CrowdStrike incident serves as a catalyst for Hong Kong to reassess its cybersecurity strategy. If organisations in Hong Kong want to leverage it, the future of cybersecurity is already here. The potential shift towards a more diverse cybersecurity strategy, incorporating local solutions, could have significant positive implications for Hong Kong's banking and finance sector. While the city's reliance on international solutions may have served it adequately in the past, the obvious benefits of incorporating Mainland Chinese and home-grown cybersecurity systems are now far too significant to ignore. For Hong Kong's banking and finance sector, this shift represents both a challenge and an opportunity. Those institutions that can successfully navigate this transition, balancing international standards with local innovation, stand to gain a significant competitive advantage. They will be better positioned to withstand global disruptions, tap into new markets, and contribute to Hong Kong's continued success as a world-leading financial hub.

The enhanced security posture, leveraging a multi-faceted and multi-layered approach that combines international, Mainland and local Hong Kong solutions, could create a far more robust defence against hackers, criminals and cyber threats. The advantages gained by banks that successfully integrate diverse cybersecurity solutions may provide a critical competitive edge, in terms of both resilience and adaptability. Hong Kong can turn a potential vulnerability into strength, ensuring its place at the forefront of global finance for many years to come.

Local technological advancement is a fact. Mainland China and Hong Kong have both made significant strides in cybersecurity technology, with some solutions rivalling or surpassing their Western counterparts. Increased use of local and Mainland Chinese solutions could spur further development of a specialised cybersecurity workforce

網絡安全的未來就在眼前

最近的CrowdStrike事件促使香港重新評估自身的網絡安全策略。香港的機構如欲把握這時機，網絡安全的未來就在眼前。改用較多元的網絡安全策略，納入本地開發的方案，對香港的銀行金融業可能產生重大的正面影響。香港向來倚賴外地方案，這在以往雖然足夠，但兼用內地和本地開發的網絡安全系統則有其明顯好處，不容忽視。對於香港的銀行金融業來說，這轉變既是挑戰，也是個機會。能成功過渡，既遵守國際標準又重視本地創意的機構，必能取得重大的競爭優勢，較能抵禦全球性的干擾，進入新市場，有助維持香港作為世界領先金融中心的地位。

利用多面和多層的安全措施，兼用外地、內地和本地的方案加強安全性，可大大增強抵抗駭客、罪犯和網絡威脅的能力。成功採用多元網絡安全方案的銀行，可從中得益，並享有關鍵的競爭優勢，能靈活應變。由此，香港可把潛在的弱點轉化為強項，往後多年持續站在環球金融業的前沿。

> “藉著促進本地創新、與地區夥伴合作以及資於人才培訓，香港正積極提高其網絡安全性。”

in Hong Kong. Closer alignment with Mainland China’s cybersecurity systems by Hong Kong’s banking and finance sector could ultimately facilitate smoother cross-boundary financial operations within the Guangdong-Hong Kong-Macao Greater Bay Area.

As Hong Kong navigates this period of cybersecurity evolution, it is laying the groundwork for a more resilient and diverse digital ecosystem. By fostering local innovation, collaborating with regional partners and investing in talent development, the city is taking proactive steps to enhance its cybersecurity posture. For the banking and finance sector, this evolution represents an opportunity to be at the forefront of cybersecurity innovation. As the global financial landscape continues to change, Hong Kong’s approach to cybersecurity could play a crucial role in maintaining its status as a leading international financial centre. While challenges remain, Hong Kong’s efforts to create a more robust and diverse cybersecurity environment demonstrate its commitment to adaptation and innovation. In doing so, it is not just responding to current threats but also preparing for the financial landscape of the future. BT

本地的科技先進是個事實。內地和香港的網絡安全科技都有顯著的進步，有些方案能與西方的方案匹敵，甚至有所超越。增加使用本地和內地的方案，可促進香港培養網絡安全的專門人才。香港的銀行金融業若能與內地的網絡安全系統接軌，最終可讓粵港澳大灣區內的跨境金融業務運作更暢順。

香港正經歷網絡安全系統的演進過程，為更靈活多元的數碼生態系統打好根基。藉着促進本地創新、與地區夥伴合作以及投資於人才培訓，香港正積極提高其網絡安全性。對銀行金融業來說，這個演進過程是個機會，機構可爭取在網絡安全創新上領先。環球金融環境持續改變，香港處理網絡安全的方式對維持領先國際金融中心的地位起着關鍵作用。挑戰仍是有的，但香港在建立更穩妥、更多元的網絡安全環境方面的努力，顯示香港致力適應與創新。這樣一來，香港不僅在應對眼前的威脅，也是在為未來的金融環境做準備。BT

ABOUT THE AUTHOR
作者簡介

Michael GAZELEY

Managing Director and Co-founder of Hong Kong-based Network Box Corporation

以香港為基地的Network Box Corporation董事總經理及聯合創辦人