How Service Providers, End-Users, and the Government Can Combat Cybercrime

服務供應商、用戶和政府可如何打擊網絡犯罪

Interviewed by : Mr. Sutton Cheung
採訪者：張悅賓先生

Mr. Franky Lai
Chairman & Chief Executive Officer
WiseSpot Company Limited
賴永雄先生
主席及行政總裁
斯博有限公司

Established in 2001 and headquartered in Hong Kong, WiseSpot is a leading provider of ICT solutions, and has extensive experience working with Greater China's significant telecom operators and enterprises implementing and supporting active installations globally. WiseSpot excels in enterprise messaging, unified communications, business operation workflow digitization and network security solutions.

With its long history identifying and utilizing novel technologies to create best-in-class solutions, WiseSpot's biggest challenge is to constantly remain one step ahead of the market's needs, which stem from rapidly evolving, highly competitive and often exceedingly hostile business environment. This is the case with Digital Transformation, where enterprises worldwide devise plans to embark on this path to gain new ways to engage with customers, enable more innovation in their workforce and garner new efficiency through increasingly automated workflows. Given today's global marketplace where Hong Kong companies are stacked directly against competition from all other the world, enterprises put themselves at a disadvantage if they do not keep up with the global trend of using technologies to transform "traditional" processes into something significantly better. To help companies in this region keep pace with global digital transformation, WiseSpot relies on its business and product planning team that looks 18 months ahead into the future for upcoming trends and applicable technologies to trigger solution development.

Cybercrime in Hong Kong

While technology has indeed brought about significant convenience to consumers and productivity gain to businesses, increasing digitization has also led to an increase in cybercrime. An estimate quantified it at having affected as many as 2 million Hong Kongers in the 12 months ending September 2017, involved losses of US$28 on average and required 19 hours to deal with

於2001年成立的斯博有限公司，總部位於香港，是領先的資訊科技解決方案供應商，與大中華地區重要的電信業運營商和企業有著豐富的合作經驗，為客戶在全球多個國家安裝及支援運營中的系統。斯博擅長企業訊息發送、統一通訊、業務營運流程數碼化和網絡安全等範疇的解決方案。

在識別和採用新技術來創造最佳解決方案方面，斯博擁有悠久的歷史，而過程中面對的最大挑戰，是需要在快速發展、競爭激烈，甚至可說是極端惡劣的營商環境下，持續地保持「先知先覺」，在洞察需求方面領先於市場。就以數碼化轉型為例，世界各地的企業都計劃走上這條道路，以獲得與客戶互動的新方式，使員工能夠進行更多的創新，並通過日益自動化的工作流程獲得新的效率。在當今的全球市場上，香港企業直接面對來自世界各地的競爭，如果它們不能跟上利用科技將傳統工序優化的全球趨勢，將處於不利地位。為了幫助不同公司跟上全球數碼化轉型的步伐，斯博依靠自己的業務和產品規劃團隊，對未來18個月的趨勢和適用技術進行展望，以啟動解決方案開發。

香港的網絡犯罪

雖然科技的確為消費者帶來巨大的便利和為企業提高生產力，日益普及的數碼化同時也導致網絡犯罪增加。有估計曾指出，在截至2017年9月的12個月內，被影響人數多達200萬香港人，並牽涉平均28美元的損失和需19個小時處理後果。另一項預測曾估計，網絡攻擊每年可能導致香港損失320億美元。面對如此巨大的直接經濟損失和聲譽損失等間接影響，斯博通過雙管齊下的方法幫助客戶解決這威脅，1）將保安功能和工作流程加入解決方案設計內，和2）在應用程式開發和測試期過程中時刻對保健因素保持警惕，以便在實施前消除潛在的弱點。舉例，自2007年起已於多個香港固網和流動網絡供應

the consequences. Another projection estimated that cyber attacks could cost Hong Kong US$32 billion annually. Faced with such massive direct economic losses and other indirect impact such as reputation damage, WiseSpot does its part to help clients address this threat via a 2-pronged approach, by 1) including security features and workflows into their solutions' design, and 2) be vigilant of hygiene factors during application development and testing to remove potential points of weakness before implementation. To illustrate, WiseSpot's Unified Communication Solution, which has been implemented for several of Hong Kong fixed and mobile telecom service providers since 2007, has session border controllers (SBC) built into its architecture as a security safeguard in a SIP-based network which is less inherently secure than the traditional time-division multiplex (TDM) networks.

As implied by its name, a SBC functions as a firewall to safeguard the service provider's SIP network borders by securing all access and interconnect/peering borders, while opening up pathways to allow only legitimate calls to go through. It preempts attacks, eliminates vulnerabilities and applies powerful mitigation to counteract events as they happen to protect the network, thus ensuring service continuity and quality. It also supports encryption for voice or video calls for added security to sensitive information might be carried.

商中實施的斯博統一通訊解決方案（Unified Communication Solution），鑒於會話發起協定（SIP）基礎網絡的安全性比傳統的時分多工（TDM）網絡的固有安全性較低，故此斯博在此方案的體系結構中內置了會話邊界控制器（Session Border Controllers, SBC），作為強化安全的保障。

顧名思義，內置的會話邊界控制器的功能是充當防火牆，通過緊固服務提供商的所有讀取和互連/ 對等邊界來保護SIP網絡的安全，只為合法的通話打開通路，讓它們通過。SBC預防攻擊，消除弱點，並在事故發生時應用強大的緩解措施以作抵消，對網絡提供保護，從而確保服務的連續性和質量。它還支持對語音或視頻通話進行加密，為敏感訊息增加安全性。

Network Security

Globally, securing network and data is paramount today because of increasing threats and massive damages due to cybercrimes and cyber attacks. Hong Kong as a metropolitan city that relies heavily on data communication and transactions for both commercial and personal uses, is no exception.

From Mr. Lai's point of view, while ICT service providers have been working to improve the integrity of their services and the security of their networks, truly effective and sustainable countermeasures against cybercrimes will need the concerted efforts of not only service providers, but also that of both enterprise and personal users, as well as the Government and its various regulatory bodies. Instead of tackling this issue individually, cross sector or industry collaboration enables timely information sharing, as well as the

網絡安全

由於網絡犯罪和網絡攻擊所帶來的威脅和巨大損失日益增加，保護網絡和數據的安全目前在全球均至關重要。而香港作為一個無論是商業或個人用途上都嚴重依賴數據通訊和交易的大城市，這點也不例外。

從賴先生的觀點來看，雖然資訊科技服務提供者一直在努力改善他們服務的完整性和網絡的安全性，但真正有效和可持續的反抗網絡犯罪措施不僅需要服務提供者，並須包括企業和個人用戶，以及政府和它的各種監管機構的共同努力。與其由各方單獨處理這個問題，跨部門或行業的合作能夠確保及時的訊息共享，並可彙集專業知識和資源來制定預防工具和行動，以減少網絡犯罪。

pooling of expertise and resources to come up with preventive tools and actions to minimize cybercrime.

As an example, short message service (SMS) was originally developed as a means for person-to-person communication, but as part of banking services' digital transformation, it has since gained widespread application for carrying one-time passwords and other sensitive data. Consequently, heighted message security must now be regarded as a vital hygiene factor for SMS delivery to prevent it from falling prey to cybercrime. Having implemented numerous SMS enterprise messaging platforms and Deep Packet Inspection (DPI) solutions for major carriers in this region, WiseSpot has assisted its service provider clients in this endeavor by building in security measures such as unauthorized access alarms and audit trails into its solution to enable timely detection & intervention.

Yet, service providers do not have access to data regarding how abusive and criminal usage is evolving in eBanking services to update alarm triggers for changing anomalous traffic patterns. To pool information and experience, a cross association task force consisting of representatives from Hong Kong Monetary Authority, The Hong Kong Association Of Banks, Hong Kong Police Force, Office of Communications Authority and Communications Association of Hong Kong was formed in 2014 with the aim to share each unit's unique perspective and expertise on eBanking cybercrimes so that proactive counter measures can be formulated to close any potential points of weakness in communication networks are used for digital banking transactions.

Users, on the other hand, have to be vigilant about their security by not blindly opening files, links, or documents that are sent to them. According to Mr. Lai who represented CAHK in the above task force, user education is a key focus to help the public recognize the risk of opening a questionable link that might turn out to be malicious, or best practices in protecting one's passwords. As an example, an expert from the University of Science and Technology sitting on the Task Force has advocated that requiring frequent password changes might not be advisable as users may either forget their passwords or even worse, write them down on paper and make them susceptible to prying eyes. Rather, the use of security questions (e.g. "what is the name of my first pet?") is on the rise as users can remember the password without keeping a record while being hard to guess by strangers.

Cybercrime and Corporate Social Responsibility (CSR)

Cybercrime is a severe problem in Hong Kong, and cyber security needs to co-evolve with the growth of cybercrime. Lai notes that from his discussions with the Police and other members on the Task Force, cybercrime and data breaches are already very commonplace and show no sign of decline at least in the foreseeable future. This alarming trend is very likely a result of cybercrime being a lucrative endeavor and is associated with high chances of success and low chances of getting caught.

Although initiatives like the above Cross Association Task Force for eBanking to tackle and promote cybercrime awareness is a good

例如，短訊服務（SMS）最初是為人與人之間通訊而開發，但作為銀行業務數碼化轉型的一部分，它在傳送一次性密碼和其他敏感數據方面得到了廣泛的應用。因此，提高訊息的安全性現在必須被視為發送短訊的一個重要保健因素，以防止它成為網絡犯罪的犧牲品。斯博為本地區內的主要運營商實現了許多SMS企業訊息傳遞平台和深度封包檢測（Deep Packet Inspection, DPI）解決方案，並通過在其解決方案中構建安全措施，如未經授權的讀取警報和審核跟蹤等，幫助其服務供應商客戶執行及時檢測和干預。

然而，服務供應商並沒有渠道獲得關於電子銀行服務中濫用和犯罪使用情況的數據，以更新因異常流量模式而啟動的系統警報。為了整合訊息和經驗，一個由香港金融管理局、香港銀行公會、香港警務處、通訊事務管理局辦公室和香港通訊業聯會組成的跨組織專案組於2014年成立，旨在分享每個組織在電子銀行網絡犯罪方面的獨特觀點和專業知識，以便可以制定積極的對策，封鎖任何可用數碼銀行交易的通訊網絡上的潛在弱點 。

另一方面，用戶必須對自己的安全性保持警惕，而不是盲目地打開發送給他們的檔案、鏈接或文件。專案組中曾代表香港通訊業聯會的賴先生表示，用戶教育是一個關鍵重點，以幫助公眾認識到打開可能是惡意的可疑鏈接的風險，或者是保護個人密碼的最佳做法等。例如，一名來自香港科技大學的專家在專案組中主張，要求頻繁更換密碼可能是不可取的，因為用戶可能會忘記他們的密碼，或者更糟，把密碼寫在紙上，讓它們更容易被窺探。相反，安全問題的使用正不斷增加（例如，我的第一隻寵物叫什麼名字？），因為用戶自己能記住密碼而無需記錄，但陌生人就很難猜到。

網絡犯罪與企業社會責任 （CSR）

網絡犯罪是香港的一個嚴重問題，網絡安全需要與網絡犯罪的增長共同發展。賴先生指出，從他與警方及專案組其他成員的討論來看，網絡犯罪和數據洩露已經非常普遍，而且至少在可預見的未來，沒有任何下降的跡象。這種令人擔憂的趨勢很可能是由於網絡犯罪是一種有利可圖的行為，成功的機率很高，被抓住的機率很低。

雖然上述為打擊和提高對網絡犯罪警覺性的電子銀行服務跨組織專案組是一個良好的開端，但由於網絡罪犯對普通市民詐騙的行為仍有許多嚴重各異的欺騙手段，因此仍需要更多集結不同組織的綜合努力。賴先生的同事提供了一件軼事作為說明：一個偽裝成 iTunes Store 公司的罪犯曾試圖向她的信用卡賬戶收費，但被發卡銀行拒絕。信用卡發行商、iTunes Store 或香港警方之間沒有共享訊息進行溝通，以防止類似的事件繼續發生。用戶不得不分別打電話給信用卡公司和蘋果公司去報告這一事件，而又不知道隨後是否會有任何跟進事情發生。這類案件表明，需要進一步開展跨行業合作，積極打擊網絡犯罪，並

start, more consolidated efforts are needed as cybercriminals have many deceptive ways – both major and minor – to scam ordinary citizens. Mr. Lai's colleague provided anecdotal evidence: a party disguised as iTunes Store tried to post a charge to her credit card account but was rejected by the card issuing bank. There was no communication between the credit card issuer, iTunes Store or the Hong Kong Police for share information in an attempt to prevent similar happenings in the future. The user had to call both the credit card company and Apple to report this incident without knowing whether anything will be done subsequently. Cases like this suggest that further cross industry collaboration to proactively combat cybercrime and promote cybercrime awareness is needed. For example, provide designated channels for people to report actual or suspected cybercrime cases, with automatic dissemination of information to relevant parties for investigation. To work hand-in-hand with its numerous digital and smart city initiatives, the HK government should consider allocating more resources to support such initiatives against cyber crimes.

Best Practice for Preventing Cybercrime

Mr. Lai sees Security-as-a-Service as an area having much potential for ICT service providers as more enterprises map out their digital transformation roadmap. In addition to hardware security (e.g. dongles, security keys), and software security (e.g. software token, two-factor authentication procedures), carriers can do more to help enterprises as they bring more and more of their workflows and processes digital. Carriers can instill secure end-to-end communication that can track down individual phones and computers because each device has a unique identity (e.g. SIM card). Doing so ensures data from device X is correctly transmitted to device Y, that calls are forwarded to the correct device, and that anomalous and irregular data transactions can be detected. Taking this train of thought one step further, enterprises can deploy a combination of DPI and artificial intelligence technologies to make their network environment more secure for the business customers when running digitized workflows and business transactions. Via the setting of policies, DPI enables the automated detection of network traffic anomalies as they happen to trigger alarms and alert for timely intervention. AI or Machine Learning (ML) then further adds to this equation by allowing automated refinement to the DPI policies for more precise detection and accurate risk assessment.

i "At least 2 million internet users in Hong Kong were hit by cybercrime in a 12-month period, survey says" by Su Xinqi, South China Morning Post, 27 March, 2018

ii "Cyber attacks could cost Hong Kong massive US$32 billion annually, according to study" by Alice Shen, South China Morning Post, 14 June, 2018

提高對防範網絡犯罪的意識。例如，設立指定的渠道，讓市民可以報告實際或懷疑網絡犯罪案件，並將資料自動通報相關機構進行調查。為配合多項數碼及智慧城市的措施，香港政府應考慮調撥更多資源，以支援打擊網絡罪行的措施。

預防網絡犯罪的最佳措施

隨著越來越多的企業製定出數碼化轉型路線圖，賴先生認為「安全即服務」是一個對資訊科技服務提供者有很大潛力的領域。除了硬件安全（例如，外置裝置、安全密鑰）和軟件安全（例如，軟件令牌、雙因素認證過程）之外，當越來越多的企業將工作流程和程序數碼化，電訊商可在過程中提供更多協助。由於每個電子設備都有一個獨特的身份（例如SIM卡），運營商可以追蹤到單一的個人手機和電腦，從而提供安全的點對點通訊。這樣做可以確保從設備X正確地將數據傳輸到設備Y，將通話轉發到正確的設備，並且可以檢測到異常和不規則的數據交易。更進一步，企業可以採用結合深度封包檢測和人工智能的技術，使商業用戶在運行數碼化工作流程和業務交易時，網絡環境更加安全。通過設定系統政策，深度封包檢測可以自動檢測到網絡流量異常，並因而觸動警示的發出，以便及時作出干預。再進一步，更可通過利用人工智能或機器學習（ML）來對深度封包檢測政策進行自動優化，從而實現更精確的檢測和準確的風險評估。