Protecting Hong Kong Businesses from Cybercrime
保護香港企業　提防網絡罪行

Interviewed by : Dr. Hubert Chan
採訪者：陳重義博士

Mr. Alex Arena
Group Managing Director
HKT*

艾維朗先生
集團董事總經理
香港電訊

HKT is Hong Kong's premier telecommunications service provider and leading operator in fixed-line, broadband and mobile communication services. HKT offers a unique quadruple-play experience in Hong Kong delivering media content on its fixed-line, broadband Internet access and mobile platforms jointly with its parent company, PCCW Limited.

HKT also provides a range of innovative and smart living services as well as a payment service beyond connectivity to make the daily lives of customers more convenient, whether they are at home, in the workplace, or on the go.

Most recently, HKT created "Iris" that allows customers to upload video streams so HKT can run data analytics (i.e. heat-mapping, facial recognition, intruder alarms, building-management) to provide robust intelligence to Iris customers.

Without doubt, new technology can unleash a plethora of benefits, but cybercriminals can also use advanced technology for malice. According to Arena, the fraudsters' methods evolve alongside advances of technology and communication methods. Scams used to be conveyed through physical means such as leaving leaflets in mailboxes, but now a scammer can target people's data in the online world via the Internet regardless of where the scammer is geographically.

In order for telecommunication to take place, at least two parties must be present: the sender and the receiver. HKT provides a highly safe and secure communication channel between A to B, and as of now, HKT has faced no serious intrusion into their networks. But even so, this does not mean there are not risks present within the user's networks in A and in B. As long as there are vulnerabilities on either side, there is potential for cybercrime.

香港電訊是本港首屈一指的電訊服務供應商及領先的固網、寬頻及流動通訊服務營運商。香港電訊在香港提供獨特的「四網合一」體驗，聯同母公司電訊盈科有限公司透過香港電訊的固網、寬頻互聯網及流動通訊平台傳送媒體內容。

香港電訊亦提供一系列傳輸以外的創新、智能生活及支付服務，無論客戶身處家中、辦公室或戶外，都能為他們的日常生活帶來更多便利。

最近，香港電訊推出名為「Iris」的服務，客戶可以上傳視象串流，讓香港電訊進行數據分析（即熱度圖表、面部識別、入侵警報、建築管理），為Iris客戶提供可靠的智能訊息。

毫無疑問，新科技可以帶來很多好處，但網絡犯罪分子也可以利用先進科技圖謀不軌。據艾維朗先生說，隨著科技和通訊方式日新月異，騙徒的手法亦逐步演變。過往騙徒會親身發放詐騙訊息，例如把單張放進別人的信箱，現在無論騙徒身處何方，都可以通過互聯網入侵他人在網絡世界的資料。

電訊流程最少涉及兩方面：發送者和接收者。香港電訊為A和B之間提供高度安全和穩妥的通訊途徑，直至目前為止，香港電訊的網絡並無遇到嚴重的入侵事故，但這並不表示A和B的用戶網絡沒有風險存在。只要其中一方存在漏洞，就有可能發生網絡罪行。企業採取網絡保安措施便可以保護其數據。如果不加以監控，網絡罪行將殃及香港電訊的客戶，給香港電訊造成業務上的損失和失去客戶信任，同時損害企業品牌。

* Ms. Susanna Hui has taken up the position of Group Managing Director of HKT following Mr. Alex Arena's retirement on August 31, 2018.

*艾維朗先生已於2018年8月31日退休，香港電訊集團董事總經理由許漢卿女士接任。

Enterprises would benefit from cybersecurity to secure their data. If left unchecked, cybercrime will cause damage to HKT's customers and it will in turn make HKT lose business, customer's trust, and damage corporates' brands.

Fortunately, HKT has provided comprehensive solutions to corporate customers to tackle cybercrime, from threat analysis, security infrastructure design and implementation, round-the-clock monitoring and support, as well as a range of network based security services. Arena believes that people are more aware of the damage cybercrime can do and are willing to pursue and invest in cybersecurity. Arena compares cybersecurity to a physical bank: as more security is implemented in banks, it resulted in fewer robberies. Similarly, if we implement security measures in the cyberworld, rates of cybercrime will drop.

HKT's Next Generation Security Operations Center (NG SOC)

HKT is dedicated to protect Hong Kong businesses and locals against cybercrime. Cyber threats are growing increasingly aggressive and the budget for cybersecurity has been historically thin for some enterprises. In-house security staff may be burdened to deal with cyber threats and various regulatory compliance requirements and may appreciate all-compassing cybersecurity services. As such, HKT offers a wide range of security services from their strong resources pool. Their all-round cybersecurity solutions suite provides end-to-end cybersecurity protection covering WAN, LAN, Wireless and Wireline environment.

These solutions defend against network base volumetric attacks, LAN and applications hacking (commonly called Zero Day Attack or Advance Persistent Threat), as well as end point desktop and mobile malware. Moreover, HKT offers practical training for IT Security practitioners in the form of hands-on online combat exercise between red team (hackers) and blue team (NG SOC detection), commonly called Cyber Range. The initial target audience would be for the IT Security practitioners from the financial sector but inevitably corporate customers from other sectors will embrace these services.

幸而香港電訊為企業客戶提供全面的解決方案以應對網絡罪行，包括威脅分析、網絡安全基礎設施的設計及安裝，全天候監控及支援，以及一系列以網絡為基礎的保安服務。艾維朗先生認為，人們更加意識到網絡罪行可以帶來的損害，因此願意投放資源加強網絡保安。艾維朗先生以實體銀行為例，説明網絡保安的作用：銀行加強保安後，劫案隨之減少。同樣道理，如果我們在網絡世界實施保安措施，網絡犯罪率將會下降。

香港電訊的新世代網絡安全監控中心（NG SOC）

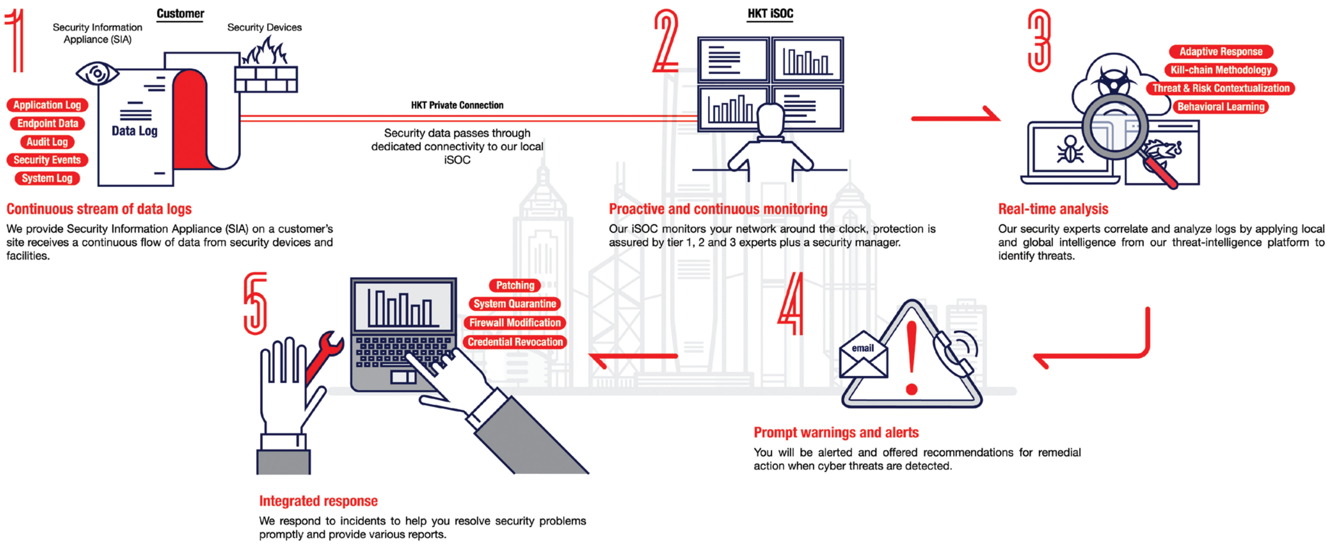
香港電訊致力保護香港商界和本港市民免受網絡罪案侵害。網絡威脅的侵略性越來越高，一些企業的網絡保安預算卻少之又少。公司內部的網絡保安人員可能要背負處理網絡威脅和遵從各種法規的重擔，全面的網絡保安服務或許是一個周全的選擇。因此，香港電訊運用其龐大的資源，提供廣泛的保安服務。他們的全方位網絡安全解決方案提供端到端的網絡保安，覆蓋廣域網、局域網、無線和有線環境。

這些解決方案可以抵禦大批量的網絡攻擊、局域網和應用程式攻擊（通常稱為「零時差攻擊」或「進階持續性滲透攻擊」），以及端點桌面和流動惡意軟件。此外，香港電訊亦為資訊科技保安人員提供實務訓練，包括紅隊（黑客）與藍隊（偵測）的網上實戰演練，一般稱為「網絡靶場」。最初的目標受眾是金融界的資訊科技保安人員，但這些服務也必然會受到其他界別的企業客戶歡迎。

是甚麼促使香港電訊在網絡安全方面取得成功？規模當然是重要的因素；香港電訊憑著龐大的客戶基礎，創造了寶貴的網絡威脅智能訊息庫及網絡安全監控最佳作業守則。香港電訊的（新世代網絡安全監控中心）資訊科技保安分析人員協助客戶檢測並應對網絡安全事故，並進行鑑證以便展開遏制攻擊和恢復系統的程序。這些分析人員都已通過一系列獲全球認可的培訓，所以最先進的網絡安全檢測和分析技術能夠應用於香港電訊的客戶環境中。

How TMS works

Architecture and Flow



Continuous stream of data logs

We provide Security Information Appliance (SIA) on a customer's site receives a continuous flow of data from security devices and facilities.

Proactive and continuous monitoring

Our iSOC monitors your network around the clock, protection is assured by tier 1, 2 and 3 experts plus a security manager.

Real-time analysis

Our security experts correlate and analyze logs by applying local and global intelligence from our threat-intelligence platform to identify threats.

Prompt warnings and alerts

You will be alerted and offered recommendations for remedial action when cyber threats are detected.

Integrated response

We respond to incidents to help you resolve security problems promptly and provide various reports.

What drives HKT's success in cybersecurity? No doubt scale is an important factor; HKT's huge customer base creates a valuable pool of threat intelligence which HKT has used to develop a set of best practices for its network security control. HKT's NG SOC IT Security Analysts help customers detect, and respond to cyber security incidents, and run forensics for the subsequent containment and recovery stages. These analysts have gone through a series of globally recognized training, so that the most advanced cyber security detection and analysis techniques could be applied to HKT's customer environments.

In addition, HKT NG SOC invests a lot of resources to enhance the capability on anomaly behavior detection and false positive cases filtering within customer's infrastructure through deploying Artificial Intelligence and Machine Learning technology. HKT NG SOC also builds a local Threat Intelligence Platform to consolidate the local cyber security threat information for the purpose of detecting real and malicious threat effectively.

The NG SOC's threat management services (TMS) keep security up to speed based on an adaptive security model. TMS benefits businesses by utilizing integrated local engineering teams and Big Data analytics to detect advanced cyber attack , protect businesses' intellectual property, reduce operational costs, and meet today's compliance standards. Moreover, TMS provides such advanced cyber security services to help corporations coping with serious shortage of IT Security talents which has become a worldwide chronical issue. The HKT NG SOC also helps enterprises respond to security problems and provides numerous reports to address compliance issues.

These efforts have been recognised by HKT's NG SOC winning the Best Managed Detection and Response Partner Award of North Asia 2018 by a renowned cyber security Big Data Vendor

此外，香港電訊的新世代網絡安全監控中心投入大量資源，通過部署人工智能和機器學習技術，提高為客戶基礎設施偵測異常行為及過濾誤判個案的能力。香港電訊的新世代網絡安全監控中心亦建立本地資訊威脅情報平台，整合本地的網絡資訊安全威脅資訊，以便有效偵測真實及惡意的威脅。

新世代網絡安全監控中心以一個適應性安全模型為基礎，令香港電訊的資訊安全威脅管理服務（TMS）能與業界的技術同步發展。資訊安全威脅管理服務利用本地工程綜合團隊和大數據分析來檢測先進網絡攻擊，以及保護企業的知識產權、降低營運成本並滿足目前的合規標準，令眾多企業受惠。此外，全球資訊科技保安人才長期嚴重短缺，威脅管理服務提供這類先進的網絡安全方案，有助企業應對這方面的人才荒。香港電訊的新世代網絡安全監控中心亦協助企業解決保安問題，並因應合規事項提供大量報告。

香港電訊的新世代網絡安全監控中心在這方面的努力深受認同，於2018年5月榮獲一間著名的資訊安全大數據供應商頒發的「The Best Managed Detection and Response Partner Award of North Asia 2018 」，彰顯香港電訊在網絡保安方面的整體能力和質素。

香港電訊夥拍世界知名的安全設備供應商開發以網絡為本的服務，稱為安全即服務。該平台提供一系列以網絡為本的網上安全防護，如過濾惡意網絡流量（DNS）、反分散式阻斷服務攻擊、管理式防火牆等。這些服務均由香港電訊的新世代網絡安全監控中心支持，不僅符合大企業的保安要求，也為中小企提供了具成本效益的解決方案。

in May 2018. This award demonstrates the global capability and quality of HKT's cybersecurity strength.

HKT partners world renowned security appliance vendors to develop network based services, namely Security-as-a-Service. A range of the network based cyber security protection is provided through this platform such as malicious traffic (DNS) filtering, Anti-DDoS, managed firewall, and etc. These services, which are supported by HKT NG SOC, not only fit the security requirement of big corporations. It also provided Small and Medium Enterprise a cost effective solution.

Since Hong Kong is a major financial hub, regulatory bodies such as the HKMA and SFC raise compliance standards in recent years. Namely, they focus on three areas in the financial institutions: IT Security fortification, certified IT Security practitioners, and continuous 24 x 7 monitoring. In response to the compliance standard, HKT helps customers to build state-of-the-art security infrastructure. They have implemented many security infrastructure projects for banks, securities brokers, and large corporations.

Telephone Deception and HKT's Star Home Call Service

Today's fraudsters use telecommunication channels – including HKT's – to deceive victims. While HKT is committed to upholding their customer's privacy and does not monitor calls, HKT utilizes alternative methods to reduce telephone deception. Recently, HKT has launched their Star Home Call Service, a smartphone app that allows users to link one's home phone to one's cell phone. When linked, users can pick up home calls with their cell phone, or use the home number to dial out even when the cell phone is abroad. This app blocks junk calls by cross-referencing incoming calls with a sophisticated junk call database.

由於香港是主要金融中心，香港金融管理局和證券及期貨事務監察委員會等監管機構近年提高了多項合規標準，聚焦金融機構的三個領域：資訊科技保安防禦工作、資訊科技保安從業員的認證以及持續執行24×7監控。為配合合規標準，香港電訊協助客戶建立最先進的保安基礎建設。他們為銀行、證券商和大企業實施了許多保安基礎建設項目。

電話詐騙和香港電訊的「升•聲•星級來電 」 服務

現今的騙徒利用包括香港電訊在內的電訊管道行騙。香港電訊致力維護客戶私隱，並無監察電話，但已採用其他方式減少電話詐騙事故。最近，香港電訊推出「升•聲•星級來電 」 服務，這是一款智能手機應用程式，用戶可以將自己的家居電話與手機連接起來。當兩者連接時，用戶可以用手機接聽家居電話，即使身處海外，也可以用家居電話號碼撥出電話。這個應用程式可以將用戶的來電與滋擾來電資料庫對照，從而攔截滋擾電話。