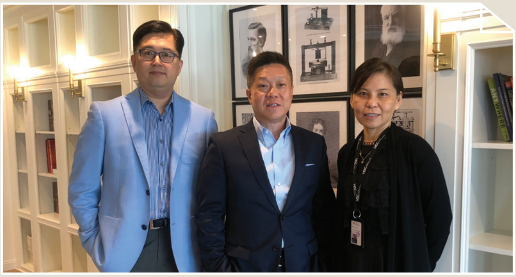
Cybersecurity As a Top Priority in the Digital Era

網絡安全 — 數碼時代下的首要任務

Interviewed by : Mr. Tony Hau

採訪者：侯東迎先生

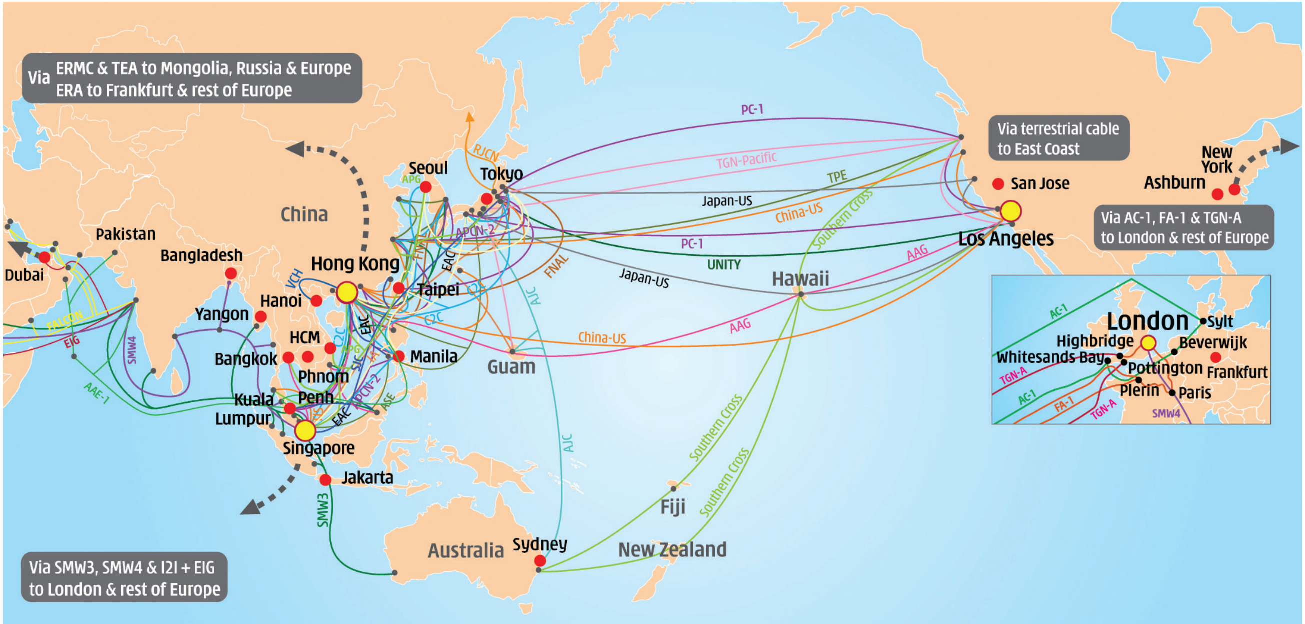


Mr. Andrew Kwok, Chief Executive Officer (Middle)
Ms. Jacqueline Teo, Chief Digital Officer (Right)
Mr. Eric Chan, Director of Network and Products (Left)
HGC Global Communications Limited

郭詠邦先生，行政總裁 (中)
Ms. Jacqueline Teo，首席數碼官 (右)
陳思源先生，網絡及產品總監 (左)
環球全域電訊有限公司

HGC Global Communications Limited ("HGC") is a fixed-line operator and ICT solutions provider that serves multi-national corporations, small to mid-sized enterprises, families, and carriers across many countries around the world. Their network products come with value-added services for data protection. For instance, HGC can help clients manage firewall, network based anti-DDoS protection, and provide encrypted private networks (e.g. Cloud connect, VPN for connection to public cloud such as Amazon Web Services or Microsoft Azure) on top of Internet as well as securing hybrid / multiple cloud platform. HGC is an official corporate member of the smart-city consortium, active in smart city initiatives that support the government's blueprint implementation and commercial projects. Securing mission critical infrastructure is very key and fundamental to a leading operator.

環球全域電訊有限公司（以下簡稱HGC）是電訊固網服務和資訊科技（ICT）方案營辦商，服務對象包括跨國企業、中小企業、住宅用戶和世界各地其他網絡商。HGC的網絡服務還提供數據保護的增值服務。例如：HGC可以幫助客戶管理防火牆、網絡式DDoS防禦保護，並於互聯網上提供加密私人專線（如：雲連線、AWS 或 Microsoft Azure 等連接公眾雲的虛擬私人網絡）以及混合/ 多項式雲平台保護服務。HGC作為香港智慧城市聯盟的成員，積極支持發展智慧城市中政府藍圖落實和商業項目。作為業界領先的營辦商，提供重要基建設施的是我們主要及基本責任。

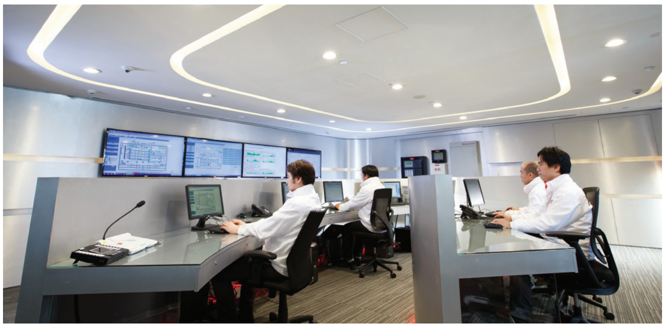


Evolution of Cybercrime

The ongoing fourth industrial revolution – the digital age – has profound influences on how we communicate and how we use data. The rapid speed and intensity of 1) Globalization, 2) Fragmentation, and 3) Personalization, together alters how we live. People can communicate with others in virtually anywhere in the world, people's lifestyles are becoming more unique and individualistic, and we can communicate in a myriad of mediums. However, these benefits also create more opportune times for cybercrime. For instance, there are millions of applications available (i.e. fragmentation) for virtually anyone with a smartphone (i.e. globalization). These applications can be malicious, but checking each one is rather tedious and require specialized skill. As such, HGC's customers tend to favor reliable, hassle-free, one-stop solutions with a proven track record from their trusted network service provider.

Cybersecurity As a Top Priority

Security is one of HGC's top priorities for our clients. Cybersecurity is embedded and integrated into HGC's solutions, both inward-looking in terms of our own corporate IT, and outward-looking in terms of products and services for clients and partners. Therefore, as a manage-security-service-provider (MSSP), HGC hardens client IT platforms and perform vulnerability tests to assess security status. HGC has a 24 x 7 network operating center that oversees all of Hong Kong's networks. At the same time, HGC has a security operating center (SOC) responsible for security activities such as incident response, risk mitigation and reporting. The data center is accredited with security certification ISO 27001.



HGC's internal data loss prevention solution has three tiers: 1) Server-based 2) Network-based 3) Device-based. Server-based protection tracks all data transactions to ensure that only the right people can access certain data (e.g. HR personnel should not have access to finance data), such that only certain people are given access to the sensitive data. Network-based protection tracks and warns users of potential data leaks (e.g. do not send sensitive data over vulnerable Email servers), and keeps record of what data is transmitted; data that is highly valuable are even blocked from sending. Lastly, device-based end-point encryption prevents data from being accessed from external devices (e.g. USB drive). Any mobile devices connected to HGC's data center is potentially vulnerable, so HGC monitors all the traffic of mobile devices in their own network and block malicious sites.

網絡犯罪的變化

數碼時代 — 就如正在上演第四次工業革命一樣，在通訊與數據應用方面有著深遠的影響。全球化、碎片化和個性化為我們的生活帶來了迅速改變。人們可以隨時隨地與別人溝通、而人們的生活方式也變得越來越獨特和個性化，還有五花八門的通訊媒體給我們使用。然而，這些便利也為網絡犯罪創造了更多機會。例如：數百萬個應用程式（如：碎片化）供任何人透過手機下載來使用（如：全球化）。當中不乏惡意應用程式，但要將它們逐一檢驗確實相當的繁複，而且也需要有專業技能才能做到。因此，HGC 的客戶都會傾向選擇可靠、省心、提供一站式方案，有信譽的網絡服務供應商。

網絡安全是首要任務

安全問題是HGC對每位客戶的首要任務之一。而網絡安全措施已融合於HGC的解決方案中，對內 — 用於自家企業的資訊科技；對外 — 為客戶和合作夥伴提供的產品和服務。所以，作為一個託管安全服務提供商（MSSP），HGC不僅為客戶的IT平台進行加固，還會進行弱點測試來評估安全狀況。HGC擁有24 x 7 全天候網絡監控中心實時監測全港網絡。同時，HGC的資訊安全管理中心（SOC）負責解決安全相關的問題，包括事故應變、風險轉移和安全報告。此外，HGC數據中心獲取了ISO 27001安全認證。

HGC的內部資料外洩防護解決方案分三個層面：1）伺服器層面；2）網絡層面；3）設備層面。伺服器層面的資料防護是以追踪所有資料存取紀錄，從而確保只有合認可人士才可以存取某些特定資料（例如：人力資源部人員是不允許存取財務部的資料），只有特定授權人士可存取敏感資料。網絡層面的資料防護是追踪和提醒用戶潛在資料洩漏行為（例如：不會將敏感資料以簡單的電子郵件伺服器發送），並且保存傳輸資料紀錄，甚至攔截重要資料發送。最後，設備層面以用戶端加密來防止資料被外來設備存取（如USB驅動器）。因為任何連接到HGC數據中心的流動設備都有潛在漏洞，所以HGC會監控所有流動設備在其網絡上的流量，並且阻止瀏覽惡意網站。

不但如此，在身份管理和存取控制方面，HGC採用身份存取管理、多重認證管理和一次性密碼。具體來説，HGC內部對於遠端存取方面採用多重認證、特選帳戶管理系統和一次性密碼，至於存取權限會按照集團員工的職務和身份制定，不合適的資料將會被加密。

在全球範圍內，分散式阻斷服務攻擊（DDoS）的案例眾多，通過利用機器和物聯網設備發出大量「垃圾郵件」務求使目標網絡癱瘓。攻擊強度達到數以十億計的流量，這意味著無論網絡強度如何，也會被堵塞和全面影響正常商業營運。HGC的DDoS防禦服務可以幫助客戶檢測網絡的異常流量，防止網絡癱瘓。DDoS防禦服務通過網絡安全運作中心為客戶攔截攻擊

Further, HGC employs identity access management, multifactor authentication management, and one-time passwords for identity management and access control. That is, HGC internally uses multifactor authentication for remote access, a privilege account management system, and one time password for managing access, where access is based on one's role and identity within an organization, and data that does not fall under one's privileges is encrypted.

Globally, there are many cases of Distributed Denial of Service (DDoS) attacks that utilize machines and IOT devices to generate 'dirty traffic' that shuts down a targeted network. This volumetric trend can create gigabytes of traffic, which means that regardless of the network's strength, the network can be clogged and normal business operations can be put to a complete halt. HGC's anti-DDoS service helps clients anticipate abnormal network activities before the network is jammed. The anti-DDoS service diverts the traffic to SOC's computers to filter out the dirty traffic and restore normal activities as if no DDoS has occurred. If HGC detects potential DDoS attacks, they will divert the clients' traffic to other route so as to maintain service availability.

Besides DDoS, there are cases of "slow-and-low" advanced threat, which are long-term efforts that aim to obtain a client's private data. HGC protects their internal data - via advanced threat prevention (ATP) - in three domains: Internet, Email, and Endpoints (PC). Regarding Internet protection, HGC inspects all network traffic that passes through their Internet gateway, (e.g. web browsing, files download, etc.). Any abnormal or suspicious traffic detected will be dropped or blocked. Regarding Email protection, all emails that enter or exit from the Exchange server are inspected. Any suspicious email content and attachment will be removed before delivery to users' mailbox. Regarding endpoints (PC), only whitelisted (IT authorized) applications can be executed at endpoints to minimize the risk being compromised / infected. HGC also records all internal sequences and details of application execution for forensic purposes.

Telephone Deception

Unlike advanced cybercrime which tend to target those with money, resources, and power, everyone is a potential target when it comes to telephone deception scams. Therefore, procedures that can help everyone against cybercrime is needed.

HGC splits telephone deception into two categories: fixed-line and mobile. Since outgoing fixed-line calls from HGC does not allow modified call-line-identification (CLI), cybercriminals won't be able to modify CLI to trick victims into believing calls come from someone familiar (e.g. one's boss, spouse, daughter). HGC tries to locate the origin of suspicious calls by collaborating with upstream operators and works with mobile operators so outgoing calls that use HGC's network will have a "+" sign added. Denoting that calls are from overseas help warn users of potential suspicious activity.

Currently, HGC collaborates closely with 1) government to follow-up cases pertaining to telephone deception, 2) OGCIO,

性流量，確保客戶業務正常運作。同時，當HGC檢測到潛在DDoS攻擊時，會把客戶的網絡服務轉換到其他路由器上以確保其網絡使用不受影響。

除了DDoS攻擊以外，還有低速網絡進階威脅，這些威脅以長期滲透式獲取客戶的私人資料。HGC以進階威脅防護（ATP）措施幫助客戶保護其內部三大範疇數據，分別是互聯網、電郵和終端機（個人電腦）。在互聯網防護方面，HGC檢查所有通過其互聯網關口的流量，包括網頁瀏覽、檔案下載等。任何異常或可疑的網絡流量一旦被監測到，便會立即被清除或攔截。在電郵防護方面，所有經伺服器發送或接收的郵件都會被監測，任何可疑的電郵內容或附件都會被移除，使它無法發送到用戶郵箱。在終端機（個人電腦）方面，為了減少被攻擊或感染病毒的風險，只有白名單上的（IT授權的）應用程式才允許安裝使用。HGC也會將所有內部流程及應用程式的使用情況作記錄用於鑑識用途。

電話騙案

一貫高技術的網絡犯罪傾向以金錢、資源和權力人仕為目標。但是電話騙案則與之不同，任何人都可以成為目標。所以，可以幫助人們防範網絡犯罪的步驟顯得更加需要。

HGC將電話騙案分成兩大類型：固網和流動網絡。由於通過HGC的固網撥出的電話不能修改其主叫線路識別（CLI），因此網絡犯罪份子不能通過修改主叫線路識別去誆騙受害人，讓受害人相信電話是來自熟悉的人（如：老闆、配偶或子女）。此外，通過與上游營辦商和流動網絡營辦商合作，HGC　能夠通過定位並以「+」標識可疑來電的撥出地區，表明該電話是來自海外，提醒用戶以防受騙。

HGC目前與多個組織展開緊密的合作：1）政府部門　—　跟進有關電話詐騙案件；2）政府資訊科技總監辦公室和3）通訊事務管理局辦公室，定期就最新科技和趨向和行業新聞等進行交流。HGC承諾積極與本地或海內外組織合作共同打擊電話騙案。至今，HGC已經和超過400個網絡合作夥伴合作，在徵得

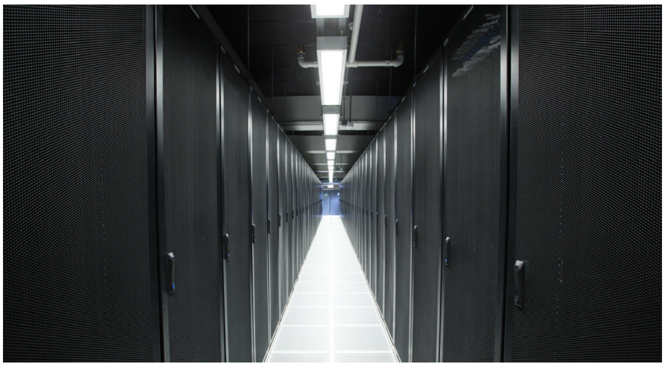
3) Office of the Communications Authority for regular updates and information exchanges on the latest technology, trend, and industry news. HGC is committed to cooperate with organizations, regardless if it is local or overseas to tackle telephone deception cases. HGC has over 400 carrier partners and we help one another out with respect to call trace and fraud investigation. A long-term solution would be having more telecommunication companies and organizations that promote to ITU, with the goal of teaming together to fight cybercrime.

HGC's Current Practices and Goals for the Near Future

HGC anticipates several key trends pertaining to cybersecurity. Firstly, the increasing need for cybersecurity will likely be driven by (perhaps global) top-down compliance initiatives. Organizations would have to comply and customers expect that service providers are fulfilling their data security needs. Secondly, devices will continue to differ on how much security is built-in. High-end smartphones (e.g. iPhones) are fine for security, but cheap phones may not be geared up to be secure devices. Customers who expect a high level of security in all types of devices may be misled into thinking their phones are secure. HGC provides Mobile Device Management (MDM) solutions to customers as part of a one-stop solution.

Thirdly, managing increasingly complex and diverse networks – including data centered IOT, smart city, and 5G devices - will only get more complex. However, these networks are not inherently secure, so cybersecurity measures (e.g. behavior analytics, machine learning) to detect anomalous behavior are needed. HGC is starting to implement artificial intelligence services to improve efficiency and accuracy of call center agents with the long-term goal of using predictive analytics to automate mitigation and incident response without human intervention. In the near future, there will be millions of devices connected to one another so automation and A.I. will need to improve the overall efficiency. Currently, HGC implements A.I. to its internal operation, and their goal is to extend this service to its customers.

Lastly, with so much data and connected devices, HGC opts to virtualize components of data and to decentralize their security infrastructure. HGC also provides a cloud backup solution as part of its Managed Services. Doing so eases the management of heterogeneous storage environments. By virtualizing storage, they can standardize the functions and features of the storage as well as the knowledge and skills to administer the storage. Such a decentralized infrastructure allows simple data migration; traditionally, data migration and restoration from one storage to another storage requires complicated procedures and downtime. Virtualized storage allows data to transfer between drives from different storage easily and with minimal downtime. On a macro-level, virtualized storage enables available capacity across different physical storage to be combined which can better utilize the available capacity. All in all, there is reduced risk of cyberattacks, improved scalability of security solutions, and increased fault tolerance as their network footprint gets wider.



同意的情況下互助互利，共同參與電話的追踪和詐騙案件的調查。長遠來看，應該鼓勵更多電訊公司和組織加入國際電信聯盟，團結起來共同對抗網絡犯罪。

HGC 的實例分享以及近期目標

HGC預期會有幾個有關網絡安全的新趨勢。第一，隨著網絡安全需求日益增加，很有可能會（或許全球性）從上而下推動責任規定。企業必須履行規定，同時客戶也希望服務供應商能夠確保其數據安全的需求。其次，各種設備的內置安全量度會持續有所不同。高端智能手機（如：蘋果手機）的安全措施比較到位，相反廉價手機不能裝配成為安全設備。客戶認為所有的設備都應該具備高水平的安全裝置，正是這種想法可能讓他們誤以為自己所使用的手機是安全的。這時，HGC為客戶提供流動裝置管理（MDM）解決方案，是一站式解決方案的一部份。

第三，隨著網絡越來越複雜和多元化，包括以數據為中心的物聯網、智慧城市和5G設備只會變得更為複雜。然而，這些網絡並非固有的安全，因此監測異常行為的網絡安全措施（例如：行為分析、機器學習）顯得尤其重要。HGC開始實施人工智能服務，以提改善其電話服務中心的效率和準確性，更從長遠的目標考慮，利用預測分析達到自動調解和無人事故處理。在不久將來，無數的設備能相互連接，所以自動化和人工智能會應用於改善整體效率。目前，HGC已經將人工智能應用於內部運作，但是他們的目標是把這項服務帶給每位客戶。

最後，面對龐大的數據及互通的設備，HGC選擇將數據部件虛擬化和將安全基礎設施分散。並推出雲端備份解決方案作為託管服務之一，是為了更方便管理多樣化的儲存環境。通過虛擬化儲存環境，他們能夠將功能和儲存特性，以及管理儲存的知識和技能標準化。這種分散式基礎設施，使數據轉移變得簡單起來。傳統上，設備之間的數據轉移和復原，都需要複雜程序和停機時間。但是通過虛擬化儲存，使不同驅動器之間的數據轉移變得簡單，並且縮短了停機時間。縱觀來看，虛擬化儲存可將不同的儲存設備的容量結合起來，從而可以更好使用其容量。總結來説，新的儲存方式可以降低網絡攻擊、改善安全解決方案的量化度和提高容錯能力。