# Hutchison Telecom Hong Kong Is Committed to Enhancing Information Security

# 和記電訊香港致力提升資訊保安

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

**Mr. Cliff Woo**
Co-deputy Chairman
**Hutchison Telecommunications Hong Kong Holdings Limited**
**胡超文先生**
聯席副主席
**和記電訊香港控股有限公司**

3 Hong Kong, the mobile arm of Hutchison Telecommunications (Hong Kong) Holdings Limited (HTHKH), is a leading mobile communications service provider that offers state-of-the-art voice, data, and roaming service under 2G, 3G, and advanced 4.5G networks. Back in the old days when telecoms operators first started selling mobile phones, communication via phone was restricted to voice calls, but data transmission today has grown incredibly complex: today's phones include data, voice, IDD, roaming, social media, and monetary transactions, currency exchange, registration, sending email. Doing business has also shifted to the virtual realm; customers can purchase products anywhere. These changes have prompted the higher and more comprehensive IT security requirements.

## 3 Hong Kong's Approach to Data Security

3 Hong Kong recognizes the value of securing data and employs teams dedicated to keeping data safe. They are governed by group level polices on information security and data security in areas such as accountability, access control, risk assessment, data retention and data deletion. They have also assigned an information security custodian to design and implement appropriate controls in compliance with group-level policies and requirements.

As mobile communications are moving toward 5G, Woo predicts that cybercriminals will have more ways to deceive users and hack device-to-device communications, or access people's data through malicious apps. In some cases, it only takes a user one mis-click to allow cybercrime to occur. Nonetheless, 5G networks treat security with utmost importance and have robust systems built-in to prevent data breaches.

To keep 3 Hong Kong well ahead in cybersecurity, Woo often consults security experts about the latest tactics in cybercrime. After consultation, 3 Hong Kong's security team conducts close inspections to ensure its security systems are equipped with up-to-date and regularly-reviewed appropriate controls.

3香港為和記電訊香港控股有限公司旗下的流動通訊業務，是香港領先的流動通訊服務營辦商，透過2G、3G及先進的4.5G網絡，提供尖端的話音、數據及漫遊服務。回顧過去，電訊營辦商剛推出手機時，流動通訊僅局限於話音通話；隨著數據傳輸日趨多元化，現今的手機已擁有數據、話音、國際長途電話、漫遊、社交媒體、支付交易、貨幣兑換、登記和發送電郵等功能。營商渠道亦已移師至虛擬領域，顧客可在任何地方購物。這些轉變觸發了市場對資訊科技安全更高更全面的需求。

## 3香港提升的數據安全措施

3香港充分瞭解數據安全的重要性，特別聘請專責團隊保障數據安全。團隊遵照集團政策，確保資訊和數據在不同領域，包括問責、存取控制、風險評估、資料儲存和資料刪除等範疇均得到保障。3香港亦遵照集團政策和要求，委派資訊保安專員設計和執行適當的監控措施。

流動通訊正邁向5G新世代，胡先生估計網絡罪犯將透過更多途徑詐騙用戶和入侵電子設備之間（D2D）的通訊，或透過惡意應用程式讀取個人資料。有些個案，用戶只是錯誤點擊便墮入網絡圈套。然而，5G網絡尤其注重網絡安全，將建基於穩固的加密系統以防止數據外洩。

為使3香港在網絡安全問題上能防患於未然，胡先生經常就最新的網絡犯罪手法諮詢網絡保安專家，再由3香港的網絡安全團隊進行嚴密檢測，確保安全系統採用最新及適當的監察措施。

為確保內部安全架構（包括防火牆、入侵防禦系統和網站應用程式防火牆）有效運作，3香港經常檢視保安系統的相容性，及確保系統裝置了最新和最適當的版本。此外，3香港有嚴謹

Regarding internal security, 3 Hong Kong ensures its security framework including firewall, IPS and WAF is implemented with the latest versions of suitable up-to-date controls as well as security systems are compatible with one another. Moreover, 3 Hong Kong's built-in protocols ensure that only authorised personnel can access sensitive data. User-IDs are reviewed regularly and obsoleted user-IDs are removed in a timely manner. Reports and warnings are promptly addressed if abnormal data access points are detected. HTHKH's parent company conducts annual internal audits, prepares a detailed audit report and recommends how 3 Hong Kong should maintain and improve IT security controls. These might include setting a budget allocated towards specific security infrastructure enhancement.

Service-wise, 3 Hong Kong also sees the need to help corporate customers protect their mobile security. The company collaborates with Check Point to launch the ZoneAlarm Mobile Security service, a downloadable software for large corporations and corporate staff that actively scans and alerts – but not shutdown – risks of malware attacks, unsafe Wi-Fi hotspots, infected apps and short message service (SMS) phishing. The service serves as a housekeeping tool that uses a multi-layered approach to protect operating systems.

## Corporate Social Responsibility (CSR) and Telephone Deception

Telecom operators provides mobile services for millions of users in Hong Kong, but are they responsible for protecting their customers by tracking/monitoring their calls while upholding data privacy? Woo expressed interest in cooperating with other operators to crack down on telephone deception, as long as the users' data remains private. Data breaches only help telephone scammers because they can use the obtained information for blackmail, manipulation, and open the door for scare tactics. This sensitive information, in turn, reduces the likelihood that victims will report their case of telephone deception out of fear that their details will be exposed.

When 3 Hong Kong customer service gets wind of suspicious telephone deception activity, they will immediately investigate and inform their users via notifications on websites, social media, SMS if irregular calls are detected. 3 Hong Kong was prompt in spreading awareness and warning users of the latest tactic of telephone deception called "one ring and cut": users would receive unexpected international calls from unknown destinations with unrecognised prefixes that immediate hang up. If the user calls the number back, they may incur international charges or will give away their caller ID for potential manipulation in the future. 3 Hong Kong issued a warning on their website, put up notices on social media, and SMS. 3 Hong Kong's dedication to CSR extends beyond deception in Hong Kong; overseas calls disguised as local calls are also of concern.

Telephone scammers often abuse communication channels put forth by operators and often launch hundreds/thousands of calls to scam as many people as possible within a short time span.

措施確保只有授權人士才可存取敏感資料，亦會定期篩查用戶賬號和迅速刪除失效賬戶。當系統偵測到有不尋常的資料存取情況時，便會立即發出報告和警告。此外，和記電訊香港控股有限公司的母公司每年均會進行內部審計，除撰寫詳細的審計報告外，亦會對3香港應如何維護和提升資訊安全監控提出建議，例如改善個別保安設施預算的配置事宜。

It only takes a user one mis-click to allow cybercrime to occur.
只是一次錯誤的點擊，用戶便會墮入網絡圈套。

在服務方面，3香港亦注意到企業客戶對流動保安的需求。因此，公司與 Check Point 合作推出 ZoneAlarm 流動保安服務，為大型企業及其員工提供可供下載的軟件，在不關機的情況下，軟件會時刻掃描並發出提示，當中包括惡意軟件攻擊的風險、不安全的 Wi-Fi 網絡熱點、受感染的應用程式和釣魚式的短訊攻擊。此服務擔當保安管家的角色，以分層方式保護操作系統。

## 企業社會責任與電話詐騙

電訊營辦商為香港數百萬市民提供流動通訊服務，在保障數據安全的同時，他們如何保護客戶的個人私隱？在防止用戶資料外洩及在保障客戶私隱的大前提下，胡先生希望與其他營辦商攜手打擊電話詐騙。資料外洩令騙徒得以利用獲取的資料進行勒索、操縱，或採取其他恐嚇手段。受害者會因懼怕其敏感資料曝光，而減低舉報電話騙案的意慾。

當3香港客戶服務團隊得悉有可疑電話騙案發生時，便會立即展開調查，同時通過網站、社交媒體或短訊通知客戶。3香港因應「一響即掛線」的最新電話詐騙手法，迅速呼籲客戶提高警覺。在此類騙案中，用戶會收到來歷不明或來自不尋常地區的國際長途電話，來電者會於鈴聲一響後立即掛線。如客戶回電，他們便有機會被收取國際長途電話費用，而他們的來電顯

Telephone scammers often abuse communication channels put forth by operators.
電話騙徒不時利用電訊營辦商的通訊渠道行騙。

Although 3 Hong Kong can technically examine call digital records to detect abnormal spikes in activity by IP location – which tracks the origin of calls and number of calls - it is hard to do this in detail because of the sheer amount of calls 3 Hong Kong faces every day. Woo estimates at least 10 million calls daily. Nonetheless, Woo notes that detecting call activity is indeed possible. Although there are currently no regulations in place on reporting abnormal call activity, 3 Hong Kong is happy to follow-up with customers and cooperate with different stakeholders to combat cybercrime.

## Registering and Authenticating Purchased SIM Cards

Some countries require people to register and authenticate their identity – via official IDs or passports - when purchasing SIM cards. Some operators in certain countries only allow a fixed number - usually within 5 to 10 - SIM cards per person at any point in time. Hong Kong, however, does not have this requirement. Understandably, there are both sides to this debate: registering SIM cards matches the SIM card's activity to an identity and allows accountability, but there are loopholes that make it difficult to verify the ID is authentic.

Woo supports this idea in principle but stresses the intricacies, policies, and sophistication needed for effective implementation. Woo has experience with SIM card authentication in Vietnam, Australia, and Sri Lanka, and notes that the process is highly complex. For instance, what happens if the ID used for registration is a fake ID? Does the person selling the SIM card can discern real from fake, and is the seller at fault for failing to do so? Fortunately, there are methods, albeit limited to some places, which allows vendors to key in IDs - which communicates via the government and operators - to reach a database of SIM card registrations. Doing so allows the vendor to determine if the buyer should be

示更有機會於將來被用作不法用途。3香港除了在其網站發出警告提示，於社交媒體發帖，更以短訊通知客戶有關電話詐騙手法。3香港一向致力履行企業社會責任，對香港的電話騙案和海外冒充本地來電騙案同樣重視。

電話騙徒不時利用營辦商的通訊渠道，在短時間內撥出數百個甚至數千個電話，務求令更多人受騙。雖然3香港的技術有能力檢視所有電子記錄，從騙徒的IP地址偵測這些不尋常的來電，並追蹤來電的來源地及來電數目，但客戶每天撥出的電話數量數以千萬計，在執行方面有一定困難。幸而胡先生指出，目前的技術已足以偵測異常來電。雖然現時沒有法例規定營辦商必須匯報異常的電話活動，但3香港樂意跟進客戶個案，並和各個持份者共同打擊網絡罪行。

## 登記及驗證SIM卡

有些國家規定客戶在購買SIM卡時，必需提供身份證或護照以登記和認證。而某些國家的營辦商，則會限制客戶在同一時間只可以擁有指定數量的SIM卡，大多為5至10張，香港卻沒有類似的規定。這種政策好壞參半，好處是登記SIM卡可以識別SIM卡的使用者，容易追查；壞處則是在驗證身份方面存在漏洞，執行上有一定困難。

胡先生原則上支持這項政策，但他強調必需採用更精密、規範和先進的程序，才可有效地執行政策。胡先生曾在越南、澳洲及斯里蘭卡的業務有SIM卡實名登記的經驗，整個過程相當繁複。例如，若有客戶以偽造的身份證登記，銷售員是否有能力辨別身份證的真偽？若銷售員未能做到，是否由他負上責任？

entitled to purchase a SIM card. In some countries, the vendor can search up if the buyer's passport immigration status is valid if the buyer is from overseas.

On a larger picture, registering and authenticating SIM cards require intricate knowledge of legalities, a set of guidelines to determine who is accountable, technicalities of SIM card databases, and issues of connectivity among sellers, government, operators, and databases. As such, registering SIM cards is a viable idea, according to Woo, but demands extensive preparation and ethical guidelines that nonetheless varies by country. Ultimately, any procedure that involves official IDs has to be treated carefully; issues also arise when people lose, or claim to lose, their ID documents.

Data security is of the utmost importance, especially in view of the increasingly sophisticated tactics employed by cyber criminals. Operators need to invest significant resources to ensure network safety, and continuous security enhancement to protect customer data poses a major challenge to daily operations.

現時，有些國家允許銷售商透過接觸政府與營辦商，讓其以客戶的身份證號碼於SIM卡註冊資料庫搜尋有關客戶的資料，從而判定客戶是否可以購買SIM卡。有些國家允許銷售商查核遊客的護照資料是否有效，才讓他們購買SIM卡。

長遠來看，SIM卡的登記和實名制措施仍需要多方面的配合，包括詳細的法律監管條例，以及一套完整的指引，包括問責制、SIM卡資料庫的技術細節，以及與銷售商、政府、營辦商及SIM卡資料庫多方配合所產生的問題。即使如胡先生所說，登記SIM卡政策是可行的，但仍需要配合多方面的準備工作和操守指引，才可在不同的國家實施。任何與身份證明有關的程序必須要審慎對待，當中或需面對用戶遺失或聲稱遺失證件時的問題。

總括來說，數據安全的重要性毋庸置疑，網絡營辦商面對駭客日新月異的攻擊手法及網上層出不窮的詐騙個案，相信必須投放大量資源以確保網絡安全，如何不斷提升保安措施以確保客戶資料安全將是日常運作的一大挑戰。